KATALOG ZABEZPIECZEŃ

Niniejszy katalog zawiera wykaz zabezpieczeń organizacyjnych i technicznych niezbędnych do zapewnienia wysokiego poziomu bezpieczeństwa informacji. Katalog opracowany został na podstawie standardu NIST 800-53 rev. 5.

W celu ułatwienia stosowania, zabezpieczenia zostały usystematyzowane w grupach tematycznych (kategoriach), z których każda skupia się na określonym aspekcie:

AC – Kontrola dostępu
AT – Świadomość i szkolenie
AU– Audyt i rozliczalność
CA – Ocena bezpieczeństwa i autoryzacja
CM – Zarządzanie konfiguracją
CP – Planowanie awaryjne
IA – Identyfikacja i uwierzytelnienie
IR – Reagowanie na incydenty
MA – Utrzymanie i wsparcie
MP – Ochrona nośników danych
PE – Ochrona fizyczna i środowiskowa
PL – Planowanie
PM – Programy bezpieczeństwa informacji
PS – Bezpieczeństwo osobowe
PT – Przejrzystość przetwarzania danych osobowych
RA – Ocena ryzyka
SA – Nabywanie systemu i usług
SC – Ochrona systemów i sieci telekomunikacyjnych
SI – Integralność systemu i informacji
SR – Zarządzanie ryzykiem w łańcuchu dostaw

Stosowanie kontroli bezpieczeństwa i ochrony danych powinno być procesem ciągłym, opartym na analizie ryzyka i dostosowanym do specyfiki działalności organizacji, który należy rozpocząć od zidentyfikowania kluczowych aktywów oraz zagrożeń, a następnie przypisać odpowiednie kontrole w celu minimalizacji ryzyka. Organizacje mogą wybierać i dostosowywać kontrole zgodnie z indywidualnymi potrzebami, uwzględniając specyfikę swojej działalności oraz poziom akceptowalnego ryzyka. Wdrożone środki bezpieczeństwa powinny być regularnie oceniane, testowane i aktualizowane w odpowiedzi na zmieniające się warunki operacyjne i nowe zagrożenia. Dokumentacja i raportowanie działań związanych z kontrolami są niezbędne do utrzymania zgodności i ciągłego doskonalenia systemu bezpieczeństwa.

Katalog zagrożeń wprowadza istotne zmiany w stosunku do wcześniejszej wersji, eliminując priorytetyzację kontroli (czyli kolejności wdrażania kontroli) i zastępując ją podejściem opartym na analizie ryzyka. Przyjęcie takiego podejścia pozwala organizacjom na bardziej elastyczny i celowy dobór zabezpieczeń w zależności od aktualnych potrzeb i zagrożeń, przy jednoczesnym zachowaniu spójności i kompleksowego podejścia.

Numer zabezpieczenia	Nazwa zabezpieczenia (lub ulepszenia zabezpieczenia)	Wyłączono (Wył.)/Włączono (Wł.)	Poziomy wpływu na atrybuty bezpieczeństwa informacji			
			Podstawowa polityka prywatności	Niski	Umiarkowany	Wysoki
Kontrola dostępu						
AC-1	Polityka i procedury kontroli dostępu		X	X	X	X
AC-2	Zarządzanie kontami			X	X	X
AC-2(1)	Zarządzanie kontami | Automatyczne zarządzanie kontem systemowym				X	X
AC-2(2)	Zarządzanie kontami | Usuwanie kont tymczasowych / awaryjnych				X	X
AC-2(3)	Zarządzanie kontami | Wyłączanie kont				X	X
AC-2(4)	Zarządzanie kontami | Automatyczne działania audytowe				X	X
AC-2(5)	Zarządzanie kontami | Wylogowanie po określonym okresie nieaktywności				X	X
AC-2(6)	Zarządzanie kontami | Dynamiczne zarządzanie uprawnieniami					
AC-2(7)	Zarządzanie kontami | Konta użytkowników uprzywilejowanych					
AC-2(8)	Zarządzanie kontami | Dynamiczne zarządzanie kontem					
AC-2(9)	Zarządzanie kontami | Ograniczenia dotyczące korzystania z kont współdzielonych i grupowych					
AC-2(10)	Zarządzanie kontami | Zmiana uwierzytelnienia kont współdzielonych i grupowych	Wł. do AC-2k.				
AC-2(11)	Zarządzanie kontami | Warunki użytkowania					X

AC-2(12)	Zarządzanie kontami | Monitorowanie konta pod kątem nietypowego użytkowania					X
AC-2(13)	Zarządzanie kontami | Wyłączanie kont dostępowych użytkownikom wysokiego ryzyka				X	X
AC-3	Egzekwowanie uprawnień dostępu			X	X	X
AC-3(1)	Egzekwowanie uprawnień dostępu | Ograniczony dostęp do funkcji uprzywilejowanych	Wł. do AC-6.				
AC-3(2)	Egzekwowanie uprawnień dostępu | Podwójna autoryzacja					
AC-3(3)	Egzekwowanie uprawnień dostępu | Obowiązkowa kontrola dostępu					
AC-3(4)	Egzekwowanie uprawnień dostępu | Uznaniowa kontrola dostępu					
AC-3(5)	Egzekwowanie uprawnień dostępu | Informacje dotyczące bezpieczeństwa					
AC-3(6)	Egzekwowanie uprawnień dostępu | Ochrona informacji użytkownika i systemu	Wł. do MP-4 i SC-28.				
AC-3(7)	Egzekwowanie uprawnień dostępu | Kontrola dostępu do roli (RBAC)					
AC-3(8)	Egzekwowanie uprawnień dostępu | Odwołanie zezwoleń na dostęp					
AC-3(9)	Egzekwowanie uprawnień dostępu | Kontrolowane udostępnienie informacji					

AC-3(10)	Egzekwowanie uprawnień dostępu | Nadzorowane obejście mechanizmów kontroli dostępu					
AC-3(11)	Egzekwowanie uprawnień dostępu | Ograniczanie dostępu do określonych typów informacji					
AC-3(12)	Egzekwowanie uprawnień dostępu | Potwierdzanie i egzekwowanie dostępu do aplikacji					
AC-3(13)	Egzekwowanie uprawnień dostępu | Kontrola dostępu oparta na atrybutach					
AC-3(14)	Egzekwowanie uprawnień dostępu | Dostęp indywidualny		X			
AC-3(15)	Egzekwowanie uprawnień dostępu | Uznaniowa i obowiązkowa kontrola dostępu					
AC-4	Egzekwowanie zasad przepływu informacji				X	X
AC-4(1)	Egzekwowanie zasad przepływu informacji | Atrybuty bezpieczeństwa i prywatności obiektu					
AC-4(2)	Egzekwowanie zasad przepływu informacji | Przetwarzanie domen					
AC-4(3)	Egzekwowanie zasad przepływu informacji | Dynamiczna kontrola przepływu informacji					
AC-4(4)	Egzekwowanie zasad przepływu informacji | Sprawdzanie zawartości zaszyfrowanej informacji					X
AC-4(5)	Egzekwowanie zasad przepływu informacji | Wbudowane rodzaje danych					

AC-4(6)	Egzekwowanie zasad przepływu informacji | Metadane					
AC-4(7)	Egzekwowanie zasad przepływu informacji | Mechanizmy przepływu jednostronnego					
AC-4(8)	Egzekwowanie zasad przepływu informacji | Filtry polityki bezpieczeństwa i prywatności					
AC-4(9)	Egzekwowanie zasad przepływu informacji | Ocena przez uprawnioną osobę					
AC-4(10)	Egzekwowanie zasad przepływu informacji | Włączanie/ wyłączanie filtrów polityki bezpieczeństwa lub prywatności					
AC-4(11)	Egzekwowanie zasad przepływu informacji | Konfiguracja filtrów polityki bezpieczeństwa lub prywatności					
AC-4(12)	Egzekwowanie zasad przepływu informacji | Identyfikatory typu danych					
AC-4(13)	Egzekwowanie zasad przepływu informacji | Dekompozycja informacji na odpowiednie podskładniki					
AC-4(14)	Egzekwowanie zasad przepływu informacji | Polityka stosowania filtrów bezpieczeństwa lub prywatności					
AC-4(15)	Egzekwowanie zasad przepływu informacji | Wykrywanie informacji nieakceptowalnych					

AC-4(16)	Egzekwowanie zasad przepływu informacji | Przekazywanie informacji pomiędzy systemami	Wł. do AC-4.				
AC-4(17)	Egzekwowanie zasad przepływu informacji | Uwierzytelnianie domen					
AC-4(18)	Egzekwowanie zasad przepływu informacji | Wiązanie atrybutu bezpieczeństwa	Wł. do AC-16.				
AC-4(19)	Egzekwowanie zasad przepływu informacji | Walidacja metadanych					
AC-4(20)	Egzekwowanie zasad przepływu informacji | Zatwierdzone rozwiązania bezpieczeństwa					
AC-4(21)	Egzekwowanie zasad przepływu informacji | Fizyczna lub logiczna separacja przepływów informacji					
AC-4(22)	Egzekwowanie zasad przepływu informacji | Tylko dostęp					
AC-4(23)	Egzekwowanie zasad przepływu informacji | Modyfikowanie nieudostępnianych informacji					
AC-4(24)	Egzekwowanie zasad przepływu informacji | Wewnętrzny znormalizowany format					
AC-4(25)	Egzekwowanie zasad przepływu informacji | Oczyszczanie danych					
AC-4(26)	Egzekwowanie zasad przepływu informacji | Audyt czynności filtrowania					
AC-4(27)	Egzekwowanie zasad przepływu informacji | Redundantne/niezależne mechanizmy filtrowania					

AC-4(28)	Egzekwowanie zasad przepływu informacji | Liniowe kanały filtrowania					
AC-4(29)	Egzekwowanie zasad przepływu informacji | Silniki orkiestracji filtrów					
AC-4(30)	Egzekwowanie zasad przepływu informacji | Mechanizmy filtrowania wykorzystujące wiele procesów					
AC-4(31)	Egzekwowanie zasad przepływu informacji | Zapobieganie nieudanemu transferowi treści					
AC-4(32)	Egzekwowanie zasad przepływu informacji | Wymagania procesowe dotyczące transferu informacji					
AC-5	Rozdział obowiązków				X	X
AC-6	Zasada wiedzy koniecznej				X	X
AC-6(1)	Zasada wiedzy koniecznej | Upoważniony dostęp do funkcji bezpieczeństwa				X	X
AC-6(2)	Zasada wiedzy koniecznej | Nieuprzywilejowany dostęp do funkcji niezwiązanych z bezpieczeństwa				X	X
AC-6(3)	Zasada wiedzy koniecznej | Dostęp sieciowy do uprzywilejowanych poleceń					X
AC-6(4)	Zasada wiedzy koniecznej | Oddzielne domeny przetwarzania					
AC-6(5)	Zasada wiedzy koniecznej | Uprzywilejowane konta				X	X

AC-6(6)	Zasada wiedzy koniecznej | Ograniczony dostęp przez użytkowników spoza organizacji					
AC-6(7)	Zasada wiedzy koniecznej | Przegląd uprawnień użytkownika				X	X
AC-6(8)	Zasada wiedzy koniecznej | Poziomy uprawnień do uruchomienia kodu					
AC-6(9)	Zasada wiedzy koniecznej | Rejestrowanie użycia funkcji uprzywilejowanych				X	X
AC-6(10)	Zasada wiedzy koniecznej | Odmowa wykonania przez nieuprzywilejowanych użytkowników uprzywilejowanych funkcji				X	X
AC-7	Nieudane próby logowania			X	X	X
AC-7(1)	Nieudane próby logowania | Automatyczna blokada konta	Wł. do AC-7.				
AC-7(2)	Nieudane próby logowania | Usuwanie informacji z urządzeń przenośnych					
AC-7(3)	Nieudane próby logowania | Ograniczanie prób biometrycznych					
AC-7(4)	Nieudane próby logowania | Użycie alternatywnego czynnika uwierzytelniania					
AC-8	Powiadomienie o zasadach użycia systemu			X	X	X
AC-9	Powiadomienie o zalogowaniu					
AC-9(1)	Powiadomienie o zalogowaniu | Nieudane logowania					

AC-9(2)	Powiadomienie o zalogowaniu | Pomyślne i nieudane logowania					
AC-9(3)	Powiadomienie o zalogowaniu | Powiadomienie o zmianach na koncie					
AC-9(4)	Powiadomienie o zalogowaniu | Dodatkowe informacje o logowaniu					
AC-10	Kontrola ilości równoczesnych sesji					X
AC-11	Blokada urządzenia				X	X
AC-11(1)	Blokada urządzenia | Wygaszacz ekranu				X	X
AC-12	Zakończenie sesji				X	X
AC-12(1)	Zakończenie sesji | Wylogowania inicjowane przez użytkownika					
AC-12(2)	Zakończenie sesji | Wiadomość o zakończeniu					
AC-12(3)	Zakończenie sesji | Komunikat ostrzegawczy o przekroczeniu limitu czasu					
AC-13	Nadzór i przegląd — kontrola dostępu	Wł. do AC-2 i AU-6.				
AC-14	Działania dozwolone bez identyfikacji lub uwierzytelnienia			X	X	X
AC-14(1)	Działania dozwolone bez identyfikacji lub uwierzytelnienia | Niezbędne zastosowania	Wł. do AC-14.				
AC-15	Zautomatyzowane znakowanie	Wł. do formatu MP-3.				
AC-16	Atrybuty bezpieczeństwa i prywatności					
AC-16(1)	Atrybuty bezpieczeństwa i prywatności | Dynamiczne skojarzenie atrybutów					

AC-16(2)	Atrybuty bezpieczeństwa i prywatności | Zmiany wartości atrybutów przez osoby upoważnione					
AC-16(3)	Atrybuty bezpieczeństwa i prywatności | Utrzymanie skojarzeń atrybutów przez system					
AC-16(4)	Atrybuty bezpieczeństwa i prywatności | Kojarzenie atrybutów przez autoryzowany personel					
AC-16(5)	Atrybuty bezpieczeństwa i prywatności | Wyświetlanie atrybutów na urządzeniach końcowych					
AC-16(6)	Atrybuty bezpieczeństwa i prywatności | Utrzymanie skojarzenia atrybutów					
AC-16(7)	Atrybuty bezpieczeństwa i prywatności | Spójna interpretacja atrybutów					
AC-16(8)	Atrybuty bezpieczeństwa i prywatności | Skojrzenie techniki i technologie					
AC-16(9)	Atrybuty bezpieczeństwa i prywatności | Ponowne przypisywanie atrybutów — mechanizmy ponownej oceny					
AC-16(10)	Atrybuty bezpieczeństwa i prywatności | Konfiguracja atrybutów przez osoby upoważnione					
AC-17	Zdalny dostęp			X	X	X
AC-17(1)	Zdalny dostęp | Monitorowanie i kontrola				X	X

AC-17(2)	Zdalny dostęp | Ochrona poufności i integralności za pomocą szyfrowania				X	X
AC-17(3)	Zdalny dostęp | Zarządzane punkty kontroli dostępu				X	X
AC-17(4)	Zdalny dostęp | Polecenia i dostęp uprzywilejowany				X	X
AC-17(5)	Zdalny dostęp | Monitorowanie nieautoryzowanych połączeń	Wł.do SI-4.				
AC-17(6)	Zdalny dostęp | Ochrona mechanizmów zdalnego dostępu					
AC-17(7)	Zdalny dostęp | Dodatkowa ochrona dostępu do funkcji bezpieczeństwa	Wł. do AC-3(10).				
AC-17(8)	Zdalny dostęp | Wyłącz niebezpieczone protokoły sieciowe	Wł. do CM-7.				
AC-17(9)	Zdalny dostęp | Rozłącz lub wyłącz dostęp					
AC-17(10)	Zdalny dostęp | Uwierzytelnianie poleceń zdalnych					
AC-18	Dostęp bezprzewodowy			X	X	X
AC-18(1)	Dostęp bezprzewodowy | Uwierzytelnianie i szyfrowanie				X	X
AC-18(2)	Dostęp bezprzewodowy | Monitorowanie połączeń nieautoryzowanych	Wł. do SI-4.				
AC-18(3)	Dostęp bezprzewodowy | Dezaktywacja sieci bezprzewodowej				X	X
AC-18(4)	Dostęp bezprzewodowy | Ograniczanie konfiguracji przez użytkowników					X
AC-18(5)	Dostęp bezprzewodowy | Anteny i poziomy mocy transmisji					X

AC-19	Kontrola dostępu realizowanego z urządzeń przenośnych (mobilnych)			X	X	X
AC-19(1)	Kontrola dostępu realizowanego z urządzeń przenośnych (mobilnych) | Korzystanie z zapisywalnych / przenośnych urządzeń magazynujących	Wł. do MP-7.				
AC-19(2)	Kontrola dostępu realizowanego z urządzeń przenośnych (mobilnych)| Wykorzystanie osobistych przenośnych urządzeń magazynujących	Wł. w MP-7.				
AC-19(3)	Kontrola dostępu realizowanego z urządzeń przenośnych (mobilnych)| Wykorzystanie ogólnodostępnych przenośnych urządzeń magazynujących	Wł. w MP-7.				
AC-19(4)	Kontrola dostępu realizowanego z urządzeń przenośnych (mobilnych)| Ograniczenia dotyczące informacji tajnych					
AC-19(5)	Kontrola dostępu realizowanego z urządzeń przenośnych (mobilnych) | Pełne szyfrowanie urządzeń lub kontenerów				X	X
AC-20	Wykorzystanie zewnętrznych systemów			X	X	X
AC-20(1)	Wykorzystanie zewnętrznych systemów | Ograniczenia autoryzowanego dostępu				X	X

AC-20(2)	Wykorzystanie zewnętrznych systemów | Urządzenia pamięci masowej przenośnej — ograniczone użytkowanie				X	X
AC-20(3)	Wykorzystanie zewnętrznych systemów | Systemy niebędące własnością organizacji — ograniczone użytkowanie					
AC-20(4)	Wykorzystanie zewnętrznych systemówh | Urządzenia pamięci masowej dostępne w sieci — zabronione użycie					
AC-20(5)	Wykorzystanie zewnętrznych systemów | Urządzenia pamięci przenośnej — zabronione użycie					
AC-21	Udostępnianie informacji				X	X
AC-21(1)	Udostępnianie informacji | Automatyczne wsparcie decyzyjne					
AC-21(2)	Udostępnianie informacji | Wyszukiwanie i odzyskiwanie informacji					
AC-22	Treści publicznie dostępne			X	X	X
AC-23	Ochrona przed przeszukiwaniem danych					
AC-24	Przyznawanie praw dostępu					
AC-24(1)	Przyznawanie praw dostępu| Przesyłanie informacji o autoryzacji dostępu					
AC-24(2)	Przyznawanie praw dostępu | Brak tożsamości użytkownika lub procesu					
AC-25	Monitor referencyjny					
Świadomość i szkolenie						
AT-1	Polityka i procedury		X	X	X	X

AT-2	Szkolenie w zakresie uświadamiania bezpieczeństwa		X	X	X	X
AT-2(1)	Szkolenie w zakresie uświadamiania bezpieczeństwa | Ćwiczenia praktyczne					
AT-2(2)	Szkolenie w zakresie uświadamiania bezpieczeństwa| Zagrożenia wewnętrzne			X	X	X
AT-2(3)	Szkolenie w zakresie uświadamiania bezpieczeństwa | Inżynieria społeczna i pozyskiwanie danych				X	X
AT-2(4)	Szkolenie w zakresie uświadamiania bezpieczeństwa | Podejrzane komunikaty i nietypowe zachowania systemów					
AT-2(5)	Szkolenie w zakresie uświadamiania bezpieczeństwa | Zaawansowane trwałe zagrożenie					
AT-2(6)	Szkolenie w zakresie uświadamiania bezpieczeństwa | Środowisko zagrożeń cybernetycznych					
AT-3	Szkolenie oparte na rolach		X	X	X	X
AT-3(1)	Szkolenia oparte na rolach | Kontrole środowiskowe					
AT-3(2)	Szkolenia oparte na rolach | Kontrole Bezpieczeństwa fizycznego					
AT-3(3)	Szkolenia oparte na rolach | Ćwiczenia praktyczne					

AT-3(4)	Szkolenia oparte na rolach | Podejrzana komunikacja i nietypowe zachowanie systemu	Wł. do AT-2(4).				
AT-3(5)	Szkolenia oparte na rolach | Przetwarzanie danych osobowych		X			
AT-4	Zapisy szkoleniowe		X	X	X	X
AT-5	Kontakty z grupami i stowarzyszeniami ds. bezpieczeństwa	Wł. do PM-15.				
AT-6	Informacje zwrotne dotyczące szkolenia					
Audyt i rozliczalność						
AU-1	Polityka i procedury		X	X	X	X
AU-2	Audyt zdarzeń		X	X	X	X
AU-2(1)	Audyt zdarzeń| Kompilacja zapisów audytu z wielu źródeł	Wł. do AU-12.				
AU-2(2)	Audyt zdarzeń | Wybór zdarzeń audytowych według komponentu	Wł.do AU-12.				
AU-2(3)	Audyt zdarzeń| Opinie i aktualizacje	Wł. do AU-2.				
AU-2(4)	Autyd zdarzeń| Uprzywilejowane funkcje	Wł. do AC-6(9).				
AU-3	Zawartość rejestrów audytu			X	X	X
AU-3(1)	Zawartość rejestrów audytu | Dodatkowe informacje kontrolne				X	X
AU-3(2)	Zawartość rejestrów audytu | Centralne zarządzanie treścią planowanego rejestru audytu	Wł. do PL-9.				
AU-3(3)	Zawartość rejestrów audytu | Ograniczenie informacji umożliwiających identyfikację osób		X			
AU-4	Pojemność pamięci zapisów audytu			X	X	X

AU-4(1)	Pojemność pamięci zapisów audytu | Transfer rekordów do alternatywnych urządzeń magazynujących					
AU-5	Reakcja na błędy procesów audytu			X	X	X
AU-5(1)	Reakcja na błędy procesów audytu | Ostrzeżenia dotyczące limitu pamięci przechowywania rekordów audytu					X
AU-5(2)	Reakcja na błędy procesów audytu | Alerty czasu rzeczywistego					X
AU-5(3)	Reakcja na błędy procesów audytu | Konfigurowalne progi natężenia ruchu					
AU-5(4)	Reakcja na błędy procesów audytu | Wyłączenie w przypadku awarii					
AU-5(5)	Reakcja na błędy procesów audytu | Zdolność alternatywnego prowadzenia rejestru audytu					
AU-6	Przeglą audytu, analiza i raportowanie			X	X	X
AU-6(1)	Przeglą audytu, analiza i raportowanie | Zautomatyzowana integracja procesów				X	X
AU-6(2)	Przeglą audytu, analiza i raportowanie | Automatyczne alarmy bezpieczeństwa	Wł. do SI-4				
AU-6(3)	Przeglą audytu, analiza i raportowanie | Korelacja zbiorów audytu				X	X
AU-6(4)	Przeglą audytu, analiza i raportowanie| Centralny przeglądanie i analizy					

AU-6(5)	Przegląd audytu, analiza i raportowanie| Zintegrowana analiza zapisów z audytu					X
AU-6(6)	Przegląd audytu, analiza i raportowanie | Korelacja audytu z monitorowaniem fizycznym					X
AU-6(7)	Przegląd audytu, analiza i raportowanie | Dopuszczalne działania					
AU-6(8)	Przegląd audytu, analiza i raportowanie | Pełna analiza tekstu uprzewilejowanych poleceń					
AU-6(9)	Przegląd audytu, analiza i raportowanie| Korelacja z informacjami uzyskanymi ze źródeł nietechnicznych					
AU-6(10)	Przegląd audytu, analiza i raportowanie| Korygowanie poziomu audytu	Wł. do AU-6.				
AU-7	Redukcja treści zapisów z audytu i generowanie raportów				X	X
AU-7(1)	Redukcja treści zapisów z audytu i generowanie raportów | Automatyzacja procesu				X	X
AU-7(2)	Redukcja treści zapisów z audytu i generowanie raportów | Automatyczne sortowanie i wyszukiwanie	Wł. do AU-7(1).				
AU-8	Znaczniki czasu			X	X	X
AU-8(1)	Znaczniki czasu | Synchronizacja z autoryzowanym źródłem czasu odniesienia	Wł. do SC-45(1).				
AU-8(2)	Znaczniki czasu | Wtórne źródło czasu odniesienia	Wł. do SC-45(2).				
AU-9	Ochrona informacji audytowych			X	X	X

AU-9(1)	Ochrona informacji audytowych | Nośniki jednokrotnego zapisu					
AU-9(2)	Ochrona informacji audytowych | Backup audytu w odseparowanym fizycznie systemie / komponencie					X
AU-9(3)	Ochrona informacji audytowych | Ochrona kryptograficzna					X
AU-9(4)	Ochrona informacji audytowych | Dostęp do podzbioru uprzywilejowanych użytkowników				X	X
AU-9(5)	Ochrona informacji audytowych | Podwójna autoryzacja					
AU-9(6)	Ochrona informacji audytowych | Dostęp tylko do odczytu					
AU-9(7)	Ochrona informacji audytowych | Przechowywanie informacji na komponentach z różnymi systemami operacyjnymi.					
AU-10	Niezaprzeczalność					X
AU-10(1)	Niezaprzeczalność | Połączenie Tożsamości					
AU-10(2)	Niezaprzeczalność | Powiązanie informacji z tożsamością twórcy					
AU-10(3)	Niezaprzeczalność | Łańcuch nadzoru					
AU-10(4)	Niezaprzeczalność | Potwierdzanie tożsamości przeglądającego informacje					
AU-10(5)	Niezaprzeczalność | Podpisy cyfrowe	Wł. do SI-7				
AU-11	Retencja zapisów audytu		X	X	X	X

AU-11(1)	Retencja zapisów audytu | Długoterminowa zdolność do odzysku					
AU-12	Tworzenie zapisów audytu			X	X	X
AU-12(1)	Tworzenie zapisów audytu | Ogólnosystemowe / skorelowane w czasie ścieżki audytu					X
AU-12(2)	Tworzenie zapisów audytu | Ujednolicone formaty					
AU-12(3)	Tworzenie zapisów audytu | Zmiany dokonywane przez uprawnione osoby					X
AU-12(4)	Tworzenie zapisów audytu | Audyty parametrów zapytań o dane osobowe					
AU-13	Monitorowanie ujawniania informacji					
AU-13(1)	Monitorowanie ujawniania informacji | Wykorzystywanie zautomatyzowanych narzędzi					
AU-13(2)	Monitorowanie ujawniania informacji | Przegląd monitorowanych stron					
AU-13(3)	Monitorowanie ujawniania informacji | Nieautoryzowane powielanie informacji					
AU-14	Audyt sesji					
AU-14(1)	Audyt sesji | Uruchamianie systemu					
AU-14(2)	Audyt sesji | Przechwyty / nagrywanie i zawartość dzienników logowania	Wł. do AU-14.				
AU-14(3)	Audyt sesji | Zdalne wyświetlanie / odsłuchiwanie					
AU-15	Zdolność do alternatywnego audytu	Wł. do AU-5(5).				
AU-16	Audyt międzyorganizacyjny					

AU-16(1)	Audyt międzyorganizacyjny | Ochrona tożsamości					
AU-16(2)	Audyt międzyorganizacyjny | Udostępnianie informacji audytowych					
AU-16(3)	Audyt międzyorganizacyjny | Oddzielanie danych osobowych					
Ocena bezpieczeństwa i autoryzacja						
CA-1	Polityka i procedury oceny, autoryzacji i monitorowania		X	X	X	X
CA-2	Ocena mechanizmów kontrolnych		X	X	X	X
CA-2(1)	Ocena mechanizmów kontrolnych| Niezależni oceniający				X	X
CA-2(2)	Ocena mechanizmów kontrolnych| Oceny specjalistyczne					X
CA-2(3)	Ocena mechanizmów kontrolnych | Wykorzystanie wyników z organizacji zewnętrznych					
CA-3	Wymiana informacji			X	X	X
CA-3(1)	Połączenia międzystemowe | Nieklasyfikowane połączenia systemów bezpieczeństwa narodowego	Wł. do SC-7(25).				
CA-3(2)	Połączenia międzystemowe | Klasyfikowane połączenia systemów bezpieczeństwa narodowego	Wł. do SC-7(26).				
CA-3(3)	Połączenia międzystemowe | Nieklasyfikowane połączenia systemów niebędących systemami bezpieczeństwa narodowego	Wł. do SC-7(27).				

CA-3(4)	Połączenia międzystemowe | Połączenia z sieciami publicznymi	Wł. do SC-7(28).				
CA-3(5)	Połączenia międzystemowe| Ograniczenia dotyczące połączeń z systemami zewnętrznymi	Wł. do SC-7(5).				
CA-3(6)	Wymiana informacji | Autoryzacje transferu					X
CA-3(7)	Wymiana informacji | Pośrednie wymiany informacji					
CA-4	Certyfikacja bezpieczeństwa	Wł. do CA-2.				
CA-5	Plan działania i kamienie milowe		X	X	X	X
CA-5(1)	Plan działania i kamienie milowe | Wsparcie automatyzacji dla dokładności i aktualności					
CA-6	Autryzacja		X	X	X	X
CA-6(1)	Autoryzacja | Wspólna autoryzacja — wewnątrzorganizacyjna					
CA-6(2)	Autoryzacja | Wwspólna autoryzacja — międzyorganizacyjna					
CA-7	Monitorowanie ciągłe		X	X	X	X
CA-7(1)	Monitorowanie ciągłe | Niezależna ocena				X	X
CA-7(2)	Monitorowanie ciągłe | Rodzaje ocen	Wł. do CA-2.				
CA-7(3)	Monitorowanie ciągłe | Analizy trendów					
CA-7(4)	Monitorowanie ciągłe | Monitorowanie ryzyka		X	X	X	X
CA-7(5)	Monitorowanie ciągłe | Analiza spójności					
CA-7(6)	Monitorowanie ciągłe | Wsparcie automatyzacji dla monitorowania					
CA-8	Testy penetracyjne					X
CA-8(1)	Testy penetracyjne | Niezależny agent lub zespół testów penetracyjnych					X

CA-8(2)	Testowanie penetracyjne | Ćwiczenia red team					
CA-8(3)	Testowanie penetracyjne | Testy penetracyjne obiektu					
CA-9	Połączenia wewnętrzne systemu			X	X	X
CA-9(1)	Połączenia wewnętrzne systemu | Kontrole zgodności					
Zarządzanie konfiguracją						
CM-1	Polityka i procedury		X	X	X	X
CM-2	Konfiguracja bazowa			X	X	X
CM-2(1)	Konfiguracja bazowa | Przeglądy i aktualizacje	Wł. do CM-2.				
CM-2(2)	Konfiguracja bazowa | Automatyzacja wspierająca aktualność /szczegółowość				X	X
CM-2(3)	Konfiguracja bazowa | Retencja zachowanych konfiguracji				X	X
CM-2(4)	Konfiguracja bazowa | Nieautoryzowane oprogramowanie	Wł. do CM-7.				
CM-2(5)	Konfiguracja bazowa | Autoryzowane oprogramowanie	Wł. do CM-7.				
CM-2(6)	Konfiguracja bazowa | Środowiska programistyczne i testowe					
CM-2(7)	Konfiguracja bazowa | Konfiguracja systemów i komponentów w obszarach wysokiego ryzyka				X	X
CM-3	Zabezpieczanie zmian konfiguracji				X	X
CM-3(1)	Zabezpieczanie zmian konfiguracji | Automatyczna dokumentacja /powiadamianie /zakaz wprowadzania zmian					X

CM-3(2)	Zabezpieczanie zmian konfiguracji | Testy, walidacja i zmiany dokumentów				X	X
CM-3(3)	Zabezpieczanie zmian konfiguracji | Automatyczne wprowadzanie zmian					
CM-3(4)	Zabezpieczanie zmian konfiguracji | Funkcyjni ds. bezpieczeństwa i ochrony prywatności				X	X
CM-3(5)	Zabezpieczanie zmian konfiguracji | Automatyczna reakcja bezpieczeństwa					
CM-3(6)	Zabezpieczanie zmian konfiguracji | Zarządzanie kryptograficzne					X
CM-3(7)	Zabezpieczanie zmian konfiguracji | Przegląd zmian w systemie					
CM-3(8)	Zabezpieczanie zmian konfiguracji | Zapobieganie lub ograniczanie zmian konfiguracji					
CM-4	Analizy wpływu		X	X	X	X
CM-4(1)	Analizy wpływu | Oddzielne środowiska badawcze					X
CM-4(2)	Analizy wpływu | Weryfikacja zabezpieczeń				X	X
CM-5	Ograniczenia możliwości dokonywania zmian			X	X	X
CM-5(1)	Ograniczenia możliwości dokonywania zmian| Automatyczne egzekwowanie uprawnień dostępu i zapisy z audytu					X
CM-5(2)	Ograniczenia możliwości dokonywania zmian | Przegląd zmian w systemie	Wł. do CM-3(7).				
CM-5(3)	Ograniczenia możliwości dokonywania zmian | Podpisane komponenty	Wł. do CM-14.				

CM-5(4)	Ograniczenia możliwości dokonywania zmian | Podwójna autoryzacja					
CM-5(5)	Ograniczenia możliwości dokonywania zmian | Ograniczenia przywilejów w zakresie wytwarzania i eksploatacji					
CM-5(6)	Ograniczenia możliwości dokonywania zmian | Ograniczanie przywilejów w bibliotekach oprogramowania					
CM-5(7)	Ograniczenia możliwości dokonywania zmian | Automatyczne wdrażanie środków bezpieczeństwa	Wł. do SI-7.				
CM-6	Ustawienia konfiguracji			X	X	X
CM-6(1)	Ustawienia konfiguracji | Automatyczne zarządzanie, stosowanie i weryfikacja					X
CM-6(2)	Ustawienia konfiguracji | Odpowiedź na nieautoryzowane zmiany					X
CM-6(3)	Ustawienia konfiguracji | Wykrywanie nieautoryzowanych zmian	Wł. do SI-7.				
CM-6(4)	Ustawienia konfiguracji | Prezentacja zgodności	Wł. do CM-4.				
CM-7	Zasada minimalnej funkcjonalności			X	X	X
CM-7(1)	Zasada minimalnej funkcjonalności | Przeglądy okresowe				X	X
CM-7(2)	Zasada minimalnej funkcjonalności | Zapobiegania wykonywaniu programu				X	X
CM-7(3)	Zasada minimalnej funkcjonalności | Stosowanie rejestracji					

CM-7(4)	Zasada minimalnej funkcjonalności| Nieautoryzowane oprogramowanie ("czarna lista")					
CM-7(5)	Zasada minimalnej funkcjonalności | Autoryzowane oprogramowanie ("biała lista")				X	X
CM-7(6)	Zasada minimalnej funkcjonalności | Zamknięte środowiska z ograniczonymi uprawnieniami					
CM-7(7)	Zasada minimalnej funkcjonalności | Wykonywanie kodu w chronionych środowiskach					
CM-7(8)	Zasada minimalnej funkcjonalności | Kod binarny lub kod wykonywalny (mobilny)					
CM-7(9)	Zasada minimalnej funkcjonalności | Zakaz używania nieautoryzowanego sprzętu					
CM-8	Inwentaryzacja komponentów systemu			X	X	X
CM-8(1)	Inwentaryzacja komponentów systemu | Aktualizacje instalacji i usuwania komponentów				X	X
CM-8(2)	Inwentaryzacja komponentów systemu | Automatyczna konserwacja (utrzymywanie)					X
CM-8(3)	Inwentaryzacja komponentów systemu | Automatyczne wykrywanie komponentów nieautoryzowanych				X	X

CM-8(4)	Inwentaryzacja komponentów systemu | Informacje dotyczące odpowiedzialności i rozliczalności					X
CM-8(5)	Inwentaryzacja komponentów systemu | Brak duplikacji komponentów	Wł. CM-8.				
CM-8(6)	Inwentaryzacja komponentów systemu | Ocena konfiguracji i zatwierdzone odstępstwa					
CM-8(7)	Inwentaryzacja komponentów systemu | Scentralizowane repozytorium					
CM-8(8)	Inwentaryzacja komponentów systemu | Automatyczne śledzenie lokalizacji					
CM-8(9)	Inwentaryzacja komponentów systemu | Przypisanie komponentów do systemów					
CM-9	Plan zarządzania konfiguracją				X	X
CM-9(1)	Plan zarządzania konfiguracją | Przypisanie odpowiedzialności					
CM-10	Ograniczenia w użyciu oprogramowania			X	X	X
CM-10(1)	Ograniczenia w użyciu oprogramowania | Oprogramowanie otwarte (open source)					
CM-11	Oprogramowanie instalowane przez użytkownika			X	X	X
CM-11(1)	Oprogramowanie instalowane przez użytkownika | Ostrzeganie o nieautoryzowanych instalacjach	Wł. CM-8(3).				

CM-11(2)	Oprogramowanie instalowane przez użytkownika | Zabroniona instalacja bez posiadania stosownych uprawnień					
CM-11(3)	Oprogramowanie instalowane przez użytkownika | Automatyczne egzekwowanie i monitorowanie					
CM-12	Położenie (lokacja) informacji				X	X
CM-12(1)	Położenie (lokacja) informacji | Automatyczne narzędzia do obsługi lokacji informacji				X	X
CM-13	Mapowanie działań na danych					
CM-14	Podpisywanie komponentów					
Planowanie awaryjne						
CP-1	Polityka i procedury			X	X	X
CP-2	Plan awaryjny			X	X	X
CP-2(1)	Plan awaryjny | Koordynacja z powiązanymi planami				X	X
CP-2(2)	Plan awaryjny | Planowanie pojemności					X
CP-2(3)	Plan awaryjny | Wznowienie misji i funkcji biznesowych				X	X
CP-2(4)	Plan awaryjny | Wznowienie wszystkich misji i funkcji biznesowych	Wł. do CP-2(3).				
CP-2(5)	Plan awaryjny | Kontynuacja misji i funkcji biznesowych					X
CP-2(6)	Plan awaryjny | Alternatywne miejsca przetwarzania i składowania					
CP-2(7)	Plan awaryjny | Współpraca z zewnętrznymi dostawcami usług					

CP-2(8)	Plan awaryjny | Identyfikacja krytycznych aktywów				X	X
CP-3	Szkolenie w zakresie planowania ciągłości działania			X	X	X
CP-3(1)	Szkolenie w zakresie planowania ciągłości działania | Wydarzenia symulowane					X
CP-3(2)	Szkolenie w zakresie planowania ciągłości działania| Mechanizmy stosowane w środowiskach szkoleniowych					
CP-4	Testowanie planu ciągłości działania			X	X	X
CP-4(1)	Testowanie planu ciągłości działania | Koordynacja z powiązanymi planami				X	X
CP-4(2)	Testowanie planu ciągłości działania | Zapasowe miejsce przetwarzania					X
CP-4(3)	Testowanie planu ciągłości działania | Testy automatyczne					
CP-4(4)	Testowanie planu ciągłości działania | Pełne odzyskiwanie					
CP-4(5)	Testowanie planu ciągłości działania | Kontrolowane awarie					
CP-5	Aktualizacja planu ciągłości działania	Wł. do CP-2.				
CP-6	Zapasowe miejsce przechowywania				X	X
CP-6(1)	Zapasowe miejsce przechowywania | Separacja od miejsca głównego				X	X
CP-6(2)	Zapasowe miejsce przechowywania | Czas odzyskiwania i punkt odzyskiwania					X

CP-6(3)	Zapasowe miejsce przechowywania | Dostępność				X	X
CP-7	Zapasowe miejsce przetwarzania				X	X
CP-7(1)	Zapasowe miejsce przetwarzania | Separacja od miejsca głównego				X	X
CP-7(2)	Zapasowe miejsce przetwarzania | Dostępność				X	X
CP-7(3)	Zapasowe miejsce przetwarzania | Priorytet usługi				X	X
CP-7(4)	Zapasowe miejsce przetwarzania | Przygotowanie do użycia					X
CP-7(5)	Zapasowe miejsce przetwarzania | Równoważne zabezpieczenia bezpieczeństwa informacji	Wł. do CP-7.				
CP-7(6)	Zapasowe miejsce przetwarzania | Brak możliwości powrotu do miejsca pierwotnego					
CP-8	Usługi telekomunikacyjne				X	X
CP-8(1)	Usługi telekomunikacyjne | Postanowienia o priorytetach usług				X	X
CP-8(2)	Usługi telekomunikacyjne | Pojedyncze punkty awarii				X	X
CP-8(3)	Usługi telekomunikacyjne | Rozdzielenie dostawców podstawowych i alternatywnych					X
CP-8(4)	Usługi telekomunikacyjne | Plan awaryjny dostawcy					X

CP-8(5)	Usługi telekomunikacyjne | Testowanie alternatywnych usług telekomunikacyjnych					
CP-9	Kopia zapasowa systemu			X	X	X
CP-9(1)	Kopia zapasowa systemu | Testowanie niezawodności i integralności				X	X
CP-9(2)	Kopia zapasowa systemu | Testowanie odtwarzania przy użyciu próbkowania					X
CP-9(3)	Kopia zapasowa systemu | Oddzielne przechowywanie informacji krytycznych					X
CP-9(4)	Kopia zapasowa systemu | Ochrona przed nieautoryzowaną modyfikacją	Wł. do CP-9.				
CP-9(5)	Kopia zapasowa systemu | Transfer do zapasowej lokalizacji przechowywania					X
CP-9(6)	Kopia zapasowa systemu | Nadmiarowy system zapasowy					
CP-9(7)	Kopia zapasowa systemu | Podwójna autoryzacja usuwania lub zniszczenia					
CP-9(8)	Kopia zapasowa systemu | Ochrona kryptograficzna				X	X
CP-10	Odzyskiwanie i odtwarzanie systemu			X	X	X
CP-10(1)	Odzyskiwanie i odtwarzanie systemu | Testowanie planu awaryjnego	Wł.do CP-4.				
CP-10(2)	Odzyskiwanie i odtwarzanie systemu | Odzyskiwanie transakcji				X	X
CP-10(3)	Odzyskiwanie i odtwarzanie systemu | Kompensujące mechanizmy kontrolne	Wył.				

CP-10(4)	Odzyskiwanie i odtwarzanie systemu | Przywracanie w określonym czasie					X
CP-10(5)	Odzyskiwanie i odtwarzania systemu | Zdolność do przełączania awaryjnego	W: Włączono do SI-13.				
CP-10(6)	Odzyskiwanie i odtwarzania systemu | Ochrona komponentów					
CP-11	Zapasowe protokoły komunikacyjne					
CP-12	Tryb awaryjny					
CP-13	Alternatywne Mechanizmy Bezpieczeństwa					
Identyfikacja i uwierzytelnianie						
IA-1	Polityka i procedury			X	X	X
IA-2	Identyfikacja i uwierzytelnianie (użytkownicy organizacyjni)			X	X	X
IA-2(1)	Identyfikacja i uwierzytelnianie (użytkownicy organizacji) | Wieloskładnikowe uwierzytelnianie do kont uprzywilejowanych			X	X	X
IA-2(2)	Identyfikacja i uwierzytelnianie (użytkownicy organizacji) | Wieloskładnikowe uwierzytelnianie kont bez uprawnień			X	X	X
IA-2(3)	Identyfikacja i uwierzytelnianie (użytkownicy organizacji) | Lokalny dostęp do kont uprzywilejowanych	W: Włączono do IA-2(1)(2).				
IA-2(4)	Identyfikacja i uwierzytelnianie (użytkownicy organizacyjni) | Lokalny dostęp do kont nieuprzywilejowanych	W: Włączono do IA-2(1)(2).				

IA-2(5)	Identyfikacja i uwierzytelnianie (użytkownicy organizacyjni) | Uwierzytelnianie indywidualne z uwierzytelnianiem grupowym					X
IA-2(6)	Identyfikacja i uwierzytelnianie (użytkownicy organizacji) | Dostęp do kont — oddzielne urządzenie					
IA-2(7)	Identyfikacja i uwierzytelnianie (użytkownicy organizacji) | Dostęp sieciowy do kont nieuprzywilejowanych — oddzielne urządzenie	W: Włączono do IA-2(6).				
IA-2(8)	Identyfikacja i uwierzytelnianie (użytkownicy organizacji) | Dostęp do kont — zabezpieczenie przed powtórnym użyciem			X	X	X
IA-2(9)	Identyfikacja i uwierzytelnianie (użytkownicy organizacji) | Dostęp sieciowy do kont nieuprzywilejowanych — odporność na odtwarzanie	W: Włączono do IA-2(8).				
IA-2(10)	Identyfikacja i uwierzytelnianie (użytkownicy organizacyjni) | Logowanie jednokrotne					
IA-2(11)	Identyfikacja i uwierzytelnianie (użytkownicy organizacji) | Dostęp zdalny — oddzielne urządzenie	W: Włączono do IA-2(6).				

IA-2(12)	Identyfikacja i uwierzytelnianie (użytkownicy organizacyjni) | Akceptacja poświadczeń PIV			X	X	X
IA-2(13)	Identyfikacja i uwierzytelnianie (użytkownicy organizacyjni) | Uwierzytelnianie "poza pasmem"					
IA-3	Identyfikacja i uwierzytelnianie urządzeń				X	X
IA-3(1)	Identyfikacja i uwierzytelnianie urządzeń | Kryptograficzne uwierzytelnianie dwukierunkowe					
IA-3(2)	Identyfikacja i uwierzytelnianie urządzeń | Kryptograficzne dwukierunkowe uwierzytelnianie sieciowe	W: Włączono do IA-3(1).				
IA-3(3)	Identyfikacja i uwierzytelnianie urządzeń | Dynamiczna alokacja adresów					
IA-3(4)	Identyfikacja i uwierzytelnianie urządzeń | Atestacja urządzeń					
IA-4	Zarządzanie identyfikatorami			X	X	X
IA-4(1)	Zarządzanie identyfikatorami | Zabroń używania identyfikatorów kont jako identyfikatorów publicznych					
IA-4(2)	Zarządzanie identyfikatorami | Autoryzacja przełożonego	W: Włączono do IA-12(1).				

IA-4(3)	Zarządzanie identyfikatorami | Wielokrotne formy certyfikacji	W: Włączono do IA-12(2)				
IA-4(4)	Zarządzanie identyfikatorami | Identyfikuj status użytkownika				X	X
IA-4(5)	Zarządzanie identyfikatorami | Zarządzanie dynamiczne					
IA-4(6)	Zarządzanie identyfikatorami | Zarządzanie międzyorganizacyjne					
IA-4(7)	Zarządzanie identyfikatorami | Rejestracja osobista	W: Włączono do IA-12(4)				
IA-4(8)	Zarządzanie identyfikatorami | Identyfikatory pseudonimowe pary					
IA-4(9)	Zarządzanie identyfikatorami | Konserwacja i ochrona atrybutów					
IA-5	Zarządzanie uwierzytelnianiem			X	X	X
IA-5(1)	Zarządzanie uwierzytelnianiem | Uwierzytelnianie oparte o hasła			X	X	X
IA-5(2)	Zarządzanie uwierzytelnianiem | Uwierzytelnianie oparte na kluczu publicznym				X	X
IA-5(3)	Zarządzanie uwierzytelnianiem | Rejestracja osobista lub zaufanej strony zewnętrznej	W: Włączono do IA-12(4)				
IA-5(4)	Zarządzanie uwierzytelnianiem | Zautomatyzowane wsparcie w określaniu siły hasła	W: Włączono do IA-5(1).				

IA-5(5)	Zarządzanie uwierzytelnianiem | Zmiana metody uwierzytelniania przed dostawą					
IA-5(6)	Zarządzanie uwierzytelnianiem | Ochrona metod uwierzytelniania				X	X
IA-5(7)	Zarządzanie uwierzytelnianiem | Brak wbudowanych niezaszyfrowanych statycznych elementów uwierzytelniania					
IA-5(8)	Zarządzanie uwierzytelnianiem | Jedno konto w wielu systemach					
IA-5(9)	Zarządzanie uwierzytelnianiem | Zarządzanie danymi uwierzytelniającymi między organizacjami					
IA-5(10)	Zarządzanie uwierzytelnianiem | Dynamiczne powiązanie poświadczeń					
IA-5(11)	Zarządzanie uwierzytelnianiem | Uwierzytelnianie oparte na tokenach sprzętowych	W: Włączono do IA-2(1) i IA-2(2).				
IA-5(12)	Zarządzanie uwierzytelnianiem | Uwierzytelnianie biometryczne					
IA-5(13)	Zarządzanie uwierzytelnianiem | Przedawnienie buforowanych elementów uwierzytelniania					
IA-5(14)	Zarządzanie uwierzytelnianiem | Zarządzanie zawartością zaufanych magazynów infrastruktury klucza publicznego					

IA-5(15)	Zarządzanie uwierzytelnianiem | Produkty i usługi					
IA-5(16)	Zarządzanie uwierzytelnianiem | Osobisty lub zaufany zewnętrzny podmiot uwierzytelniający					
IA-5(17)	Zarządzanie uwierzytelnianiem | Wykrywanie ataków prezentacyjnych przy uwierzytelnianiu biometrycznym					
IA-5(18)	Zarządzanie uwierzytelnianiem | Menedżer haseł					
IA-6	Informacja zwrotna uwierzytelniania			X	X	X
IA-7	Uwierzytelnianie modułu kryptograficznego			X	X	X
IA-8	Identyfikacja i uwierzytelnianie (użytkownicy spoza organizacji)			X	X	X
IA-8(1)	Identyfikacja i uwierzytelnianie (użytkownicy spoza organizacji) | Akceptacja poświadczeń tożsamości wydanych przez inne organizacje			X	X	X
IA-8(2)	Identyfikacja i uwierzytelnianie (użytkownicy spoza organizacji) | Akceptacja poświadczeń stron trzecich			X	X	X
IA-8(3)	Identyfikacja i uwierzytelnianie (użytkownicy spoza organizacji) | Korzystanie z produktów zatwierdzonych przez FICAM	W: Włączono do IA-8(2).				

IA-8(4)	Identyfikacja i uwierzytelnianie (użytkownicy spoza organizacji) | Wykorzystanie zdefiniowanych profili			X	X	X
IA-8(5)	Identyfikacja i uwierzytelnianie (użytkownicy spoza organizacji) | Akceptacja poświadczeń					
IA-8(6)	Identyfikacja i uwierzytelnianie (użytkownicy spoza organizacji) | Rozłączność					
IA-9	Identyfikacja i uwierzytelnianie usług					
IA-9(1)	Identyfikacja i uwierzytelnianie usług | Wymiana informacji	W: Włączone do IA-9.				
IA-9(2)	Identyfikacja i uwierzytelnianie usług | Przesyłanie decyzji	W: Włączone do IA-9.				
IA-10	Uwierzytelnianie adaptacyjne					
IA-11	Ponowne uwierzytelnianie			X	X	X
IA-12	Weryfikacja tożsamości				X	X
IA-12(1)	Weryfikacja tożsamości | Autoryzacja przełożonego					
IA-12(2)	Weryfikacja tożsamości | Dowód tożsamości				X	X
IA-12(3)	Weryfikacja tożsamości | Walidacja i weryfikacja dowodów tożsamości				X	X
IA-12(4)	Weryfikacja tożsamości | Weryfikacja i walidacja osobista					X
IA-12(5)	Weryfikacja tożsamości | Potwierdzenie adresu				X	X
IA-12(6)	Weryfikacja tożsamości | Akceptacja tożsamości zweryfikowanych zewnętrznie					
Reagowanie na incydenty						
IR-1	Polityka i procedury		X	X	X	X

IR-2	Szkolenie w zakresie reagowania na incydenty		X	X	X	X
IR-2(1)	Szkolenie w zakresie reagowania na incydenty | Symulowane wydarzenia					X
IR-2(2)	Szkolenie w zakresie reagowania na incydenty | Zautomatyzowane środowiska szkoleniowe					X
IR-2(3)	Szkolenie w zakresie reagowania na incydenty | Naruszenie		X			
IR-3	Testowanie reakcji na incydenty		X		X	X
IR-3(1)	Testowanie reakcji na incydenty | Testowanie automatyczne					
IR-3(2)	Testowanie reagowania na incydenty | Koordynacja z powiązanymi planami				X	X
IR-3(3)	Testowanie reakcji na incydenty | Ciągłe doskonalenie					
IR-4	Obsługa incydentów		X	X	X	X
IR-4(1)	Obsługa Incydentów | Zautomatyzowane procesy obsługi incydentów				X	X
IR-4(2)	Obsługa incydentów | Dynamiczna rekonfiguracja					
IR-4(3)	Obsługa Incydentów | Ciągłość działania					
IR-4(4)	Obsługa Incydentów | Korelacja Informacji					X
IR-4(5)	Obsługa incydentów | Automatyczne wyłączanie systemu					
IR-4(6)	Obsługa incydentów | Zagrożenia wewnętrzne					
IR-4(7)	Obsługa incydentów | Zagrożenia wewnętrzne — koordynacja wewnątrzorganizacyjna					

IR-4(8)	Obsługa incydentów | Korelacja z organizacjami zewnętrznymi					
IR-4(9)	Obsługa incydentów | Zdolność do dynamicznej reakcji					
IR-4(10)	Obsługa incydentów | Koordynacja łańcucha dostaw					
IR-4(11)	Obsługa incydentów | Zintegrowany zespół reagowania na incydenty					X
IR-4(12)	Obsługa incydentów | Złośliwy kod i analiza kryminalistyczna					
IR-4(13)	Obsługa incydentów | Analiza zachowań					
IR-4(14)	Obsługa Incydentów | Centrum Operacji Bezpieczeństwa					
IR-4(15)	Obsługa Incydentów | Public relations i naprawa reputacji					
IR-5	Monitorowanie incydentów		X	X	X	X
IR-5(1)	Monitorowanie incydentów | Automatyczne śledzenie, zbieranie danych i analiza					X
IR-6	Raportowanie incydentów		X	X	X	X
IR-6(1)	Raportowanie incydentów | Automatyczne raportowanie				X	X
IR-6(2)	Raportowanie incydentów | Podatność na incydenty					
IR-6(3)	Raportowanie incydentów | Koordynacja łańcucha dostaw				X	X
IR-7	Wsparcie reagowania na incydenty		X	X	X	X

IR-7(1)	Wsparcie reagowania na incydenty | Automatyczne wsparcie dostępności informacji / obsługi				X	X
IR-7(2)	Wsparcie reagowania na incydenty | Koordynacja z zewnętrznymi dostawcami					
IR-8	Plan reagowania na incydenty		X	X	X	X
IR-8(1)	Plan reagowania na incydenty | Naruszenia		X			
IR-9	Reakcja na wyciek / ujawnienie informacji					
IR-9(1)	Reakcja na wyciek / ujawnienie informacji | Personel odpowiedzialny	W: Włączono do IR-9				
IR-9(2)	Reakcja na wyciek / ujawnienie informacji | Szkolenie					
IR-9(3)	Reakcja na wyciek / ujawnienie informacji | Operacje po wycieku					
IR-9(4)	Reakcja na wyciek / ujawnienie informacji | Narażenie na kontakt z nieupoważnionym personelem					
IR-10	Zespół ds. zintegrowanej analizy bezpieczeństwa informacji	W: Przeniesiono do IR-4(11).				
Utrzymanie i wsparcie						
MA-1	Polityka i procedury			X	X	X
MA-2	Kontrolowana konserwacja			X	X	X
MA-2(1)	Kontrolowana konserwacja | Zawartość rekordu	W: Włączone do MA-2.				
MA-2(2)	Kontrolowana konserwacja | Zautomatyzowane działania konserwacyjne					X
MA-3	Narzędzia konserwacyjne				X	X
MA-3(1)	Narzędzia konserwacyjne | Inspekcja narzędzi				X	X

MA-3(2)	Narzędzia konserwacyjne | Inspekcja nośników				X	X
MA-3(3)	Narzędzia konserwacyjne | Zapobiegaj nieautoryzowanemu usuwaniu				X	X
MA-3(4)	Narzędzia konserwacyjne | Ograniczone użycie narzędzi					
MA-3(5)	Narzędzia konserwacyjne | Wykonywanie z uprawnieniami					
MA-3(6)	Narzędzia konserwacyjne | Aktualizacje oprogramowania i poprawki					
MA-4	Konserwacja zdalna			X	X	X
MA-4(1)	Konserwacja zdalna | Rejestrowanie i przegląd					
MA-4(2)	Konserwacja zdalna | Dokumentowanie konserwacji zdalnej	W: Włączone do MA-1 i MA-4.				
MA-4(3)	Konserwacja zdalna | Porównywalne zabezpieczenia i sanityzacja					X
MA-4(4)	Konserwacja zdalna | Uwierzytelnianie i rozdzielanie sesji konserwacyjnych					
MA-4(5)	Konserwacja zdalna | Zatwierdzenia i powiadomienia					
MA-4(6)	Konserwacja zdalna | Ochrona kryptograficzna					
MA-4(7)	Konserwacja zdalna | Weryfikacja rozłączenia					
MA-5	Personel konserwacyjny			X	X	X
MA-5(1)	Personel konserwacyjny | Osoby bez odpowiedniego dostępu					X

MA-5(2)	Personel konserwacyjny | Uprawnienia bezpieczeństwa dla systemów niejawnych					
MA-5(3)	Personel konserwacyjny | Wymagania dotyczące obywatelstwa dla systemów niejawnych					
MA-5(4)	Personel konserwacyjny | Cudzoziemcy					
MA-5(5)	Personel konserwacyjny | Konserwacja niezwiązana z utrzymaniem systemu					
MA-6	Terminowa konserwacja				X	X
MA-6(1)	Terminowa konserwacja | Konserwacja zapobiegawcza					
MA-6(2)	Terminowa konserwacja | Konserwacja predykcyjna					
MA-6(3)	Terminowa konserwacja | Zautomatyzowane wsparcie dla konserwacji predykcyjnej					
MA-7	Konserwacja w terenie					
Ochrona nośników danych						
MP-1	Polityka i procedury		X	X	X	X
MP-2	Dostęp do nośników			X	X	X
MP-2(1)	Dostęp do nośników | Zautomatyzowany ograniczony dostęp	W: Włączono do MP-4(2)				
MP-2(2)	Dostęp do nośników | Ochrona kryptograficzna	W: Włączono do SC-28(1).				
MP-3	Oznakowanie nośników				X	X
MP-4	Przechowywanie nośników				X	X
MP-4(1)	Przechowywanie nośników | Ochrona kryptograficzna	W: Włączono do SC-28(1).				
MP-4(2)	Przechowywanie nośników | Zautomatyzowany ograniczony dostęp					
MP-5	Transport mediów				X	X
MP-5(1)	Transport mediów | Ochrona poza obszarami kontrolowanymi	W: Wbudowany w MP-5.				

MP-5(2)	Transport mediów | Dokumentacja działań	W: Wbudowany w MP-5.				
MP-5(3)	Transport mediów | Opiekunowie					
MP-5(4)	Transport mediów | Ochrona kryptograficzna	W: Włączono do SC-28(1).				
MP-6	Kasowanie nośników		X	X	X	X
MP-6(1)	Kasowanie nośników| Przeglądać, zatwierdzać, śledzić, dokumentować i weryfikować					X
MP-6(2)	Kasowanie nośników | Testowanie sprzętu					X
MP-6(3)	Kasowanie nośników | Techniki nieniszczące					X
MP-6(4)	Kasowanie nośników | Kontrolowane informacje jawne	W: Wbudowany w MP-6.				
MP-6(5)	Kasowanie nośników | Informacje niejawne	W: Wbudowany w MP-6.				
MP-6(6)	Kasowanie nośników | Niszczenie nośników	W: Wbudowany w MP-6.				
MP-6(7)	Kasowanie nośników| Podwójna autoryzacja					
MP-6(8)	Kasowanie nośników | Zdalne usuwanie lub wymazywanie informacji					
MP-7	Używanie nośników			X	X	X
MP-7(1)	Używanie nośników | Zabroń używania bez właściciela	W: Wbudowany w MP-7.				
MP-7(2)	Używanie nośników | Zakaz stosowania nośników odpornych na kasowanie					
MP-8	Deklasyfikacja nośników					
MP-8(1)	Deklasyfikacja nośników| Dokumentacja procesu					
MP-8(2)	Deklasyfikacja nośników | Testowanie sprzętu					
MP-8(3)	Deklasyfikacja nośników| Kontrolowane informacje jawne					
MP-8(4)	Deklasyfikacja nośników | Informacje niejawne					

Ochrona fizyczna i środowiskowa						
PE-1	Polityka i procedury			X	X	X
PE-2	Zezwolenia na dostęp fizyczny			X	X	X
PE-2(1)	Zezwolenia na dostęp fizyczny | Dostęp według stanowiska lub roli					
PE-2(2)	Zezwolenia na dostęp fizyczny |Podwójna identyfikacja					
PE-2(3)	Zezwolenia na dostęp fizyczny | Ograniczenie dostępu bez asysty					
PE-3	Kontrola dostępu fizycznego			X	X	X
PE-3(1)	Kontrola dostępu fizycznego | Dostęp do systemu					X
PE-3(2)	Kontrola dostępu fizycznego | Obiekt / obszar systemu					
PE-3(3)	Kontrola dostępu fizycznego | Stała ochrona fizyczna					
PE-3(4)	Kontrola dostępu fizycznego | Zamykane obudowy					
PE-3(5)	Kontrola dostępu fizycznego | Ochrona przed manipulacją					
PE-3(6)	Kontrola dostępu fizycznego | Testy penetracyjne obiektu	W: Włączone do CA-8.				
PE-3(7)	Kontrola dostępu fizycznego | Bariery fizyczne					
PE-3(8)	Kontrola dostępu fizycznego | Śluzy w kontroli dostępu					
PE-4	Kontrola dostępu do medium transmisyjnego				X	X
PE-5	Kontrola dostępu do urządzeń wejścia - wyjścia				X	X
PE-5(1)	Kontrola dostępu do urządzeń wejścia - wyjścia | Dostęp upoważnionych osób do urządzeń	W: Włączone do PE-5.				

PE-5(2)	Kontrola dostępu do urządzeń wejścia - wyjścia | Powiązanie z tożsamością jednostki					
PE-5(3)	Kontrola dostępu do urządzeń wejścia - wyjścia | Oznaczanie urządzeń wejścia - wyjścia	W: Włączone do PE-22.				
PE-6	Monitorowanie dostępu fizycznego			X	X	X
PE-6(1)	Monitorowanie dostępu fizycznego | Alarmy antywłamaniowe i sprzęt monitorujący				X	X
PE-6(2)	Monitorowanie dostępu fizycznego | Automatyczne rozpoznawanie włamań i reagowanie na nie					
PE-6(3)	Monitorowanie dostępu fizycznego | Monitoring wizyjny					
PE-6(4)	Monitorowanie dostępu fizycznego | Monitorowanie dostępu fizycznego do systemów					X
PE-7	Kontrola gości	W: Włączone do PE-2 i PE-3.				
PE-8	Rejestry dostępu gości			X	X	X
PE-8(1)	Rejestry dostępu gości | Automatyczna rejestracja / przegląd					X
PE-8(2)	Rejestry dostępu gości | Ewidencja dostępu fizycznego	W: Włączone do PE-2.				
PE-8(3)	Rejestry dostępu gości | Ograniczenie elementów informacji umożliwiających identyfikację osoby		X			
PE-9	Urządzenia energetyczne i okablowanie				X	X
PE-9(1)	Urządzenia energetyczne i okablowanie | Redundancja okablowania					

PE-9(2)	Urządzenia energetyczne i okablowanie | Automatyczna kontrola jakości napięcia					
PE-10	Wyłączenie awaryjne				X	X
PE-10(1)	Wyłączenie awaryjne | Przypadkowa i nieautoryzowana aktywacja	W: Włączone do PE-10.				
PE-11	Zasilanie awaryjne				X	X
PE-11(1)	Zasilanie awaryjne | Alternatywne źródło zasilania — minimalna zdolność operacyjna					X
PE-11(2)	Zasilanie awaryjne | Alternatywne źródło zasilania — autonomiczne					
PE-12	Oświetlenie awaryjne			X	X	X
PE-12(1)	Oświetlenie awaryjne | Zasadnicze działania / funkcje biznesowe					
PE-13	Ochrona przeciwpożarowa			X	X	X
PE-13(1)	Ochrona przeciwpożarowa | Systemy detekcji – automatyczna aktywacja i powiadamianie				X	X
PE-13(2)	Ochrona przeciwpożarowa | Systemy tłumienia – automatyczna aktywacja i powiadamianie					X
PE-13(3)	Ochrona przeciwpożarowa | Automatyczne gaszenie pożaru	W: Włączono do PE-13(2)				
PE-13(4)	Ochrona przeciwpożarowa | Inspekcje					
PE-14	Kontrole środowiskowe			X	X	X
PE-14(1)	Kontrole środowiskowe | Sterowanie automatyczne					
PE-14(2)	Kontrole środowiskowe | Monitorowanie, alarmowanie i powiadomianie					

PE-15	Ochrona przed zalaniem			X	X	X
PE-15(1)	Ochrona przed zalaniem | Automatyczne wykrywanie					X
PE-16	Dostawa i usuwanie			X	X	X
PE-17	Zapasowe miejsce pracy				X	X
PE-18	Lokalizacja komponentów systemu					X
PE-18(1)	Lokalizacja komponentów systemu | Lokalizacja obiektu	W: Przeniesiono do PE-23.				
PE-19	Wyciek informacji					
PE-19(1)	Wyciek informacji | Krajowe zasady i procedury dotyczące emisji ujawniającej					
PE-20	Monitorowanie i śledzenie aktywów					
PE-21	Ochrona przed impulsami elektromagnetycznymi					
PE-22	Znakowanie komponentów					
PE-23	Lokalizacja obiektu					
Planowanie						
PL-1	Polityka i procedury		X	X	X	X
PL-2	Plany bezpieczeństwa systemu i ochrony prywatności		X	X	X	X
PL-2(1)	Plany bezpieczeństwa systemu i ochrony prywatności | Koncepcja działania	W: Włączone do PL-7.				
PL-2(2)	Plany bezpieczeństwa systemu i ochrony prywatności | Architektura funkcjonalna	W: Włączone do PL-8.				
PL-2(3)	Plany bezpieczeństwa systemu i ochrony prywatności | Planowanie / koordynacja z innymi podmiotami organizacyjnymi	W: Włączone do PL-2.				
PL-3	Aktualizacja planu bezpieczeństwa systemu	W: Włączone do PL-2.				
PL-4	Zasady zachowania		X	X	X	X

PL-4(1)	Zasady zachowania | Zasady korzystania z mediów społecznościowych i zewnętrznych stron/aplikacji		X	X	X	X
PL-5	Ocena wpływu na prywatność	W: Włączono do RA-8.				
PL-6	Planowanie działalności związanej z bezpieczeństwem	W: Włączone do PL-2.				
PL-7	Koncepcja bezpieczeństwa działań operacyjnych					
PL-8	Architektura bezpieczeństwa i ochrona prywatności		X		X	X
PL-8(1)	Architektura bezpieczeństwa i ochrona prywatności | Zabezpieczenie wielostopniowe (ochrona warstwowa)					
PL-8(2)	Architektura bezpieczeństwa i ochrona prywatności | Dywersyfikacja dostawcy					
PL-9	Zarządzanie centralne		X			
PL-10	Wybór zabezpieczeń bazowych			X	X	X
PL-11	Dopasowanie bazowe			X	X	X
Programy bezpieczeństwa informacji						
PM-1	Plan programu bezpieczeństwa informacji			N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji
PM-2	Osoba odpowiedzialna za bezpieczeństwo informacji (CSO)			N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji
PM-3	Środki bezpieczeństwa i prywatności informacji		X	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji

PM-4	Plan działania i etapy wprowadzania zabezpieczeń		X	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji
PM-5	Inwentaryzacja systemu informacyjnego			N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji
PM-5(1)	Inwentaryzacja systemu informacyjnego | Inwentaryzacja danych osobowych		X	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji
PM-6	Miary wydajności		X	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji
PM-7	Struktura organizacyjna		X	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji
PM-7(1)	Struktura organizacyjna | Odciążanie			N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji
PM-8	Plan infrastruktury krytycznej		X	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji
PM-9	Strategia zarządzania ryzykiem		X	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji
PM-10	Proces autoryzacji		X	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji

PM-11	Definicja misji i procesów biznesowych		X	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji
PM-12	Zagrożenia wewnętrzne			N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji
PM-13	Pracownicy ds. bezpieczeństwa i prywatności		X	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji
PM-14	Testowanie, szkolenia i monitorowanie		X	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji
PM-15	Grupy i stowarzyszenia ds. bezpieczeństwa i prywatności			N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji
PM-16	Ostrzeganie o zagrożeniach			N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji
PM-16(1)	Ostrzeganie o zagrożeniach | Zautomatyzowane środki udostępniania informacji o zagrożeniach			N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji
PM-17	Ochrona kontrolowanych informacji niejawnych w systemach zewnętrznych		X	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji
PM-18	Plan programu ochrony prywatności		X	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji

PM-19	Rola kierownicza programu ochrony prywatności		X	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji
PM-20	Rozpowszechnianie informacji o programie ochrony prywatności		X	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji
PM-20(1)	Rozpowszechnianie informacji o programie ochrony prywatności | Zasady ochrony prywatności w witrynach internetowych, aplikacjach i usługach cyfrowych		X	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji
PM-21	Rozliczanie udostępnień		X	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji
PM-22	Zarządzanie jakością informacji umożliwiających identyfikację osoby		X	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji
PM-23	Zarządzanie danymi			N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji
PM-24	Rada ds. integralności danych		X	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji
PM-25	Minimalizacja danych osobowych wykorzystywanych w testach, szkoleniach i badaniach		X	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji

PM-26	Zarządzanie skargami		X	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji
PM-27	Raportowanie prywatności		X	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji
PM-28	Ujęcie ryzyka		X	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji
PM-29	Role kierownicze w programie zarządzania ryzykiem			N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji
PM-30	Strategia zarządzania ryzykiem łańcucha dostaw			N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji
PM-30(1)	Strategia zarządzania ryzykiem łańcucha dostaw | Dostawcy artykułów krytycznych lub niezbędnych do realizacji misji			N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji
PM-31	Strategia ciągłego monitorowania		X	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji
PM-32	Celowość			N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji	N/A – Wdrożono w całej organizacji
Bezpieczweństwo osobowe						
PS-1	Polityka i procedury			X	X	X
PS-2	Określanie ryzyka dla stanowiska pracy			X	X	X
PS-3	Dobór personelu			X	X	X

PS-3(1)	Dobót personelu | Informacje niejawne					
PS-3(2)	Dobór personelu | Postępowania sprawdzające					
PS-3(3)	Dobót personelu | Informacje wymagające szczególnej ochrony					
PS-3(4)	Dobór personelu | Wymagania dotyczące obywatelstwa					
PS-4	Zakończenie zatrudnienia			X	X	X
PS-4(1)	Zakończenie zatrudnienia | Zobowiązania po zakończeniu zatrudnienia					
PS-4(2)	Zakończenie zatrudnienia | Automatyczne powiadamianie					X
PS-5	Obsadzenie lub przeniesienie stanowiska			X	X	X
PS-6	Umowy dostępu / współpracy		X	X	X	X
PS-6(1)	Umowy dostępu / współpracy | Informacje wymagające szczególnej ochrony	W: Włączono do PS-3.				
PS-6(2)	Umowy dostępu / współpracy | Informacje niejawne wymagające ochrony specjalnej					
PS-6(3)	Umowy dostępu / współpracy | Wymogi po zakończeniu zatrudnienia					
PS-7	Bezpieczeństwo osobowe stron trzecich			X	X	X
PS-8	Sankcje personalne			X	X	X
PS-9	Opisy stanowisk pracy			X	X	X
Przejrzystość przetwarzania danych osobowych						

PT-1	Polityka i procedury		X	Nie przydzielono do bazowych linii kontroli bezpieczeństwa	Nie przydzielono do bazowych linii kontroli bezpieczeństwa	Nie przydzielono do bazowych linii kontroli bezpieczeństwa
PT-2	Uprawnienia do przetwarzania danych osobowych		X	Nie przydzielono do bazowych linii kontroli bezpieczeństwa	Nie przydzielono do bazowych linii kontroli bezpieczeństwa	Nie przydzielono do bazowych linii kontroli bezpieczeństwa
PT-2(1)	Uprawnienia do przetwarzania danych osobowych | Oznaczanie danych			Nie przydzielono do bazowych linii kontroli bezpieczeństwa	Nie przydzielono do bazowych linii kontroli bezpieczeństwa	Nie przydzielono do bazowych linii kontroli bezpieczeństwa
PT-2(2)	Uprawnienia do przetwarzania danych osobowych | Automatyzacja			Nie przydzielono do bazowych linii kontroli bezpieczeństwa	Nie przydzielono do bazowych linii kontroli bezpieczeństwa	Nie przydzielono do bazowych linii kontroli bezpieczeństwa
PT-3	Cele przetwarzania danych osobowych		X	Nie przydzielono do bazowych linii kontroli bezpieczeństwa	Nie przydzielono do bazowych linii kontroli bezpieczeństwa	Nie przydzielono do bazowych linii kontroli bezpieczeństwa

PT-3(1)	Cele przetwarzania danych osobowych | Oznaczanie danych			Nie przydzielono do bazowych linii kontroli bezpieczeństwa	Nie przydzielono do bazowych linii kontroli bezpieczeństwa	Nie przydzielono do bazowych linii kontroli bezpieczeństwa
PT-3(2)	Cele przetwarzania danych osobowych | Automatyzacja			Nie przydzielono do bazowych linii kontroli bezpieczeństwa	Nie przydzielono do bazowych linii kontroli bezpieczeństwa	Nie przydzielono do bazowych linii kontroli bezpieczeństwa
PT-4	Zgody		X	Nie przydzielono do bazowych linii kontroli bezpieczeństwa	Nie przydzielono do bazowych linii kontroli bezpieczeństwa	Nie przydzielono do bazowych linii kontroli bezpieczeństwa
PT-4(1)	Zgody | Upoważnienie			Nie przydzielono do bazowych linii kontroli bezpieczeństwa	Nie przydzielono do bazowych linii kontroli bezpieczeństwa	Nie przydzielono do bazowych linii kontroli bezpieczeństwa
PT-4(2)	Zgody | Zgoda typu "just-in-time"			Nie przydzielono do bazowych linii kontroli bezpieczeństwa	Nie przydzielono do bazowych linii kontroli bezpieczeństwa	Nie przydzielono do bazowych linii kontroli bezpieczeństwa

PT-4(3)	Zgody | Wycofanie zgody			Nie przydzielono do bazowych linii kontroli bezpieczeństwa	Nie przydzielono do bazowych linii kontroli bezpieczeństwa	Nie przydzielono do bazowych linii kontroli bezpieczeństwa
PT-5	Informacja o ochronie prywatności		X	Nie przydzielono do bazowych linii kontroli bezpieczeństwa	Nie przydzielono do bazowych linii kontroli bezpieczeństwa	Nie przydzielono do bazowych linii kontroli bezpieczeństwa
PT-5(1)	Informacja o ochronie prywatności | Informacja na żądanie			Nie przydzielono do bazowych linii kontroli bezpieczeństwa	Nie przydzielono do bazowych linii kontroli bezpieczeństwa	Nie przydzielono do bazowych linii kontroli bezpieczeństwa
PT-5(2)	Informacja o ochronie prywatności | Oświadczenie o ochronie prywatności		X	Nie przydzielono do bazowych linii kontroli bezpieczeństwa	Nie przydzielono do bazowych linii kontroli bezpieczeństwa	Nie przydzielono do bazowych linii kontroli bezpieczeństwa
PT-6	Informacja o prowadzonych rejestrach		X	Nie przydzielono do bazowych linii kontroli bezpieczeństwa	Nie przydzielono do bazowych linii kontroli bezpieczeństwa	Nie przydzielono do bazowych linii kontroli bezpieczeństwa

PT-6(1)	Informacja o prowadzonych rejestrach | Rutynowe zastosowania		X	Nie przydzielono do bazowych linii kontroli bezpieczeństwa	Nie przydzielono do bazowych linii kontroli bezpieczeństwa	Nie przydzielono do bazowych linii kontroli bezpieczeństwa
PT-6(2)	Informacja o prowadzonych rejestrach | Zasady wyłączenia		X	Nie przydzielono do bazowych linii kontroli bezpieczeństwa	Nie przydzielono do bazowych linii kontroli bezpieczeństwa	Nie przydzielono do bazowych linii kontroli bezpieczeństwa
PT-7	Szczególne kategorie danych osobowych		X	Nie przydzielono do bazowych linii kontroli bezpieczeństwa	Nie przydzielono do bazowych linii kontroli bezpieczeństwa	Nie przydzielono do bazowych linii kontroli bezpieczeństwa
PT-7(1)	Szczególne kategorie danych osobowych | Identyfikator osoby np. numer PESEL		X	Nie przydzielono do bazowych linii kontroli bezpieczeństwa	Nie przydzielono do bazowych linii kontroli bezpieczeństwa	Nie przydzielono do bazowych linii kontroli bezpieczeństwa
PT-7(2)	Szczególne kategorie danych osobowych | Przetwarzanie wrażliwych danych osobowych		X	Nie przydzielono do bazowych linii kontroli bezpieczeństwa	Nie przydzielono do bazowych linii kontroli bezpieczeństwa	Nie przydzielono do bazowych linii kontroli bezpieczeństwa

PT-8	Wymagania dotyczące zgodności przy automatycznym przetwarzaniu danych		X	Nie przydzielono do bazowych linii kontroli bezpieczeństwa	Nie przydzielono do bazowych linii kontroli bezpieczeństwa	Nie przydzielono do bazowych linii kontroli bezpieczeństwa
Ocena ryzyka						
RA-1	Polityka i procedury		X	X	X	X
RA-2	Kategoryzacja bezpieczeństwa			X	X	X
RA-2(1)	Kategoryzacja bezpieczeństwa | Priorytetyzacja poziomów wpływu					
RA-3	Szacowanie ryzyka		X	X	X	X
RA-3(1)	Szacowanie ryzyka | Szacowanie ryzyka w łańcuchu dostaw			X	X	X
RA-3(2)	Szacowanie ryzyka | Wykorzystanie informacji ze wszystkich źródeł					
RA-3(3)	Szacowanie ryzyka | Świadomość dynamicznego zagrożenia					
RA-3(4)	Szacowanie ryzyka | Predykcyjna analityka cyberbezpieczeństwa					
RA-4	Aktualizacja oceny ryzyka	W: Włączono do RA-3				
RA-5	Monitorowanie i skanowanie podatności			X	X	X
RA-5(1)	Monitorowanie i skanowanie podatności | Aktualizacja narzędzi	W: Włączone do RA-5.				
RA-5(2)	Monitorowanie i skanowanie podatności | Aktualizacja skanowanych podatności			X	X	X
RA-5(3)	Monitorowanie i skanowanie podatności | Zakres i głębokość pokrycia					

RA-5(4)	Monitorowanie i skanowanie podatności | Informacje możliwe do odkrycia					X
RA-5(5)	Monitorowanie i skanowanie podatności | Dostęp uprzywilejowany				X	X
RA-5(6)	Monitorowanie i skanowanie podatności| Zautomatyzowane analizy trendów					
RA-5(7)	Monitorowanie i skanowanie podatności | Automatyczne wykrywanie i powiadamianie o nieautoryzowanych komponentach	W: Włączono do CM-8.				
RA-5(8)	Monitorowanie i skanowanie podatności | Przegląd historycznych logów audytu					
RA-5(9)	Monitorowanie i skanowanie podatności | Testowanie penetracyjne i analizy	W: Włączono do CA-8				
RA-5(10)	Monitorowanie i skanowanie podatności | Korelacja informacji ze skanowania					
RA-5(11)	Monitorowanie i skanowanie podatności | Program ujawniania publicznego			X	X	X
RA-6	Przegląd środków przeciwdziałania inwigilacji technicznej					
RA-7	Odpowiedź na ryzyko		X	X	X	X
RA-8	Oceny wpływu na prywatność		X			
RA-9	Analiza krytyczności				X	X
RA-10	Wykrywanie zagrożeń					
Nabywanie systemu i usług						
SA-1	Polityka i procedury		X	X	X	X
SA-2	Alokacja zasobów		X	X	X	X
SA-3	Cykl życia systemu		X	X	X	X

SA-3(1)	Cykl życia systemu | Zarządzanie środowiskiem przedprodukcyjnym					
SA-3(2)	Cykl życia systemu | Wykorzystanie danych produkcyjnych bieżących lub operacyjnych					
SA-3(3)	Cykl życia systemu | Odświeżanie technologii					
SA-4	Proces nabywania		X	X	X	X
SA-4(1)	Proces nabywania | Właściwości funkcjonalne mechanizmów kontrolnych				X	X
SA-4(2)	Proces nabywania | Projektowanie i implementacja mechanizmów kontrolnych				X	X
SA-4(3)	Proces nabywania | Metody rozwoju, techniki i praktyki					
SA-4(4)	Proces nabywania | Przypisanie komponentów do systemów	W: Włączono do CM-8(9).				
SA-4(5)	Proces nabywania | Konfiguracja systemu, komponentu i usługi					X
SA-4(6)	Proces nabywania | Używanie produktów zapewniających bezpieczeństwo informacji					
SA-4(7)	Proces nabywania | Zatwierdzone profile ochrony					
SA-4(8)	Proces nabywania | Plan ciągłego monitorowania mechanizmów kontrolnych					
SA-4(9)	Proces nabywania | Funkcje, porty, protokoły i usługi w użyciu				X	X

SA-4(10)	Proces nabywania | Wykorzystanie zatwierdzonych produktów			X	X	X
SA-4(11)	Proces nabywania | System rejestrów					
SA-4(12)	Proces nabywania | Własność danych					
SA-5	Dokumentacja systemu			X	X	X
SA-5(1)	Dokumentacja systemu | Funkcjonalne właściwości środków bezpieczeństwa	W: Włączono do SA-4(1).				
SA-5(2)	Dokumentacja systemu | Bezpieczeństwo interfejsów systemu zewnętrznego	W: Włączono do SA-4(2).				
SA-5(3)	Dokumentacja systemu | Projektowanie wysokopoziomowe	W: Włączono do SA-4(2).				
SA-5(4)	Dokumentacja systemu | Projektowanie niskopoziomowe	W: Włączono do SA-4(2).				
SA-5(5)	Dokumentacja systemu | Kod źródłowy	W: Włączono do SA-4(2).				
SA-6	Ograniczenia w użyciu oprogramowania	W: Włączono do CM-10 i SI-7.				
SA-7	Oprogramowanie instalowane przez użytkownika	W: Włączono do CM-11 i SI-7.				
SA-8	Zasady inżynierii bezpieczeństwa i prywatności			X	X	X
SA-8(1)	Zasady inżynierii bezpieczeństwa i prywatności | Przejrzystość interfejsów/ukrywanie informacji					
SA-8(2)	Zasady inżynierii bezpieczeństwa i prywatności | Minimalny współdzielony mechanizm					

SA-8(3)	Zasady inżynierii bezpieczeństwa i prywatności | Modułowość i warstwowość					
SA-8(4)	Zasady inżynierii bezpieczeństwa i prywatności | Częściowo uporządkowane zależności					
SA-8(5)	Zasady inżynierii bezpieczeństwa i prywatności | Efektywnie kontrolowany dostęp					
SA-8(6)	Zasady inżynierii bezpieczeństwa i prywatności | Minimalizacja współdzielenia					
SA-8(7)	Zasady inżynierii bezpieczeństwa i prywatności | Zmniejszona złożoność					
SA-8(8)	Zasady inżynierii bezpieczeństwa i prywatności | Bezpieczna zdolność do stopniowego rozwoju					
SA-8(9)	Zasady inżynierii bezpieczeństwa i prywatności | Zaufane komponenty					
SA-8(10)	Zasady inżynierii bezpieczeństwa i prywatności | Hierarchiczne zaufanie					
SA-8(11)	Zasady inżynierii bezpieczeństwa i prywatności | Odwrotny próg modyfikacji					
SA-8(12)	Zasady inżynierii bezpieczeństwa i prywatności | Ochrona hierarchiczna					

SA-8(13)	Zasady inżynierii bezpieczeństwa i prywatności | Zminimalizowane elementy bezpieczeństwa					
SA-8(14)	Zasady inżynierii bezpieczeństwa i prywatności | Najmniejsze uprawnienia					
SA-8(15)	Zasady inżynierii bezpieczeństwa i prywatności | Uprawnienia warunkowe					
SA-8(16)	Zasady inżynierii bezpieczeństwa i prywatności | Samodzielna wiarygodność					
SA-8(17)	Zasady inżynierii bezpieczeństwa i prywatności | Bezpieczna rozproszona kompozycja					
SA-8(18)	Zasady inżynierii bezpieczeństwa i prywatności | Zaufane kanały komunikacyjne					
SA-8(19)	Zasady inżynierii bezpieczeństwa i prywatności | Ochrona ciągła					
SA-8(20)	Zasady inżynierii bezpieczeństwa i prywatności | Bezpieczne zarządzanie metadanymi					
SA-8(21)	Zasady inżynierii bezpieczeństwa i prywatności | Samoocena					
SA-8(22)	Zasady inżynierii bezpieczeństwa i prywatności | Odpowiedzialność i możliwość śledzenia					

SA-8(23)	Zasady inżynierii bezpieczeństwa i prywatności | Bezpieczne ustawienia domyślne					
SA-8(24)	Zasady inżynierii bezpieczeństwa i prywatności | Kopia bezpieczeństwa i odzyskiwanie danych					
SA-8(25)	Zasady inżynierii bezpieczeństwa i prywatności | Bezpieczeństwo ekonomiczne					
SA-8(26)	Zasady inżynierii bezpieczeństwa i prywatności | Bezpieczeństwo wydajnościowe					
SA-8(27)	Zasady inżynierii bezpieczeństwa i prywatności | Bezpieczeństwo uwzględniające czynnik ludzki					
SA-8(28)	Zasady inżynierii bezpieczeństwa i prywatności | Akceptowalne bezpieczeństwo					
SA-8(29)	Zasady inżynierii bezpieczeństwa i prywatności | Powtarzalne i udokumentowane procedury					
SA-8(30)	Zasady inżynierii bezpieczeństwa i prywatności | Rygor proceduralny					
SA-8(31)	Zasady inżynierii bezpieczeństwa i prywatności | Bezpieczna modyfikacja systemu					

SA-8(32)	Zasady inżynierii bezpieczeństwa i prywatności | Wystarczająca dokumentacja					
SA-8(33)	Zasady inżynierii bezpieczeństwa i prywatności | Minimalizacja		X			
SA-9	Usługi systemu zewnętrznego		X	X	X	X
SA-9(1)	Usługi systemu zewnętrznego | Oceny ryzyka i zatwierdzenia organizacyjne					
SA-9(2)	Usługi systemu zewnętrznego | Identyfikacja funkcji, portów, protokołów i usług				X	X
SA-9(3)	Usługi systemu zewnętrznego | Ustanowienie i utrzymanie relacji zaufania z dostawcami					
SA-9(4)	Usługi systemu zewnętrznego | Zgodność interesów konsumentów i dostawców					
SA-9(5)	Usługi systemu zewnętrznego | Obszar procesowania, przechowywania i obsługi technicznej					
SA-9(6)	Usługi systemu zewnętrznego | Klucze kryptograficzne kontrolowane przez organizację					
SA-9(7)	Usługi systemu zewnętrznego | Kontrola integralności kontrolowana przez organizację					
SA-9(8)	Usługi systemu zewnętrznego | Lokalizacja przetwarzania i przechowywania					

SA-10	Zarządzanie konfiguracją oprogramowania				X	X
SA-10(1)	Zarządzanie konfiguracją oprogramowania | Weryfikacja integralności oprogramowania i firmware					
SA-10(2)	Zarządzanie konfiguracją oprogramowania | Alternatywne procesy zarządzania konfiguracją					
SA-10(3)	Zarządzanie konfiguracją oprogramowania | Weryfikacja integralności sprzętu					
SA-10(4)	Zarządzanie konfiguracją oprogramowania | Zaufana generacja					
SA-10(5)	Zarządzanie konfiguracją oprogramowania | Integralność mapowania kontroli wersji					
SA-10(6)	Zarządzanie konfiguracją oprogramowania | Zaufana dystrybucja					
SA-10(7)	Zarządzanie konfiguracją oprogramowania | Przedstawiciele ds. bezpieczeństwa i prywatności					
SA-11	Testowanie i ocena oprogramowania		X		X	X
SA-11(1)	Testowanie i ocena oprogramowania | Analiza kodu statycznego					
SA-11(2)	Testowanie i ocena oprogramowania | Modelowanie zagrożeń i analizy podatności					
SA-11(3)	Testowanie i ocena oprogramowania | Niezależna weryfikacja planów oceny i ewidencji					

SA-11(4)	Testowanie i ocena oprogramowania | Manualny przegląd kodu					
SA-11(5)	Testowanie i ocena oprogramowania | Testy penetracyjne					
SA-11(6)	Testowanie i ocena oprogramowania | Przegląd płaszczyzny ataku					
SA-11(7)	Testowanie i ocena oprogramowania | Weryfikacja zakresu testów i oceny					
SA-11(8)	Testowanie i ocena oprogramowania | Analiza dynamiczna kodu					
SA-11(9)	Testowanie i ocena oprogramowania | Interaktywne testowanie bezpieczeństwa aplikacji					
SA-12	Bezpieczeństwo łańcucha dostaw	W: Przeniesiono do rodziny SR				
SA-12(1)	Bezpieczeństwo łańcucha dostaw | Strategie / narzędzia / metody pozyskiwania	W: Przeniesiono do SR-5.				
SA-12(2)	Bezpieczeństwo łańcucha dostaw | Przegląd dostawców	W: Przeniesiono do SR-6.				
SA-12(3)	Bezpieczeństwo łańcucha dostaw | Zaufana wysyłka i magazynowanie	W: Włączone do SR-3.				
SA-12(4)	Bezpieczeństwo łańcucha dostaw | Różnorodność dostawców	W: Przeniesiono do SR-3(1).				
SA-12(5)	Bezpieczeństwo łańcucha dostaw | Ograniczenie szkód	W: Przeniesiono do SR-3(2).				
SA-12(6)	Bezpieczeństwo łańcucha dostaw | Minimalizacja czasu	W: Włączono do SR-5(1).				

SA-12(7)	Bezpieczeństwo łańcucha dostaw | Oceny przed wyborem / akceptacją / aktualizacją	W: Przeniesiono do SR-5(2).				
SA-12(8)	Bezpieczeństwo łańcucha dostaw | Wykorzystanie informacji ze wszystkich źródeł	W: Włączono do RA-3(2).				
SA-12(9)	Bezpieczeństwo łańcucha dostaw | Bezpieczeństwo operacji	W: Przeniesiono do SR-7.				
SA-12(10)	Bezpieczeństwo łańcucha dostaw | Walidacja autentyczności i niezmienności	W: Przeniesiono do SR-4(3).				
SA-12(11)	Bezpieczeństwo łańcucha dostaw | Testy penetracyjne / analiza elementów, procesów i podmiotów	W: Przeniesiono do SR-6(1).				
SA-12(12)	Bezpieczeństwo łańcucha dostaw | Porozumienia międzyorganizacyjne	W: Przeniesiono do SR-8.				
SA-12(13)	Bezpieczeństwo łańcucha dostaw | Krytyczne komponenty systemu informacyjnego	W: Włączone do MA-6 i RA-9.				
SA-12(14)	Bezpieczeństwo łańcucha dostaw | Tożsamość i identyfikowalność	W: Przeniesiono do SR-4(1) i SR-4(2).				
SA-12(15)	Bezpieczeństwo łańcucha dostaw | Procesy dotyczące słabości lub niedociągnięć	W: Włączone do SR-3.				
SA-13	Wiarygodność	W: Włączono do SA-8.				
SA-14	Analiza krytyczności	W: Włączono do RA-9.				
SA-14(1)	Analiza krytyczności | Komponenty krytyczne bez alternatywnych źródeł pozyskania	W: Włączone do SA-20.				
SA-15	Proces rozwoju, standardy i narzędzia				X	X

SA-15(1)	Proces rozwoju, standardy i narzędzia | Metryki jakości					
SA-15(2)	Proces rozwoju, standardy i narzędzia | Narzędzia śledzenia bezpieczeństwa i prywatności					
SA-15(3)	Proces rozwoju, standardy i narzędzia | Analiza krytyczności				X	X
SA-15(4)	Proces rozwoju, standardy i narzędzia | Modelowanie zagrożeń i analiza podatności	W: Włączono do SA-11(2).				
SA-15(5)	Proces rozwoju, standardy i narzędzia | Ograniczenie płaszczyzny ataku					
SA-15(6)	Proces rozwoju, standardy i narzędzia | Ciągłe doskonalenie					
SA-15(7)	Proces rozwoju, standardy i narzędzia | Automatyczna analiza podatności					
SA-15(8)	Proces rozwoju, standardy i narzędzia | Ponowne użycie informacji o zagrożeniach i podatnościach					
SA-15(9)	Proces rozwoju, standardy i narzędzia | Kreatywne wykorzystanie danych	W: Włączono do SA-3(2).				
SA-15(10)	Proces rozwoju, standardy i narzędzia | Plan reagowania na incydenty					
SA-15(11)	Proces rozwoju, standardy i narzędzia | Archiwizacja systemu lub komponentu					
SA-15(12)	Proces rozwoju, standardy i narzędzia | Minimalizacja danych osobowych					
SA-16	Szkolenia dostarczane przez dewelopera					X

SA-17	Architektura i projekt bezpieczeństwa i prywatności oprogramowania					X
SA-17(1)	Architektura i projekt bezpieczeństwa i prywatności oprogramowania | Formalny model polityki					
SA-17(2)	Architektura i projekt bezpieczeństwa i prywatności oprogramowania | Komponenty istotne dla bezpieczeństwa					
SA-17(3)	Architektura i projekt bezpieczeństwa i prywatności oprogramowania | Formalna zgodność					
SA-17(4)	Architektura i projekt bezpieczeństwa i prywatności oprogramowania | Nieformalna zgodność					
SA-17(5)	Architektura i projekt bezpieczeństwa i prywatności oprogramowania | Prosty koncepcyjnie projekt					
SA-17(6)	Architektura i projekt bezpieczeństwa i prywatności oprogramowania | Struktura testowania					
SA-17(7)	Architektura i projekt bezpieczeństwa i prywatności oprogramowania | Struktura dla najniższych uprawnień					
SA-17(8)	Architektura i projekt bezpieczeństwa i prywatności oprogramowania | Orkiestracja					

SA-17(9)	Architektura i projekt bezpieczeństwa i prywatności oprogramowania | Różnorodność projektów					
SA-18	Odporność na sabotaż i wykrywanie manipulacji	W: Przeniesiono do SR-9.				
SA-18(1)	Odporność na sabotaż i wykrywanie manipulacji | Wielofazowość cyklu życia systemu	W: Przeniesiono do SR-9(1).				
SA-18(2)	Odporność na sabotaż i wykrywanie manipulacji | Kontrola systemów lub komponentów	W: Przeniesiono do SR-10.				
SA-19	Autentyczność komponentów	W: Przeniesiono do SR-11.				
SA-19(1)	Autentyczność komponentów | Szkolenie / rozpoznawanie autentyczności	W: Przeniesiono do SR-11(1).				
SA-19(2)	Autentyczność komponentów | Kontrola konfiguracji na potrzeby serwisowania / naprawy komponentów	W: Przeniesiono do SR-11(2).				
SA-19(3)	Autentyczność komponentów | Utylizacja komponentów	W: Przeniesiono do SR-12.				
SA-19(4)	Autentyczność komponentów | Skanowanie autentyczności	W: Przeniesiono do SR-11(3).				
SA-20	Dedykowane tworzenie krytycznych komponentów					
SA-21	Kontrola programisty					X
SA-21(1)	Kontrola programisty | Ocena przeglądu	W: Włączone do SA-21.				
SA-22	Komponenty systemu bez wsparcia			X	X	X
SA-22(1)	Komponenty systemu bez wsparcia | Alternatywne źródła stałego wsparcia	W: Włączone do SA-22.				
SA-23	Specjalizacja					

Ochrona systemów i sieci telekomunikacyjnych						
SC-1	Polityka i procedury			X	X	X
SC-2	Separacja				X	X
SC-2(1)	Separacja | Interfejsy dla użytkowników nieuprzywilejowanych					
SC-2(2)	Separacja | Rozłączenie					
SC-3	Izolacja funkcji bezpieczeństwa					X
SC-3(1)	Izolacja funkcji bezpieczeństwa | Separacja sprzętowa					
SC-3(2)	Izolacja funkcji bezpieczeństwa | Funkcje kontroli dostępu i przepływu					
SC-3(3)	Izolacja funkcji bezpieczeństwa | Minimalizacja funkcjonalności niebędących funkcjami bezpieczeństwa					
SC-3(4)	Izolacja funkcji bezpieczeństwa | Sprzęganie i spójność modułów					
SC-3(5)	Izolacja funkcji bezpieczeństwa | Struktury warstwowe					
SC-4	Informacje w zasobach współdzielonego systemu				X	X
SC-4(1)	Informacje w zasobach współdzielonego systemu | Poziomy bezpieczeństwa	W: Włączone do SC-4.				
SC-4(2)	Informacje w zasobach współdzielonego systemu | Przetwarzanie wielopoziomowe lub okresowe					
SC-5	Ochrona przed odmową usługi			X	X	X
SC-5(1)	Ochrona przed odmową usługi | Ograniczenie możliwości atakowania innych systemów					

SC-5(2)	Ochrona przed odmową usługi | Pojemność, przepustowość i redundancja					
SC-5(3)	Ochrona przed odmową usługi | Wykrywanie i monitorowanie					
SC-6	Dostępność zasobów					
SC-7	Ochrona połączeń brzegowych			X	X	X
SC-7(1)	Ochrona połączeń brzegowych| Podsieci fizycznie wydzielone	W: Włączone do SC-7.				
SC-7(2)	Ochrona połączeń brzegowych | Dostęp publiczny	W: Włączone do SC-7.				
SC-7(3)	Ochrona połączeń brzegowych | Punkty dostępu				X	X
SC-7(4)	Ochrona połączeń brzegowych | Zewnętrzne usługi telekomunikacyjne				X	X
SC-7(5)	Ochrona połączeń brzegowych | Odmów domyślnie — zezwól na zasadzie wyjątku				X	X
SC-7(6)	Ochrona połączeń brzegowych | Reakcja na wykryte awarie	W: Włączono do SC-7(18).				
SC-7(7)	Ochrona połączeń brzegowych | Tunelowanie dzielone dla urządzeń zdalnych				X	X
SC-7(8)	Ochrona połączeń brzegowych | Kierowanie ruchu do uwierzytelnionych serwerów proxy				X	X
SC-7(9)	Ochrona połączeń brzegowych | Ograniczanie zagrażającego ruchu komunikacyjnego wychodzącego					
SC-7(10)	Ochrona połączeń brzegowych| Zapobieganie eksfiltracji					

SC-7(11)	Ochrona połączeń brzegowych | Ograniczenie ruchu przychodzącego					
SC-7(12)	Ochrona połączeń brzegowych | Ochrona oparta na hoście					
SC-7(13)	Ochrona połączeń brzegowych | Izolacja narzędzi bezpieczeństwa, mechanizmów i komponentów pomocniczych					
SC-7(14)	Ochrona połączeń brzegowych | Ochrona przed nieautoryzowanymi połączeniami fizycznymi					
SC-7(15)	Ochrona połączeń brzegowych | Sieciowe uprzywilejowane dostępy					
SC-7(16)	Ochrona połączeń brzegowych | Zapobieganie wykrywaniu składników systemu					
SC-7(17)	Ochrona połączeń brzegowych | Automatyczne egzekwowanie formatów protokołów					
SC-7(18)	Ochrona połączeń brzegowych | Fail Secure					X
SC-7(19)	Ochrona połączeń brzegowych | Blokowanie komunikacji z hostów nieskonfigurowanych organizacyjnie					
SC-7(20)	Ochrona połączeń brzegowych | Dynamiczna izolacja i separacja					
SC-7(21)	Ochrona połączeń brzegowych | Izolacja komponentów systemu					X

SC-7(22)	Ochrona połączeń brzegowych | Oddzielne podsieci do łączenia się z różnymi domenami zabezpieczeń					
SC-7(23)	Ochrona połączeń brzegowych | Wyłącz informacje zwrotne nadawcy o niepowodzeniu walidacji protokołu					
SC-7(24)	Ochrona połączeń brzegowych | Informacje umożliwiające identyfikację osoby		X			
SC-7(25)	Ochrona połączeń brzegowych | Połączenia z systemami państwowymi przetwarzającymi informacje jawne					
SC-7(26)	Ochrona połączeń brzegowych | Połączenia z systemami państwowymi przetwarzającymi informacje niejawne					
SC-7(27)	Ochrona połączeń brzegowych | Połączenia z jawnymi systemami niemającymi znaczenia dla bezpieczeństwa narodowego					
SC-7(28)	Ochrona połączeń brzegowych | Połączenia z sieciami publicznymi					
SC-7(29)	Ochrona połączeń brzegowych | Oddzielne podsieci w celu odizolowania funkcji					
SC-8	Poufność i integralność transmisji				X	X
SC-8(1)	Poufność i integralność transmisji | Ochrona kryptograficzna				X	X
SC-8(2)	Poufność i integralność transmisji | Postępowanie przed i po transmisji					

SC-8(3)	Poufność i integralność transmisji | Ochrona kryptograficzna zewnętrznych elementów wiadomości					
SC-8(4)	Poufność i integralność transmisji | Ukrywanie lub losowe łączenie komunikatów					
SC-8(5)	Poufność i integralność transmisji | Chroniony system dystrybucji					
SC-9	Poufność transmisji	W: Włączone do SC-8.				
SC-10	Rozłączenie sieci				X	X
SC-11	Zaufana ścieżka					
SC-11(1)	Zaufana ścieżka | Niepodważalna ścieżka komunikacji					
SC-12	Ustanawianie i zarządzanie kluczami kryptograficznymi			X	X	X
SC-12(1)	Ustanawianie i zarządzanie kluczami kryptograficznymi | Dostępność					X
SC-12(2)	Ustanawianie i zarządzanie kluczami kryptograficznymi | Klucze symetryczne					
SC-12(3)	Ustanawianie i zarządzanie kluczami kryptograficznymi | Klucze asymetryczne					
SC-12(4)	Ustanawianie i zarządzanie kluczami kryptograficznymi | Certyfikaty PKI	W: Włączono do SC-12(3).				
SC-12(5)	Ustanawianie i zarządzanie kluczami kryptograficznymi | Certyfikaty PKI / Tokeny sprzętowe	W: Włączono do SC-12(3).				
SC-12(6)	Ustanawianie i zarządzanie kluczami kryptograficznymi | Kontrola fizyczna kluczy					
SC-13	Ochrona kryptograficzna			X	X	X

SC-13(1)	Ochrona kryptograficzna | Kryptografia zgodna z FIPS	W: Włączone do SC-13.				
SC-13(2)	Ochrona kryptograficzna | Kryptografia zatwierdzona przez NSA	W: Włączone do SC-13.				
SC-13(3)	Ochrona kryptograficzna | Osoby indywidualne bez formalnych zatwierdzeń na dostęp	W: Włączone do SC-13.				
SC-13(4)	Ochrona kryptograficzna | Podpisy cyfrowe	W: Włączone do SC-13.				
SC-14	Ochrona dostępu publicznego	W: Włączone do AC-2, AC-3, AC-5, SI-3, SI-4, SI-5, SI-7 i SI-10.				
SC-15	Współpracujące urządzenia komputerowe			X	X	X
SC-15(1)	Współpracujące urządzenia komputerowe | Rozłączenie fizyczne lub logiczne					
SC-15(2)	Współpracujące urządzenia komputerowe| Blokowanie ruchu wejściowego / wyjściowego	W: Włączone do SC-7.				
SC-15(3)	Współpracujące urządzenia komputerowe | Wyłączanie i usuwanie w bezpiecznych obszarach roboczych					
SC-15(4)	Współpracujące urządzenia komputerowe| Wyraźnie wskaż bieżących uczestników					
SC-16	Przesyłanie atrybutów bezpieczeństwa i prywatności					
SC-16(1)	Przesyłanie atrybutów bezpieczeństwa i prywatności | Weryfikacja integralności					

SC-16(2)	Przesyłanie atrybutów bezpieczeństwa i prywatności | Mechanizmy antyspoofingowe					
SC-16(3)	Przesyłanie atrybutów bezpieczeństwa i prywatności | Kryptograficzne wiązanie					
SC-17	Certyfikaty infrastruktury klucza publicznego				X	X
SC-18	Kod mobilny				X	X
SC-18(1)	Kod mobilny | Identyfikuj niedopuszczalny kod i podejmuj działania naprawcze					
SC-18(2)	Kod mobilny | Nabywanie, rozwój i użytkowanie					
SC-18(3)	Kod mobilny | Zapobiegaj pobieraniu i wykonywaniu					
SC-18(4)	Kod mobilny | Zapobiegaj automatycznemu wykonywaniu					
SC-18(5)	Kod mobilny | Zezwalaj na wykonywanie tylko w ograniczonych środowiskach					
SC-19	VOIP	W: Specyficzne dla technologii; traktowane jak każda inna technologia lub protokół.				
SC-20	Usługa bezpiecznego rozpoznawania nazw/adresów (źródło wiarygodne)			X	X	X
SC-20(1)	Usługa bezpiecznego rozpoznawania nazw/adresów (źródło wiarygodne) | Podobszary podrzędne	W: Włączone do SC-20.				

SC-20(2)	Usługa bezpiecznego rozpoznawania nazw/adresów (źródło wiarygodne) | Pochodzenie i integralność danych					
SC-21	Usługa bezpiecznego rozpoznawania nazw/adresów (rekurencyjna lub buforująca)			X	X	X
SC-21(1)	Usługa bezpiecznego rozpoznawania nazw/adresów (rekurencyjna lub buforująca) | Pochodzenie i integralność danych	W: Włączone do SC-21.				
SC-22	Architektura i dostarczanie usług rozpoznawania nazw/adresów			X	X	X
SC-23	Autentyczność sesji				X	X
SC-23(1)	Autentyczność sesji | Unieważnij identyfikatory sesji przy wylogowaniu					
SC-23(2)	Autentyczność sesji | Wylogowania inicjowane przez użytkownika i wyświetlanie komunikatów	W: Włączono do AC-12(1).				
SC-23(3)	Autentyczność sesji | Unikalne identyfikatory sesji generowane przez system					
SC-23(4)	Autentyczność sesji | Unikalne identyfikatory sesji z randomizacją	W: Włączono do SC-23(3).				
SC-23(5)	Autentyczność sesji | Dozwolone centra certyfikacji					
SC-24	Przejście do określonego stanu systemu po błędzie					X
SC-25	Thin nodes / terminalowe stacje robocze					
SC-26	Honeypots					

SC-26(1)	Honeypots | Wykrywanie złośliwego kodu	W: Włączone do SC-35.				
SC-27	Aplikacje niezależne od platformy					
SC-28	Ochrona informacji w spoczynku				X	X
SC-28(1)	Ochrona informacji w spoczynku | Ochrona kryptograficzna				X	X
SC-28(2)	Ochrona informacji w spoczynku | Przechowywanie offline					
SC-28(3)	Ochrona informacji w spoczynku | Klucze kryptograficzne					
SC-29	Heterogeniczność systemu					
SC-29(1)	Heterogeniczność systemu | Techniki wirtualizacji					
SC-30	Masakowanie i dezinformacja					
SC-30(1)	Maskowanie i dezinformacja| Techniki wirtualizacji	W: Włączono do SC-29(1).				
SC-30(2)	Maskowanie i dezinformacja | Losowość					
SC-30(3)	Maskowanie i dezinformacja| Zmiana lokalizacji przetwarzania i przechowywania					
SC-30(4)	Maskowanie i dezinformacja | Informacje wprowadzające w błąd					
SC-30(5)	Maskowanie i dezinformacja | Ukrywanie komponentów systemu					
SC-31	Analiza ukrytego kanału komunikacji					
SC-31(1)	Analiza ukrytego kanału komunikacji | Testowanie kanałów ukrytych pod kątem podatności na wykorzystanie					

SC-31(2)	Analiza ukrytego kanału komunikacji | Maksymalna przepustowość					
SC-31(3)	Analiza ukrytego kanału komunikacji | Pomiar przepustowości w środowiskach operacyjnych					
SC-32	Partycjonowanie systemu					
SC-32(1)	Partycjonowanie systemu | Oddzielne domeny fizyczne dla funkcji uprzywilejowanych					
SC-33	Integralność transmisji	W: Włączone do SC-8.				
SC-34	Niemodyfikowalne programy wykonywalne					
SC-34(1)	Niemodyfikowalne programy wykonywalne | Brak możliwości zapisu w pamięci masowej					
SC-34(2)	Niemodyfikowalne programy wykonywalne | Ochrona integralności na nośnikach tylko do odczytu					
SC-34(3)	Niemodyfikowalne programy wykonywalne | Ochrona sprzętowa	W: Przeniesiono do SC-51.				
SC-35	Identyfikacja zewnętrznego złośliwego kodu (honeyclients)					
SC-36	Rozproszone przetwarzanie i przechowywanie					
SC-36(1)	Rozproszone przetwarzanie i przechowywanie | Techniki sondowania					
SC-36(2)	Rozproszone przetwarzanie i przechowywanie | Synchronizacja					
SC-37	Kanały pozapasmowe					

SC-37(1)	Kanały pozapasmowe | Zapewnij dostarczanie i transmisję					
SC-38	Bezpieczeństwo operacyjne					
SC-39	Izolacja procesu			X	X	X
SC-39(1)	Izolacja procesu | Separacja sprzętowa					
SC-39(2)	Izolacja procesu | Oddzielna domena wykonania na wątek					
SC-40	Ochrona łącza bezprzewodowego					
SC-40(1)	Ochrona łącza bezprzewodowego | Zakłócenia elektromagnetyczne					
SC-40(2)	Ochrona łącza bezprzewodowego | Zmniejszenie potencjału wykrywania					
SC-40(3)	Ochrona łącza bezprzewodowego | Oszustwo komunikacyjne imitacyjne lub manipulacyjne					
SC-40(4)	Ochrona łącza bezprzewodowego | Identyfikacja parametrów sygnału					
SC-41	Dostęp do portu i urządzenia wejścia / wyjścia					
SC-42	Funkcjonalności i dane czujników					
SC-42(1)	Funkcjonalności i dane czujników | Raportowanie do upoważnionych osób lub ról					
SC-42(2)	Funkcjonalności i dane czujników | Autoryzowane użycie					
SC-42(3)	Funkcjonalności i dane czujników | Zakaz używania urządzeń	W: Włączone do SC-42.				

SC-42(4)	Funkcjonalności i dane czujników | Powiadomienie o gromadzeniu					
SC-42(5)	Funkcjonalności i dane czujników | Minimalizacja gromadzenia danych					
SC-43	Ograniczenia użytkowania					
SC-44	Komory detonacyjne					
SC-45	Synchronizacja czasu systemowego					
SC-45(1)	Synchronizacja czasu systemowego | Synchronizacja z autorytatywnym źródłem czasu					
SC-45(2)	Synchronizacja czasu systemowego | Drugorzędne autorytatywne źródło czasu					
SC-46	Egzekwowanie polityki między domenami					
SC-47	Alternatywne ścieżki komunikacji					
SC-48	Przeniesienie czujnika					
SC-48(1)	Przeniesienie czujnika | Dynamiczne przenoszenie czujników lub możliwości monitorowania					
SC-49	Separacja wymuszona sprzętowo i egzekwowanie zasad					
SC-50	Separacja wymuszana programowo i egzekwowanie zasad					
SC-51	Ochrona oparta na sprzęcie					
Integralność systemu i informacji						
SI-1	Polityka i procedury		X	X	X	X
SI-2	Naprawa usterek			X	X	X
SI-2(1)	Naprawa usterek | Centralne zarządzanie	W: Włączone do PL-9.				

SI-2(2)	Naprawa usterek | Zautomatyzowany status naprawy usterek				X	X
SI-2(3)	Naprawa usterek | Czas na naprawę usterek i punkty odniesienia dla działań korygujących					
SI-2(4)	Naprawa błędów | Zautomatyzowane narzędzia do zarządzania poprawkami					
SI-2(5)	Naprawa błędów | Automatyczne aktualizacje oprogramowania i oprogramowania sprzętowego					
SI-2(6)	Naprawa błędów | Usuwanie poprzednich wersji oprogramowania i oprogramowania sprzętowego					
SI-3	Ochrona przed złośliwym kodem			X	X	X
SI-3(1)	Ochrona przed złośliwym kodem | Centralne zarządzanie	W: Włączone do PL-9.				
SI-3(2)	Ochrona przed złośliwym kodem | Automatyczne aktualizacje	W: Włączono do SI-3.				
SI-3(3)	Ochrona przed złośliwym kodem | Użytkownicy bez uprawnień	W: Włączono do AC-6(10).				
SI-3(4)	Ochrona przed złośliwym kodem | Aktualizacje tylko dla użytkowników uprzywilejowanych					
SI-3(5)	Ochrona przed złośliwym kodem | Urządzenia pamięci masowej przenośnej	W: Wbudowany w MP-7.				
SI-3(6)	Ochrona przed złośliwym kodem | Testowanie i weryfikacja					

SI-3(7)	Ochrona przed złośliwym kodem | Wykrywanie nieoparte na sygnaturach	W: Włączono do SI-3.				
SI-3(8)	Ochrona przed złośliwym kodem | Wykrywanie nieautoryzowanych poleceń					
SI-3(9)	Ochrona przed złośliwym kodem | Uwierzytelnianie poleceń zdalnych	W: Przeniesiono do AC-17(10).				
SI-3(10)	Ochrona przed złośliwym kodem | Analiza złośliwego kodu					
SI-4	Monitorowanie systemu			X	X	X
SI-4(1)	Monitorowanie systemu | System wykrywania włamań w całym systemie					
SI-4(2)	Monitorowanie systemu | Zautomatyzowane narzędzia i mechanizmy do analizy w czasie rzeczywistym				X	X
SI-4(3)	Monitorowanie systemu | Zautomatyzowana integracja narzędzi i mechanizmów					
SI-4(4)	Monitorowanie systemu | Ruch komunikacyjny przychodzący i wychodzący				X	X
SI-4(5)	Monitorowanie systemu | Alerty generowane przez system				X	X
SI-4(6)	Monitorowanie systemu | Ograniczanie użytkowników bez uprawnień	W: Włączono do AC-6(10).				
SI-4(7)	Monitorowanie systemu | Automatyczna reakcja na podejrzane zdarzenia					
SI-4(8)	Monitorowanie systemu | Ochrona informacji monitorowanych	W: Włączono do SI-4.				

SI-4(9)	Monitorowanie Systemu | Testowanie narzędzi i mechanizmów monitorujących					
SI-4(10)	Monitorowanie systemu | Widoczność szyfrowanej komunikacji					X
SI-4(11)	Monitorowanie systemu | Analiza anomalii ruchu komunikacyjnego					
SI-4(12)	Monitorowanie systemu | Automatyczne alerty generowane przez organizację					X
SI-4(13)	Monitorowanie systemu | Analiza wzorców ruchu i zdarzeń					
SI-4(14)	Monitorowanie systemu | Wykrywanie włamań bezprzewodowych					X
SI-4(15)	Monitorowanie systemu | Komunikacja bezprzewodowa do przewodowej					
SI-4(16)	Monitorowanie systemu | Powiązanie informacji o monitorowaniu					
SI-4(17)	Monitorowanie systemu | Zintegrowana świadomość sytuacyjna					
SI-4(18)	Monitorowanie systemu | Analiza ruchu i ukrytej eksfiltracji					
SI-4(19)	Monitorowanie systemu | Ryzyko dla osób fizycznych					
SI-4(20)	Monitorowanie systemu | Użytkownicy uprzywilejowani					X
SI-4(21)	Monitorowanie systemu | Okresy próbne					
SI-4(22)	Monitorowanie systemu | Nieautoryzowane usługi sieciowe					X
SI-4(23)	Monitorowanie systemu | Urządzenia hostowe					

SI-4(24)	Monitorowanie systemu | Wskaźniki zagrożenia					
SI-4(25)	Monitorowanie systemu | Optymalizacja analizy ruchu sieciowego					
SI-5	Alerty bezpieczeństwa, porady i dyrektywy			X	X	X
SI-5(1)	Alerty bezpieczeństwa, porady i dyrektywy | Automatyczne alerty i porady					X
SI-6	Weryfikacja funkcji bezpieczeństwa i prywatności					X
SI-6(1)	Weryfikacja funkcji bezpieczeństwa i prywatności | Powiadomienie o nieudanych testach bezpieczeństwa	W: Włączono do SI-6.				
SI-6(2)	Weryfikacja funkcji bezpieczeństwa i prywatności | Obsługa automatyzacji dla rozproszonych testów					
SI-6(3)	Weryfikacja funkcji bezpieczeństwa i prywatności | Raportuj wyniki weryfikacji					
SI-7	Oprogramowanie, oprogramowanie sprzętowe i integralność informacji				X	X
SI-7(1)	Oprogramowanie, oprogramowanie sprzętowe i integralność informacji | Kontrole integralności				X	X
SI-7(2)	Oprogramowanie, oprogramowanie sprzętowe i integralność informacji | Automatyczne powiadomienia o naruszeniach integralności					X

SI-7(3)	Oprogramowanie, oprogramowanie sprzętowe i integralność informacji| Centralnie zarządzane narzędzia do zapewniania integralności					
SI-7(4)	Oprogramowanie, oprogramowanie sprzętowe i integralność informacji | Opakowanie zabezpieczające przed manipulacją	W: Włączone do SR-9.				
SI-7(5)	Oprogramowanie, oprogramowanie sprzętowe i integralność informacji | Automatyczna odpowiedź na naruszenia integralności					X
SI-7(6)	Oprogramowanie, oprogramowanie sprzętowe i integralność informacji | Ochrona kryptograficzna					
SI-7(7)	Oprogramowanie, oprogramowanie sprzętowe i integralność informacji | Integracja wykrywania i reagowania				X	X
SI-7(8)	Oprogramowanie, oprogramowanie sprzętowe i integralność informacji | Możliwość audytu istotnych zdarzeń					
SI-7(9)	Oprogramowanie, oprogramowanie sprzętowe i integralność informacji | Weryfikacja procesu rozruchu					
SI-7(10)	Oprogramowanie, oprogramowanie sprzętowe i integralność informacji | Ochrona oprogramowania sprzętowego rozruchowego					

SI-7(11)	Oprogramowanie, oprogramowanie sprzętowe i integralność informacji | Środowiska zamknięte z ograniczonymi uprawnieniami	W: Przeniesiono do CM-7(6).				
SI-7(12)	Oprogramowanie, oprogramowanie sprzętowe i integralność informacji | Weryfikacja integralności					
SI-7(13)	Oprogramowanie, oprogramowanie sprzętowe i integralność informacji | Wykonywanie kodu w środowiskach chronionych	W: Przeniesiono do CM-7(7).				
SI-7(14)	Oprogramowanie, oprogramowanie sprzętowe i integralność informacji | Kod wykonywalny binarny lub maszynowy	W: Przeniesiono do CM-7(8).				
SI-7(15)	Oprogramowanie, oprogramowanie sprzętowe i integralność informacji | Uwierzytelnianie kodem					X
SI-7(16)	Oprogramowanie, oprogramowanie sprzętowe i integralność informacji | Ograniczenie czasowe wykonywania procesów bez nadzoru					
SI-7(17)	Oprogramowanie, oprogramowanie sprzętowe i integralność informacji | Samodzielna ochrona aplikacji w czasie wykonywania					
SI-8	Ochrona przed spamem				X	X
SI-8(1)	Ochrona przed spamem | Centralne zarządzanie	W: Włączone do PL-9.				
SI-8(2)	Ochrona przed spamem | Automatyczne aktualizacje				X	X

SI-8(3)	Ochrona przed spamem | Możliwość ciągłego uczenia się					
SI-9	Ograniczenia wprowadzania informacji	W: Włączone do AC-2, AC-3, AC5 i AC-6.				
SI-10	Walidacja wprowadzanych informacji				X	X
SI-10(1)	Walidacja wprowadzanych informacji | Możliwość ręcznego nadpisywania					
SI-10(2)	Walidacja wprowadzanych informacji | Przeglądanie i rozwiązywanie błędów					
SI-10(3)	Walidacja wprowadzanych informacji | Przewidywalne zachowanie					
SI-10(4)	Walidacja wprowadzanych informacji | Interakcje czasowe					
SI-10(5)	Walidacja wprowadzanych informacji | Ograniczanie danych wejściowych do zaufanych źródeł i zatwierdzonych formatów					
SI-10(6)	Walidacja wprowadzanych informacji | Zapobieganie iniekcji					
SI-11	Obsługa błędów				X	X
SI-12	Zarządzanie informacją i jej przechowywanie		X	X	X	X
SI-12(1)	Zarządzanie informacją i jej przechowywanie | Ograniczanie elementów informacji umożliwiających identyfikację osoby		X			

SI-12(2)	Zarządzanie informacją i jej przechowywanie | Minimalizowanie danych osobowych podczas testów, szkoleń i badań		X			
SI-12(3)	Zarządzanie informacją i jej przechowywanie | Usuwanie informacji		X			
SI-13	Przewidywalne zapobieganie awariom					
SI-13(1)	Przewidywalne zapobieganie awariom | Przenoszenie odpowiedzialności za komponenty					
SI-13(2)	Przewidywalne zapobieganie awariom | Limit czasu na wykonanie procesu bez nadzoru	W: Włączono do SI-7(16).				
SI-13(3)	Przewidywalne zapobieganie awariom | Ręczne przesyłanie między komponentami					
SI-13(4)	Przewidywalne zapobieganie awariom | Instalacja i powiadamianie o komponentach w trybie gotowości					
SI-13(5)	Przewidywalne zapobieganie awariom | Możliwość przełączania awaryjnego					
SI-14	Nietrwałość					
SI-14(1)	Nietrwałość | Odśwież z zaufanych źródeł					
SI-14(2)	Nietrwałość | Informacje nietrwałe					
SI-14(3)	Nietrwałość | Nietrwała łączność					
SI-15	Filtrowanie danych wyjściowych					
SI-16	Ochrona pamięci				X	X
SI-17	Procedury bezpieczeństwa					
SI-18	Operacje związane z jakością danych osobowych		X			

SI-18(1)	Operacje związane z jakością danych osobowych | Wsparcie automatyzacji					
SI-18(2)	Operacje związane z jakością danych osobowych| Znaczniki danych					
SI-18(3)	Operacje związane z jakością danych osobowych | Gromadzenie					
SI-18(4)	Operacje związane z jakością danych osobowych| Indywidualne żądania		X			
SI-18(5)	Operacje związane z jakością danych osobowych | Powiadomienie o korekcie lub usunięciu					
SI-19	De-identyfikacja		X			
SI-19(1)	De-identyfikacja | Kolekcja					
SI-19(2)	De-identyfikacja | Archiwizacja					
SI-19(3)	De-identyfikacja | Wydanie					
SI-19(4)	De-identyfikacja | Usuwanie, maskowanie, szyfrowanie, haszowanie lub zastępowanie bezpośrednich identyfikatorów					
SI-19(5)	De-identyfikacja | Kontrola ujawniania danych statystycznych					
SI-19(6)	De-identyfikacja | Różnicowa prywatność					
SI-19(7)	De-identyfikacja | Zweryfikowane algorytmy i oprogramowanie					
SI-19(8)	De-identyfikacja | Test "zmotywowanego intruza"					
SI-20	Oznaczanie danych					
SI-21	Odświeżanie informacji					
SI-22	Różnorodność informacji					
SI-23	Fragmentacja informacji					

Zarządzanie ryzykiem w łańcuchu dostaw						
SR-1	Polityka i procedury			X	X	X
SR-2	Plan zarządzania ryzykiem w łańcuchu dostaw			X	X	X
SR-2(1)	Plan zarządzania ryzykiem w łańcuchu dostaw | Powołanie zespołu zarządzania ryzykiem w łańcuchu dostaw			X	X	X
SR-3	Zabezpieczenia i procesy w łańcuchu dostaw			X	X	X
SR-3(1)	Zabezpieczenia i procesy w łańcuchu dostaw | Zróżnicowana baza dostaw					
SR-3(2)	Zabezpieczenia i procesy w łańcuchu dostaw| Ograniczanie szkód					
SR-3(3)	Zabezpieczenie i procesy w łańcuchu dostaw | Podwykonawcy					
SR-4	Pochodzenie					
SR-4(1)	Pochodzenie | Tożsamość					
SR-4(2)	Pochodzenie | Śledzenie przesyłek					
SR-4(3)	Pochodzenie | Potwierdzanie autentyczności i niezmienności					
SR-4(4)	Pochodzenie | Integralność łańcucha dostaw - pochodzenie					
SR-5	Strategie, narzędzia i metody nabycia			X	X	X
SR-5(1)	Strategie, narzędzia i metody nabycia | Odpowiednie zaopatrzenie					
SR-5(2)	Strategie, narzędzia i metody nabycia | Oceny przed wyborem, akceptacją, modyfikacją lub aktualizacją					
SR-6	Oceny i recenzje dostawców				X	X

SR-6(1)	Oceny i recenzje dostawców | Badania i analizy					
SR-7	Bezpieczeństwo operacji w ramach łańcucha dostaw					
SR-8	Umowy dotyczące powiadomień			X	X	X
SR-9	Odporność na manipulacje i wykrywanie sabotażu					X
SR-9(1)	Odporność na manipulacje i wykrywanie sabotażu | Wieloetapowy cykl życia systemu					X
SR-10	Kontrola systemów / komponentów			X	X	X
SR-11	Autentyczność komponentu			X	X	X
SR-11(1)	Autentyczność komponentu| Szkolenie z zakresu zapobiegania fałszerstwom			X	X	X
SR-11(2)	Autentyczność komponentu| Zabezpieczenie konfiguracji serwisowanych i naprawianych komponentów			X	X	X
SR-11(3)	Autentyczność komponentu | Skanowanie antyfałszerskie					
SR-12	Usuwanie komponentów			X	X	X

KATEGORIA: AC – KONTROLA DOSTĘPU

AC-1 POLITYKA I PROCEDURY KONTROLI DOSTĘPU

Zabezpieczenie:

a. [Realizacja: personel lub role zdefiniowane przez organizację] Opracowuj, udokumentuj i rozpowszechniaj wśród:
   1. [Wybór (jeden lub więcej): Poziom organizacji; Poziom misji/procesu biznesowego; Poziom systemu] politykę kontroli dostępu, która:

(a) dotyczy celu, zakresu, ról, obowiązków, zaangażowania kierownictwa, koordynacji między jednostkami organizacyjnymi i zgodności;

(b) jest zgodna z obowiązującymi przepisami prawa, rozporządzeniami wykonawczymi, dyrektywami, regulacjami, politykami, normami i wytycznymi;

(c) Procedury ułatwiające wdrażanie polityki kontroli dostępu i powiązanych kontroli dostępu;

b. Wyznacz [Realizacja: osoby zdefiniowanej przez organizację] do zarządzania opracowywaniem, dokumentowaniem i rozpowszechnianiem polityki i procedur kontroli dostępu;

c. Przeglądaj i aktualizuj bieżącą kontrolę dostępu:

1. Polityki [Realizacja: częstotliwość zdefiniowana przez organizację] i następujące [Realizacja: zdarzenia zdefiniowane przez organizację];

2. Procedur [Realizacja: częstotliwość zdefiniowana przez organizację] i następujące [Realizacja: zdarzenia zdefiniowane przez organizację].

Zabezpieczenia powiązane: IA-1, PM-9, PM-24, PS-8, SI-12.

Zabezpieczenia rozszerzone: nie dotyczy.

AC-2 ZARZĄDZANIE KONTAMI

Zabezpieczenie:

a. Zdefiniuj i udokumentuj typy kont dozwolonych i konkretnie zabronionych do użycia w systemie;
b. Przypisz menedżerów kont;
c. Wymagaj [Realizacja: zdefiniowania przez organizację wymagań wstępnych i kryteriów] dla członkostwa w grupie i roli;
d. Określ:
    1. Upoważnionych użytkowników systemu;
    2. Członkostwo w grupie i roli;
    3. Uprawnienia dostępu (tj. uprawnienia) i [Realizacja: zdefiniowane przez organizację atrybuty (w razie potrzeby)] dla każdego konta;
e. Wymagaj zatwierdzeń przez [Realizacja: zdefiniowany przez organizację personel lub role] dla wniosków o utworzenie kont;
f. Twórz, włączaj, modyfikuj, wyłączaj i usuwaj konta zgodnie z [Realizacja: zdefiniowaną przez organizację polityką, procedurami, wymaganiami wstępnymi i kryteriami];
g. Monitoruj korzystanie z kont;
h. Powiadom menedżerów kont i [Realizacja: zdefiniowany przez organizację personel lub role] w ciągu:
    1. [Realizacja: zdefiniowany przez organizację okres czasu], gdy konta nie są już wymagane;

2. [Realizacja: okres czasu zdefiniowany przez organizację], gdy użytkownicy są zwalniani lub przenoszeni;
3. [Realizacja: okres czasu zdefiniowany przez organizację], gdy użytkowanie systemu lub konieczność wiedzy zmienia się dla danej osoby;

i. Autoryzuj dostęp do systemu na podstawie:
   1. Ważnej autoryzacji dostępu;
   2. Zamierzonego użytkowania systemu;
   3. [Realizacja: atrybuty zdefiniowane przez organizację (w razie potrzeby)];
j. Przejrzyj konta pod kątem zgodności z wymogami zarządzania kontami [Realizacja: częstotliwość zdefiniowana przez organizację];
k. Ustanów i wprowadź proces zmiany środków uwierzytelniających współdzielonych lub grupowych kont (jeśli wdrożono), gdy osoby są usuwane z grupy;
l. Dostosuj procesy zarządzania kontami do procesów zwalniania i przenoszenia personelu.

Zabezpieczenia powiązane: AC-3, AC-5, AC-6, AC-17, AC-18, AC-20, AC-24, AU-2, AU-12, CM-5, IA-2, IA-4, IA-5, IA-8, MA-3, MA-5, PE-2, PL-4, PS-2, PS-4, PS-5, PS-7, PT-2, PT-3, SC-7, SC-12, SC-13, SC-37.

Zabezpieczenia rozszerzone:

(1) ZARZĄDZANIE KONTAMI | AUTOMATYCZNE ZARZĄDZANIE KONTEM SYSTEMOWYM

Wspieraj zarządzanie kontami systemowymi przy użyciu [Realizacja: zautomatyzowanych mechanizmów zdefiniowanych przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(2) ZARZĄDZANIE KONTAMI | USUWANIE KONT TYMCZASOWYCH / AWARYJNYCH

Automatycznie [Wybór: usuń; wyłącz] konta tymczasowe i awaryjne po [Realizacja: okres czasu zdefiniowany przez organizację dla każdego typu konta].

Zabezpieczenia powiązane: nie dotyczy.

(3) ZARZĄDZANIE KONTAMI | WYŁĄCZANIE KONT

Wyłącz konta w ciągu [Realizacja: okres czasu określony przez organizację], jeśli:

a. wygasły;

b. nie są już powiązane z użytkownikiem lub osobą;

c. naruszają zasady organizacji;

d. były nieaktywne przez [Realizacja: okres czasu określony przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(4) ZARZĄDZANIE KONTAMI | AUTOMATYCZNE DZIAŁANIA AUDYTOWE

Automatycznie audytuj działania związane z tworzeniem, modyfikowaniem, włączaniem, wyłączaniem i usuwaniem kont.

Zabezpieczenia powiązane: AU-2, AU-6.

(5) ZARZĄDZANIE KONTAMI | WYLOGOWANIE PO OKREŚLONYM OKRESIE NIEAKTYWNOŚCI

Wymagaj, aby użytkownicy wylogowywali się, gdy [Realizacja: upłynął zdefiniowany przez organizację okres bezczynności lub automatyczne wylogowanie po ustalonym okresie bezczynności].

Zabezpieczenia powiązane: AC-11.

(6) ZARZĄDZANIE KONTAMI | DYNAMICZNE ZARZĄDZANIE UPRAWNIENIAMI

Wprowadź [Realizacja: możliwości dynamicznego zarządzania uprawnieniami zdefiniowane przez organizację].

Zabezpieczenia powiązane: AC-16.

(7) ZARZĄDZANIE KONTAMI | KONTA UŻYTKOWNIKÓW UPRZEWILEJOWANYCH

a. Twórz i administruj kontami użytkowników uprzywilejowanych zgodnie z [Wybór: schematem dostępu opartym na rolach; schematem dostępu opartym na atrybutach];

b. Monitoruj przydziały ról uprzywilejowanych lub atrybutów;

c. Monitoruj zmiany ról lub atrybutów;

d. Odwołuj dostęp, gdy przydziały ról uprzywilejowanych lub atrybutów nie są już odpowiednie.

Zabezpieczenia powiązane: nie dotyczy.

(8) ZARZĄDZANIE KONTAMI | DYNAMICZNE ZARZĄDZANIE KONTEM

Dynamicznie twórz, aktywuj, zarządzaj i dezaktywuj [Realizacja: konta systemowe zdefiniowane przez organizację].

Zabezpieczenia powiązane: AC-16.

(9) ZARZĄDZANIE KONTAMI | OGRANICZENIA DOTYCZĄCE KORZYSTANIA Z KONT WSPÓŁDZIELONYCH I GRUPOWYCH

Zezwalaj wyłącznie na korzystanie z kont współdzielonych i grupowych, które spełniają [Realizacja: warunki określone przez organizację dotyczące tworzenia kont współdzielonych i grupowych].

Zabezpieczenia powiązane: nie dotyczy.

(10) ZARZĄDZANIE KONTAMI | ZMIANA UWIERZYTELNIENIA KONT WSPÓŁDZIELONYCH I GRUPOWYCH

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(11) ZARZĄDZANIE KONTAMI | WARUNKI UŻYTKOWANIA

Wymuś [Realizacja: okoliczności i/lub warunki użytkowania zdefiniowane przez organizację] dla [Realizacja: konta systemowe zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(12) ZARZĄDZANIE KONTAMI | MONITOROWANIE KONTA POD KĄTEM NIETYPOWEGO UŻYTKOWANIA

a. Monitoruj konta systemowe pod kątem [Realizacja: nietypowego użycia zdefiniowanego przez organizację];

b. Zgłaszaj nietypowe użycie kont systemowych do [Realizacja: personelu lub ról zdefiniowanych przez organizację].

Zabezpieczenia powiązane: AU-6, AU-7, CA-7, IR-8, SI-4.

(13) ZARZĄDZANIE KONTAMI | WYŁĄCZANIE KONT DOSTĘPOWYCH UŻYTKOWNIKOM WYSOKIEGO RYZYKA

Wyłącz konta osób w [Realizacja: okres czasu określony przez organizację] od wykrycia [Realizacja: znaczące ryzyko określone przez organizację].

Zabezpieczenia powiązane: AU-6, SI-4.

AC-3 EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU

Zabezpieczenie:

Wymuszaj na użytkowniku stosowanie zatwierdzonych zasad uzyskiwania uprawnień logicznego dostępu do informacji i zasobów systemowych zgodnie z obowiązującymi w organizacji zasadami kontroli dostępu.

Zabezpieczenia powiązane: AC-2, AC-4, AC-5, AC-6, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AC-24, AC-25, AT-2, AT-3, AU-9, CA-9, CM-5, CM-11, IA-2, IA-5, IA-6, IA-7, IA-11, MA-3, MA-4, MA-5, MP-4, PM-2, PS-3, PT-2, PT-3, SA-17, SC-2, SC-3, SC-4, SC-12, SC-13, SC-28, SC-31, SC-34, SI-4, SI-8.

Zabezpieczenia rozszerzone:

(1) EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU | OGRANICZONY DOSTĘP DO FUNKCJI UPRZYWILEJOWANYCH

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(2) EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU | PODWÓJNA AUTORYZACJA

Dla działań uprzywilejowanych [Realizacja: uprzywilejowane polecenia zdefiniowane przez organizację i/lub inne działania zdefiniowane przez organizację] skonfiguruj system teleinformatyczny tak, aby wymuszał podwójną autoryzację.

Zabezpieczenia powiązane: CP-9 i MP-6.

(3) EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU | OBOWIĄZKOWA KONTROLA DOSTĘPU

Wymuszaj, zgodnie z [Realizacja: obowiązkowa polityka kontroli dostępu zdefiniowana przez organizację], w stosunku do wszystkich podmiotów i obiektów, ustaloną w organizacji politykę kontroli dostępu, która:

a. jest jednolicie egzekwowana wobec wszystkich podmiotów i obiektów w obszarze danego systemu;
b. określa, że podmiot, któremu udzielono dostępu do informacji, nie może wykonywać żadnej z następujących czynności:
    1. przekazywania informacji nieautoryzowanym podmiotom lub obiektom;
    2. udzielania przydzielonych przywilejów innym podmiotom;
    3. jakiejkolwiek zmiany atrybutów (właściwości) bezpieczeństwa podmiotów, obiektów systemu lub jego elementów;
    4. wyboru atrybutów bezpieczeństwa i wartości w odniesieniu do obiektów nowo tworzonych lub zmodyfikowanych;
    5. zmiany zasad zarządzania kontrolą dostępu;

c. stanowi, że dla jednoznacznie określonych w tej polityce podmiotów [Realizacja: podmioty zdefiniowane przez organizację] mogą zostać przyznane uprawnienia, które nie podlegają wybranym lub wszystkimi powyższym ograniczeniom [Realizacja: uprawnienia zdefiniowane przez organizację], tak aby podmioty te nie były obarczone niektórymi lub wszystkimi powyższymi ograniczeniami.

Zabezpieczenia powiązane: SC-7.

(4) EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU | UZNANIOWA KONTROLA DOSTĘPU

Dla ściśle zdefiniowanych sytuacji stosuj uznaniową politykę kontroli dostępu [Realizacja: zdefiniowana przez organizację uznaniowa polityka kontroli dostępu] według, której podmioty i obiekty, mogą wykonać co najmniej jedną z następujących czynności:

a. przekazywanie informacji innym podmiotom lub obiektom;

b. przyznawanie swoich przywilejów (atrybutów) innym obiektom;

c. zmienianie atrybutów bezpieczeństwa dotyczące podmiotów, obiektów, systemu lub jego elementów;

d. wskazywanie atrybutów bezpieczeństwa, które zostaną powiązane z nowo utworzonymi lub skorygowanymi obiektami;

e. zmienianie zasady dotyczącej kontroli dostępu.

Zabezpieczenia powiązane: nie dotyczy.

(5) EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU | INFORMACJE DOTYCZĄCE BEZPIECZEŃSTWA

Zapobiegaj dostępowi do [Realizacja: określonej przez organizację informacji istotnej dla bezpieczeństwa], za wyjątkiem sytuacji, gdy system znajduje się w stanie nieoperacyjnym.

Zabezpieczenia powiązane: CM-6, SC-39.

(6) EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU | OCHRONA INFORMACJI UŻYTKOWNIKA I SYSTEMU

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(7) EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU | KONTROLA DOSTĘPU DO ROLI (RBAC)

Wymuszaj zdefiniowaną przez organizację dla podmiotów i obiektów politykę kontroli dostępu opartą na rolach [Realizacja: role zdefiniowane przez organizację i użytkownicy upoważnieni do przyjmowania takich ról].

Zabezpieczenia powiązane: nie dotyczy.

(8) EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU | ODWOŁANIE ZEZWOLEŃ NA DOSTĘP

Wymuszaj według reguły zdefiniowanej przez organizację cofanie zezwoleń na dostęp w wyniku zmian atrybutów bezpieczeństwa podmiotów i obiektów, na podstawie [Realizacja: reguły zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(9) EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU | KONTROLOWANE UDOSTĘPNIENIE INFORMACJI

Udostępniaj informacje poza systemem tylko wtedy, gdy:

a. odbiorca informacji [Realizacja: system lub komponent zdefiniowany przez organizację] spełnia wymagania zdefiniowane przez organizację [Realizacja: środki kontroli zdefiniowane przez organizację];

b. [Realizacja: kontrole zdefiniowane przez organizację] służą do sprawdzania czy informacje przeznaczone do udostępnienia są właściwe.

Zabezpieczenia powiązane: CA-3, PT-7, PT-8, SA-9, SC-16.

(10) EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU | NADZOROWANE OBEJŚCIE MECHANIZMÓW KONTROLI DOSTĘPU

W warunkach [Realizacja: warunkach zdefiniowanych przez organizację] stosuj nadzorowane obejścia mechanizmów automatycznej kontroli dostępu.

Zabezpieczenia powiązane: AU-2, AU-6, AU-10, AU-12, AU-14.

(11) EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU | OGRANICZANIE DOSTĘPU DO OKREŚLONYCH TYPÓW INFORMACJI

Ogranicz dostęp do repozytoriów danych zawierających [Realizacja: typy informacji zdefiniowane przez organizację].

Zabezpieczenia powiązane: CM-8, CM-12, CM-13, PM-5.

(12) EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU | POTWIERDZANIE I EGZEKWOWANIE DOSTĘPU DO APLIKACJI

a. Wymagaj, aby aplikacje potwierdzały jako część procesu instalacji, dostęp niezbędny do następujących aplikacji i funkcji systemowych: [Realizacja: aplikacje i funkcje systemowe zdefiniowane przez organizację];

b. Zapewnij mechanizmom egzekwowania, w celu zapobiegania nieautoryzowanemu dostępowi;

c. Zatwierdzać zmiany dostępu po początkowej instalacji aplikacji.

Zabezpieczenia powiązane: CM-7.

(13) EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU | KONTROLA DOSTĘPU OPARTA NA ATRYBUTACH

Wdrażaj zasady kontroli dostępu oparte na atrybutach w odniesieniu do zdefiniowanych podmiotów i obiektów oraz kontroluj dostęp na podstawie [Realizacja: atrybuty zdefiniowane przez organizację w celu uzyskania uprawnień dostępu].

Zabezpieczenia powiązane: nie dotyczy.

(14) EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU | DOSTĘP INDYWIDUALNY

Zapewnij [Realizacja: mechanizmy zdefiniowane przez organizację] zapewniający dostęp do następujących elementów ich danych osobowych: [Realizacja: elementy zdefiniowane przez organizację].

Zabezpieczenia powiązane: IA-8, PM-22, PM-20, PM-21, PT-6.

(15) EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU | UZNANIOWA I OBOWIĄZKOWA KONTROLA DOSTĘPU

a. Wyegzekwuj [Realizacja: obowiązkowa polityka kontroli dostępu zdefiniowana przez organizację], w odniesieniu do zestawu objętych podmiotów i obiektów określonych w polityce;

b. Wyegzekwuj [Realizacja: uznaniowa polityka kontroli dostępu zdefiniowana przez organizację] w odniesieniu do zestawu objętych podmiotów i obiektów określonych w polityce.

Zabezpieczenia powiązane: SC-2, SC-3, AC-4.

AC-4 EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI

Zabezpieczenie: Wdrażanie zatwierdzonych uprawnień do kontrolowania przepływu informacji w systemie i między połączonymi systemami w oparciu o [Realizacja: zasady kontroli przepływu informacji zdefiniowane przez organizację].

Zabezpieczenia powiązane: AC-3, AC-6, AC-16, AC-17, AC-19, AC-21, AU-10, CA-3, CA-9, CM-7, PL-9, PM-24, SA- 17, SC-4, SC-7, SC-16, SC-31.

Zabezpieczenia rozszerzone:

(1) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | ATRYBUTY BEZPIECZEŃSTWA I PRYWATNOŚCI OBIEKTU

Użyj [Realizacja: atrybuty bezpieczeństwa i prywatności zdefiniowane przez organizację] powiązane z [Realizacja: obiekty informacji, źródła i miejsca docelowego zdefiniowane przez organizację] w celu wyegzekwowania [Realizacja: zasady kontroli przepływu informacji zdefiniowane przez organizację] jako podstawy decyzji dotyczących kontroli przepływu.

Zabezpieczenia powiązane: nie dotyczy.

(2) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | PRZETWARZANIE DOMEN

Użyj chronionych domen przetwarzania, aby wymusić [Realizacja: zasady kontroli przepływu informacji zdefiniowane przez organizację] jako podstawę decyzji dotyczących kontroli przepływu.

Zabezpieczenia powiązane: SC-39.

(3) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | DYNAMICZNA KONTROLA PRZEPŁYWU INFORMACJI

Wymuś [Realizacja: zasady kontroli przepływu informacji zdefiniowane przez organizację].

Zabezpieczenia powiązane: SI-4.

(4) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | SPRAWDZANIE ZAWARTOŚCI ZASZYFROWANEJ INFORMACJI

Zapobiegaj omijaniu zaszyfrowanych informacji przez [Realizacja: mechanizmy kontroli przepływu informacji zdefiniowane przez organizację] poprzez [Wybór (jeden lub więcej): odszyfrowanie informacji; zablokowanie przepływu zaszyfrowanych informacji; zakończenie sesji komunikacyjnych próbujących przesłać zaszyfrowane informacje; [Realizacja: procedura lub metoda zdefiniowana przez organizację]].

Zabezpieczenia powiązane: SI-4.

(5) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | WBUDOWANE RODZAJE DANYCH

Wymuś [Realizacja: ograniczenia zdefiniowane przez organizację] podczas osadzania typów danych w innych typach danych.

Zabezpieczenia powiązane: nie dotyczy.

(6) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | METADANE

Wymuś kontrolę przepływu informacji na podstawie [Realizacja: metadane zdefiniowane przez organizację].

Zabezpieczenia powiązane: AC-16, SI-7.

(7) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | MECHANIZMY PRZEPŁYWU JEDNOSTRONNEGO

Wymuszaj jednokierunkowy przepływ informacji poprzez mechanizmy kontroli przepływu oparte na sprzęcie.

Zabezpieczenia powiązane: nie dotyczy.

(8) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | FILTRY POLITYKI BEZPIECZEŃSTWA I PRYWATNOŚCI

a. Wyegzekwuj kontrolę przepływu informacji przy użyciu [Realizacja: zdefiniowanych przez organizację filtrów zasad bezpieczeństwa lub prywatności] jako podstawy decyzji dotyczących kontroli przepływu dla [Realizacja: zdefiniowanych przez organizację przepływów informacji];

b. [Wybór (jednego lub więcej): Blokowanie; Usuwanie; Modyfikowanie; Kwarantanna] danych po niepowodzeniu przetwarzania filtra zgodnie z [Realizacja: zdefiniowaną przez organizację polityką bezpieczeństwa lub prywatności].

Zabezpieczenia powiązane: nie dotyczy.

(9) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | OCENA PRZEZ UPRAWNIONĄ OSOBĘ

Zastosuj obowiązkowe oceny dokonywane przez ludzi dla [Realizacja: przepływy informacji zdefiniowane przez organizację] pod następującymi warunkami: [Realizacja: warunki zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(10) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | WŁĄCZANIE/ WYŁĄCZANIE FILTRÓW POLITYKI BEZPIECZEŃSTWA LUB PRYWATNOŚCI

Udostępnij administratorom z uprawnieniami możliwość włączania i wyłączania [Realizacja: zdefiniowane przez organizację filtry zasad bezpieczeństwa lub prywatności] pod następującymi warunkami: [Realizacja: warunki zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(11) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | KONFIGURACJA FILTRÓW POLITYKI BEZPIECZEŃSTWA LUB PRYWATNOŚCI

Udostępnij administratorom z uprawnieniami możliwość konfigurowania [Realizacja: filtrów zasad bezpieczeństwa lub prywatności zdefiniowanych w organizacji] w celu obsługi różnych zasad bezpieczeństwa lub prywatności.

Zabezpieczenia powiązane: nie dotyczy.

(12) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | IDENTYFIKATORY TYPU DANYCH

Podczas przesyłania informacji pomiędzy różnymi domenami zabezpieczeń używaj [Realizacja: identyfikatorów typów danych zdefiniowanych przez organizację] w celu walidacji danych niezbędnych do podejmowania decyzji dotyczących przepływu informacji.

Zabezpieczenia powiązane: nie dotyczy.

(13) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | DEKOMPOZYCJA INFORMACJI NA ODPOWIEDNIE PODSKŁADNIKI

Podczas przesyłania informacji pomiędzy różnymi domenami zabezpieczeń podziel je na [Realizacja: zdefiniowane przez organizację podkomponenty istotne z punktu widzenia zasad] w celu przesłania ich do mechanizmów egzekwowania zasad.

Zabezpieczenia powiązane: nie dotyczy.

(14) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | POLITYKA STOSOWANIA FILTRÓW BEZPIECZEŃSTWA LUB PRYWATNOŚCI

Podczas przesyłania informacji pomiędzy różnymi domenami zabezpieczeń wdrażaj [Realizacja: filtry zasad bezpieczeństwa lub prywatności zdefiniowane przez organizację] wymagające w pełni wyliczonych formatów, które ograniczają strukturę i zawartość danych.

Zabezpieczenia powiązane: nie dotyczy.

(15) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | WYKRYWANIE INFORMACJI NIEAKCEPTOWANYCH

Podczas przesyłania informacji pomiędzy różnymi domenami zabezpieczeń sprawdzaj, czy informacje te nie zawierają [Realizacja: niezatwierdzonych informacji zdefiniowanych przez organizację] i

zabraniają przesyłania takich informacji zgodnie z [Realizacja: polityką bezpieczeństwa lub prywatności zdefiniowaną przez organizację].

Zabezpieczenia powiązane: SI-3.

(16) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | PRZEKAZYWANIE INFORMACJI POMIĘDZY SYSTEMAMI TELEINFORMATYCZNYMI

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(17) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | UWIERZYTELNIANIE DOMEN

Stosuj unikalną identyfikację i uwierzytelnianie punktów źródłowych i docelowych według [wyboru (jednego lub więcej): organizacji; systemu; aplikacji; usługi; osoby] w celu przesyłania informacji.

Zabezpieczenia powiązane: IA-2, IA-3, IA-9.

(18) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | WIĄZANIE ATRYBUTU BEZPIECZEŃSTWA

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(19) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | WALIDACJA METADANYCH

Podczas przesyłania informacji pomiędzy różnymi domenami zabezpieczeń wdrażaj [Realizacja: filtry zasad bezpieczeństwa lub prywatności zdefiniowane przez organizację] w metadanych.

Zabezpieczenia powiązane: nie dotyczy.

(20) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | ZATWIERDZONE ROZWIĄZANIA BEZPIECZEŃSTWA

Wdrażaj [Realizacja: rozwiązania zdefiniowane przez organizację w zatwierdzonych konfiguracjach] w celu kontrolowania przepływu [Realizacja: informacje zdefiniowane przez organizację] pomiędzy domenami zabezpieczeń.

Zabezpieczenia powiązane: nie dotyczy.

(21) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | FIZYCZNA LUB LOGICZNA SEPARACJA PRZEPŁYWÓW INFORMACJI

Oddziel przepływy informacji logicznie lub fizycznie, wykorzystując [Realizacja: mechanizmy i/lub techniki zdefiniowane przez organizację] w celu osiągnięcia [Realizacja: wymagane rozdzielenia zdefiniowane przez organizację według typów informacji].

Zabezpieczenia powiązane: nie dotyczy.

(22) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI |TYLKO DOSTĘP

Umożliwiaj dostęp z jednego urządzenia do platform obliczeniowych, aplikacji lub danych znajdujących się w wielu różnych domenach bezpieczeństwa, zapobiegając jednocześnie przepływowi informacji pomiędzy różnymi domenami bezpieczeństwa.

Zabezpieczenia powiązane: nie dotyczy.

(23) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | MODYFIKOWANIE NIEUDOSTĘPNIONYCH INFORMACJI

Podczas przesyłania informacji pomiędzy różnymi domenami zabezpieczeń modyfikuj informacje niepodlegające udostępnieniu, wdrażając [Realizacja: działanie modyfikujące zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(24) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | WEWNĘTRZNY ZNORMALIZOWANY FORMAT

Podczas przesyłania informacji pomiędzy różnymi domenami zabezpieczeń analizuj przychodzące dane, konwertuj je na wewnętrznie znormalizowany format i ponownie generuj, aby były zgodne z zamierzoną specyfikacją.

Zabezpieczenia powiązane: nie dotyczy.

(25) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | OCZYSZCZANIE DANYCH

Podczas przesyłania informacji pomiędzy różnymi domenami zabezpieczeń przeprowadzaj czyszczenie danych w celu zminimalizowania [Wybór (jeden lub więcej): dostarczania złośliwej zawartości, dowodzenia i kontroli nad złośliwym kodem, rozszerzania złośliwego kodu i zakodowanych danych steganograficznych; wycieku poufnych informacji] zgodnie z [Realizacja: polityka zdefiniowana przez organizację]].

Zabezpieczenia powiązane: MP-6.

(26) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | AUDYT CZYNNOŚCI FILTROWANIA

Podczas przesyłania informacji pomiędzy różnymi domenami zabezpieczeń rejestruj i weryfikuj działania filtrowania treści oraz wyniki filtrowania informacji.

Zabezpieczenia powiązane: AU-2, AU-3, AU-12.

(27) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | REDUNDANTNE/NIEZALEŻNE MECHANIZMY FILTROWANIA

Podczas przesyłania informacji pomiędzy różnymi domenami zabezpieczeń wdrażaj rozwiązania filtrowania treści zapewniające redundantne i niezależne mechanizmy filtrowania dla każdego typu danych.

Zabezpieczenia powiązane: nie dotyczy.

(28) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | LINIOWE KANAŁY FILTROWANIA

Podczas przesyłania informacji pomiędzy różnymi domenami zabezpieczeń wdrażaj liniowy proces filtrowania treści, który będzie egzekwowany za pomocą uznaniowych i obowiązkowych kontroli dostępu.

Zabezpieczenia powiązane: nie dotyczy.

(29) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | SILNIKI ORKIESTRACJI FILTRÓW

Podczas przesyłania informacji pomiędzy różnymi domenami zabezpieczeń stosuj mechanizmy koordynacji filtrów treści, aby mieć pewność, że:

a. mechanizmy filtrowania treści pomyślnie ukończą działanie bez błędów;

b. działania filtrowania treści będą wykonywane we właściwej kolejności i będą zgodne z [Realizacja: polityka zdefiniowana przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(30) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | MECHANIZMY FILTROWANIA WYKORZYSTUJĄCE WIELE PROCESÓW

Podczas przesyłania informacji pomiędzy różnymi domenami zabezpieczeń wdrażaj mechanizmy filtrowania treści wykorzystujące wiele procesów.

Zabezpieczenia powiązane: nie dotyczy.

(31) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | ZAPOBIEGANIE NIEUDANEMU TRANSFEROWI TREŚCI

Podczas przesyłania informacji pomiędzy różnymi domenami zabezpieczeń zapobiegaj przesyłaniu wadliwej zawartości do domeny odbiorczej.

Zabezpieczenia powiązane: nie dotyczy.

(32) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI | WYMAGANIA PROCESOWE DOTYCZĄCE TRANSFERU INFORMACJI

Podczas przesyłania informacji pomiędzy różnymi domenami zabezpieczeń proces przesyłania informacji pomiędzy kanałami filtrowania:

a. nie filtruje zawartości wiadomości;

b. sprawdza poprawność metadanych filtrowania;

c. upewnia się, że zawartość skojarzona z metadanymi filtrowania została pomyślnie przefiltrowana;

d. przesyła zawartość do docelowego kanału filtrowania.

Zabezpieczenia powiązane: nie dotyczy.

AC-5 ROZDZIAŁ OBOWIĄZKÓW

Zabezpieczenie:

a. Zidentyfikuj i udokumentuj [Realizacja: obowiązki zdefiniowane przez organizację dla osób wymagających separacji];

b. Zdefiniuj uprawnienia dostępu do systemu w celu wsparcia separacji obowiązków.

Zabezpieczenia powiązane: AC-2, AC-3, AC-6, AU-9, CM-5, CM-11, CP-9, IA-2, IA-4, IA-5, IA-12, MA-3, MA- 5, PS-2, SA-8, SA-17.

AC-6 ZASADA WIEDZY KONIECZNEJ

Zabezpieczenie:

Stosuj zasadę wiedzy koniecznej, zezwalając użytkownikom (lub procesom działającym w imieniu użytkowników) wyłącznie na autoryzowany dostęp niezbędny do wykonania przypisanych zadań organizacyjnych.

Zabezpieczenia powiązane: AC-2, AC-3, AC-5, AC-16, CM-5, CM-11, PL-2, PM-12, SA-8, SA-15, SA-17, SC-38.

Zabezpieczenia rozszerzone:

(1) ZASADA WIEDZY KONIECZNEJ | UPOWAŻNIONY DOSTĘP DO FUNKCJI BEZPIECZEŃSTWA

Autoryzuj dostęp dla [Realizacja: osoby lub role zdefiniowane przez organizację] do: (a) [Realizacja: funkcje bezpieczeństwa zdefiniowane przez organizację (wdrożone w sprzęcie, oprogramowaniu i oprogramowaniu sprzętowym)]; i (b) [Realizacja: informacje istotne dla bezpieczeństwa zdefiniowane przez organizację].

Zabezpieczenia powiązane: AC-17, AC-18, AC-19, AU-9, PE-2.

(2) ZASADA WIEDZY KONIECZNEJ | NIEUPRZYWILEJOWANY DOSTĘP DO FUNKCJI NIEZWIĄZANYCH Z BEZPIECZEŃSTWEM

Wymagaj, aby użytkownicy kont systemowych (lub ról) z dostępem do [Realizacja: funkcje zabezpieczeń zdefiniowane przez organizację lub informacje istotne z punktu widzenia zabezpieczeń] korzystali z kont lub ról nieuprzywilejowanych podczas uzyskiwania dostępu do funkcji niezwiązanych z zabezpieczeniami.

Zabezpieczenia powiązane: AC-17, AC-18, AC-19, PL-4.

(3) ZASADA WIEDZY KONIECZNEJ | DOSTĘP SIECIOWY DO UPRZYWILEJOWANYCH POLECEŃ

Udzielaj autoryzacji dostępu do sieci wyłącznie do [Realizacja: polecenia uprzywilejowane zdefiniowane przez organizację] w przypadku [Realizacja: ważne potrzeby operacyjne zdefiniowane przez organizację] i udokumentuj uzasadnienie takiego dostępu w planie bezpieczeństwa systemu.

Zabezpieczenia powiązane: AC-17, AC-18, AC-19.

(4) ZASADA WIEDZY KONIECZNEJ | ODDZIELNE DOMENY PRZETWARZANIA

Zapewnij oddzielne domeny przetwarzania, aby umożliwić bardziej szczegółowy przydział uprawnień użytkowników.

Zabezpieczenia powiązane: AC-4, SC-2, SC-3, SC-30, SC-32, SC-39.

(5) ZASADA WIEDZY KONIECZNEJ | UPRZYWILEJOWANE KONTA

Ogranicz konta uprzywilejowane w systemie do [Realizacja: personel lub role zdefiniowane przez organizację].

Zabezpieczenia powiązane: IA-2, MA-3, MA-4.

(6) ZASADA WIEDZY KONIECZNEJ | OGRANICZONY DOSTĘP PRZEZ UŻYTKOWNIKÓW SPOZA ORGANIZACJI

Zabroń uprzywilejowanego dostępu do systemu użytkownikom spoza organizacji.

Zabezpieczenia powiązane: AC-18, AC-19, IA-2, IA-8.

(7) ZASADA WIEDZY KONIECZNEJ | PRZEGLĄD UPRAWNIEŃ UŻYTKOWNIKA

a. Przejrzyj [Realizacja: częstotliwość zdefiniowana przez organizację] uprawnienia przypisane do [Realizacja: role lub klasy użytkowników zdefiniowane przez organizację], aby sprawdzić potrzebę przyznania takich uprawnień;

b. W razie potrzeby ponownie przypisz lub usuń uprawnienia, aby prawidłowo odzwierciedlały misję organizacji i potrzeby biznesowe.

Zabezpieczenia powiązane: CA-7.

(8) ZASADA WIEDZY KONIECZNEJ | POZIOMY UPRAWNIEŃ DO URUCHAMIANIA KODU

Zabezpiecz następujące oprogramowanie przed uruchamianiem z wyższymi poziomami uprawnień niż użytkownicy uruchamiający to oprogramowanie: [Realizacja: oprogramowanie zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(9) ZASADA WIEDZY KONIECZNEJ | REJESTROWANIE UŻYCIA FUNKCJI UPRZEWILEJOWANYCH

Rejestruj wykonywanie funkcji uprzywilejowanych.

Zabezpieczenia powiązane: AU-2, AU-3, AU-12.

(10) ZASADA WIEDZY KONIECZNEJ | ODMOWA WYKONYWANIA PRZEZ NIEUPRZYWILEJOWANYCH UŻYTKOWNIKÓW UPRZYWILEJOWANYCH FUNKCJI

Zapobiegaj wykonywaniu funkcji uprzywilejowanych przez użytkowników nieposiadających uprawnień.

Zabezpieczenia powiązane: nie dotyczy.

AC-7 NIEUDANE PRÓBY LOGOWANIA

Zabezpieczenie:

a. Wymuś limit [Realizacja: zdefiniowana przez organizację liczba] kolejnych nieudanych prób logowania przez użytkownika w [Realizacja: zdefiniowany przez organizację okres czasu];

b. Automatycznie [Wybór (jeden lub więcej): zablokuj konto lub węzeł na [Realizacja: zdefiniowany przez organizację okres czasu]; zablokuj konto lub węzeł do czasu zwolnienia przez administratora; opóźnij następny monit logowania zgodnie z [Realizacja: zdefiniowany przez organizację algorytm opóźnienia]; powiadom administratora systemu; podejmij inne [Realizacja: zdefiniowane przez organizację działanie]], gdy zostanie przekroczona maksymalna liczba nieudanych prób.

Zabezpieczenia powiązane: AC-2, AC-9, AU-2, AU-6, IA-5.

Zabezpieczenia rozszerzone:

(1) NIEUDANE PRÓBY LOGOWANIA | AUTOMATYCZNA BLOKADA KONTA

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(2) NIEUDANE PRÓBY LOGOWANIA | USUWANIE INFORMACJI Z URZĄDZEŃ PRZENOŚNYCH

Usuń lub wyczyść informacje z [Realizacja: urządzeń mobilnych zdefiniowanych przez organizację] na podstawie [Realizacja: wymagań i technik usuwania lub wymazywania zdefiniowanych przez organizację] po [Realizacja: liczba zdefiniowana przez organizację] kolejnych nieudanych prób zalogowania do urządzenia.

Zabezpieczenia powiązane: Wersja AC-19, MP-5, MP-6.

(3) NIEUDANE PRÓBY LOGOWANIA | OGRANICZANIE PRÓB BIOMETRYCZNYCH

Ogranicz liczbę nieudanych prób logowania biometrycznego do [Przypisanie: liczba zdefiniowana przez organizację].

Zabezpieczenia powiązane: IA-3

(4) NIEUDANE PRÓBY LOGOWANIA | UŻYCIE ALTERNATYWNEGO CZYNNIKA UWIERZYTELNIANIA

a. Zezwalaj na używanie [Realizacja: zdefiniowane przez organizację czynniki uwierzytelniania], które różnią się od głównych czynników uwierzytelniania po przekroczeniu określonej przez organizację liczby kolejnych nieudanych prób logowania;

b. Wymuszaj limit [Realizacja: zdefiniowana przez organizację liczba] kolejnych nieudanych prób logowania poprzez używanie alternatywnych czynników przez użytkownika w ciągu [Realizacja: zdefiniowany przez organizację okres czasu].

Zabezpieczenia powiązane: IA-3

AC-8 POWIADOMIENIE O ZASADACH UŻYCIA SYSTEMU

Zabezpieczenie:

a. Wyświetl [Realizacja: komunikat powiadomienia o korzystaniu z systemu zdefiniowanego przez organizację lub baner] użytkownikom przed udzieleniem dostępu do systemu, który zapewnia powiadomienia o prywatności i bezpieczeństwie zgodne z obowiązującymi przepisami prawa, rozporządzeniami wykonawczymi, dyrektywami, regulacjami, zasadami, standardami i wytycznymi, i oświadcz, że:

    1. Użytkownicy uzyskują dostęp do systemu organizacji;

    2. Korzystanie z systemu może być monitorowane, rejestrowane i podlegać audytowi;

    3. Nieautoryzowane korzystanie z systemu jest zabronione i podlega karom karnym i cywilnym;

    4. Korzystanie z systemu oznacza zgodę na monitorowanie i rejestrowanie;

b. Zachowaj komunikat powiadomienia lub baner na ekranie, dopóki użytkownicy nie potwierdzą warunków korzystania i nie podejmą wyraźnych działań w celu zalogowania się do systemu lub uzyskania do niego dalszego dostępu;

c. W przypadku systemów publicznie dostępnych:

    1. Wyświetl informacje o korzystaniu z systemu [Realizacja: warunki zdefiniowane przez organizację] przed udzieleniem dalszego dostępu do systemu publicznie dostępnego;

    2. Wyświetl odniesienia, jeśli takie istnieją, do monitorowania, rejestrowania lub audytu, które są zgodne z udogodnieniami prywatności dla takich systemów, które generalnie zabraniają takich działań;

    3. Dołącz opis autoryzowanych zastosowań systemu.

Zabezpieczenia powiązane: AC-14, PL-4, SI-4.

Zabezpieczenia rozszerzone: nie dotyczy.

AC-9 POWIADOMIENIE O ZALOGOWANIU

Zabezpieczenie:

Powiadom użytkownika po pomyślnym zalogowaniu się do systemu o dacie i godzinie ostatniego logowania.

Zabezpieczenia powiązane: AC-7, PL-4.

Zabezpieczenia rozszerzone:

(1) POPRZEDNIE POWIADOMIENIE O LOGOWANIU | NIEUDANE LOGOWANIA

Powiadom użytkownika po pomyślnym zalogowaniu o liczbie nieudanych prób logowania od ostatniego pomyślnego logowania.

Zabezpieczenia powiązane: nie dotyczy.

(2) POPRZEDNIE POWIADOMIENIE O LOGOWANIU | POMYŚLNE I NIEUDANE LOGOWANIA

Powiadom użytkownika po pomyślnym zalogowaniu o liczbie [Wybór: udanych logowań; nieudanych prób logowania; obu] w ciągu [Realizacja: okres czasu zdefiniowany przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(3) POPRZEDNIE POWIADOMIENIE O LOGOWANIU | POWIADOMIENIE O ZMIANACH NA KONCIE

Powiadom użytkownika po pomyślnym zalogowaniu o zmianach w [Realizacja: zdefiniowane przez organizację cechy lub parametry związane z bezpieczeństwem konta użytkownika] w [Realizacja: okres czasu zdefiniowany przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(4) POPRZEDNIE POWIADOMIENIE O LOGOWANIU | DODATKOWE INFORMACJE O LOGOWANIU

Powiadom użytkownika po pomyślnym zalogowaniu, podając następujące dodatkowe informacje: [Realizacja: dodatkowe informacje zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

AC-10 KONTROLA ILOŚCI RÓWNOCZESNYCH SESJI

Ogranicz liczbę równoczesnych sesji dla każdego [Realizacja: konto zdefiniowane przez organizację i/lub typ konta] do [Realizacja: liczba zdefiniowana przez organizację].

Zabezpieczenia powiązane: SC-23.

AC-11 BLOKADA URZĄDZENIA

Zabezpieczenie:

a. Zapobiegaj dalszemu dostępowi do systemu poprzez [Wybór (jeden lub więcej): zainicjowanie blokady urządzenia po [Realizacja: okres czasu zdefiniowany przez organizację] bezczynności; wymaganie od użytkownika zainicjowania blokady urządzenia przed pozostawieniem systemu bez nadzoru];

b. Utrzymuj blokadę urządzenia do momentu, aż użytkownik ponownie nawiąże dostęp, korzystając z ustalonych procedur identyfikacji i uwierzytelniania.

Zabezpieczenia powiązane: AC-2, AC-7, IA-11, PL-4.

Zabezpieczenia rozszerzone:

(1) BLOKADA URZĄDZENIA | WYGASZACZ EKRANU

Ukryj informacje wcześniej widoczne na wyświetlaczu za pomocą obrazu dostępnego publicznie, blokując urządzenie.

Zabezpieczenia powiązane: nie dotyczy.

AC-12 ZAKOŃCZENIE SESJI

Zabezpieczenie:

Automatyczne zakończenie sesji użytkownika po [Realizacja: warunki zdefiniowane przez organizację lub zdarzenia wyzwalające wymagające rozłączenia sesji].

Zabezpieczenia powiązane: MA-4, SC-10, SC-23.

Zabezpieczenia rozszerzone:

(1) ZAKOŃCZENIE SESJI | WYLOGOWANIA INICJOWANE PRZEZ UŻYTKOWNIKA

Udostępnij możliwość wylogowania inicjowanego przez użytkownika z sesji komunikacyjnych, gdy do uzyskania dostępu do [Realizacja: zasoby informacji zdefiniowane przez organizację] używane jest uwierzytelnianie.

Zabezpieczenia powiązane: nie dotyczy.

(2) ZAKOŃCZENIE SESJI | WIADOMOŚĆ O ZAKOŃCZENIU

Wyświetl użytkownikom wyraźny komunikat o wylogowaniu informujący o zakończeniu uwierzytelnionych sesji komunikacyjnych.

Zabezpieczenia powiązane: nie dotyczy.

(3) ZAKOŃCZENIE SESJI | KOMUNIKAT OSTRZEGAWCZY O PRZEKROCZENIU LIMITU CZASU

Wyświetl użytkownikom wyraźną wiadomość wskazującą, że sesja zakończy się za [Realizacja: czas określony przez organizację do końca sesji].

Zabezpieczenia powiązane: nie dotyczy.

AC-13 NADZÓR I PRZEGLĄD-KONTROLA DOSTĘPU

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

AC-14 DZIAŁANIA DOZWOLONE BEZ IDENTYFIKACJI LUB UWIERZYTELNIANIA

Zabezpieczenie:

a) Zidentyfikuj [Realizacja: działania użytkownika zdefiniowane przez organizację], które można wykonać w systemie bez identyfikacji lub uwierzytelniania, zgodnie z misją organizacji i funkcjami biznesowymi;

b) Udokumentuj i podaj uzasadnienie w planie bezpieczeństwa systemu, działania użytkownika nie wymagające identyfikacji lub uwierzytelniania.

Zabezpieczenia powiązane: AC-8, IA-2, PL-2.

Zabezpieczenia rozszerzone: nie dotyczy.

(1) DZIAŁANIA DOZWOLONE BEZ IDENTYFIKACJI LUB UWIERZYTELNIANIA | NIEZBĘDNE ZASTOSOWANIA

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

AC-15 ZAUTOMATYZOWANE ZNAKOWANIE

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

AC-16 ATRYBUTY BEZPIECZEŃSTWA I PRYWATNOŚCI

Zabezpieczenie:

a. Zapewnij mechanizmy umożliwiające powiązanie [Realizacja: zdefiniowane przez organizację typy atrybutów bezpieczeństwa i prywatności] z [Realizacja: zdefiniowane przez organizację wartości atrybutów bezpieczeństwa i prywatności] dla informacji w pamięci masowej, w procesie i/lub w transmisji;

b. Upewnij się, że skojarzenia atrybutów są tworzone i zachowywane z informacjami;

c. Ustal następujące dozwolone atrybuty bezpieczeństwa i prywatności z atrybutów zdefiniowanych w AC-16a dla [Realizacja: zdefiniowane przez organizację systemy]: [Realizacja: zdefiniowane przez organizację atrybuty bezpieczeństwa i prywatności];

d. Określ następujące dozwolone wartości atrybutów lub zakresy dla każdego z ustalonych atrybutów: [Realizacja: zdefiniowane przez organizację wartości atrybutów lub zakresy dla ustalonych atrybutów];

e. Przeprowadź audyt zmian atrybutów;

f. Przejrzyj [Realizacja: zdefiniowane przez organizację atrybuty bezpieczeństwa i prywatności] pod kątem stosowalności [Realizacja: zdefiniowana przez organizację częstotliwość].

Zabezpieczenia powiązane: AC-3, AC-4, AC-6, AC-21, AC-25, AU-2, AU-10, MP-3, PE-22, PT-2, PT-3, PT-4, SC- 11, SC-16, SI-12, SI-18.

Zabezpieczenia rozszerzone:

(1) ATRYBUTY BEZPIECZEŃSTWA I PRYWATNOŚCI | DYNAMICZNE SKOJARZENIE ATRYBUTÓW

Dynamicznie powiąż atrybuty bezpieczeństwa i prywatności z [Realizacja: podmiotami i obiektami zdefiniowanymi przez organizację] zgodnie z następującymi zasadami bezpieczeństwa i prywatności w miarę tworzenia i łączenia informacji: [Realizacja: zasady bezpieczeństwa i prywatności zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(2) ATRYBUTY BEZPIECZEŃSTWA I PRYWATNOŚCI | ZMIANY WARTOŚCI ATRYBUTÓW PRZEZ OSOBY UPOWAŻNIONE

Umożliwiaj upoważnionym osobom (lub procesom działającym w imieniu osób) definiowanie lub zmianę wartości powiązanych atrybutów bezpieczeństwa i prywatności.

Zabezpieczenia powiązane: nie dotyczy.

(3) ATRYBUTY BEZPIECZEŃSTWA I PRYWATNOŚCI | UTRZYMANIE SKOJARZEŃ ATRYBUTÓW PRZEZ SYSTEM

Utrzymuj skojarzenie i integralność [Realizacja: atrybuty bezpieczeństwa i prywatności zdefiniowane przez organizację] z [Realizacja: podmiotami i obiektami zdefiniowanymi przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(4) ATRYBUTY BEZPIECZEŃSTWA I PRYWATNOŚCI | KOJARZENIE ATRYBUTÓW PRZEZ AUTORYZOWANY PERSONEL

Umożliwiaj powiązanie [Realizacja: atrybutów bezpieczeństwa i prywatności zdefiniowanych przez organizację] z [Realizacja: podmiotami i obiektami zdefiniowanymi przez organizację] przez upoważnione osoby (lub procesy działające w imieniu osób).

Zabezpieczenia powiązane: nie dotyczy.

(5) ATRYBUTY BEZPIECZEŃSTWA I PRYWATNOŚCI | WYŚWIETLANIE ATRYBUTÓW NA URZĄDZENIACH KOŃCOWYCH

Wyświetlaj atrybuty bezpieczeństwa i prywatności w formie czytelnej dla pracownika na każdym obiekcie, który system przesyła do urządzeń wyjściowych, aby zidentyfikować [Realizacja: specjalne instrukcje dotyczące rozpowszechniania, obsługi lub dystrybucji zdefiniowane przez organizację] przy użyciu [Realizacja: standardowe, czytelne dla pracownika, zdefiniowane przez organizację konwencje nazewnictwa].

Zabezpieczenia powiązane: nie dotyczy.

(6) ATRYBUTY BEZPIECZEŃSTWA I PRYWATNOŚCI | UTRZYMANIE SKOJARZENIA ATRYBUTÓW

Wymagaj od personelu powiązania i utrzymania powiązania [Realizacja: atrybuty bezpieczeństwa i prywatności zdefiniowane przez organizację] z [Realizacja: podmioty i obiekty zdefiniowane przez organizację] zgodnie z [Realizacja: zasady bezpieczeństwa i prywatności zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(7) ATRYBUTY BEZPIECZEŃSTWA I PRYWATNOŚCI | SPÓJNA INTERPRETACJA ATRYBUTÓW

Zapewnij spójną interpretację atrybutów bezpieczeństwa i prywatności przesyłanych pomiędzy rozproszonymi komponentami systemu.

Zabezpieczenia powiązane: nie dotyczy.

(8) ATRYBUTY BEZPIECZEŃSTWA I PRYWATNOŚCI | SKOJARZENIE TECHNIKI I TECHNOLOGIE

Wdrażaj [Realizacja: techniki i technologie zdefiniowane przez organizację] w celu powiązania atrybutów bezpieczeństwa i prywatności z informacjami.

Zabezpieczenia powiązane: SC-12, SC-13.

(9) ATRYBUTY BEZPIECZEŃSTWA I PRYWATNOŚCI | PONOWNE PRZYPISYWANIE ATRYBUTÓW — MECHANIZMY PONOWNEJ OCENY

Zapewnij, aby zmiana atrybutów bezpieczeństwa i prywatności powiązanych z informacjami możliwa była wyłącznie za pośrednictwem mechanizmów ponownej oceny zweryfikowanych przy użyciu [Realizacja: techniki lub procedury zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(10) ATRYBUTY BEZPIECZEŃSTWA I PRYWATNOŚCI | KONFIGURACJA ATRYBUTÓW PRZEZ OSOBY UPOWAŻNIONE

Umożliwiaj upoważnionym osobom definiowanie lub zmienianie typu i wartości atrybutów bezpieczeństwa i prywatności dostępnych w powiązaniu z podmiotami i obiektami.

Zabezpieczenia powiązane: nie dotyczy.

AC-17 ZDALNY DOSTĘP

Zabezpieczenie:

a. Ustanawiaj i udokumentuj ograniczenia użytkowania, wymagania dotyczące konfiguracji/połączenia i wskazówki dotyczące wdrażania dla każdego typu dozwolonego zdalnego dostępu;

b. Autoryzuj każdy typ zdalnego dostępu do systemu przed zezwoleniem na takie połączenia.

Zabezpieczenia powiązane: AC-2, AC-3, AC-4, AC-18, AC-19, AC-20, CA-3, CM-10, IA-2, IA-3, IA-8, MA-4, PE- 17, PL-2, PL-4, SC-10, SC-12, SC-13, SI-4.

Zabezpieczenia rozszerzone:

(1) ZDALNY DOSTĘP | MONITOROWANIE I KONTROLA

Wdrażaj zautomatyzowane mechanizmy monitorowania i kontrolowania metod dostępu zdalnego.

Zabezpieczenia powiązane: AU-2, AU-6, AU-12, AU-14.

(2) ZDALNY DOSTĘP | OCHRONA POUFNOŚCI I INTEGRALNOŚCI ZA POMOCĄ SZYFROWANIA

Wprowadź mechanizmy kryptograficzne w celu ochrony poufności i integralności sesji dostępu zdalnego.

Zabezpieczenia powiązane: SC-8, SC-12, SC-13.

(3) ZDALNY DOSTĘP | ZARZĄDZANE PUNKTY KONTROLI DOSTĘPU

Skieruj zdalny dostęp przez autoryzowane i zarządzane punkty kontroli dostępu do sieci.

Zabezpieczenia powiązane: SC-7.

(4) ZDALNY DOSTĘP | POLECENIA I DOSTĘP UPRZYWILEJOWANY

a. Autoryzuj wykonywanie poleceń uprzywilejowanych i dostęp do informacji istotnych z punktu widzenia bezpieczeństwa wyłącznie za pośrednictwem dostępu zdalnego w formacie

zapewniającym możliwe do oceny dowody oraz w celu zaspokojenia następujących potrzeb: [Realizacja: potrzeby określone przez organizację];

b. Udokumentuj uzasadnienie dostępu zdalnego w planie bezpieczeństwa systemu.

Zabezpieczenia powiązane: AC-6, SC-12, SC-13.

(5) ZDALNY DOSTĘP | MONITOROWANIE NIEAUTORYZOWANYCH POŁĄCZEŃ

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(6) ZDALNY DOSTĘP | OCHRONA MECHANIZMÓW ZDALNEGO DOSTĘPU

Chroń informacje o mechanizmach zdalnego dostępu przed nieautoryzowanym użyciem i ujawnieniem.

Zabezpieczenia powiązane: AT-2, AT-3, PS-6.

(7) ZDALNY DOSTĘP | DODATKOWA OCHRONA DOSTĘPU DO FUNKCJI BEZPIECZEŃSTWA

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(8) ZDALNY DOSTĘP | WYŁĄCZ NIEBEZPIECZNE PROTOKOŁY SIECIOWE

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(9) ZDALNY DOSTĘP | ROZŁĄCZ LUB WYŁĄCZ DOSTĘP

Zapewnij możliwość rozłączenia lub wyłączenia zdalnego dostępu do systemu w [Realizacja: okres czasu zdefiniowany przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(10) ZDALNY DOSTĘP | UWIERZYTELNIANIE POLECEŃ ZDALNYCH

Wdrażaj [Realizacja: mechanizmy zdefiniowane przez organizację] w celu uwierzytelniania [Realizacja: polecenia zdalne zdefiniowane przez organizację].

Zabezpieczenia powiązane: SC-12, SC-13, SC-23.

AC-18 DOSTĘP BEZPRZEWODOWY

Zabezpieczenie:

a. Ustal wymagania konfiguracyjne, wymagania dotyczące połączeń i wskazówki dotyczące wdrażania dla każdego typu dostępu bezprzewodowego;

b. Autoryzuj każdy typ dostępu bezprzewodowego do systemu przed zezwoleniem na takie połączenia.

Zabezpieczenia powiązane: AC-2, AC-3, AC-17, AC-19, CA-9, CM-7, IA-2, IA-3, IA-8, PL-4, SC-40, SC-43, SI- 4.

Zabezpieczenia rozszerzone:

(1) DOSTĘP BEZPRZEWODOWY | UWIERZYTELNIANIE I SZYFROWANIE

Chroń bezprzewodowy dostęp do systemu, korzystając z uwierzytelniania [Wybierz (jeden lub więcej): użytkownicy; urządzenia] i szyfrowania.

Zabezpieczenia powiązane: SC-8, SC-12, SC-13.

(2) DOSTĘP BEZPRZEWODOWY | MONITOROWANIE POŁĄCZEŃ NIEAUTORYZOWANYCH

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(3) DOSTĘP BEZPRZEWODOWY | DEZAKTYWACJA SIECI BEZPRZEWODOWEJ

Przed wydaniem i wdrożeniem wyłączaj funkcje obsługi sieci bezprzewodowych wbudowane w komponenty systemu, jeśli nie są przeznaczone do użytku.

Zabezpieczenia powiązane: nie dotyczy.

(4) DOSTĘP BEZPRZEWODOWY | OGRANICZANIE KONFIGURACJI PRZEZ UŻYTKOWNIKÓW

Zidentyfikuj i wyraźnie autoryzuj użytkowników, którzy mają prawo do samodzielnej konfiguracji funkcji sieci bezprzewodowej.

Zabezpieczenia powiązane: SC-7, SC-15.

(5) DOSTĘP BEZPRZEWODOWY | ANTENY I POZIOMY MOCY TRANSMISJI

Wybierz anteny radiowe i skalibruj poziomy mocy transmisji, aby zmniejszyć prawdopodobieństwo, że sygnały z punktów dostępu bezprzewodowego zostaną odebrane poza granicami kontrolowanymi przez organizację.

Zabezpieczenia powiązane: PE-19.

AC-19 KONTROLA DOSTĘPU REALIZOWANEGO Z URZĄDZEŃ PRZENOŚNYCH (MOBILNYCH)

Zabezpieczenie:

a) Ustal wymagania dotyczące konfiguracji, wymagania dotyczące połączeń i wskazówki dotyczące wdrażania dla urządzeń mobilnych kontrolowanych przez organizację, w tym, gdy takie urządzenia znajdują się poza kontrolowanymi obszarami;

b) Autoryzuj połączenie urządzeń mobilnych z systemami organizacji.

Zabezpieczenia powiązane: AC-3, AC-4, AC-7, AC-11, AC-17, AC-18, AC-20, CA-9, CM-2, CM-6, IA-2, IA-3, MP- 2, MP-4, MP-5, MP-7, PL-4, SC-7, SC-34, SC-43, SI-3, SI-4.

Zabezpieczenia rozszerzone:

(1) KONTROLA DOSTĘPU REALIZOWANEGO Z URZĄDZEŃ PRZENOŚNYCH (MOBILNYCH) | KORZYSTANIE Z ZAPISYWALNYCH / PRZENOŚNYCH URZĄDZEŃ MAGAZYNUJĄCYCH

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(2) KONTROLA DOSTĘPU REALIZOWANEGO Z URZĄDZEŃ PRZENOŚNYCH (MOBILNYCH) | WYKORZYSTANIE OSOBISTYCH PRZENOŚNYCH URZĄDZEŃ MAGAZYNUJĄCYCH

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(3) KONTROLA DOSTĘPU REALIZOWANEGO Z URZĄDZEŃ PRZENOŚNYCH (MOBILNYCH) | WYKORZYSTANIE OGÓLNODOSTĘPNYCH PRZENOŚNYCH URZĄDZEŃ MAGAZYNUJĄCYCH

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(4) KONTROLA DOSTĘPU REALIZOWANEGO Z URZĄDZEŃ PRZENOŚNYCH (MOBILNYCH) | OGRANICZENIA DOTYCZĄCE INFORMACJI TAJNYCH

a. Zakazuj używania niesklasyfikowanych urządzeń mobilnych w obiektach zawierających systemy przetwarzające, przechowujące lub przesyłające informacje niejawne, chyba że wyraźnie zezwoli na to urzędnik upoważniający;

b. Wyegzekwuj następujące ograniczenia wobec osób, którym urzędnik upoważniający zezwolił na używanie niesklasyfikowanych urządzeń mobilnych w obiektach zawierających systemy przetwarzające, przechowujące lub przesyłające informacje niejawne:

    1. Podłączanie niesklasyfikowanych urządzeń mobilnych do niesklasyfikowanych systemów jest zabronione;

    2. Podłączanie niesklasyfikowanych urządzeń mobilnych do niesklasyfikowanych systemów wymaga zgody urzędnika upoważniającego;

    3. Zabronione jest używanie wewnętrznych lub zewnętrznych modemów lub interfejsów bezprzewodowych w niesklasyfikowanych urządzeniach mobilnych;

    4. Niesklasyfikowane urządzenia mobilne oraz informacje przechowywane na tych urządzeniach podlegają losowym przeglądom i inspekcjom przeprowadzanym przez [Realizacja: funkcjonariusze ds. bezpieczeństwa zdefiniowani przez organizację], a w przypadku znalezienia niejawnych informacji przestrzegana jest polityka obsługi incydentów.

c. Ogranicz podłączanie niesklasyfikowanych urządzeń mobilnych do niesklasyfikowanych systemów zgodnie z [Realizacja: zasady bezpieczeństwa zdefiniowane przez organizację].

Zabezpieczenia powiązane: CM-8, IR-4.

(5) KONTROLA DOSTĘPU REALIZOWANEGO Z URZĄDZEŃ PRZENOŚNYCH (MOBILNYCH) | PEŁNE SZYFROWANIE URZĄDZEŃ LUB KONTENERÓW

Zastosuj [Wybór: szyfrowanie całego urządzenia; szyfrowanie oparte na kontenerach] w celu ochrony poufności i integralności informacji na [Realizacja: urządzeniach mobilnych zdefiniowanych przez organizację].

Zabezpieczenia powiązane: SC-12, SC-13, SC-28.

AC-20 WYKORZYSTANIE ZEWNĘTRZNYCH SYSTEMÓW

Zabezpieczenie:

a. [Wybór (jeden lub więcej): Ustal [Realizacja: warunki i postanowienia zdefiniowane przez organizację]; Zidentyfikuj [Realizacja: kontrole zdefiniowane przez organizację, które mają zostać wdrożone w systemach zewnętrznych]], zgodnie z relacjami zaufania ustanowionymi z innymi organizacjami będącymi właścicielami, obsługującymi i/lub utrzymującymi systemy zewnętrzne, umożliwiając upoważnionym osobom:

    1. Dostęp do systemu z systemów zewnętrznych;

    2. Przetwarzanie, przechowywanie lub przesyłanie informacji kontrolowanych przez organizację przy użyciu systemów zewnętrznych; lub

b. Zabroń używania [Realizacja: typy systemów zewnętrznych zdefiniowane przez organizację].

Zabezpieczenia powiązane: AC-2, AC-3, AC-17, AC-19, CA-3, PL-2, PL-4, SA-9, SC-7.

Zabezpieczenia rozszerzone:

(1) WYKORZYSTANIE ZEWNĘTRZNYCH SYSTEMÓW | OGRANICZENIA AUTORYZOWANEGO DOSTĘPU

Zezwalaj upoważnionym osobom na korzystanie z zewnętrznego systemu w celu uzyskania dostępu do systemu lub przetwarzania, przechowywania lub przesyłania informacji kontrolowanych przez organizację wyłącznie po:

a. sprawdzeniu wdrożenia kontroli w zewnętrznym systemie zgodnie ze specyfikacją w polityce bezpieczeństwa i prywatności organizacji oraz planach bezpieczeństwa i prywatności; lub

b. zachowaniu zatwierdzonych umów dotyczących połączenia z systemem lub przetwarzania z jednostką organizacyjną będącą hostem zewnętrznego systemu.

Zabezpieczenia powiązane: CA-2.

(2) WYKORZYSTANIE ZEWNĘTRZNYCH SYSTEMÓW | URZĄDZENIA PAMIĘCI MASOWEJ PRZENOŚNEJ — OGRANICZONE UŻYTKOWANIE

Ogranicz korzystanie z przenośnych urządzeń pamięci masowej kontrolowanych przez organizację przez osoby upoważnione w systemach zewnętrznych, korzystając z [Realizacja: ograniczenia zdefiniowane przez organizację].

Zabezpieczenia powiązane: MP-7, SC-41.

(3) WYKORZYSTANIE ZEWNĘTRZNYCH SYSTEMÓW | SYSTEMY NIEBĘDĄCE WŁASNOŚCIĄ ORGANIZACJI — OGRANICZONE UŻYTKOWANIE

Ogranicz korzystanie z systemów lub komponentów systemów niebędących własnością organizacji w celu przetwarzania, przechowywania lub przesyłania informacji organizacyjnych przy użyciu [Realizacja: ograniczenia zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(4) WYKORZYSTANIE ZEWNĘTRZNYCH SYSTEMÓW | URZĄDZENIA PAMIĘCI MASOWEJ DOSTĘPNE W SIECI — ZABRONIONE UŻYCIE

Zabroń używania [Realizacja: urządzeń pamięci masowej dostępnych w sieci zdefiniowanych przez organizację] w systemach zewnętrznych.

Zabezpieczenia powiązane: nie dotyczy.

(5) WYKORZYSTANIE ZEWNĘTRZNYCH SYSTEMÓW | URZĄDZENIA PAMIĘCI PRZENOŚNEJ — ZABRONIONE UŻYCIE

Zakaż korzystania przez osoby upoważnione z przenośnych urządzeń pamięci masowej kontrolowanych przez organizację w systemach zewnętrznych.

Zabezpieczenia powiązane: MP-7, PL-4, PS-6, SC-41.

AC-21 UDOSTĘPNIANIE INFORMACJI

Zabezpieczenie:

a. Umożliw autoryzowanym użytkownikom ustalenie czy uprawnienia dostępu przypisane partnerowi udostępniającemu odpowiadają ograniczeniom dostępu i użytkowania informacji dla [Realizacja: okoliczności udostępniania informacji zdefiniowane przez organizację, w których wymagana jest dyskrecja użytkownika];

b. Zastosuj [Realizacja: zautomatyzowane mechanizmy lub procesy ręczne zdefiniowane przez organizację], aby pomóc użytkownikom w podejmowaniu decyzji dotyczących udostępniania informacji i współpracy.

Zabezpieczenia powiązane: AC-3, AC-4, AC-16, PT-2, PT-7, RA-3, SC-15.

Zabezpieczenia rozszerzone:

(1) UDOSTĘPNIANIE INFORMACJI | AUTOMATYCZNE WSPARCIE DECYZJI

Wdrażaj [Realizacja: zautomatyzowanych mechanizmów zdefiniowanych przez organizację] w celu egzekwowania decyzji dotyczących udostępniania informacji przez upoważnionych użytkowników na podstawie uprawnień dostępu partnerów udostępniających informacje i ograniczeń dostępu do udostępnianych informacji.

Zabezpieczenia powiązane: nie dotyczy.

(2) UDOSTĘPNIANIE INFORMACJI | WYSZUKIWANIE I ODZYSKIWANIE INFORMACJI

Wdrażaj usługi wyszukiwania i pobierania informacji, które wymuszają [Realizacja: ograniczenia udostępniania informacji określone przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

AC-22 TREŚCI PUBLICZNIE DOSTĘPNE

Zabezpieczenie:

a. Wyznacz osoby upoważnione do udostępniania informacji publicznie;

b. realizuj szkolenia dla upoważnionych osoby, aby zapewnić się, że publicznie dostępne informacje nie zawierają informacji niepublicznych;

c. Przeglądaj proponowaną treść informacji przed opublikowaniem w publicznie dostępnym systemie, aby upewnić się, że nie są w niej zawarte informacje niepubliczne;

d. Przeglądaj treść w publicznie dostępnym systemie pod kątem informacji niepublicznych [Realizacja: częstotliwość zdefiniowana przez organizację] i usunąć takie informacje, jeśli zostaną odkryte.

Zabezpieczenia powiązane: AC-3, AT-2, AT-3, AU-13.

Zabezpieczenia powiązane: nie dotyczy.

AC-23 OCHRONA PRZED PRZESZUKIWANIEM DANYCH

Zabezpieczenie:

Zastosuj [Realizacja: techniki zapobiegania eksploracji danych zdefiniowane przez organizację i wykrywania takich przypadków] dla [Realizacja: obiekty przechowywania danych zdefiniowane przez organizację] w celu wykrywania i ochrony przed nieautoryzowanym eksplorowaniem danych.

Zabezpieczenia powiązane: nie dotyczy.

AC-24 PRZYZNAWANIE PRAW DOSTĘPU

Zabezpieczenie:

[Wybór: Ustanowienie procedur; Wdrożenie mechanizmów] w celu zapewnienia, że [Realizacja: decyzje dotyczące kontroli dostępu określone przez organizację] będą stosowane do każdego żądania dostępu przed wyegzekwowaniem dostępu.

Zabezpieczenia powiązane: AC-2, AC-3.

Zabezpieczenia rozszerzone:

(1) PRZYZNAWANIE PRAW DOSTĘPU | PRZESYŁANIE INFORMACJI O AUTORYZACJI DOSTĘPU

Przekaż [Realizacja: informacje o autoryzacji dostępu zdefiniowanej przez organizację] przy użyciu [Realizacja: kontrole zdefiniowane przez organizację] do [Realizacja: systemy zdefiniowane przez organizację], które wymuszają decyzje dotyczące kontroli dostępu.

Zabezpieczenia powiązane: AU-10.

(2) PRZYZNAWANIE PRAW DOSTĘPU | BRAK TOŻSAMOŚCI UŻYTKOWNIKA LUB PROCESU

Wymuszaj decyzje dotyczące kontroli dostępu na podstawie [Realizacja: atrybuty bezpieczeństwa lub prywatności zdefiniowane przez organizację], które nie obejmują tożsamości użytkownika ani procesu działającego w imieniu użytkownika.

Zabezpieczenia powiązane: nie dotyczy.

AC-25 MONITOR REFERENCYJNY

Zabezpieczenie:

Wprowadź monitor referencyjny dla [Realizacja: zasady kontroli dostępu zdefiniowane przez organizację], który jest odporny na manipulacje, zawsze wywoływany i na tyle mały, aby można było poddać go analizie i testom, a którego kompletność można zagwarantować.

Zabezpieczenia powiązane: AC-3, AC-16, SA-8, SA-17, SC-3, SC-11, SC-39, SI-13.

KATEGORIA: AT - ŚWIADOMOŚĆ I SZKOLENIE

AT-1 POLITYKA I PROCEDURY

Zabezpieczenie:

a. Opracuj, udokumentuj i rozpowszechnij wśród [Realizacja: personel lub role zdefiniowane w organizacji]:

   1. [Wybierz (jedno lub więcej): na poziomie organizacji, na poziomie misji/procesu biznesowego, na poziomie systemu] politykę podnoszenia świadomości i szkolenia, która:

      (a) Dotyczy celu, zakresu, ról, obowiązków, zaangażowania kierownictwa, koordynacji między jednostkami organizacyjnymi i zgodności;

      (b) Jest zgodna z obowiązującymi przepisami prawa, rozporządzeniami wykonawczymi, dyrektywami, regulacjami, zasadami, normami i wytycznymi;

   2. Procedury ułatwiające wdrażanie polityki w zakresie podnoszenia świadomości i szkoleń oraz powiązanych z nią kontroli w zakresie świadomości i szkoleń;

b. Wyznacz [Realizacja: osobę określoną przez organizację] do zarządzania opracowywaniem, dokumentowaniem i rozpowszechnianiem polityki i procedur dotyczących podnoszenia świadomości i szkoleń;

c. Dokonaj przeglądu i aktualizuj poziom świadomości (w organizacji) i szkoleń w zakresie:

   1. Polityki [Realizacja: częstotliwość zdefiniowana przez organizację] i następujących po niej [Realizacja: zdarzenia zdefiniowane przez organizację];

   2. Procedur [Realizacja: częstotliwość zdefiniowana przez organizację] i następujących po nich [Realizacja: zdarzenia zdefiniowane przez organizację].

Zabezpieczenia powiązane: PM-9, PS-8, SI-12.

Zabezpieczenia rozszerzone: nie dotyczy.

AT-2 SZKOLENIE W ZAKRESIE UŚWIADAMIANIA BEZPIECZEŃSTWA

Zabezpieczenie:

a. Zapewnij użytkownikom systemu (w tym menedżerom, kadrze kierowniczej wyższego szczebla i kontraktorom) szkolenia z zakresu bezpieczeństwa i prywatności:

   1. W ramach wstępnego szkolenia dla nowych użytkowników i [Realizacja: częstotliwość określona przez organizację] w późniejszym czasie;

   2. Gdy wymagają tego zmiany w systemie lub następujące [Realizacja: zdarzenia zdefiniowane przez organizację];

b. Zastosuj następujące techniki w celu zwiększenia świadomości bezpieczeństwa i prywatności użytkowników systemu [Realizacja: techniki świadomości zdefiniowane przez organizację];

c. Aktualizuj treści dotyczące szkoleń oraz podnoszenia świadomości [Realizacja: częstotliwość określona przez organizację] i po [Realizacja: wydarzenia określone przez organizację];

d. Włącz wnioski wyciągnięte z wewnętrznych lub zewnętrznych incydentów związanych z bezpieczeństwem lub prywatnością do szkoleń oraz technik podnoszenia świadomości.

Zabezpieczenia powiązane: AC-3, AC-17, AC-22, AT-3, AT-4, CP-3, IA-4, IR-2, IR-7, IR-9, PL-4, PM-13, PM- 21, PS-7, PT-2, SA-8, SA-16.

Zabezpieczenia rozszerzone:

(1) SZKOLENIE W ZAKRESIE UŚWIADAMIANIA BEZPIECZEŃSTWA | ĆWICZENIA PRAKTYCZNE

Przeprowadzaj praktyczne ćwiczenia, które symulują wydarzenia i incydenty.

Zabezpieczenia powiązane: CA-2, CA-7, CP-4, IR-3.

(2) SZKOLENIE W ZAKRESIE UŚWIADAMIANIA BEZPIECZEŃSTWA | ZAGROŻENIA WEWNĘTRZNE

Przeprowadzaj szkolenia z zakresu rozpoznawania i zgłaszania potencjalnych oznak zagrożeń wewnętrznych.

Zabezpieczenia powiązane: PM-12.

(3) SZKOLENIE W ZAKRESIE UŚWIADAMIANIA BEZPIECZEŃSTWA | INŻYNIERIA SPOŁECZNA I POZYSKIWANIE DANYCH

Przeprowadzaj szkolenia z zakresu rozpoznawania i zgłaszania potencjalnych i faktycznych przypadków inżynierii społecznej i eksploracji informacji za pomocą socjotechniki.

Zabezpieczenia powiązane: nie dotyczy.

(4) SZKOLENIE W ZAKRESIE UŚWIADAMIANIA BEZPIECZEŃSTWA | PODEJRZANE KOMUNIKATY I NIETYPOWE ZACHOWANIA SYSTEMÓW

Przeprowadzaj szkolenia z zakresu rozpoznawania podejrzanych komunikatów i zachowań nietypowych w systemach organizacyjnych, korzystając z [Realizacja: wskaźników złośliwego kodu zdefiniowanych przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(5) SZKOLENIE W ZAKRESIE UŚWIADAMIANIA BEZPIECZEŃSTWA | ZAAWANSOWANE TRWAŁE ZAGROŻENIE

Zapewnij szkolenia na temat zaawansowanych, trwałych zagrożeń.

Zabezpieczenia powiązane: nie dotyczy.

(6) SZKOLENIE W ZAKRESIE UŚWIADAMIANIA BEZPIECZEŃSTWA | ŚRODOWISKO ZAGROŻEŃ CYBERNETYCZNYCH

a. Zapewnij szkolenia na temat środowiska zagrożeń cybernetycznych;

b. Odzwierciedlaj bieżące informacje o zagrożeniach cybernetycznych w operacjach systemowych.

Zabezpieczenia powiązane: RA-3.

AT-3 SZKOLENIE OPARTE NA ROLACH

Zabezpieczenie:

a. Zapewnij szkolenia z zakresu bezpieczeństwa i prywatności oparte na rolach dla personelu o następujących rolach i obowiązkach: [Realizacja: role i obowiązki zdefiniowane przez organizację]:

    1. Przed udzieleniem autoryzacji dostępu do systemu, informacji lub wykonaniem przydzielonych obowiązków oraz [Realizacja: częstotliwość określona przez organizację] po tym fakcie;

    2. Gdy wymagają tego zmiany w systemie;

b. Aktualizuj treści szkoleń opartych na rolach [Realizacja: częstotliwość zdefiniowana przez organizację] i następujące po [Realizacja: zdarzenia zdefiniowane przez organizację];

c. Włącz wnioski wyciągnięte z wewnętrznych lub zewnętrznych incydentów związanych z bezpieczeństwem lub prywatnością do szkoleń opartych na rolach.

Zabezpieczenia powiązane: AC-3, AC-17, AC-22, AT-2, AT-4, CP-3, IR-2, IR-4, IR-7, IR-9, PE-1, PE-2, PE-3, PE-4, PE-11, PE-13, PE-14, PE-15, PL-4, PM-13, PM-23, PS-7, PS-9, PT-2, PT-3, PT-5, PT-6, SA-3, SA-8, SA-11, SA-16, SR-5, SR-6, SR-11.

Zabezpieczenia rozszerzone:

(1) SZKOLENIA OPARTE NA ROLACH | KONTROLE ŚRODOWISKOWE

Zapewnij [Realizacja: personel lub role określone przez organizację] szkolenie początkowe i [Realizacja: częstotliwość określona przez organizację] w zakresie stosowania i obsługi kontroli środowiskowych.

Zabezpieczenia powiązane: PE-1, PE-11, PE-13, PE-14, PE-15.

(2) SZKOLENIA OPARTE NA ROLACH | KONTROLE BEZPIECZEŃSTWA FIZYCZNEGO

Zapewnij [Realizacja: personel lub role określone przez organizację] szkolenie początkowe i [Realizacja: częstotliwość określona przez organizację] w zakresie stosowania i obsługi kontroli bezpieczeństwa fizycznego.

Zabezpieczenia powiązane: PE-2, PE-3, PE-4.

(3) SZKOLENIA OPARTE NA ROLACH | ĆWICZENIA PRAKTYCZNE

Zapewnij praktyczne ćwiczenia w zakresie bezpieczeństwa i prywatności, które wzmocnią cele szkolenia.

Zabezpieczenia powiązane: nie dotyczy.

(4) SZKOLENIA OPARTE NA ROLACH | PODEJRZANA KOMUNIKACJA I NIETYPOWE ZACHOWANIE SYSTEMU

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(5) SZKOLENIA OPARTE NA ROLACH | PRZETWARZANIE DANYCH OSOBOWYCH

Zapewnij [Realizacja: personel lub role określone przez organizację] szkolenie początkowe i [Realizacja: częstotliwość określona przez organizację] w zakresie stosowania i obsługi przetwarzania danych osobowych oraz kontroli przejrzystości.

Zabezpieczenia powiązane: PT-2, PT-3, PT-5, PT-6.

AT-4 ZAPISY SZKOLENIOWE

Zabezpieczenie:

a. Dokumentuj i monitoruj szkolenia w zakresie bezpieczeństwa informacji i prywatności, w tym szkolenia podnoszące świadomość w zakresie bezpieczeństwa i prywatności oraz szkolenia w zakresie bezpieczeństwa i prywatności opartych na konkretnych rolach;

b. Przechowuj indywidualne zapisy szkoleń przez [Realizacja: okres czasu określony przez organizację].

Zabezpieczenia powiązane: AT-2, AT-3, CP-3, IR-2, PM-14, SI-12.

Zabezpieczenia rozszerzone: nie dotyczy.

AT-5 KONTAKTY Z GRUPAMI I STOWARZYSZENIAMI DS. BEZPIECZEŃSTWA

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

AT-6 INFORMACJE ZWROTNE DOTYCZĄCE SZKOLENIA

Zabezpieczenie:

Przekaż opinię na temat wyników szkoleń organizacyjnych następującym pracownikom [Realizacja: częstotliwość określona przez organizację]: [Realizacja: personel określony przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

Zabezpieczenia rozszerzone: nie dotyczy.

KATEGORIA: AU – AUDYT I ROZLICZALNOŚĆ

AU-1 POLITYKA I PROCEDURY

Zabezpieczenie:

a. Opracowuj, dokumentuj i rozpowszechniaj wśród [Realizacja: personel lub role określone przez organizację]:

    1. [Wybór (jeden lub więcej): poziom organizacji; poziom misji/procesu biznesowego; poziom systemu] polityki audytu i rozliczalności, która:

        (a) Adresuje cel, zakres, role, obowiązki, zaangażowanie kierownictwa, koordynację między jednostkami organizacyjnymi i zgodność z przepisami;

        (b) Jest zgodna z obowiązującym prawem, rozporządzeniami, dyrektywami, przepisami, zasadami, standardami i wytycznymi;

    2. Procedury ułatwiające realizację polityki audytu i rozliczalności oraz powiązanych zabezpieczeń w zakresie audytu i rozliczalności;

b. Wyznaczaj [Realizacja: osoba wyznaczona przez organizację] do zarządzania rozwojem, dokumentacją i rozpowszechnianiem polityki i procedur audytu oraz rozliczalności;

c. Przeglądanie i aktualizowanie bieżącej:

    1. Polityki audytu i rozliczalności z [Realizacja: częstotliwość określona przez organizację] i następujących [Realizacja: zdarzenia określone przez organizację];

    2. Procedur dotyczących audytu i rozliczalności z [Realizacja: częstotliwość określona przez organizację] i następujących [Realizacja: zdarzenia określone przez organizację].

Zabezpieczenia powiązane: PM-9, PS-8, SI-12.

Zabezpieczenia rozszerzone: nie dotyczy.

AU-2 AUDYT ZDARZEŃ

Zabezpieczenie:

a. Określaj rodzaje zdarzeń, które system jest w stanie kontrolować na potrzeby funkcji audytu: [Realizacja: zdefiniowane przez organizację typy zdarzeń, które system jest w stanie rejestrować];

b. Koordynuj funkcje rejestrowania zdarzeń z innymi jednostkami organizacyjnymi wymagającymi informacji związanych z audytem w celu prowadzenia i informowania o kryteriach wyboru zdarzeń, które mają być rejestrowane;

c. Określaj następujące typy zdarzeń do logowania w systemie: [Realizacja: zdefiniowane przez organizację typy zdarzeń (podzbiór typów zdarzeń zdefiniowanych w zabezpieczeniu rozszerzonym AU-2a.) wraz z częstotliwością (lub sytuacją wymagającą) logowania dla każdego zidentyfikowanego typu zdarzenia];

d. Przedstawiaj uzasadnienia, dlaczego rodzaje zdarzeń wybrane do logowania uznaje się za odpowiednie do celów badania zdarzeń po fakcie;

e. Przeglądaj i aktualizuj typy zdarzeń wybranych do logowania z [Realizacja: częstotliwość zdefiniowana przez organizację].

Zabezpieczenia powiązane: AC-2, AC-3, AC-6, AC-7, AC-8, AC-16, AC-17, AU-3, AU-4, AU-5, AU-6, AU-7, AU- 11, AU-12, CM-3, CM-5, CM-6, CM-13, IA-3, MA-4, MP-4, PE-3, PM-21, PT-2, PT-7, RA-8, SA-8, SC-7, SC-18, SI-3, SI-4, SI-7, SI-10, SI-11.

Zabezpieczenia rozszerzone:

(1) AUDYT ZDARZEŃ | KOMPILACJA ZAPISÓW AUDYTU Z WIELU ŹRÓDEŁ

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2].

(2) AUDYT ZDARZEŃ | WYBÓR ZDARZEŃ AUDYTOWYCH WEDŁUG KOMPONENTÓW

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2].

(3) AUDYT ZDARZEŃ | OPINIE I AKTUALIZACJE

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2].

(4) AUDYT ZDARZEŃ | UPRZYWILEJOWANE FUNKCJE

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2].

AU-3 ZAWARTOŚĆ REJESTRÓW AUDYTU

Zabezpieczenie:

Zapewnij, że zapisy z audytu zawierają informacje, które ustalają:

a. Jakiego rodzaju zdarzenie miało miejsce;

b. Kiedy zdarzenie miało miejsce;

c. Gdzie to zdarzenie miało miejsce;

d. Źródło zdarzenia;

e. Rezultaty zdarzenia;

f. Tożsamość wszelkich osób, podmiotów lub przedmiotów/podmiotów związanych ze zdarzeniem.

Zabezpieczenia powiązane: AU-2, AU-8, AU-12, AU-14, MA-4, PL-9, RA-3, SA-8, SI-7, SI-11.

Zabezpieczenia rozszerzone:

(1) ZAWARTOŚĆ REJESTRÓW AUDYTU | DODATKOWE INFORMACJE KONTROLNE

Zapewniaj zapisy audytu zawierające następujące dodatkowe informacje:

[Realizacja: informacje dodatkowe określone przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(2) ZAWARTOŚĆ REJESTRÓW AUDYTU | CENTRALNE ZARZĄDZANIE TREŚCIĄ PLANOWANEGO REJESTRU AUDYTU

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2].

(3) ZAWARTOŚĆ REJESTRÓW AUDYTU | OGRANICZENIE INFORMACJI UMOŻLIWIAJĄCYCH IDENTYFIKACJĘ OSÓB

Ograniczaj informacje umożliwiające identyfikację osób zawartych w dokumentacji z audytu do następujących elementów określonych w ocenie ryzyka naruszenia prywatności: [Realizacja: elementy określone przez organizację].

Zabezpieczenia powiązane: RA-3.

AU-4 POJEMNOŚĆ PAMIĘCI ZAPISÓW AUDYTU

Zabezpieczenie:

Wyznacz miejsca na przechowywanie dziennika audytów, aby zapewnić [Realizacja: wymagania dotyczące przechowywania dziennika audytów określone przez organizację].

Zabezpieczenia powiązane: AU-2, AU-5, AU-6, AU-7, AU-9, AU-11, AU-12, AU-14, SI-4.

Zabezpieczenia rozszerzone:

(1) POJEMNOŚĆ PAMIĘCI ZAPISÓW AUDYTU | TRANSFER REKORDÓW DO ALTERNATYWNYCH URZĄDZEŃ MAGAZYNUJĄCYCH

Przenoś dzienniki audytowe z częstotliwością [Realizacja: częstotliwość zdefiniowana przez organizację] do innego systemu, komponentu systemu lub nośnika innego niż system lub komponent systemu przeprowadzającego logowanie.

Zabezpieczenia powiązane: nie dotyczy.

AU-5 REAKCJA NA BŁĘDY PROCESÓW AUDYTU

Zabezpieczenie:

a. Alarmuj [Realizacja: określonego przez organizację personelu lub ról] w ramach [Realizacja: określony przez organizację okres czasu] w przypadku niewykonania procesów audytu;

b. Podejmuj następujące dodatkowe działania: [Realizacja: dodatkowe działania zdefiniowane przez organizację].

Zabezpieczenia powiązane: AU-2, AU-4, AU-5(5), AU-7, AU-9, AU-11, AU-12, AU-14, SI-4, SI-12.

Zabezpieczenia rozszerzone:

(1) REAKCJA NA BŁĘDY PROCESÓW AUDYTU |OSTRZEŻENIA DOTYCZĄCE LIMITU PAMIĘCI PRZECHOWYWANIA REKORDÓW AUDYTU

Ostrzegaj [Realizacja: określonego przez organizację personelu, ról i/lub lokalizacji] w ciągu [Realizacja: określony przez organizację okres czasu], kiedy przydzielona pojemność pamięci masowej dziennika audytu osiągnie [Realizacja: określony przez organizację procent] maksymalnej pojemności pamięci masowej dziennika audytu.

Zabezpieczenia powiązane: nie dotyczy.

(2) REAKCJA NA BŁĘDY PROCESÓW AUDYTU | ALERTY CZASU RZECZYWISTEGO

W ciągu [Realizacja: zdefiniowany przez organizację okres czasu rzeczywistego] do [Realizacja: zdefiniowany przez organizację personel, role i/lub lokalizacje] powiadamiaj o wystąpieniu następujących zdarzeń niepowodzeń audytu: [Realizacja: zdefiniowany przez organizację rejestr zdarzeń związanych z rejestrowaniem audytów wymagających alertów w czasie rzeczywistym].

Zabezpieczenia powiązane: nie dotyczy.

(3) REAKCJA NA BŁĘDY PROCESÓW AUDYTU | KONFIGUROWALNE PROGI NATĘŻENIA RUCHU

Egzekwuj konfigurowalne progi natężenia ruchu sieciowego odzwierciedlające limity pojemności pamięci masowej dziennika audytu oraz [Wybór: odrzucenie; opóźnienie] ruchu sieciowego powyżej tych progów.

Zabezpieczenia powiązane: nie dotyczy.

(4) REAKCJA NA BŁĘDY PROCESÓW AUDYTU | WYŁĄCZENIE W PRZYPADKU AWARII

Wymuszaj [Wybór: pełne wyłączenie systemu; częściowe wyłączenie systemu; awaryjny tryb pracy z ograniczoną dostępnością funkcji misji lub działalności biznesowych] w przypadku [Realizacja: niepowodzenie audytu zdefiniowane przez organizację], chyba, że istnieje alternatywna możliwość prowadzenia audytów.

Zabezpieczenia powiązane: AU-5(5).

(5) REAKCJA NA BŁĘDY PROCESÓW AUDYTU | ZDOLNOŚĆ ALTERNATYWNEGO PROWADZENIA REJESTRU AUDYTÓW

Zapewnij możliwości alternatywnego rejestrowania audytów w przypadku awarii podstawowej funkcji rejestrowania audytów, która implementuje [Realizacja: zdefiniowana przez organizację funkcja alternatywnego rejestrowania audytów].

Zabezpieczenia powiązane: AU-9.

AU-6 PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE

Zabezpieczenie:

a. Przeglądaj i analizuj zapisy z audytu systemu [Realizacja: częstotliwość określona przez organizację] pod kątem wskazań [Realizacja: działalność określona przez organizację, jako nieodpowiednia lub nietypowa] oraz potencjalnego wpływu działalności nieodpowiedniej lub nietypowej;

b. Zgłaszaj ustalenia do [Realizacja: personel lub role określone przez organizację];

c. Dostosowuj poziom przeglądu dokumentacji audytowej, analizy i sprawozdawczości w ramach systemu w przypadku zmiany ryzyka w oparciu o informacje dotyczące egzekwowania prawa, informacje wywiadowcze lub inne wiarygodne źródła informacji.

Zabezpieczenia powiązane: AC-2, AC-3, AC-5, AC-6, AC-7, AC-17, AU-2, AU-3, AU-7, AU-9, AU-11, AU-12, AU-16, CA-2, CA-7, CM-2, CM-5, CM-6, CM-10, CM-11, IA-2, IA-3, IA-5, IA-8, IR-4, IR-5, MA-4, MP-4, PE-3, PE-6, PM-7, PM-12, RA-5, SA-8, S.C.-7, SI-3, SI-4, SI-7.

Zabezpieczenia rozszerzone:

(1) PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE | ZAUTOMATYZOWANA INTEGRACJA PROCESÓW

Integruj procesy przeglądu, analizy i raportowania zapisów audytowych za pomocą [Realizacja: automatyczne mechanizmy zdefiniowane przez organizację].

Zabezpieczenia powiązane: PM-7.

(2) PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE | AUTOMATYCZNE ALARMY BEZPIECZEŃSTWA

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2].

(3) PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE | KORELACJA ZBIORÓW AUDYTU

Analizuj i koreluj zapisy z audytów w różnych repozytoriach w celu zwiększenia świadomości sytuacyjnej w całej organizacji.

Zabezpieczenia powiązane: AU-12, IR-4.

(4) PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE | CENTRALNE PRZEGLĄDANIE I ANALIZY

Zapewnij i wdrażaj możliwości centralnego przeglądania i analizowania zapisów audytowych z wielu komponentów systemu.

Zabezpieczenia powiązane: AU-2, AU-12.

(5) PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE | ZINTEGROWANA ANALIZA ZAPISÓW Z AUDYTU

Integruj analizy zapisów z audytu z analizą [Wybór (jeden lub więcej): informacje o skanowaniu podatności; dane o wydajności; informacje o monitorowaniu systemu; [Realizacja: dane/informacje określone przez organizację zebrane z innych źródeł]] w celu dalszego zwiększenia możliwości identyfikacji niewłaściwych lub nietypowych działań.

Zabezpieczenia powiązane: AU-12, IR-4.

(6) PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE | KORELACJA AUDYTU Z MONITOROWANIEM FIZYCZNYM

Koreluj informacje z rejestrów audytowych z informacjami uzyskanymi z monitorowania dostępu fizycznego w celu dalszego zwiększenia zdolności do identyfikacji podejrzanych, niewłaściwych, nietypowych lub złośliwych działań.

Zabezpieczenia powiązane: nie dotyczy.

(7) PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE | DOPUSZCZALNE DZIAŁANIA

Określ dozwolone działania dla każdego z [Wybór (jeden lub więcej): proces systemowy; rola; użytkownik] związane z przeglądem, analizą i raportowaniem informacji z zapisów audytu.

Zabezpieczenia powiązane: nie dotyczy.

(8) PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE | PEŁNA ANALIZA TEKSTU UPRZYWILEJOWANYCH POLECEŃ

Przeprowadzaj pełną analizę tekstową zarejestrowanych uprzywilejowanych poleceń w fizycznie odrębnym komponencie lub podsystemie systemu, lub w innym systemie, który jest dedykowany do tej analizy.

Zabezpieczenia powiązane: AU-3, AU-9, AU-11, AU-12.

(9) PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE | KORELACJA Z INFORMACJAMI UZYSKANYMI ZE ŹRÓDEŁ NIETECHNICZNYCH

Koreluj informacje ze źródeł nietechnicznych z informacjami z zapisów audytów w celu zwiększenia świadomości sytuacyjnej w całej organizacji.

Zabezpieczenia powiązane: PM-12.

(10) PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE | KORYGOWANIE POZIOMU AUDYTU

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2].

AU-7 REDUKCJA TREŚCI ZAPISÓW Z AUDYTU I GENEROWANIE RAPORTÓW

Zabezpieczenie: Zapewnij i wprowadź redukcję treści zapisów audytowych i zdolności generowania raportów, które:

a. Wspierają przegląd treści zapisów z audytu na żądanie, analizę i wymogi w zakresie sprawozdawczości oraz badania powykonawcze po wystąpieniu incydentów;

b. Nie zmieniają pierwotnej treści ani kolejności czasowej zapisów z audytu.

Zabezpieczenia powiązane: AC-2, AU-2, AU-3, AU-4, AU-5, AU-6, AU-12, AU-16, CM-5, IA-5, IR-4, PM-12, SI- 4.

Zabezpieczenia rozszerzone:

(1) REDUKCJA TREŚCI ZAPISÓW Z AUDYTU I GENEROWANIE RAPORTÓW | AUTOMATYZACJA PROCESU

Zapewnij i wprowadź możliwości przetwarzania, sortowania i wyszukiwania zapisów audytów interesujących nas zdarzeń w oparciu o następującą treść:

[Realizacja: pola zdefiniowane przez organizację w dokumentacji audytowej].

Zabezpieczenia powiązane: nie dotyczy.

(2) REDUKCJA TREŚCI ZAPISÓW Z AUDYTU I GENEROWANIE RAPORTÓW | AUTOMATYCZNE SORTOWANIE I WYSZUKIWANIE

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2].

AU-8 ZNACZNIKI CZASU

Zabezpieczenie:

a. Wykorzystaj wewnętrzne zegary systemowe do generowania znaczników czasu dla rekordów audytów;

b. Zapisuj znaczniki czasu dla rekordów audytowych, które spełniają [Realizacja: zdefiniowana przez organizację granulacja pomiaru czasu] i które wykorzystują uniwersalny czas koordynowany (UTC), mają stałe przesunięcie czasu lokalnego w stosunku do uniwersalnego czasu koordynowanego lub które zawierają przesunięcie czasu lokalnego, jako część znacznika czasu.

Zabezpieczenia powiązane: AU-3, AU-12, AU-14, S.C.-45.

Zabezpieczenia rozszerzone:

(1) ZNACZNIKI CZASU | SYNCHRONIZACJA Z AUTORYZOWANYM ŹRÓDŁEM CZASU ODNIESIENIA

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2].

(2) ZNACZNIKI CZASU | WTÓRNE ŹRÓDŁO CZASU ODNIESIENIA

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2].

AU-9 OCHRONA INFORMACJI AUDYTOWYCH

Zabezpieczenie:

a. Ochraniaj informacje audytowe i narzędzia rejestrujące audyt przed nieautoryzowanym dostępem, modyfikacją i usuwaniem;

b. Alarmuj [Realizacja: zdefiniowany przez organizację personel lub role] w przypadku wykrycia nieautoryzowanego dostępu, modyfikacji lub usunięcia informacji o audycie.

Zabezpieczenia powiązane: AC-3, AC-5, AC-6, AU-4, AU-5, AU-5(5), AU-6, AU-10, AU-11, AU-14, MP-2, MP-4, PE-2, PE-3, PE-6, SA-8, S.C.-8, S.C.-12, S.C.-13, S.C.-29, SI-4.

Zabezpieczenia rozszerzone:

(1) OCHRONA INFORMACJI AUDYTOWYCH | NOŚNIKI JEDNOKROTNEGO ZAPISU

Zapisuj ścieżki audytu na wymuszonych sprzętowo nośnikach jednorazowego zapisu.

Zabezpieczenia powiązane: AU-4, AU-5.

(2) OCHRONA INFORMACJI AUDYTOWYCH | BACKUP AUDYTU W ODSEPAROWANYM FIZYCZNIE SYSTEMIE / KOMPONENCIE

Przechowuj zapisy z audytu [Realizacja: częstotliwość określona przez organizację] w repozytorium, które jest fizycznie częścią innego systemu lub komponentu systemu niż system lub komponent będący przedmiotem audytu.

Zabezpieczenia powiązane: AU-4, AU-5.

(3) OCHRONA INFORMACJI AUDYTOWYCH | OCHRONA KRYPTOGRAFICZNA

Wprowadź mechanizmy kryptograficzne w celu ochrony integralności informacji dotyczących audytu i narzędzi audytu.

Zabezpieczenia powiązane: AU-10, SC-12, SC-13.

(4) OCHRONA INFORMACJI AUDYTOWYCH | DOSTĘP DO PODZBIORU UPRZYWILEJOWANYCH UŻYTKOWNIKÓW

Zezwalaj na dostęp do zarządzania funkcjami audytu tylko do [Realizacja: zdefiniowany przez organizację podzbiór uprzywilejowanych użytkowników lub ról].

Zabezpieczenia powiązane: AC-5.

(5) OCHRONA INFORMACJI AUDYTOWYCH | PODWÓJNA AUTORYZACJA

Egzekwuj podwójną autoryzację dla [Wybór (jeden lub więcej): przemieszczenie; usunięcie] [Realizacja: informacja o audycie zdefiniowana przez organizację].

Zabezpieczenia powiązane: AC-3.

(6) OCHRONA INFORMACJI AUDYTOWYCH | DOSTĘP TYLKO DO ODCZYTU

Zezwalaj na dostęp tylko do odczytu do informacji o audycie [Realizacja: zdefiniowany przez organizację podzbiór uprzywilejowanych użytkowników lub ról].

Zabezpieczenia powiązane: nie dotyczy.

(7) OCHRONA INFORMACJI AUDYTOWYCH | PRZECHOWYWANIE INFORMACJI NA KOMPONENTACH Z RÓŻNYMI SYSTEMAMI OPERACYJNYMI

Przechowuj informacje o audycie na komponencie wykonującym inny system operacyjny niż system lub komponent będący przedmiotem audytu.

Zabezpieczenia powiązane: AU-4, AU-5, AU-11, SC-29.

AU-10 NIEZAPRZECZALNOŚĆ

Zabezpieczenie:

Dostarczaj niezbite dowody na to, że osoba (lub proces działający w imieniu osoby) wykonała [Realizacja: działania zdefiniowane przez organizację, które mają być objęte zakazem odrzucania].

Zabezpieczenia powiązane: AC-3, AC-4, AC-16, AU-9, PM-12, SA-8, SC-8, SC-12, SC-13, SC-16, SC-17, SC-23.

Zabezpieczenia rozszerzone:

(1) NIEZAPRZECZALNOŚĆ | POŁĄCZENIE TOŻSAMOŚCI

a. Powiąż tożsamość twórcy informacji z informacją z [Realizacja: siła wiążąca określona przez organizację];

b. Zapewnij upoważnionym osobom środki umożliwiające ustalenie tożsamości twórcy informacji.

Zabezpieczenia powiązane: AC-4, AC-16.

(2) NIEZAPRZECZALNOŚĆ | POWIĄZANIE INFORMACJI Z TOŻSAMOŚCIĄ TWÓRCY

a. Zatwierdzaj powiązania tożsamości twórcy informacji z informacjami z [Realizacja: częstotliwość określona przez organizację];

b. Wykonuj [Realizacja: czynności zdefiniowane przez organizację] w przypadku błędu sprawdzania poprawności powiązania.

Zabezpieczenia powiązane: AC-3, AC-4, AC-16.

(3) NIEZAPRZECZALNOŚĆ | ŁAŃCUCH NADZORU

Utrzymuj tożsamość recenzenta / wydawcy informacji w ramach ustalonego łańcucha dowodowego odnoszącego się do informacji poddanych przeglądowi lub opublikowaniu.

Zabezpieczenia powiązane: AC-4, AC-16.

(4) NIEZAPRZECZALNOŚĆ | POTWIERDZANIE TOŻSAMOŚCI PRZEGLĄDAJĄCEGO INFORMACJE

a. Zatwierdzaj powiązania tożsamości recenzenta wiadomości z informacjami w punktach transferu lub udostępniania, przed ich udostępnieniem lub transferem pomiędzy [Realizacja: zdefiniowane przez organizację domeny bezpieczeństwa];

b. Wykonuj [Realizacja: czynności zdefiniowane przez organizację] w przypadku błędu potwierdzania (walidacji).

Zabezpieczenia powiązane: AC-4, AC-16.

(5) NIEZAPRZECZALNOŚĆ | PODPISY CYFROWE

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2].

AU-11 RETENCJA ZAPISÓW AUDYTU

Zabezpieczenie:

Przechowuj zapisy z audytu przez okres [Realizacja: okres zdefiniowany przez organizację zgodnie z polityką przechowywania rejestru] w celu zapewnienia wsparcia procesów dochodzeniowych dotyczących incydentów bezpieczeństwa oraz w celu spełnienia wymagań prawnych i organizacyjnych dotyczących przechowywania informacji.

Zabezpieczenia powiązane: AU-2, AU-4, AU-5, AU-6, AU-9, AU-14, MP-6, RA-5, SI-12.

Zabezpieczenia rozszerzone:

(1) RETENCJA ZAPISÓW AUDYTU | DŁUGOTERMINOWA ZDOLNOŚĆ DO ODZYSKU

Stosuj [Realizacja: środki określone przez organizację] w celu zapewnienia możliwości odzyskania zapisów z audytu generowanych przez system.

Zabezpieczenia powiązane: nie dotyczy.

AU-12 TWORZENIE ZAPISÓW AUDYTU

Zabezpieczenie:

a. Udostępniaj możliwość generowania zapisów audytowych dla typów zdarzeń, które system jest w stanie audytować zgodnie z definicją zawartą w AU-2a w obszarze [Realizacja: komponenty systemu zdefiniowane przez organizację];

b. Zezwalaj [Realizacja: personel lub role zdefiniowane przez organizację] na wybór typów zdarzeń, które mają być rejestrowane przez określone elementy systemu;

c. Generuj zapisy audytowe dla typów zdarzeń zdefiniowanych w AU-2c, które zawierają zawartość zapisów audytowych określonych w zabezpieczeniach AU-3.

Zabezpieczenia powiązane: AC-3, AC-6, AC-17, AU-2, AU-3, AU-4, AU-5, AU-6, AU-7, AU-8, AU-14, CM-5, MA-4, MP-4, PM-12, SA-8, SC-18, SC-45, SI-3, SI-4, SI-7, SI-10.

Zabezpieczenia rozszerzone:

(1) TWORZENIE ZAPISÓW AUDYTU | OGÓLNOSYSTEMOWE / SKORELOWANE W CZASIE ŚCIEŻKI AUDYTU

Skoreluj zapisy audytu z [Realizacja: zdefiniowane przez organizację składniki systemu] do ogólnosystemowej (logicznej lub fizycznej) ścieżki audytu, która jest związana z czasem w ramach [Realizacja: zdefiniowany przez organizację poziom tolerancji dla relacji pomiędzy znacznikami czasu poszczególnych zapisów w ścieżce audytu].

Zabezpieczenia powiązane: AU-8, SC-45.

(2) TWORZENIE ZAPISÓW AUDYTU | UJEDNOLICONE FORMATY

Stwórz ogólnosystemową (logicznej lub fizycznej) ścieżkę audytu składającą się z zapisów audytowych w znormalizowanym (ujednoliconym) formacie.

Zabezpieczenia powiązane: nie dotyczy.

(3) TWORZENIE ZAPISÓW AUDYTU | ZMIANY DOKONYWANE PRZEZ UPRAWNIONE OSOBY

Zapewnij i wprowadź zdolność [Realizacja: osoby lub role określone przez organizację] do zmiany logowania, które ma być wykonywane na [Realizacja: komponenty systemu określone przez organizację] w oparciu o [Realizacja: kryteria zdarzeń do wyboru określone przez organizację] w ramach [Realizacja: progi czasowe określone przez organizację].

Zabezpieczenia powiązane: AC-3.

(4) TWORZENIE ZAPISÓW AUDYTU | AUDYT PARAMETRÓW ZAPYTAŃ O DANE OSOBOWE

Zapewnij i wprowadź możliwości audytowania parametrów zapytań użytkowników o zbiory danych zawierające dane osobowe.

Zabezpieczenia powiązane: nie dotyczy.

AU-13 MONITOROWANIE UJAWNIANIA INFORMACJI

Zabezpieczenie:

a. Monitoruj [Realizacja: zdefiniowanych przez organizację informacji o otwartym kodzie źródłowym i/lub witryn informatycznych] z częstotliwością [Realizacja: zdefiniowana przez organizację częstotliwość] pod kątem dowodów nieautoryzowanego ujawnienia informacji organizacyjnych;

b. W przypadku ujawnienia informacji:

    1. Powiadamiaj [Realizacja: personel lub role określone przez organizację];

    2. Podejmuj następujące dodatkowe działania: [Realizacja: dodatkowe działania zdefiniowane przez organizację].

Zabezpieczenia powiązane: AC-22, PE-3, PM-12, RA-5, SC-7, SI-20.

Zabezpieczenia rozszerzone:

(1) MONITOROWANIE UJAWNIANIA INFORMACJI | WYKORZYSTYWANIE ZAUTOMATYZOWANYCH NARZĘDZI

Monitoruj informacje i witryny informatyczne o otwartym kodzie źródłowym za pomocą [Realizacja: organizacyjnie zdefiniowane mechanizmy automatyczne].

Zabezpieczenia powiązane: nie dotyczy.

(2) MONITOROWANIE UJAWNIANIA INFORMACJI | PRZEGLĄD MONITOROWANYCH STRON

Przeglądaj listy monitorowanych stron internetowych z otwartym kodem źródłowym z częstotliwością [Realizacja: częstotliwość określona przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(3) MONITOROWANIE UJAWNIANIA INFORMACJI | NIEAUTORYZOWANE POWIELANIE INFORMACJI

Stosuj techniki wykrywania, procesów i narzędzi do w celu ustalenia czy podmioty zewnętrzne powielają informacje organizacyjne w sposób nieautoryzowany.

Zabezpieczenia powiązane: nie dotyczy.

AU-14 AUDYT SESJI

Zabezpieczenie:

a. Zapewnij i wprowadź możliwości [Realizacja: zdefiniowani przez organizację użytkownicy lub role] do [Wybór (jeden lub więcej): nagrywania; przeglądania; słuchania; dziennik] zawartości sesji użytkownika w ramach [Realizacja: okoliczności zdefiniowane przez organizację];

b. Opracowuj, integruj i wykorzystuj audyty sesji w porozumieniu z działem prawnym oraz zgodnie z obowiązującymi przepisami prawa, rozporządzeniami, dyrektywami, polityką, standardami i wytycznymi.

Zabezpieczenia powiązane: AC-3, AC-8, AC-17, AU-2, AU-3, AU-4, AU-5, AU-8, AU-9, AU-11, AU-12.

Zabezpieczenia rozszerzone:

(1) AUDYT SESJI | URUCHAMIANIE SYSTEMU

Automatyczne inicjuj audyty sesji przy uruchamianiu systemu.

Zabezpieczenia powiązane: nie dotyczy.

(2) AUDYT SESJI | PRZECHWYTY / NAGRYWANIE I ZAWARTOŚĆ DZIENNIKÓW LOGOWANIA

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2].

(3) AUDYT SESJI | ZDALNE WYŚWIETLANIE / ODSŁUCHIWANIE

Zapewnij i wprowadź możliwości zdalnego przeglądania i odsłuchiwania w czasie rzeczywistym przez uprawnionych użytkowników treści związanych z ustaloną sesją użytkownika.

Omówienie: nie dotyczy.

Zabezpieczenia powiązane: AC-17.

AU-15 ZDOLNOŚĆ DO ALTERNATYWNEGO AUDYTU

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2].

AU-16 AUDYT MIĘDZYORGANIZACYJNY

Zabezpieczenie: Stosuj [Realizacja: metody zdefiniowane przez organizację] do koordynacji [Realizacja: informacje o audycie zdefiniowane przez organizację] pomiędzy zewnętrznymi organizacjami, w przypadku przekazywania informacje o audycie poza granice organizacji.

Zabezpieczenia powiązane: AU-3, AU-6, AU-7, CA-3, IA-2, IA-4, IA-5, IA-8, IR-4, PT-7, SI-4.

Zabezpieczenia rozszerzone:

(1) AUDYT MIĘDZYORGANIZACYJNY | OCHONA TOŻSAMOŚCI

Zachowaj tożsamość osób w ścieżkach audytu między organizacjami.

Zabezpieczenia powiązane: IA-2, IA-4, IA-5, IA-8.

(2) AUDYT MIĘDZYORGANIZACYJNY | UDOSTĘPNIANIE INFORMACJI AUDYTOWYCH

Dostarczaj informacji o audycie międzyorganizacyjnym do [Realizacja: organizacyjnie zdefiniowane organizacje udostępniające informacje audytowe] w oparciu o [Realizacja: umowy międzyorganizacyjne dotyczące udostępniania informacji audytowych].

Zabezpieczenia powiązane: IR-4, SI-4.

(3) AUDYT MIĘDZYORGANIZACYJNY |ODDZIELANIE DANYCH OSOBOWYCH

Wprowadź [Realizacja: środki określone przez organizację] w celu oddzielenia osób od informacji audytowych przekazywanych poza granice organizacji.

Zabezpieczenia powiązane: nie dotyczy.

KATEGORIA: CA – OCENA, AUTORYZACJA I MONITOROWANIE

CA-1 POLITYKA I PROCEDURY OCENY, AUTORYZACJI I MONITOROWANIA

Zabezpieczenie:

a. [Realizacja: personel lub role zdefiniowane przez organizację] opracowuje, dokumentuje i rozpowszechnia:

1. [Realizacja (jeden lub więcej): poziom organizacji, poziom procesów misji/biznesu, poziom systemu] politykę oceny, autoryzacji i monitorowania, która:

   (a) Dotyczy celu, zakresu, ról, obowiązków, zaangażowania kierownictwa, koordynacji między jednostkami organizacyjnymi i ich przestrzegania;

   (b) Jest zgodna z obowiązującymi przepisami prawa, zarządzeniami wykonawczymi, dyrektywami, regulacjami, politykami, standardami i wytycznymi;

2. Procedury umożliwiające wdrożenie polityki oceny, autoryzacji i monitorowania oraz powiązanych zabezpieczeń oceny, autoryzacji i monitorowania;

b. Wyznacz [Realizacja: wskazany przez organizację pracownik] do zarządzania rozwojem, dokumentowaniem oraz rozpowszechnianiem polityki oceny i udzielania zezwoleń, monitorowania, procedur;

c. Przeglądaj i aktualizuj bieżącą ocenę, autoryzacji i monitorowania:

   1. Polityki [Realizacja: częstotliwość określona przez organizację] i następne [Realizacja: zdarzenia zdefiniowane przez organizację];

   2. Procedur [Realizacja: częstotliwość określona przez organizację] i kolejne [Realizacja: zdarzenia zdefiniowane przez organizację].

Zabezpieczenia powiązane: PM-9, PS-8, SI-12.

Zabezpieczenia rozszerzone: nie dotyczy.

CA-2 OCENA MECHANIZMÓW KONTROLNYCH

Zabezpieczenie:

a. Wybieraj odpowiedniego oceniającego lub zespół oceniający dla danego typu oceny;

b. Opracowuj plan oceny mechanizmów kontrolnych, który opisuje zakres oceny, w tym:

   1. Mechanizmy kontrolne i rozszerzenia mechanizmów kontrolnych podlegające ocenie;

   2. Procedury oceny stosowane do określenia skuteczności mechanizmów kontrolnych;

   3. Środowisko oceny, zespół oceniający oraz role i obowiązki związane z oceną;

c. Zapewniaj, że plan oceny mechanizmów kontrolnych jest przeglądany i zatwierdzany przez administratora autoryzującego lub wyznaczonego przedstawiciela przed przeprowadzeniem oceny;

d. Oceniaj mechanizmy kontrolne w systemie i jego środowisku operacyjnym [*Realizacja: częstotliwość określona przez organizację*] w celu określenia zakresu, w jakim mechanizmy kontrolne są prawidłowo wdrożone, działają zgodnie z zamierzeniami i dają pożądane rezultaty w odniesieniu do spełnienia ustalonych wymagań bezpieczeństwa i prywatności;

e. Wykonuj raport z oceny mechanizmów kontrolnych dokumentujący wyniki oceny;

f. Przekazuj wyniki oceny mechanizmów kontrolnych [Realizacja: osobom lub rolom zdefiniowanym przez organizację].

Zabezpieczenia powiązane: AC-20, CA-5, CA-6, CA-7, PE-3, PM-9, RA-5, RA-10, SA-4, SA-11, SC-38, SI-2, SI-3, SI-12, SR-2, SR-3.

Zabezpieczenia rozszerzone:

(1) OCENA MECHANIZMÓW KONTROLNYCH | NIEZALEŻNI OCENIAJĄCY

Zatrudnij niezależnych oceniających lub zespoły oceniające do przeprowadzania ocen mechanizmów kontrolnych.

Zabezpieczenia powiązane: nie dotyczy.

Zabezpieczenia rozszerzone: nie dotyczy.

(2) OCENA MECHANIZMÓW KONTROLNYCH | OCENY SPECJALISTYCZNE

Uwzględnij jako część ocen mechanizmów kontrolnych, [Realizacja: częstotliwość określona przez organizację], [Realizacja: zapowiedziane, niezapowiedziane], [Wybór (jeden lub więcej): szczegółowe monitorowanie, oprzyrządowanie bezpieczeństwa, automatyczne przypadki testowe bezpieczeństwa, skanowanie podatności, testowanie złośliwych użytkowników, ocena zagrożeń wewnętrznych, testowanie wydajności i obciążenia, ocena wycieku lub utraty danych, [Realizacja: inne formy oceny zdefiniowane przez organizację]].

Zabezpieczenia powiązane: PE-3, SI-2

Zabezpieczenia rozszerzone: nie dotyczy.

(3) OCENA MECHANIZMÓW KONTROLNYCH | WYKORZYSTANIE WYNIKÓW Z ORGANIZACJI ZEWNĘTRZNYCH

Wykorzystaj wyniki ocen mechanizmów kontrolnych wykonanych przez [Realizacja: organizację zewnętrzną zdefiniowaną przez organizację] na [Realizacja: systemie zdefiniowanym przez organizację], gdy ocena spełnia [Realizacja: wymagania zdefiniowane przez organizację].

Zabezpieczenia powiązane: SA-4

Zabezpieczenia rozszerzone: nie dotyczy.

CA-3 WYMIANA INFORMACJI

Zabezpieczenie:

a. Zatwierdzaj i zarządzaj wymianą informacji między systemem a innymi systemami przy użyciu [Wybór (jeden lub więcej): umowy bezpieczeństwa połączeń, umowy bezpieczeństwa wymiany

informacji, protokoły ustaleń lub porozumienia, umowy o poziomie usług, umowy użytkownika, umowy o zachowaniu poufności, [Realizacja: typ umowy zdefiniowany przez organizację]];

b. Dokumentuj jako część każdej umowy o wymianie, charakterystykę interfejsu, wymagania bezpieczeństwa i prywatności, mechanizmy kontrolne i obowiązki dla każdego systemu oraz poziom wpływu przekazywanych informacji; oraz

c. Przeglądaj i aktualizuj umowy [Realizacja: częstotliwość określona przez organizację].

Zabezpieczenia powiązane: AC-2, AC-3, AC-4, AC-20, AU-16, CA-6, IA-3, IR-4, PL-2, PT-7, RA-3, SA-9, SC-7, SI-12.

Zabezpieczenia rozszerzone:

(1) POŁĄCZENIA MIĘDZYSTEMOWE | NIEKLASYFIKOWANE POŁĄCZENIA SYSTEMÓW BEZPIECZEŃSTWA NARODOWEGO

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(2) POŁĄCZENIA MIĘDZYSTEMOWE | KLASYFIKOWANE POŁĄCZENIA SYSTEMÓW BEZPIECZEŃSTWA NARODOWEGO

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(3) POŁĄCZENIA MIĘDZYSTEMOWE | NIEKLASYFIKOWANE POŁĄCZENIA SYSTEMÓW NIEBĘDĄCYCH SYSTEMAMI BEZPIECZEŃSTWA NARODOWEGO

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(4) POŁĄCZENIA MIĘDZYSTEMOWE | POŁĄCZENIA Z SIECIAMI PUBLICZNYMI

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(5) POŁĄCZENIA MIĘDZYSTEMOWE | OGRANICZENIA DOTYCZĄCE POŁĄCZEŃ Z SYSTEMAMI ZEWNĘTRZNYMI

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(6) WYMIANA INFORMACJI | AUTORYZACJE TRANSFERU

Zweryfikuj, czy osoby lub systemy przesyłające dane między połączonymi systemami posiadają wymagane uprawnienia (tj. prawa do zapisu lub odpowiednie przywileje) przed akceptacją tych danych.

Zabezpieczenia powiązane: AC-2, AC-3, AC-4.

Zabezpieczenia rozszerzone: nie dotyczy.

(7) WYMIANA INFORMACJI | POŚREDNIE WYMIANY INFORMACJI

a. Zidentyfikuj pośrednie (przekazywane dalej) wymiany informacji z innymi systemami poprzez systemy określone w *CA-3a*;

b. Podejmij działania zapewniające, że pośrednia (przekazywana dalej) wymiana informacji zostanie zatrzymana, gdy nie można zweryfikować lub zatwierdzić mechanizmów kontrolnych w zidentyfikowanych systemach pośrednich (przekazujących dane dalej).

Zabezpieczenia powiązane: SC-7

Zabezpieczenia rozszerzone: nie dotyczy.

CA-4 CERTYFIKACJA BEZPIECZEŃSTWA

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

CA-5 PLAN DZIAŁANIA I KAMIENIE MILOWE

Zabezpieczenie:

a. Opracuj plan działań i kamienie milowe dla systemu w celu udokumentowania planowanych działania naprawcze organizacji mające na celu skorygowanie słabości lub braków zauważonych podczas oceny kontroli oraz zmniejszenie lub wyeliminowanie znanych luk w zabezpieczeniach systemu;

b. Zaktualizuj istniejący plan działania i kamienie milowe [Realizacja: częstotliwość zdefiniowana przez organizację] w oparciu o ustalenia z ocen kontrolnych, niezależnych audytów lub przeglądów oraz ciągłych działań monitorujących.

Zabezpieczenia powiązane: CA-2, CA-7, PM-4, PM-9, RA-7, SI-2, SI-12

Zabezpieczenia rozszerzone:

(1) PLAN DZIAŁANIA I KAMIENIE MILOWE | WSPARCIE AUTOMATYZACJI DLA DOKŁADNOŚCI I AKTUALNOŚCI

Zapewnij dokładność, aktualność i dostępność planu działania i celów pośrednich dla systemu przy użyciu [Realizacja: zdefiniowane przez organizację mechanizmy automatyczne].

Zabezpieczenia powiązane: AC-2, AC-3, AC-4.

Zabezpieczenia rozszerzone: nie dotyczy.

CA-6 AUTORYZACJA

Zabezpieczenie:

a. Wyznacz osobę z wyższymi kompetencjami jako administratora autoryzującego dla systemu;

b. Wyznacz osobę z wyższymi kompetencjami jako administratora autoryzującego dla wspólnych mechanizmów kontrolnych dostępnych do dziedziczenia przez systemy organizacji;

c. Zapewnij, aby administrator autoryzujący system, przed rozpoczęciem działań:

d. Zaakceptował wykorzystanie wspólnych mechanizmów kontrolnych dziedziczonych przez system;

e. Autoryzował działanie systemu;

f. Zapewnij, aby administrator autoryzujący wspólne mechanizmy kontrolne autoryzował użycie tych mechanizmów do dziedziczenia przez systemy organizacji;

g. Aktualizuj autoryzacje [*Realizacja:* częstotliwość określona przez organizację].

Zabezpieczenia powiązane: AC-6, CA-2, CA-3, CA-7, PM-9, PM-10, RA-3, SA-10, SI-12

Zabezpieczenia rozszerzone:

(1) AUTORYZACJA |WSPÓLNA AUTORYZACJA – WEWNĄTRZORGANIZACYJNA

Zastosuj wspólny proces autoryzacji dla systemu, który obejmuje wielu administratorów bezpieczeństwa z tej samej organizacji przeprowadzających autoryzację.

Zabezpieczenia powiązane: AC-6

Zabezpieczenia rozszerzone: nie dotyczy.

(2) AUTORYZACJA | WSPÓLNA AUTORYZACJA – MIĘDZYORGANIZACYJNA

Zastosuj wspólny proces autoryzacji dla systemu, który obejmuje wielu administratorów bezpieczeństwa, z których co najmniej jeden administrator bezpieczeństwa pochodzi z organizacji zewnętrznej względem organizacji przeprowadzającej autoryzację.

Zabezpieczenia powiązane: AC-6

Zabezpieczenia rozszerzone: nie dotyczy.

CA-7 MONITOROWANIE CIĄGŁE

Zabezpieczenie:

Opracuj strategię monitorowania ciągłego na poziomie systemu i wdrażaj monitorowanie ciągłe zgodnie ze strategią monitorowania ciągłego na poziomie organizacji, która obejmuje:

a. Ustanowienie następujących metryk na poziomie systemu do monitorowania: [Realizacja: metryki na poziomie systemu zdefiniowane przez organizację];

b. Ustanowienie [Realizacja: częstotliwości zdefiniowane przez organizację] dla monitorowania i [Realizacja: częstotliwości zdefiniowane przez organizację] dla oceny skuteczności mechanizmów kontrolnych;

c. Bieżące oceny mechanizmów kontrolnych zgodnie ze strategią monitorowania ciągłego;

d. Bieżące monitorowanie systemu i metryk zdefiniowanych przez organizację zgodnie ze strategią monitorowania ciągłego;

e. Korelację i analizę informacji generowanych przez oceny mechanizmów kontrolnych i monitorowanie;

f. Działania naprawcze w celu rozwiązania wyników analizy informacji z oceny mechanizmów kontrolnych i monitorowania;

g. Raportowanie stanu bezpieczeństwa i prywatności systemu do [Realizacja: personel lub role zdefiniowane przez organizację] [Realizacja: częstotliwość określona przez organizację].

Zabezpieczenia powiązane: AC-2, AC-6, AC-17, AT-4, AU-6, AU-13, CA-2, CA-5, CA-6, CM-3, CM-4, CM-6, CM-11, IA-5, IR-5, MA-2, MA-3, MA-4, PE-3, PE-6, PE-14, PE-16, PE-20, PL-2, PM-4, PM-6, PM-9, PM-10, PM-12, PM-14, PM-23, PM-28, PM-31, PS-7, PT-7, RA-3, RA-5, RA-7, RA-10, SA-8, SA-9, SA-11, SC-5, SC-7, SC-18, SC-38, SC-43, SI-3, SI-4, SI-12, SR-6.

Zabezpieczenia rozszerzone:

(1) MONITOROWANIE CIĄGŁE | NIEZALEŻNA OCENA

Zatrudnij niezależnych oceniających lub zespoły oceniające do ciągłego monitorowania mechanizmów kontrolnych w systemie.

Zabezpieczenia powiązane: nie dotyczy.

(2) MONITOROWANIE CIĄGŁE | RODZAJE OCEN

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(3) MONITOROWANIE CIĄGŁE | ANALIZY TRENDÓW

Zastosuj analizy trendów, aby określić, czy implementacje mechanizmów kontrolnych, częstotliwość działań monitorowania ciągłego oraz rodzaje działań używanych w procesie monitorowania ciągłego wymagają modyfikacji w oparciu o dane empiryczne.

Zabezpieczenia powiązane: nie dotyczy.

(4) MONITOROWANIE CIĄGŁE | MONITOROWANIE RYZYKA

Zapewnij, aby monitorowanie ryzyka było integralną częścią strategii ciągłego monitorowania, która obejmuje:

a. Monitorowanie efektywności;

b. Monitorowanie zgodności; oraz

c. Monitorowanie zmian.

Zabezpieczenia powiązane: nie dotyczy.

(5) MONITOROWANIE CIĄGŁE | ANALIZA SPÓJNOŚCI

Zastosuj następujące działania, aby potwierdzić, że polityki są ustalone, a wdrożone mechanizmy kontrolne działają w spójny sposób: [Realizacja*:* działania zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(6) MONITOROWANIE CIĄGŁE | WSPARCIE AUTOMATYZACJI DLA MONITOROWANIA

Zapewnij dokładność, aktualność i dostępność wyników monitorowania systemu przy użyciu [Realizacja*:* zdefiniowane przez organizację mechanizmy automatyczne].

Zabezpieczenia powiązane: nie dotyczy.

Zabezpieczenia rozszerzone: CA-8(1), CA-8(2), CA-8(3).

CA-8 TESTY PENETRACYJNE

Zabezpieczenie:

Przeprowadź testy penetracyjne [*Zadanie:* częstotliwość określona przez organizację] na [*Zadanie:* systemy lub komponenty systemu zdefiniowane przez organizację].

Zabezpieczenia powiązane: CA-2, PE-3, RA-5, RA-10, SA-11, SR-5, SR-6.

Zabezpieczenia rozszerzone: nie dotyczy.

(1) TESTY PENETRACYJNE | NIEZALEŻNY AGENT LUB ZESPÓŁ TESTÓW PENETRACYJNYCH

Zatrudnij niezależnego testera lub zespół testów penetracyjnych do przeprowadzenia testów penetracyjnych systemu lub komponentów systemu.

Zabezpieczenia powiązane: CA-2

Zabezpieczenia rozszerzone: nie dotyczy.

(2) TESTY PENETRACYJNE | ĆWICZENIA RED TEAM

Zastosuj następujące ćwiczenia „red team” do symulacji prób naruszenia systemów organizacji przez przeciwników zgodnie z obowiązującymi zasadami zaangażowania: [Realizacja: ćwiczenia zespołu czerwonego zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

Zabezpieczenia rozszerzone: nie dotyczy.

(3) TESTY PENETRACYJNE | TESTY PENETRACYJNE OBIEKTU

Zastosuj proces testów penetracyjnych, który obejmuje [Zadanie: częstotliwość określona przez organizację] [Realizacja: zapowiedziane, niezapowiedziane] próby obejścia lub ominięcia mechanizmów kontrolnych związanych z punktami fizycznego dostępu do obiektu.

Zabezpieczenia powiązane: CA-2, PE-3

Zabezpieczenia rozszerzone: nie dotyczy.

CA-9 POŁĄCZENIA WEWNĘTRZNE SYSTEMU

Zabezpieczenie:

a. Autoryzuj wewnętrzne połączenia [Realizacja*:* komponenty systemu lub klasy komponentów zdefiniowane przez organizację] do systemu;

b. Dokumentuj, dla każdego połączenia wewnętrznego, charakterystykę interfejsu, wymagania bezpieczeństwa i prywatności oraz charakter przekazywanych informacji;

c. Zakończ połączenia wewnętrzne systemu po [Realizacja: warunki zdefiniowane przez organizację]; oraz

d. Przeglądaj [Realizacja: częstotliwość określona przez organizację] ciągłą potrzebę każdego połączenia wewnętrznego

Zabezpieczenia powiązane: AC-3, AC-4, AC-18, AC-19, CM-2, CM-6, IA-3, SC-7, SI-12

Zabezpieczenia rozszerzone:

(1) POŁĄCZENIA WEWNĘTRZNE SYSTEMU | KONTROLE ZGODNOŚCI

Przeprowadź kontrole zgodności bezpieczeństwa i prywatności na składowych komponentach systemu przed ustanowieniem połączenia wewnętrznego.

Zabezpieczenia powiązane: CM-6

Zabezpieczenia rozszerzone: nie dotyczy.

KATEGORIA: CM - ZARZĄDZANIE KONFIGURACJĄ

CM-1 POLITYKA I PROCEDURY

Zabezpieczenie:

a. Opracowuj, dokumentuj i rozpowszechniaj wśród [Realizacja: personel lub role określone przez organizację]:

   1. [Wybór (jeden lub więcej): poziom organizacji; poziom misji/procesu biznesowego; poziom systemu] polityki zarządzania konfiguracją, która:

      (a) Adresuje cel, zakres, role, obowiązki, zaangażowanie kierownictwa, koordynację między jednostkami organizacyjnymi i zgodność z przepisami;

      (b) Jest zgodna z obowiązującym prawem, rozporządzeniami, dyrektywami**,** przepisami, zasadami, standardami i wytycznymi;

   2. Procedur ułatwiających realizację polityki w zakresie zarządzania konfiguracją oraz powiązanych ocen w zakresie zarządzania konfiguracją;

b. Wyznaczaj [Realizacja: osoba wyznaczona przez organizację] do zarządzania rozwojem, dokumentacją i rozpowszechnianiem polityki i procedur zarządzania konfiguracją;

c. Przeglądaj i aktualizuj na bieżąco:

   1. Polityki zarządzania konfiguracją z [Realizacja: częstotliwość określona przez organizację] i następujących [Realizacja: zdarzenia określone przez organizację];

   2. Procedury zarządzania konfiguracją z [Realizacja: częstotliwość określona przez organizację] i następujących [Realizacja: zdarzenia określone przez organizację]**.**

Zabezpieczenia powiązane: PM-9, PS-8, SA-8, SI-12.

Zabezpieczenia rozszerzone: Nie dotyczy.

CM-2 KONFIGURACJA BAZOWA

Zabezpieczenie:

a. Opracowuj, udokumentuj i utrzymuj pod kontrolą bieżącą konfigurację bazową systemu;

b. Przeglądaj i aktualizuj konfigurację bazową systemu:

   1. [Realizacja: częstotliwość określona przez organizację];

   2. Jeżeli jest to wymagane ze względu na [Realizacja: okoliczności określone przez organizację];

   3. Podczas instalacji lub modernizacji komponentów systemu.

Zabezpieczenia powiązane: AC-19, AU-6, CA-9, CM-1, CM-3, CM-4, CM-5, CM-6, CM-7, CM-8, CM- 9, CP-9, CP-10, CP-12, IA-3, MA-2, MP-4, MP-5, PL-8, PM-5, RA-5, SA-8, SA-10, SA-15, SC-3, SC-7, SC-18.

Zabezpieczenia rozszerzone:

(1) KONFIGURACJA BAZOWA | PRZEGLĄDY I AKTUALIZACJE

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(2) KONFIGURACJA BAZOWA | AUTOMATYZACJA WSPIERAJĄCA AKTUALNOŚĆ /SZCZEGÓŁOWOŚĆ

Utrzymuj aktualność, kompletność, dokładność i dostępność konfiguracji bazowej systemu przy użyciu [*Realizacja: organizacyjnie zdefiniowane zautomatyzowane mechanizmy wspomagające*].

Zabezpieczenia powiązane: CM-7, IA-3, RA-5.

(3) KONFIGURACJA BAZOWA | RETENCJA ZACHOWANYCH KONFIGURACJI

Zachowaj [*Realizacja: liczba zdefiniowany przez organizację*] poprzednich wersji konfiguracji bazowych systemu w celu obsługi wycofanych wersji konfiguracji bazowych.

Zabezpieczenia powiązane: nie dotyczy.

(4) KONFIGURACJA BAZOWA | NIEAUTORYZOWANE OPROGRAMOWANIE

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(5) KONFIGURACJA BAZOWA | AUTORYZOWANE OPROGRAMOWANIE

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(6) KONFIGURACJA BAZOWA | ŚRODOWISKA PROGRAMISTYCZNE I TESTOWE

Utrzymuj konfigurację bazową do rozbudowy systemów i środowiska testowego, które są zarządzane niezależnie od operacyjnej konfiguracji bazowej.

Zabezpieczenia powiązane: CM-4, SC-3, SC-7.

(7) KONFIGURACJA BAZOWA | KONFIGURACJA SYSTEMÓW I KOMPONENTÓWW OBSZARACH WYSOKIEGO RYZYKA

a. Przydzielaj [Realizacja: systemy lub komponenty systemowe zdefiniowane przez organizację] z [Realizacja: konfiguracje zdefiniowane przez organizację] osobom udającym się do lokalizacji, które organizacja uważa za miejsca o istotnym ryzyku;

b. Zastosuj następujące zabezpieczenia w systemach lub komponentach będących w posiadaniu osób powracających z lokalizacji, które organizacja uważa za miejsca o istotnym ryzyku: [Realizacja: zabezpieczenia zdefiniowane przez organizację].

Zabezpieczenia powiązane: MP-4, MP-5.

CM-3 ZABEZPIECZANIE ZMIAN KONFIGURACJI

Zabezpieczenie:

a. Określ i dokumentuj rodzaje zmian w systemie, które są zabezpieczane konfiguracyjnie;

b. Dokonaj przeglądu proponowanych zmian konfiguracji zabezpieczeń w systemie i zatwierdzaj lub odrzucaj takich zmiany, z wyraźnym uwzględnieniem analizy wpływu na bezpieczeństwo systemu i prywatność;

c. Dokumentuj decyzje związane ze zmianą konfiguracji systemu;

d. Wprowadzaj zatwierdzone zmiany w zabezpieczeniach konfiguracji systemu;

e. Przechowuj wdrożone zapisy zmian w zabezpieczeniach systemu przez okres [Realizacja: okres czasu określony przez organizację];

f. Monitoruj i przeglądaj czynności związane z dokonywanymi zmianami w zabezpieczeniach konfiguracji systemu;

g. Koordynuj i nadzoruj działania związane z dokonywanymi zmianami w zabezpieczeniach konfiguracji przez [Realizacja: zdefiniowany przez organizację element zabezpieczeń zmian konfiguracyjnych], który wywołuje z [Wybór (jeden lub więcej)]: [Realizacja: częstotliwość zdefiniowana przez organizację]; występowanie [Realizacja: warunki zmiany konfiguracji zdefiniowanej przez organizację].

Zabezpieczenia powiązane: AU-6, AU-7, CA-7, CM-2, CM-3, CM-4, CM-5, CM-6, CM-9, CM-11, IA-3, MA-2, PE-16, PT-6, RA-8, SA-8, SA-10, S.C.-12, SC-28, SC-34, SC-37, SI-2, SI-3, SI-4, SI-7, SI-10, SR-11.

Zabezpieczenia rozszerzone:

(1) ZABEZPIECZENIE ZMIAN KONFIGURACJI | AUTOMATYCZNA DOKUMENTACJA / POWIADAMIANIE / ZAKAZWPROWADZANIA ZMIAN

Stosuj [Realizacja: mechanizmy automatyczne zdefiniowane przez organizację] do:

a. Dokumentowania proponowanych zmian w systemie;

b. Powiadamiania [Realizacja: określone przez organizację organy zatwierdzające] o proponowanych zmianach w systemie i zażądanie zatwierdzenia zmian;

c. Wskazania proponowanych zmian w systemie, które nie zostały zatwierdzone lub odrzucone w ciągu [Realizacja: okres czasu określony przez organizację];

d. Zakazywania wprowadzania zmian w systemie do czasu otrzymania stosownych akceptacji;

e. Dokumentowania wszystkich zmian w systemie;

f. Powiadamiania [Realizacja: personel zdefiniowany przez organizację] o zakończeniu wprowadzania zatwierdzonych zmian w systemie.

Zabezpieczenia powiązane: nie dotyczy.

(2) ZABEZPIECZENIE ZMIAN KONFIGURACJI | TESTY, WALIDACJA I ZMIANY DOKUMENTÓW

Testuj, zatwierdzaj i dokumentuj zmiany w systemie przed ich wdrożeniem.

Zabezpieczenia powiązane: nie dotyczy.

(3) ZABEZPIECZENIE ZMIAN KONFIGURACJI | AUTOMATYCZNE WPROWADZANIE ZMIAN

Implementuj zmiany w aktualnej bazie systemu i wdrożenie uaktualnionej konfiguracji bazowej w zainstalowanej bazie za pomocą [Realizacja: automatyczne mechanizmy zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(4) ZABEZPIECZENIE ZMIAN KONFIGURACJI | FUNKCYJNI DS. BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

Wymagaj, aby [Realizacja: zdefiniowani przez organizację przedstawiciele ds. bezpieczeństwa i ochrony prywatności], byli członkami [Realizacja: zdefiniowany przez organizację zespół zabezpieczeń zmiany konfiguracji].

Zabezpieczenia powiązane: nie dotyczy.

(5) ZABEZPIECZANIE ZMIAN KONFIGURACJI | AUTOMATYCZNA REAKCJA BEZPIECZEŃSTWA

Implementuj następujące automatyczne reakcje środków bezpieczeństwa na nieautoryzowane zmiany konfiguracji bazowych: [Realizacja: reakcje środków bezpieczeństwa zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(6) ZABEZPIECZENIE ZMIAN KONFIGURACJI | ZARZĄDZANIE KRYPTOGRAFICZNE

Zapewnij, że mechanizmy kryptograficzne używane do zapewnienia [Realizacja: środki bezpieczeństwa zdefiniowane przez organizację] podlegają zarządzaniu konfiguracji.

Zabezpieczenia powiązane: SC-12.

(7) ZABEZPIECZENIE ZMIAN KONFIGURACJI | PRZEGLĄD ZMIAN W SYSTEMIE

Przeglądaj zmiany w systemie z [Realizacja: częstotliwość zdefiniowana przez organizację] lub wystąpienia [Realizacja: okoliczności zdefiniowane przez organizację] w celu ustalenia, czy wystąpiły nieautoryzowane zmiany.

Zabezpieczenia powiązane: AU-6, AU-7, CM-3.

(8) ZABEZPIECZANIE ZMIAN KONFIGURACJI | ZAPOBIEGANIE LUB OGRANICZANIE ZMIAN KONFIGURACJI

Zapobiegaj lub ograniczaj zmiany w konfiguracji systemu w następujących okolicznościach: [Realizacja: okoliczności zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

CM-4 ANALIZY WPŁYWU

Zabezpieczenie:

Analizuj zmiany w systemie w celu określenia potencjalnego wpływu na bezpieczeństwo i prywatność przed wprowadzeniem zmian.

Zabezpieczenia powiązane: CA-7, CM-3, CM-8, CM-9, MA-2, RA-3, RA-5, RA-8, SA-5, SA-8, SA-10, SA-11, S.C.-3, SC-7, SI-2, SI-6.

Zabezpieczenia rozszerzone:

(1) ANALIZY WPŁYWU | ODDZIELNE ŚRODOWISKA BADAWCZE

Analizuj zmiany w systemie w oddzielnym środowisku testowym przed ich wdrożeniem w środowisku operacyjnym, zwracając uwagę na wpływ na bezpieczeństwo i prywatność z powodu wad, słabości, niekompatybilności lub celowego złośliwego działania.

Zabezpieczenia powiązane: SA-11, SC-7.

(2) ANALIZY WPŁYWU | WERYFIKACJA ZABEZPIECZEŃ

Po dokonaniu zmian w systemie, sprawdzaj, czy zabezpieczenie jest wdrożone prawidłowo, działa zgodnie z założeniami i przynosi pożądany rezultat w odniesieniu do spełnienia wymogów bezpieczeństwa i ochrony prywatności systemu.

Zabezpieczenia powiązane: SA-11, SC-3, SI-6.

CM-5 OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN

Zabezpieczenie:

Definiuj, dokumentuj, zatwierdzanie i egzekwowanie fizycznych i logicznych ograniczeń dostępu związanych ze zmianami w systemie.

Zabezpieczenia powiązane: AC-2, AC-3, AC-5, AC-6, AU-2, AU-6, AU-7, AU-12, CM-3, CM-6, CM-9, CM-11, PE-3, SC-28, SC-34, SC-37, SI-2, SI-10, SI-12.

Zabezpieczenia rozszerzone:

(1) OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN | AUTOMATYCZNE EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU I ZAPISY Z AUDYTU

a. Egzekwuj ograniczenia dostępu przy użyciu [Realizacja: automatyczne mechanizmy zdefiniowane przez organizację];

b. Automatycznie generuj zapisy z audytu działań wykonawczych.

Zabezpieczenia powiązane: AU-2, AU-6, AU-7, AU-12, CM-6, CM-11, SI-12.

(2) OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN | PRZEGLĄD ZMIAN W SYSTEMIE

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(3) OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN | PODPISANE KOMPONENTY

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(4) OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN | PODWÓJNA AUTORYZACJA

Egzekwuj podwójną autoryzację do wprowadzania zmian w [Realizacja: zdefiniowane przez organizacje komponenty systemu i informacje na poziomie systemu].

Zabezpieczenia powiązane: AC-2, AC-5, CM-3.

(5) OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN | OGRANICZANIE PRZYWILEJÓW W ZAKRESIE WYTWARZANIA I EKSPLOATACJI

a. Ograniczaj uprawnienia do zmiany komponentów systemu i informacji związanych z systemem w ramach środowiska produkcyjnego lub operacyjnego;

b. Przeglądaj i ponownie oceniaj uprawnienia [Realizacja: częstotliwość określona przez organizację].

Zabezpieczenia powiązane: AC-2.

(6) OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN | OGRANICZANIE PRZYWILEJÓW W BIBLIOTEKACH OPROGRAMOWANIA

Ograniczaj uprawnienia do zmiany oprogramowania rezydenta w bibliotekach oprogramowania.

Zabezpieczenia powiązane: AC-2.

(7) OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN | AUTOMATYCZNE WDRAŻANIE ŚRODKÓW BEZPIECZEŃSTWA

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

CM-6 USTAWIENIA KONFIGURACJI

Zabezpieczenie:

a. Ustalaj i dokumentuj ustawienia konfiguracyjne komponentów stosowanych w systemie, które odzwierciedlają najbardziej restrykcyjny tryb zgodny z wymogami operacyjnymi, korzystając z [Realizacja: listy kontrolne konfiguracji zabezpieczeń zdefiniowane przez organizację];

b. Implementuj ustawienia konfiguracyjne;

c. Określaj, dokumentuj i zatwierdzaj wszelkie odstępstwa od ustalonych ustawień konfiguracyjnych dla [Realizacja: zdefiniowane przez organizację komponenty systemu] w oparciu o [Realizacja: zdefiniowane przez organizację wymagania operacyjne];

d. Monitoruj i zabezpieczaj zmiany w ustawieniach konfiguracyjnych zgodnie z zasadami i procedurami organizacji.

Zabezpieczenia powiązane: AC-3, AC-19, AU-2, AU-6, CA-9, CM-2, CM-3, CM-5, CM-7, CM-11, CP-7, CP-9, CP-10, IA-3, IA-5, PL-8, PL-9, RA-5, SA-4, SA-5, SA-8, SA-9, SC-18, SC-28, SC-43, SI-2, SI-4, SI-6.

Zabezpieczenia rozszerzone:

(1) USTAWIENIA KONFIGURACJI | AUTOMATYCZNE ZARZĄDZANIE, STOSOWANIE I WERYFIKACJA

Zarządzaj, realizuj i weryfikuj ustawienia konfiguracyjne dla [Realizacja: zdefiniowane przez organizację komponenty systemu] za pomocą [Realizacja: zdefiniowane przez organizację automatyczne mechanizmy].

Zabezpieczenia powiązane: CA-7.

(2) USTAWIENIA KONFIGURACJI | ODPOWIEDŹ NA NIEAUTORYZOWANE ZMIANY

W odpowiedzi na nieautoryzowane zmiany w [Realizacja: ustawienia konfiguracyjne zdefiniowane przez organizację] wykonuj następujące czynności: [Realizacja: ustawienia konfiguracyjne zdefiniowane przez organizację]: [Realizacja: działania zdefiniowane przez organizację].

Zabezpieczenia powiązane: IR-4, IR-6, SI-7.

(3) USTAWIENIA KONFIGURACJI | WYKRYWANIE NIEAUTORYZOWANYCH ZMIAN

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(4) USTAWIENIA KONFIGURACJI | PREZENTACJA ZGODNOŚCI

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

CM-7 ZASADA MINIMALNEJ FUNKCJONALNOŚCI

Zabezpieczenie:

a. Skonfiguruj system tak, aby zapewniał tylko [Realizacja: niezbędne wymagane funkcje];

b. Zakaż lub ogranicz korzystanie z następujących funkcji, portów, protokołów, oprogramowania i/lub usług: [Realizacja: zdefiniowane przez organizację zabronione lub ograniczone funkcje, porty systemowe, protokoły, oprogramowanie i/lub usługi].

Zabezpieczenia powiązane: AC-3, AC-4, CM-2, CM-5, CM-6, CM-11, RA-5, SA-4, SA-5, SA-8, SA-9, SA-15, SC2, SC-3, SC-7, SC-37, SI-4.

Zabezpieczenia rozszerzone:

(1) ZASADA MINIMALNEJ FUNKCJONALNOŚCI | PRZEGLĄDY OKRESOWE

a. Przeglądaj system [Realizacja: częstotliwość określona przez organizację] w celu zidentyfikowania niepożądanych i/lub niezabezpieczonych funkcji, portów, protokołów, oprogramowania i usług;

b. Wyłącz lub usuń [Realizacja: funkcje zdefiniowane przez organizację, porty, protokoły, oprogramowanie i usługi w ramach systemu uznane za niepożądane i/lub niezabezpieczone].

Zabezpieczenia powiązane: AC-18.

(2) ZASADA MINIMALNEJ FUNKCJONALNOŚCI | ZAPOBIEGANIA WYKONYWANIU PROGRAMU

Zapobiegaj wykonywaniu programu zgodnie z [Wybór (jeden lub więcej): [Realizacja: zasady określone przez organizację, zasady zachowania i/lub umowy dostępu dotyczące użytkowania i ograniczeń w użytkowaniu oprogramowania]; zasady autoryzujące warunki użytkowania oprogramowania].

Zabezpieczenia powiązane: CM-8, PL-4, PL-9, PM-5, PS-6.

(3) ZASADA MINIMALNEJ FUNKCJONALNOŚCI | STOSOWANIE REJESTRACJI

Zapewnij zgodność z [Realizacja: określone przez organizację wymagania rejestracyjne dla funkcji, portów, protokołów i usług].

Zabezpieczenia powiązane: nie dotyczy.

(4) ZASADA MINIMALNEJ FUNKCJONALNOŚCI | NIEAUTORYZOWANE OPROGRAMOWANIE („CZARNA LISTA”)

a. Zidentyfikuj [Realizacja: programy zdefiniowane przez organizację, które nie są uprawnione do wykonywania w systemie];

b. Stosuj polityki „zezwalaj na wszystko za wyjątkiem” (ang. "allow-all, deny-by-exception") w celu zakazania wykonywania nieautoryzowanych programów w systemie;

c. Przeglądaj i aktualizuj listy nieautoryzowanych programów [Realizacja: częstotliwość zdefiniowana przez organizację].

Zabezpieczenia powiązane: CM-6, CM-8, CM-10, PL-9, PM-5.

(5) ZASADA MINIMALNEJ FUNKCJONALNOŚCI | AUTORYZOWANE OPROGRAMOWANIE („BIAŁA LISTA")

a. Zidentyfikuj [Realizacja: programy zdefiniowane przez organizację uprawnione do zainstalowania w systemie];

b. Stosuj zasady „odmawiaj wszystkiego za wyjątkiem" (ang. "deny-all", "permit-by-exception"), aby umożliwić wykonanie autoryzowanych programów w systemie;

c. Przeglądaj i aktualizuj listy autoryzowanych programów [Realizacja: częstotliwość zdefiniowana przez organizację].

Zabezpieczenia powiązane: CM-2, CM-6, CM-8, CM-10, PL-9, PM-5, SA-10, SC-34, SI-7.

(6) ZASADA MINIMALNEJ FUNKCJONALNOŚCI | ZAMKNIĘTE ŚRODOWISKA Z OGRANICZONYMI UPRAWNIENIAMI

Wymagaj, aby poniższe oprogramowanie zainstalowane przez użytkownika było uruchamiane w ograniczonym fizycznym lub wirtualnym środowisku urządzenia z limitowanymi uprawnieniami: [Realizacja: oprogramowanie zainstalowane przez użytkownika, zdefiniowane przez organizację].

Zabezpieczenia powiązane: CM-11, SC-44.

(7) ZASADA MINIMALNEJ FUNKCJONALNOŚCI | WYKONYWANIE KODU W CHRONIONYCH ŚRODOWISKACH

Zezwalaj na wykonanie kodu binarnego lub maszynowego tylko w ograniczonym fizycznym lub wirtualnym środowisku urządzenia i za jednoznacznym zatwierdzeniem [Realizacja: personel lub role określone przez organizację], gdy taki kod jest:

a. Uzyskany ze źródeł z ograniczonym zaufaniem lub niezaufanych;

b. Bez podania kodu źródłowego.

Zabezpieczenia powiązane: CM-10, SC-44.

(8) ZASADA MINIMALNEJ FUNKCJONALNOŚCI | KOD BINARNY LUB KOD WYKONYWALNY (MOBILNY)

a. Zakazuj używanie kodu binarnego lub maszynowego ze źródeł z ograniczonym zaufaniem lub niezaufanych lub bez podania kodu źródłowego;

b. Zezwalaj na wyjątki tylko w przypadku istotnych wymogów dotyczących misji lub operacji oraz za zgodą osoby autoryzującej (ang. authorizing offcial – AO).

Zabezpieczenia powiązane: SA-5, SA-22.

(9) ZASADA MINIMALNEJ FUNKCJONALNOŚCI | ZAKAZ UŻYWANIA NIEAUTORYZOWANEGO SPRZĘTU

a. Zidentyfikuj [Realizacja: zdefiniowane przez organizację komponenty sprzętowe dopuszczone do eksploatacji w systemie];

b. Zakazuj używania lub podłączania nieautoryzowanych komponentów sprzętowych;

c. Przeglądaj i aktualizuj listy autoryzowanych komponentów sprzętowych [Realizacja: częstotliwość zdefiniowana przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

CM-8 INWENTARYZACJA KOMPONENTÓW SYSTEMU

Zabezpieczenie:

a. Opracuj i udokumentuj inwentaryzację komponentów systemu, która:

   1. Dokładnie odzwierciedla system;

   2. Zawiera wszystkie komponenty systemu;

   3. Nie obejmuje podwójnego księgowania tych samych komponentów lub komponentów przypisanych do jakiegokolwiek innego systemu;

   4. Jest na poziomie szczegółowości uznanym za niezbędny do śledzenia i raportowania;

   5. Zawiera następujące informacje umożliwiające rozliczalność komponentów systemu: [Realizacja: informacje zdefiniowane przez organizację uznane za niezbędne do osiągnięcia skutecznej rozliczalności komponentów systemu teleinformatycznego];

b. Przeglądaj i aktualizuj spisu komponentów systemu [Realizacja: częstotliwość określona przez organizację].

Zabezpieczenia powiązane: CM-2, CM-7, CM-9, CM-10, CM-11, CM-13, CP-2, CP-9, MA-2, MA-6, PE-20, PL-9, PM-5, SA-4, SA-5, SI-2, SR-4.

Zabezpieczenia rozszerzone:

(1) INWENTARYZACJA KOMPONENTÓW SYSTEMU | AKTUALIZACJE INSTALACJI I USUWANIA KOMPONENTÓW

Aktualizuj spis komponentów systemu w ramach instalacji, usuwania i aktualizacji komponentów systemu.

Zabezpieczenia powiązane: PM-16.

(2) INWENTARYZACJA KOMPONENTÓW SYSTEMU | AUTOMATYCZNA KONSERWACJA (UTRZYMYWANIE)

Utrzymuj aktualność, kompletność, dokładność i dostępność zapasów komponentów systemu przy użyciu [Realizacja: organizacyjnie zdefiniowane mechanizmy automatyczne].

Zabezpieczenia powiązane: nie dotyczy.

(3) INWENTARYZACJA KOMPONENTÓW SYSTEMU | AUTOMATYCZNE WYKRYWANIE KOMPONENTÓW NIEAUTORYZOWANYCH

a. Wykrywaj obecność nieautoryzowanego sprzętu, aplikacji oprogramowania układowego w systemie przy użyciu [Realizacja: mechanizmy automatyczne zdefiniowane przez organizację] [Realizacja: częstotliwość zdefiniowana przez organizację];

b. W przypadku wykrycia nieautoryzowanych komponentów podejmuj następujące działania: Wybór (jeden lub więcej): wyłączenie dostępu do sieci przez takie komponenty; odizolowanie komponentów; powiadomienie [Realizacja: personel lub role zdefiniowane przez organizację]].

Zabezpieczenia powiązane: AC-19, CA-7, RA-5, SC-3, SC-39, SC-44, SI-3, SI-4, SI-7.

(4) INWENTARYZACJA KOMPONENTÓW SYSTEMU | INFORMACJE DOTYCZĄCE ODPOWIEDZIALNOŚCI I ROZLICZALNOŚCI

Uwzględnij w spisie komponenty informacje o sposobie identyfikacji osób odpowiedzialnych za administrowanie tymi składnikami [Wybór (jeden lub więcej): imię i nazwisko; stanowisko; rola].

Zabezpieczenia powiązane: AC-3.

(5) INWENTARYZACJA KOMPONENTÓW SYSTEMU | BRAK DUPLIKACJI KOMPONENTÓW

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(6) INWENTARYZACJA KOMPONENTÓW SYSTEMU | OCENA KONFIGURACJI I ZATWIERDZONE ODSTĘPSTWA

Uwzględnij w spisie komponentów systemu konfigurację ocenianych komponentów oraz wszelkich zatwierdzonych odstępstw od aktualnie stosowanych konfiguracji.

Zabezpieczenia powiązane: nie dotyczy.

(7) INWENTARYZACJA KOMPONENTÓW SYSTEMU | SCENTRALIZOWANE REPOZYTORIUM

Zapewnij scentralizowane repozytorium spisu komponentów systemu.

Zabezpieczenia powiązane: nie dotyczy.

(8) INWENTARYZACJA KOMPONENTÓW SYSTEMU | AUTOMATYCZNE ŚLEDZENIE LOKALIZACJI

Wspieraj śledzenie komponentów systemu według lokalizacji geograficznej za pomocą [Realizacja: mechanizmy automatyczne zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(9) INWENTARYZACJA KOMPONENTÓW SYSTEMU | PRZYPISANIE KOMPONENTÓW DO SYSTEMÓW

a. Przypisuj posiadane komponenty do systemu;

b. Uzyskaj od [Realizacja: personel lub role określone przez organizację] potwierdzeń wykonania tego zadania.

Zabezpieczenia powiązane: nie dotyczy.

CM-9 PLAN ZARZĄDZANIA KONFIGURACJĄ

Zabezpieczenie:

Opracowuj, udokumentuj i wprowadź plan zarządzania konfiguracją systemu, który:

a. Adresuje role, obowiązki oraz procesy i procedury zarządzania konfiguracją;

b. Ustanawia proces identyfikacji elementów konfiguracji w całym cyklu życia systemu oraz zarządzania konfiguracją elementów konfiguracji;

c. Określa elementy konfiguracyjne systemu i włącza je do zarządzania konfiguracją;

d. Jest weryfikowany i zatwierdzany przez [Realizacja: personel lub role określone przez organizację];

e. Jest chroniony przed nieautoryzowanym ujawnieniem i modyfikacją.

Zabezpieczenia powiązane: CM-2, CM-3, CM-4, CM-5, CM-8, PL-2, RA-8, SA-10, SI-12.

Zabezpieczenia rozszerzone:

(1) PLAN ZARZĄDZANIA KONFIGURACJĄ | PRZYPISANIE ODPOWIEDZIALNOŚCI

Powierzaj odpowiedzialności za rozwój procesu zarządzania konfiguracją personelowi organizacyjnemu, który nie jest bezpośrednio zaangażowany w rozwój systemu.

Zabezpieczenia powiązane: nie dotyczy.

CM-10 OGRANICZENIA W UŻYCIU OPROGRAMOWANIA

Zabezpieczenie:

a. Korzystaj z oprogramowania i związanej z nim dokumentacji zgodnie z postanowieniami umownymi prawami autorskimi;

b. Śledź korzystanie z oprogramowania i związanej z nim dokumentacji chronionej licencjami ilościowymi w celu kontroli kopiowania i dystrybucji; oraz

c. Kontroluj i dokumentuj korzystanie z technologii wymiany plików w systemie „peer-to-peer" w celu zapewnienia, że funkcja ta nie jest wykorzystywana do nieautoryzowanego rozpowszechniania, wyświetlania, wykonywania lub reprodukcji utworów chronionych prawem autorskim.

Zabezpieczenia powiązane: AC-17, AU-6, CM-7, CM-8, PM-30, SC-7.

Zabezpieczenia rozszerzone:

(1) OGRANICZENIA W UŻYCIU OPROGRAMOWANIA | OPROGRAMOWANIE OTWARTE (OPEN-SOURCE)

Wprowadź następujące ograniczenia w korzystaniu z oprogramowania otwartego (typu „open-source"): [Realizacja: ograniczenia zdefiniowane przez organizację].

Zabezpieczenia powiązane: SI-7.

CM-11 OPROGRAMOWANIE INSTALOWANE PRZEZ UŻYTKOWNIKA

Zabezpieczenie:

a. Wprowadź [Realizacja: zasady zdefiniowane przez organizację] regulujące instalację oprogramowania przez użytkowników;

b. Egzekwuj polityki instalacji oprogramowania za pomocą następujących metod: [Realizacja: metody zdefiniowane przez organizację];

c. Monitoruj zgodności polityki z częstotliwością [Realizacja: częstotliwość określona przez organizację].

Zabezpieczenia powiązane: AC-3, AC-5, AC-6, AU-6, CM-2, CM-3, CM-5, CM-6, CM-7, CM-8, PL-4, SI-4, SI-7.

Zabezpieczenia rozszerzone:

(1) OPROGRAMOWANIE INSTALOWANE PRZEZ UŻYTKOWNIKA | OSTRZEGANIE O NIEAUTORYZOWANYCH INSTALACJACH

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(2) OPROGRAMOWANIE INSTALOWANE PRZEZ UŻYTKOWNIKA | ZABRONIONA INSTALACJA BEZ POSIADANIA STOSOWNYCH UPRAWNIEŃ

Zezwalaj na instalację oprogramowania tylko przez użytkownika jednoznacznie określonym statusem uprzywilejowania.

Zabezpieczenia powiązane: AC-5, AC-6.

(3) OPROGRAMOWANIE INSTALOWANE PRZEZ UŻYTKOWNIKA | AUTOMATYCZNE EGZEKWOWANIE I MONITOROWANIE

Egzekwuj i monitoruj zgodności z zasadami instalacji oprogramowania za pomocą [Realizacja: mechanizmy automatyczne zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

CM-12 POŁOŻENIE (LOKACJA) INFORMACJI

Zabezpieczenie:

a. Określ i udokumentuj lokalizację [Realizacja: informacje określone przez organizację] oraz określone składniki systemu, na których informacje są przetwarzane i przechowywane;

b. Określ i udokumentuj użytkowników, którzy mają dostęp do systemu i komponentów systemu, w których informacje są przetwarzane;

c. Dokumentuj zmiany lokalizacji (tj. systemu lub komponentów systemu), w których informacje są przetwarzane.

Zabezpieczenia powiązane: AC-2, AC-3, AC-4, AC-6, AC-23, CM-8, PM-5, RA-2, SA-4, SA-8, SA-17, SC-4, SC- 16, SC-28, SI-4, SI-7.

Zabezpieczenia rozszerzone:

(1) POŁOŻENIE (LOKACJA) INFORMACJI | AUTOMATYCZNE NARZĘDZIA DO OBSŁUGI LOKACJI INFORMACJI

Używaj zautomatyzowanych narzędzi do identyfikacji [Realizacja: informacje określone przez organizację według typu informacji] przetwarzanych w [Realizacja: komponenty systemu określone przez organizację] w celu upewnienia się, że stosowane są zabezpieczenia informacji organizacyjnych i ochrony prywatności osób.

Zabezpieczenia powiązane: nie dotyczy.

CM-13 MAPOWANIE DZIAŁAŃ NA DANYCH

Zabezpieczenie:

Opracuj i udokumentuj mapy działań dotyczących danych systemowych.

Zabezpieczenia powiązane: AC-3, CM-4, CM-12, PM-5, PM-27, PT-2, PT-3, RA-3, RA-8.

CM-14 PODPISYWANIE KOMPONENTÓW

Zabezpieczenie:

Zapobiegaj instalacji [Realizacja: zdefiniowane przez organizację komponenty aplikacji i oprogramowania układowego] bez weryfikacji czy komponent został podpisany cyfrowo za pomocą certyfikatu, który jest uznawany i zatwierdzony przez organizację.

Zabezpieczenia powiązane: CM-7, SC-12, SC-13, SI-7.

KATEGORIA: CP - PLANOWANIE AWARYJNE

CP-1 POLITYKA I PROCEDURY

Zabezpieczenie:

a. Opracuj, udokumentuj i rozpowszechnij wśród [Realizacja: personel lub role zdefiniowane przez organizację]:

    1. [Realizacja (jedno lub więcej): na poziomie organizacji, na poziomie misji/procesu biznesowego, na poziomie systemu] politykę planowania awaryjnego, która:

        (a) Uwzględnia cel, zakres, role, obowiązki, zaangażowanie kierownictwa, koordynację między jednostkami organizacyjnymi i zgodność;

        (b) Jest zgodna z obowiązującymi przepisami prawa, rozporządzeniami wykonawczymi, dyrektywami, regulacjami, politykami, standardami i wytycznymi;

    2. Procedury ułatwiające wdrażanie polityki planowania awaryjnego i powiązanych kontroli planowania awaryjnego;

b. Wyznacz [Realizacja: urzędnika zdefiniowanego przez organizację] do zarządzania opracowywaniem, dokumentowaniem i rozpowszechnianiem polityki i procedur planowania awaryjnego;

c. Przeglądaj i aktualizuj na bieżąco plany awaryjne:

   1. Polityki [Realizacja: częstotliwość zdefiniowana przez organizację] i następujących [Realizacja: zdarzenia zdefiniowane przez organizację];

   2. Procedur [Realizacja: częstotliwość zdefiniowana przez organizację] i następujących po nich [Realizacja: zdarzenia zdefiniowane przez organizację].

Zabezpieczenia powiązane: PM-9, PS-8, SI-12.

Zabezpieczenia rozszerzone: nie dotyczy.

CP-2 PLAN AWARYJNY

Zabezpieczenie:

a. Opracuj plan awaryjny dla systemu, który:

   1. Identyfikuje podstawowe funkcje misji i działalności oraz powiązane wymagania awaryjne;

   2. Zapewnia cele odzyskiwania, priorytety przywracania i wskaźniki;

   3. Zajmuje się rolami awaryjnymi, obowiązkami, przydzielonymi osobami wraz z danymi kontaktowymi;

   4. Zajmuje się utrzymaniem podstawowych funkcji misji i biznesu pomimo zakłóceń, zagrożeń lub awarii systemu;

   5. Zajmuje się ostatecznym, pełnym przywróceniem systemu bez pogorszenia jakości pierwotnie zaplanowanych i wdrożonych kontroli;

   6. Dotyczy udostępniania informacji awaryjnych;

   7. Został sprawdzony i zatwierdzony przez [Realizacja: personel lub role zdefiniowane w organizacji];

b. Rozpowszechnij kopie planu awaryjnego wśród [Realizacja: kluczowego personelu określonego przez organizację (określonego według nazwiska i/lub roli) oraz elementów organizacji];

c. Koordynuj działania w zakresie planowania awaryjnego z działaniami w zakresie obsługi incydentów;

d. Przeglądaj plany awaryjne dla systemu [Realizacja: częstotliwość zdefiniowana przez organizację];

e. Aktualizuj plany awaryjne, aby uwzględnić zmiany w organizacji, systemie lub środowisku operacyjnym oraz problemy napotkane podczas wdrażania, wykonywania lub testowania planu awaryjnego;

f. Komunikuj zmiany w planie awaryjnym [Realizacja: kluczowemu personelowi określonemu przez organizację (określonemu według nazwiska i/lub roli) oraz elementom organizacji];

g. Włącz wnioski wyciągnięte z testowania planów awaryjnych, do szkoleń lub rzeczywistych działań awaryjnych oraz do testów i szkoleń awaryjnych;

h. Zabezpiecz plany awaryjne przed nieautoryzowanym ujawnieniem i zmianą.

Zabezpieczenia powiązane: CP-3, CP-4, CP-6, CP-7, CP-8, CP-9, CP-10, CP-11, CP-13, IR-4, IR-6, IR-8, IR-9, MA-6, MP-2, MP-4, MP-5, PL-2, PM-8, PM-11, SA-15, SA-20, SC-7, SC-23, SI-12.

Zabezpieczenia rozszerzone:

(1) PLAN AWARYJNY | KOORDYNACJA Z POWIĄZANYMI PLANAMI

Koordynuj opracowywanie planu awaryjnego elementami jednostkach organizacji odpowiedzialnych za powiązane plany.

Zabezpieczenia powiązane: nie dotyczy.

(2) PLAN AWARYJNY | PLANOWANIE POJEMNOŚCI

Przeprowadzaj planowanie pojemności tak, aby podczas działań awaryjnych istniała niezbędna pojemność dla przetwarzania informacji, telekomunikacji i wsparcia środowiskowego.

Zabezpieczenia powiązane: PE-11, PE-12, PE-13, PE-14, PE-18, SC-5.

(3) PLAN AWARYJNY | WZNOWIENIE MISJI I FUNKCJI BIZNESOWYCH

Zaplanuj wznawianie [Realizacja: wszystkie; niezbędne] misji i funkcji biznesowych w ciągu [Realizacja: okres czasu określony przez organizację] od momentu uruchomienia planu awaryjnego.

Zabezpieczenia powiązane: nie dotyczy.

(4) PLAN AWARYJNY | WZNOWIENIE WSZYSTKICH MISJI I FUNKCJI BIZNESOWYCH

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(5) PLAN AWARYJNY | KONTYNUACJA MISJI I FUNKCJI BIZNESOWYCH

Zaplanuj kontynuację [Realizacja: wszystkie, niezbędne] misji i funkcji biznesowych przy minimalnej lub bez żadnej utraty ciągłości operacyjnej i utrzymuj tą ciągłość do czasu całkowitego przywrócenia systemu w głównych miejscach przetwarzania i/lub przechowywania.

Zabezpieczenia powiązane: nie dotyczy.

(6) PLAN AWARYJNY | ALTERNATYWNE MIEJSCA PRZETWARZANIA I SKŁADOWANIA

Zaplanuj przeniesienie [Realizacja: wszystkich; niezbędnych] misji i funkcji biznesowych do alternatywnych miejsc przetwarzania i/lub przechowywania przy minimalnej lub bez żadnej utraty ciągłości operacyjnej i utrzymuj tą ciągłość do czasu przywrócenia systemu do głównych miejsc przetwarzania i/lub przechowywania.

Zabezpieczenia powiązane: nie dotyczy.

(7) PLAN AWARYJNY | WSPÓŁPRACA Z ZEWNĘTRZNYMI DOSTAWCAMI USŁUG

Skoreluj plan awaryjny z planami awaryjnymi zewnętrznych dostawców usług w celu zapewnienia spełnienia wymogów awaryjnych.

Zabezpieczenia powiązane: SA-9.

(8) PLAN AWARYJNY | IDENTYFIKACJA KRYTYCZNYCH AKTYWÓW

Zidentyfikuj krytyczne aktywa systemowe wspierające [Realizacja: wszystkie; niezbędne] misje i funkcje biznesowe.

Zabezpieczenia powiązane: CM-8, RA-9.

CP-3 SZKOLENIE W ZAKRESIE PLANOWANIA CIĄGŁOŚCI DZIAŁANIA

Zabezpieczenie:

a. Zapewnij użytkownikom systemów teleinformatycznych szkolenia w zakresie planowania ciągłości działania na wypadek awarii, zgodnie z przypisanymi rolami i obowiązkami:

    1. W ciągu [Realizacja: okres zdefiniowany przez organizację] od przyjęcia roli lub odpowiedzialności w zakresie planowania ciągłości działania;

    2. W przypadku wystąpienia zmian konfiguracji systemu teleinformatycznego;

    3. Z częstotliwością [Realizacja: częstotliwość określona przez organizację w danym okresie czasowym].

b. Przeglądaj i aktualizuj treści szkoleń planowania ciągłości działania [Realizacja: częstotliwość zdefiniowana przez organizację] i przestrzegaj [Realizacja: zdarzenia zdefiniowane przez organizację].

Zabezpieczenia powiązane: AT-2, AT-3, AT-4, CP-2, CP-4, CP-8, IR-2, IR-4, IR-9.

Zabezpieczenia rozszerzone:

(1) SZKOLENIE W ZAKRESIE PLANOWANIA CIĄGŁOŚCI DZIAŁANIA | WYDARZENIA SYMULOWANE

Wprowadź symulację zdarzeń do szkoleń w zakresie ciągłości działania, aby ułatwić personelowi skuteczną reakcję w sytuacjach kryzysowych.

Zabezpieczenia powiązane: nie dotyczy.

(2) SZKOLENIE W ZAKRESIE PLANOWANIA CIĄGŁOŚCI DZIAŁANIA | MECHANIZMY STOSOWANE W ŚRODOWISKACH SZKOLENIOWYCH

Wprowadź mechanizmy stosowane w praktyce, aby zapewnić bardziej dokładne i realistyczne środowisko szkolenia w zakresie planowania ciągłości działania.

Zabezpieczenia powiązane: nie dotyczy.

CP-4 TESTOWANIE PLANU CIĄGŁOŚCI DZIAŁANIA

Zabezpieczenie:

a. Testuj plan awaryjny dla systemu [Realizacja: częstotliwość zdefiniowana przez organizację], używając następujących testów, aby określić skuteczność planu i gotowość do wykonania planu: [Realizacja: testy zdefiniowane przez organizację];

b. Analizuj wyniki testów planu awaryjnego;

c. W razie potrzeby podejmuj działania naprawcze.

Zabezpieczenia powiązane: AT-3, CP-2, CP-3, CP-8, CP-9, IR-3, IR-4, PL-2, PM-14, SR-2.

Zabezpieczenia rozszerzone:

(1) TESTOWANIE PLANU CIĄGŁOŚCI DZIAŁANIA | KOORDYNACJA Z POWIĄZANYMI PLANAMI

Koordynuj testowanie planu awaryjnego elementami jednostkach organizacji odpowiedzialnych za powiązane plany.

Zabezpieczenia powiązane: IR-8, PM-8.

(2) TESTOWANIE PLANU CIĄGŁOŚCI DZIAŁANIA | ZAPASOWE MIEJSCE PRZETWARZANIA

Testuje plan awaryjny w zapasowym miejscu przetwarzania:

a. Aby zapoznać personel rezerwowy z obiektem i dostępnymi zasobami;

b. Aby ocenić możliwości alternatywnego miejsca przetwarzania w zakresie wspierania operacji awaryjnych.

Zabezpieczenia powiązane: CP-7.

(3) TESTOWANIE PLANU CIĄGŁOŚCI DZIAŁANIA | TESTY AUTOMATYCZNE

Testuj plan awaryjny, poprzez [Realizacja: zautomatyzowane mechanizmy zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(4) TESTOWANIE PLANU CIĄGŁOŚCI DZIAŁANIA | PEŁNE ODZYSKIWANIE

W ramach testowania planu awaryjnego uwzględnij pełne odzyskanie i odtworzenie systemu do akceptowalnego stanu.

Zabezpieczenia powiązane: CP-10, SC-24.

(5) TESTOWANIE PLANU CIĄGŁOŚCI DZIAŁANIA | KONTROLOWANE AWARIE

Zastosuj [Realizacja: mechanizmy zdefiniowane przez organizację] do [Realizacja: system lub składników systemu zdefiniowanych przez organizację] w celu zakłócenia i negatywnego wpływu na system lub składnik systemu.

Zabezpieczenia powiązane: nie dotyczy.

CP-5 AKTUALIZACJA PLANU CIĄGŁOŚCI DZIAŁANIA

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

CP-6 ZAPASOWE MIEJSCE PRZECHOWYWANIA

Zabezpieczenie:

a. Wyznacz zapasowe miejsce przechowywania, w tym niezbędne umowy umożliwiające przechowywanie i pobieranie informacji o kopii zapasowej systemu;

b. Zagwarantuj, aby zapasowe miejsce przechowywania zapewniało zabezpieczenia równoważne z tymi w miejscu podstawowym.

Zabezpieczenia powiązane: CP-2, CP-7, CP-8, CP-9, CP-10, MP-4, MP-5, PE-3, SC-36, SI-13.

Zabezpieczenia rozszerzone:

(1) ZAPASOWE MIEJSCE PRZECHOWYWANIA | SEPARACJA OD MIEJSCA GŁÓWNEGO

Zapewnij takie zapasowe miejsce przechowywania danych, które będzie oddzielone od podstawowego miejsca przechowywania głównego, w celu ograniczenia podatności na te same zagrożenia.

Zabezpieczenia powiązane: RA-3.

(2) ZAPASOWE MIEJSCE PRZECHOWYWANIA | CZAS ODZYSKIWANIA I PUNKT ODZYSKIWANIA

Skonfiguruj zapasową lokalizację przechowywania danych, tak aby ułatwić operacje odzyskiwania zgodnie z celami dotyczącymi czasu odzyskiwania i punktu odzyskiwania.

Zabezpieczenia powiązane: nie dotyczy.

(3) ZAPASOWE MIEJSCE PRZECHOWYWANIA | DOSTĘPNOŚĆ

Zidentyfikuj potencjalne problemy z dostępnością do zapasowego miejsca przechowywania w przypadku zakłóceń lub katastrofy na obszarze całego obszaru i określenie szczegółowych działań łagodzących

Zidentyfikuj potencjalne problemy z dostępnością do zapasowego miejsca przechowywania w przypadku zakłóceń lub katastrofy na dużym obszarze i określ konkretne działania zaradcze.

Zabezpieczenia powiązane: RA-3.

CP-7 ZAPASOWE MIEJSCE PRZETWARZANIA

Zabezpieczenie:

a. Wyznacz zapasowe miejsce przetwarzania, w tym niezbędne umowy umożliwiające przeniesienie i wznowienie [Realizacja: zdefiniowane przez organizację operacje systemowe] w celu realizacji podstawowych misji i funkcji biznesowych w [Realizacja: zdefiniowany przez organizację okres czasu zgodny z celami czasu odzyskiwania i punktu odzyskiwania] , gdy podstawowe możliwości przetwarzania są niedostępne;

b. Zapewnij w zapasowym miejscu przetwarzania sprzęt i materiały niezbędne do przeniesienia i wznowienia działalności lub zawrzyj umowy wspierające dostawę do miejsca w określonym przez organizację okresie czasu na przeniesienie i wznowienie;

c. Zapewnij w zapasowym miejscu przetwarzania elementy sterujące równoważne elementom w miejscu głównym.

Zabezpieczenia powiązane: CP-2, CP-6, CP-8, CP-9, CP-10, MA-6, PE-3, PE-11, PE-12, PE-17, SC-36, SI-13.

Zabezpieczenia rozszerzone:

(1) ZAPASOWE MIEJSCE PRZETWARZANIA | SEPARACJA OD MIEJSCA GŁÓWNEGO

Zapewnij alternatywne miejsce przetwarzania, które jest wystarczająco oddzielone od miejsca przetwarzania głównego, aby zmniejszyć podatność na te same zagrożenia.

Zabezpieczenia powiązane: RA-3.

(2) ZAPASOWE MIEJSCE PRZETWARZANIA | DOSTĘPNOŚĆ

Zidentyfikuj potencjalne problemy z dostępnością do alternatywnych miejsc przetwarzania w przypadku zakłóceń lub katastrofy na obszarze całego regionu i określ konkretne działania łągodzące.

Zabezpieczenia powiązane: RA-3.

(3) ZAPASOWE MIEJSCE PRZETWARZANIA | PRIORYTET USŁUGI

Opracuj umowy dotyczącej alternatywnych miejsc przetwarzania, zawierającej postanowienia dotyczące priorytetu świadczenia usług zgodnie z wymogami dostępności (w tym celami dotyczącymi czasu odzyskiwania).

Zabezpieczenia powiązane: nie dotyczy.

(4) ZAPASOWE MIEJSCE PRZETWARZANIA | PRZYGOTOWANIE DO UŻYTKU

Przygotuj alternatywne miejsce przetwarzania, tak aby mogło ono służyć jako miejsce operacyjne wspierające podstawowe misje i funkcje biznesowe.

Zabezpieczenia powiązane: CM-2, CM-6, CP-4.

(5) ZAPASOWE MIEJSCE PRZETWARZANIA | RÓWNOWAŻNE ZABEZPIECZENIA BEZPIECZEŃSTWA INFORMACJI

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(6) ZAPASOWE MIEJSCE PRZETWARZANIA | BRAK MOŻLIWOŚCI POWROTU DO MIEJSCA PIERWOTNEGO

Zaplanuj i przygotuj się na okoliczności, które uniemożliwiają powrót do głównego miejsca przetwarzania.

Zabezpieczenia powiązane: nie dotyczy.

CP-8 USŁUGI TELEKOMUNIKACYJNE

Zabezpieczenie:

Zapewnij alternatywne usługi telekomunikacyjne, w tym niezbędne umowy umożliwiające wznowienie [Realizacja: operacje systemu zdefiniowane przez organizację] dla podstawowych funkcji misji i biznesowych w ciągu [Realizacja: okres czasu zdefiniowany przez organizację], gdy podstawowe możliwości telekomunikacyjne są niedostępne zarówno w głównej, jak i zapasowej lokalizacji przetwarzania lub przechowywania.

Zabezpieczenia powiązane: CP-2, CP-6, CP-7, CP-11, SC-7.

Zabezpieczenia rozszerzone:

(1) USŁUGI TELEKOMUNIKACYJNE | POSTANOWIENIA O PRIORYTETACH USŁUG

a. Opracuj główne i alternatywne umowy o świadczenie usług telekomunikacyjnych zawierające postanowienia o priorytetach usług zgodnie z wymaganiami dostępności (w tym celami czasu odtworzenia);

b. Wnioskuje o Priorytet Usług Telekomunikacyjnych dla wszystkich usług telekomunikacyjnych wykorzystywanych do gotowości w sytuacjach kryzysowych bezpieczeństwa narodowego, jeśli główne i/lub alternatywne usługi telekomunikacyjne są świadczone przez operatora publicznego.

Zabezpieczenia powiązane: nie dotyczy.

(2) USŁUGI TELEKOMUNIKACYJNE | POJEDYNCZE PUNKTY AWARII

Pozyskaj alternatywne usługi telekomunikacyjne w celu zmniejszenia prawdopodobieństwa współdzielenia pojedynczego punktu awarii z podstawowymi usługami telekomunikacyjnymi.

Zabezpieczenia powiązane: nie dotyczy.

(3) USŁUGI TELEKOMUNIKACYJNE | ROZDZIELENIE DOSTAWCÓW PODSTAWOWYCH I ALTERNATYWNYCH

Pozyskaj alternatywne usługi telekomunikacyjne od dostawców, którzy są oddzieleni od podstawowych dostawców usług w celu zmniejszenia podatności na te same zagrożenia.

(4) USŁUGI TELEKOMUNIKACYJNE | PLAN AWARYJNY DOSTAWCY

a. Wymagaj od podstawowych i alternatywnych dostawców usług telekomunikacyjnych posiadania planów awaryjnych;
b. Przeglądaj plany awaryjne dostawców w celu zapewnienia, że plany spełniają organizacyjne wymagania dotyczące planów awaryjnych;
c. Uzyskaj dowody testowania i szkoleń awaryjnych przeprowadzanych przez dostawców [Realizacja: częstotliwość zdefiniowana przez organizację].

Zabezpieczenia powiązane: CP-3, CP-4.

(5) USŁUGI TELEKOMUNIKACYJNE | TESTOWANIE ALTERNATYWNYCH USŁUG TELEKOMUNIKACYJNYCH

Testuj alternatywne usługi telekomunikacyjne [Realizacja: częstotliwość zdefiniowana przez organizację].

Zabezpieczenia powiązane: CP-3.

CP-9 KOPIA ZAPASOWA SYSTEMU

Zabezpieczenie:

1. Wykonuj kopie zapasowe informacji na poziomie użytkownika przechowywane w [Realizacja: komponenty systemu zdefiniowane przez organizację] z [Realizacja: częstotliwość zdefiniowana przez organizację zgodnie z celami czasu i punktu odtworzenia];

2. Wykonuj kopie zapasowe informacji na poziomie systemu przechowywane w systemie [Realizacja: częstotliwość zdefiniowana przez organizację zgodnie z celami czasu i punktu odtworzenia];

3. Wykonuj kopie zapasowe dokumentacji systemu, w tym dokumentacji związanej z bezpieczeństwem i prywatnością [Realizacja: częstotliwość zdefiniowana przez organizację zgodnie z celami czasu i punktu odtworzenia];

4. Zabezpieczaj poufność, integralność i dostępność informacji zawartych w kopiach zapasowych.

Zabezpieczenia powiązane: CP-2, CP-6, CP-10, MP-4, MP-5, SC-8, SC-12, SC-13, SI-4, SI-13.

Zabezpieczenia rozszerzone:

(1) KOPIA ZAPASOWA SYSTEMU | TESTOWANIE NIEZAWODNOŚCI I INTEGRALNOŚCI

Sprawdzaj informacje zawarte w kopiach zapasowych [Realizacja: częstotliwość zdefiniowana przez organizację] w celu weryfikacji niezawodności nośników i integralności informacji.

Zabezpieczenia powiązane: CP-4.

(2) KOPIA ZAPASOWA SYSTEMU | TESTOWANIE ODTWARZANIA PRZY UŻYCIU PRÓBKOWANIA

W ramach testowania planu awaryjnego przeprowadź odtwarzanie wybranych funkcji systemu, przy wykorzystaniu próbki informacji z kopii zapasowej.

Zabezpieczenia powiązane: CP-4.

(3) KOPIA ZAPASOWA SYSTEMU | ODDZIELNE PRZECHOWYWANIE INFORMACJI KRYTYCZNYCH

Przechowuj kopie zapasowe [Realizacja: krytyczne oprogramowanie systemowe i inne informacje związane z bezpieczeństwem zdefiniowane przez organizację] w innej lokalizacji lub w pojemniku o określonej odporności ogniowej, który nie znajduje się w tej samej lokalizacji co system operacyjny.

Zabezpieczenia powiązane: CM-4, CM-6, CM-8.

(4) KOPIA ZAPASOWA SYSTEMU | OCHRONA PRZED NIEAUTORYZOWANĄ MODYFIKACJĄ

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(5) KOPIA ZAPASOWA SYSTEMU | TRANSFER DO ZAPASOWEJ LOKALIZACJI PRZECHOWYWANIA

Przesyłaj informacje z kopii zapasowej systemu do zapasowej lokalizacji przechowywania [Realizacja: okres czasu i szybkość transferu zdefiniowane przez organizację zgodnie z celami czasu i punktu odtworzenia].

Zabezpieczenia powiązane: CP-7, MP-3, MP-4, MP-5

(6) KOPIA ZAPASOWA SYSTEMU | NADMIAROWY SYSTEM ZAPASOWY

Wykonuj kopie zapasowe systemu poprzez utrzymywanie redundantnego systemu zapasowego, który nie jest zlokalizowany w tym samym miejscu co system podstawowy i który może zostać aktywowany bez utraty informacji lub zakłócenia działania.

Zabezpieczenia powiązane: CP-7.

(7) KOPIA ZAPASOWA SYSTEMU | PODWÓJNA AUTORYZACJA USUWANIA LUB ZNISZCZENIA

Wymuszaj podwójną autoryzację dla usuwania lub niszczenia [Realizacja: informacje z kopii zapasowych zdefiniowane przez organizację].

Zabezpieczenia powiązane: AC-3, AC-5, MP-2.

(8) KOPIA ZAPASOWA SYSTEMU | OCHRONA KRYPTOGRAFICZNA

Wprowadź mechanizmy kryptograficzne w celu zapobiegania nieuprawnionemu ujawnieniu i modyfikacji [Realizacja: informacje z kopii zapasowych zdefiniowane przez organizację].

Zabezpieczenia powiązane: SC-12, SC-13, SC-28.

CP-10 ODZYSKIWANIE I ODTWARZANIE SYSTEMU

Zabezpieczenie:

Zapewnij odzyskanie i odtwarzanie systemu do akceptowalnego stanu w ciągu [Realizacja: okres czasu zdefiniowany przez organizację zgodny z celami czasu i punktu odtworzenia] po zakłóceniu, naruszeniu lub awarii.

Zabezpieczenia powiązane: CP-2, CP-4, CP-6, CP-7, CP-9, IR-4, SA-8, SC-24, SI-13.

Zabezpieczenia rozszerzone:

(1) ODZYSKIWANIE I ODTWARZANIE SYSTEMU | TESTOWANIE PLANU AWARYJNEGO

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(2) ODZYSKIWANIE I ODTWARZANIE SYSTEMU | ODZYSKIWANIE TRANSAKCJI

Wprowadź odzyskiwanie transakcji dla systemów opartych na transakcjach.

Zabezpieczenia powiązane: nie dotyczy.

(3) ODZYSKIWANIE I ODTWARZANIE SYSTEMU | KOMPENSUJĄCE MECHANIZMY KONTROLNE

[Wycofane: Uwzględnione poprzez dostosowanie.]

(4) ODZYSKIWANIE I ODTWARZANIE SYSTEMU | PRZYWRACANIE W OKREŚLONYM CZASIE

Zapewnij możliwość przywrócenia komponentów systemu w ciągu [Realizacja: okresy przywracania zdefiniowane przez organizację] z informacji kontrolowanych konfiguracyjnie i chronionych pod względem integralności, reprezentujących znany, operacyjny stan komponentów.

Zabezpieczenia powiązane: CM-2, CM-6.

(5) ODZYSKIWANIE I ODTWARZANIE SYSTEMU | ZDOLNOŚĆ DO PRZEŁĄCZANIA AWARYJNEGO

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(6) ODZYSKIWANIE I ODTWARZANIE SYSTEMU | OCHRONA KOMPONENTÓW

Zabezpieczaj komponenty systemu używane do odzyskiwania i odtwarzania.

Zabezpieczenia powiązane: AC-3, AC-6, MP-2, MP-4, PE-3, PE-6.

CP-11 ZAPASOWE PROTOKOŁY KOMUNIKACYJNE

Zabezpieczenie:

Zapewnij możliwość wykorzystania [Realizacja: zapasowe protokoły komunikacyjne zdefiniowane przez organizację] w celu utrzymania ciągłości działania.

Zabezpieczenia powiązane: CP-2, CP-8, CP-13.

Zabezpieczenia rozszerzone: nie dotyczy.

CP-12 TRYB AWARYJNY

Zabezpieczenie:

W przypadku wykrycia [Realizacja: warunki zdefiniowane przez organizację] przełącz się na bezpieczny tryb działania z [Realizacja: ograniczeniami bezpiecznego trybu działania zdefiniowanymi przez organizację].

Zabezpieczenia powiązane: CM-2, SA-8, SC-24, SI-13, SI-17.

Zabezpieczenia rozszerzone: nie dotyczy.

CP-13 ALTERNATYWNE MECHANIZMY BEZPIECZEŃSTWA

Zabezpieczenie:

Zastosuj [Realizacja: alternatywne lub uzupełniające mechanizmy bezpieczeństwa zdefiniowane przez organizację] w celu spełnienia [Realizacja: funkcje bezpieczeństwa zdefiniowane przez organizację], gdy podstawowy sposób wdrażania funkcji bezpieczeństwa jest niedostępny lub naruszony.

Zabezpieczenia powiązane: CP-2, CP-11, SI-13.

Zabezpieczenia rozszerzone: nie dotyczy.

KATEGORIA: IA - IDENTYFIKACJA I UWIERZYTELNIANIE

IA-1 POLITYKA I PROCEDURY

Zabezpieczenie:

a. Opracuj, udokumentuj i rozpowszechnij wśród [Realizacja: personel lub role zdefiniowane przez organizację]:

    1. [Wybór (jeden lub więcej): Poziom organizacji; Poziom misji/procesu biznesowego; Poziom systemu] politykę identyfikacji i uwierzytelniania, która:

        (a) Uwzględnia cel, zakres, role, obowiązki, zaangażowanie kierownictwa, koordynację między jednostkami organizacyjnymi i zgodność;

        (b) Jest zgodna z obowiązującymi przepisami prawa, rozporządzeniami wykonawczymi, dyrektywami, regulacjami, politykami, standardami i wytycznymi;

    2. Procedury ułatwiające wdrażanie polityki identyfikacji i uwierzytelniania oraz powiązanych kontroli identyfikacji i uwierzytelniania;

b. Wyznacz [Realizacja: urzędnik zdefiniowany przez organizację] do zarządzania rozwojem, dokumentowaniem i rozpowszechnianiem polityki i procedur identyfikacji i uwierzytelniania;

c. Przeglądaj i aktualizuj na bieżąco polityki identyfikacji i uwierzytelniania:

    1. Polityki [Realizacja: częstotliwość zdefiniowana przez organizację] i następujących [Realizacja: zdarzenia zdefiniowane przez organizację];

    2. Procedury [Realizacja: częstotliwość zdefiniowana przez organizację] i następujące po nich [Realizacja: zdarzenia zdefiniowane przez organizację].

Zabezpieczenia powiązane: AC-1, PM-9, PS-8, SI-12.

Zabezpieczenia rozszerzone: nie dotyczy.

IA-2 IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY ORGANIZACYJNI)

Zabezpieczenie:

Stosuj unikalną identyfikację i uwierzytelnianie użytkowników organizacyjnych oraz powiązanie tej unikalnej identyfikację z procesami działającymi w imieniu tych użytkowników.

Zabezpieczenia powiązane: AC-2, AC-3, AC-4, AC-14, AC-17, AC-18, AU-1, AU-6, IA-4, IA-5, IA-8, MA-4, MA- 5, PE-2, PL-4, SA-4, SA-8.

Zabezpieczenia rozszerzone:

(1) IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY ORGANIZACJI) | WIELOSKŁADNIKOWE UWIERZYTELNIANIE DO KONT UPRZYWILEJOWANYCH

Wprowadź uwierzytelnianie wieloskładnikowe w celu uzyskania dostępu do kont uprzywilejowanych.

Zabezpieczenia powiązane: AC-5, AC-6.

(2) IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY ORGANIZACJI) | WIELOSKŁADNIKOWE UWIERZYTELNIANIE KONT BEZ UPRAWNIEŃ

Wprowadź uwierzytelnianie wieloskładnikowe w celu uzyskania dostępu do kont nieuprzywilejowanych.

Zabezpieczenia powiązane: AC-5.

(3) IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY ORGANIZACYJNI) | LOKALNY DOSTĘP DO KONT UPRZYWILEJOWANYCH

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(4) IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY ORGANIZACYJNI) | LOKALNY DOSTĘP DO KONT NIEUPRZYWILEJOWANYCH

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(5) IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY ORGANIZACYJNI) | UWIERZYTELNIANIE INDYWIDUALNE Z UWIERZYTELNIANIEM GRUPOWYM

W przypadku korzystania ze współdzielonych kont lub środków uwierzytelniających należy wymagać od użytkowników indywidualnego uwierzytelnienia przed udzieleniem dostępu do współdzielonych kont lub zasobów.

Zabezpieczenia powiązane: nie dotyczy.

(6) IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY ORGANIZACJI) | DOSTĘP DO KONT — ODDZIELNE URZĄDZENIE

Wprowadź uwierzytelnianie wieloskładnikowe dla [Wybór (jeden lub więcej): lokalny; sieciowy; zdalny] dostępu do [Wybór (jeden lub więcej): kont uprzywilejowanych; kont nieuprzywilejowanych] w taki sposób, aby:

a. jeden z czynników był zapewniany przez urządzenie oddzielne od systemu uzyskującego dostęp; oraz

b. urządzenie spełniało [Realizacja: wymagania dotyczące siły mechanizmu zdefiniowane przez organizację].

Zabezpieczenia powiązane: AC-6.

(7) IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY ORGANIZACYJNI) | DOSTĘP SIECIOWY DO KONT NIEUPRZYWILEJOWANYCH - ODDZIELNE URZĄDZENIE

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(8) IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY ORGANIZACJI) | DOSTĘP DO KONT — ZABEZPIECZENIE PRZED POWTÓRNYM UŻYCIEM

Wprowadź mechanizmy uwierzytelniania odporne na powtórne użycie w celu uzyskania dostępu do [Wybór (jeden lub więcej): kont uprzywilejowanych; kont nieuprzywilejowanych].

Zabezpieczenia powiązane: nie dotyczy.

(9) IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY ORGANIZACYJNI) | DOSTĘP SIECIOWY DO KONT NIEUPRZYWILEJOWANYCH - ODPORNOŚĆ NA ODTWARZANIE

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(10) IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY ORGANIZACJI) | LOGOWANIE JEDNOKROTNE

Zapewnij możliwość jednokrotnego logowania dla [Realizacja: zdefiniowanych przez organizację kont systemowych i usług].

Zabezpieczenia powiązane: nie dotyczy.

(11) IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY ORGANIZACYJNI) | DOSTĘP ZDALNY - ODDZIELNE URZĄDZENIE

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(12) IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY ORGANIZACYJNI) | AKCEPTACJA POŚWIADCZEŃ PIV

Akceptuj i elektronicznie weryfikuj poświadczenia zgodne z weryfikacją tożsamości osobistej (PIV).

Zabezpieczenia powiązane: nie dotyczy.

(13) IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY ORGANIZACYJNI) | UWIERZYTELNIANIE “POZA PASMEM”

Wprowadź następujące mechanizmy uwierzytelniania “poza pasmem” (OUT-OF-BAND) w ramach [Realizacja: warunki zdefiniowane przez organizację]: [Realizacja: uwierzytelnianie poza pasmem zdefiniowane przez organizację].

Zabezpieczenia powiązane: IA-10, IA-11, SC-37

IA-3 IDENTYFIKACJA I UWIERZYTELNIANIE URZĄDZEŃ

Zabezpieczenie:

Stosuj unikalną identyfikację i uwierzytelnianie [Realizacja: urządzenia i/lub typy urządzeń zdefiniowane przez organizację] przed nawiązaniem połączenia [Wybór (jeden lub więcej): lokalnego; zdalnego; sieciowego].

Zabezpieczenia powiązane: AC-17, AC-18, AC-19, AU-6, CA-3, CA-9, IA-4, IA-5, IA-9, IA-11, SI-4.

Zabezpieczenia rozszerzone:

(1) IDENTYFIKACJA I UWIERZYTELNIANIE URZĄDZEŃ | KRYPTOGRAFICZNE UWIERZYTELNIANIE DWUKIERUNKOWE

Stosuj uwierzytelnianie [Realizacja: urządzenia i/lub typy urządzeń zdefiniowane przez organizację] przed nawiązaniem połączenia [Wybór (jeden lub więcej): lokalne; zdalne; sieciowe], korzystając z dwukierunkowego uwierzytelniania opartego na kryptografii.

Zabezpieczenia powiązane: SC-8, SC-12, SC-13.

(2) IDENTYFIKACJA I UWIERZYTELNIANIE URZĄDZEŃ | KRYPTOGRAFICZNE DWUKIERUNKOWE UWIERZYTELNIANIE SIECIOWE

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(3) IDENTYFIKACJA I UWIERZYTELNIANIE URZĄDZEŃ | DYNAMICZNA ALOKACJA ADRESÓW

a. W przypadku adresów przydzielanych dynamicznie należy ujednolicić informacje o dzierżawie dynamicznego przydziału adresów oraz czas trwania dzierżawy przypisany do urządzeń zgodnie z [Przypisanie: informacje o dzierżawie zdefiniowane przez organizację i czas trwania dzierżawy];

b. przeprowadzić audyt informacji o dzierżawie po przypisaniu do urządzenia.

Zabezpieczenia powiązane: AU-2.

(4) IDENTYFIKACJA I UWIERZYTELNIANIE URZĄDZEŃ | ATESTACJA URZĄDZEŃ

Obsługa identyfikacji i uwierzytelniania urządzeń na podstawie poświadczeń przez [Realizacja: proces zarządzania konfiguracją zdefiniowany przez organizację].

Zabezpieczenia powiązane: CM-2, CM-3, CM-6.

IA-4 ZARZĄDZANIE IDENTYFIKATORAMI

Zabezpieczenie:

Zarządzaj identyfikatorami systemu poprzez:

a. Otrzymanie autoryzacji od [Realizacja: personel lub role zdefiniowane przez organizację] w celu przypisania identyfikatora osoby, grupy, roli, usługi lub urządzenia;

b. Wybranie identyfikatora identyfikującego osobę, grupę, rolę, usługę lub urządzenie;

c. Przypisanie identyfikatora do zamierzonej osoby, grupy, roli, usługi lub urządzenia;

d. Zapobieganie ponownemu użyciu identyfikatorów dla [Realizacja: okres czasu zdefiniowany przez organizację].

Zabezpieczenia powiązane: AC-5, IA-2, IA-3, IA-5, IA-8, IA-9, IA-12, MA-4, PE-2, PE-3, PE-4, PL-4, PM-12, PS-3, PS-4, PS-5, SC-37

Zabezpieczenia rozszerzone:

(1) ZARZĄDZANIE IDENTYFIKATORAMI | ZABROŃ UŻYWANIA IDENTYFIKATORÓW KONT JAKO IDENTYFIKATORÓW PUBLICZNYCH

Zakazuj używania identyfikatorów kont systemowych, które są takie same jak identyfikatory publiczne dla indywidualnych kont.

Zabezpieczenia powiązane: AT-2, PT-7

(2) ZARZĄDZANIE IDENTYFIKATORAMI | AUTORYZACJA PRZEŁOŻONEGO

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(3) ZARZĄDZANIE IDENTYFIKATORAMI | WIELOKROTNE FORMY CERTYFIKACJI

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(4) ZARZĄDZANIE IDENTYFIKATORAMI | IDENTYFIKUJ STATUS UŻYTKOWNIKA

Zarządzaj indywidualnymi identyfikatorami, jednoznacznie identyfikując każdą osobę jako [Realizacja: zdefiniowana przez organizację cecha identyfikująca status jednostki].

Zabezpieczenia powiązane: nie dotyczy.

(5) ZARZĄDZANIE IDENTYFIKATORAMI | ZARZĄDZANIE DYNAMICZNE

Zarządzaj dynamicznie indywidualnymi identyfikatorami zgodnie z [Realizacja: polityka dotycząca dynamicznych identyfikatorów zdefiniowana przez organizację].

Zabezpieczenia powiązane: AC-16.

(6) ZARZĄDZANIE IDENTYFIKATORAMI | ZARZĄDZANIE MIĘDZYORGANIZACYJNE

Współpracuj z podmiotami zewnętrznymi w celu zarządzania identyfikatorami w obrębie organizacji: [Realizacja: organizacje zewnętrzne zdefiniowane przez organizację].

Zabezpieczenia powiązane: AU-16, IA-2, IA-5.

(7) ZARZĄDZANIE IDENTYFIKATORAMI | REJESTRACJA OSOBISTA

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(8) ZARZĄDZANIE IDENTYFIKATORAMI | PARY IDENTYFIKATORÓW PSEUDONIMOWYCH

Generuj pary pseudonimowych identyfikatorów.

Zabezpieczenia powiązane: IA-5.

(9) ZARZĄDZANIE IDENTYFIKATORAMI | KONSERWACJA I OCHRONA ATRYBUTÓW

Zachowaj atrybuty dla każdej jednoznacznie zidentyfikowanej osoby, urządzenia lub usługi w [Realizacja: zdefiniowane przez organizację chronione centralne przechowywanie].

Zabezpieczenia powiązane: nie dotyczy.

IA-5 ZARZĄDZANIE UWIERZYTELNIANIEM

Zabezpieczenie:

Zarządzaj metodami uwierzytelniania w systemie poprzez:

a. Weryfikację, w ramach początkowego procesu uwierzytelnienia, tożsamości osoby, grupy, roli, usługi lub urządzenia otrzymującego dokument uwierzytelniający;

b. Ustanowienie wstępnej treści uwierzytelniającej odnoszącej się do osób uwierzytelnianych

c. Zapewnienie, że mechanizmy uwierzytelnienia mają wystarczającą siłę, która umożliwia ich wykorzystanie;

d. Ustanowienie i wdrożenie procedur administracyjnych dotyczących wstępnej dystrybucji elementów uwierzytelniających, postępowania z zagubionymi / zagrożonymi lub uszkodzonymi elementami uwierzytelniania oraz odwoływania metod i elementów uwierzytelniających

e. Zmianę domyślnej zawartości metod uwierzytelnienia przed pierwszym użyciem;

f. Zmienianie lub odświeżanie metod uwierzytelniania [Realizacja: okres czasu zdefiniowany przez organizację w zależności od rodzaju uwierzytelnienia] lub gdy wystąpi [Realizacja: zdarzenia zdefiniowane przez organizację];

g. Ochronę treści uwierzytelniających przed nieuprawnionym ujawnieniem i modyfikacją;

h. Wymaganie od osób fizycznych wdrażania i stosowania określonych metod zabezpieczeń urządzeń w celu zapewnienia uwierzytelniania;

i. Zmianę metod uwierzytelnienia kont grupowych / ról w przypadku zmiany członkostwa w tych kontach

Zabezpieczenia powiązane: AC-3, AC-6, CM-6, IA-2, IA-4, IA-7, IA-8, IA-9, MA-4, PE-2, PL-4, SC-12, SC-13.

Zabezpieczenia rozszerzone:

(1) ZARZĄDZANIE UWIERZYTELNIANIEM | UWIERZYTELNIANIE OPARTE O HASŁA

W przypadku uwierzytelniania opartego na haśle:

a. Prowadź listy często używanych, oczekiwanych lub naruszonych haseł i aktualizuj je [Realizacja: częstotliwość określona przez organizację] oraz kiedy podejrzewasz, że hasła organizacyjne zostały naruszone bezpośrednio lub pośrednio;

b. Sprawdzaj czy tworzone lub aktualizowane hasła użytkowników nie zostały znalezione na stronie liście powszechnie używanych, oczekiwanych lub naruszonych haseł w IA-5(1)(a);

c. Przesyłaj hasła tylko przez kanały chronione kryptograficznie;

d. Przechowuj hasła przy użyciu zatwierdzonej funkcji wyprowadzania klucza z dodaną solą, najlepiej przy użyciu skrótu klucza;

e. Wymagaj natychmiastowego wyboru nowego hasła po odzyskaniu konta;

f. Umożliw użytkownikowi wybór długich haseł i fraz, w tym spacji i wszystkich znaków drukowalnych oraz spacje;

g. Wprowadź zautomatyzowane narzędzia pomagające użytkownikowi w wyborze silnych haseł;

h. Egzekwuj następujące zasady kompozycji i złożoności: [Realizacja: zdefiniowane przez organizację reguły kompozycji i złożoności].

Zabezpieczenia powiązane: IA-6.

(2) ZARZĄDZANIE UWIERZYTELNIANIEM | UWIERZYTELNIANIE OPARTE NA KLUCZU PUBLICZNYM

a. W przypadku uwierzytelniania opartego na kluczu publicznym:

    1. Wymuś autoryzowany dostęp do odpowiadającego mu klucza prywatnego;

    2. Przypisz uwierzytelnioną tożsamość do konta osoby lub grupy;

b. Gdy używana jest infrastruktura klucza publicznego (PKI):

    1. Weryfikuj certyfikaty poprzez konstruowanie i weryfikowanie ścieżki certyfikacji do zaakceptowanego zaufanego punktu zaczepienia, w tym sprawdzanie informacji o stanie certyfikatu;

    2. Zaimplementuj w lokalnej pamięci podręcznej dane o odwołaniach w celu obsługi wykrywania ścieżki i sprawdzania statusu.

Zabezpieczenia powiązane: IA-3, SC-17.

(3) ZARZĄDZANIE UWIERZYTELNIANIEM | REJESTRACJA OSOBISTA LUB ZAUFANEJ STRONY ZEWNĘTRZNEJ

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(4) ZARZĄDZANIE UWIERZYTELNIANIEM | ZAUTOMATYZOWANE WSPARCIE W OKREŚLANIU SIŁY HASŁA

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(5) ZARZĄDZANIE UWIERZYTELNIANIEM | ZMIANA METODY UWIERZYTELNIANIA PRZED DOSTAWĄ

Wymagaj od deweloperów i instalatorów komponentów systemu dostarczenia unikatowych uwierzytelnień lub zmiany domyślnych uwierzytelnień przed dostawą / instalacją elementu systemu.

Zabezpieczenia powiązane: nie dotyczy.

(6) ZARZĄDZANIE UWIERZYTELNIANIEM | OCHRONA METOD UWIERZYTELNIANIA

Chroń czynniki uwierzytelniające współmiernie do kategorii bezpieczeństwa informacji, które mają być chronione, do których dostęp umożliwia użycie elementu uwierzytelniającego.

Zabezpieczenia powiązane: RA-2.

(7) ZARZĄDZANIE UWIERZYTELNIANIEM | BRAK WBUDOWANYCH NIEZASZYFROWANYCH STATYCZNYCH ELEMENTÓW UWIERZYTELNIANIA

Upewnij się, że niezaszyfrowane statyczne elementy uwierzytelniające nie są osadzone w aplikacjach ani innych formach statycznego przechowywania danych.

Zabezpieczenia powiązane: nie dotyczy.

(8) ZARZĄDZANIE UWIERZYTELNIANIEM | JEDNO KONTO W WIELU SYSTEMACH

Wprowadź [Realizacja: kontrole bezpieczeństwa zdefiniowane przez organizację] w celu zarządzania ryzykiem naruszenia bezpieczeństwa wynikającego z posiadania przez poszczególne osoby tego samego konta w wielu systemach.

Zabezpieczenia powiązane: PS-6.

(9) ZARZĄDZANIE UWIERZYTELNIANIEM | ZARZĄDZANIE DANYMI UWIERZYTELNIAJĄCYMI MIĘDZY ORGANIZACJAMI

Wykorzystuj podmioty zewnętrzne: [Realizacja: organizacje zewnętrzne zdefiniowane przez organizację] w zakresie zarządzania metodami uwierzytelniania między organizacjami.

Zabezpieczenia powiązane: AU-7, AU-16.

(10) ZARZĄDZANIE UWIERZYTELNIANIEM | DYNAMICZNE POWIĄZANIE POŚWIADCZEŃ

Dynamicznie powiąż tożsamości i środki uwierzytelniające, korzystając z następujących reguł: [Realizacja: reguły powiązania zdefiniowane przez organizację].

Zabezpieczenia powiązane: AU-16, IA-5.

(11) ZARZĄDZANIE UWIERZYTELNIANIEM | UWIERZYTELNIANIE OPARTE NA TOKENACH SPRZĘTOWYCH

[Wycofano: Włączono do IA-2(1) i IA-2(2).]

(12) ZARZĄDZANIE UWIERZYTELNIANIEM | UWIERZYTELNIANIE BIOMETRYCZNE

W przypadku uwierzytelniania opartego na biometrii stosuj mechanizmy spełniające następujące wymagania jakościowe dotyczące danych biometrycznych [Realizacja: wymagania jakościowe dotyczące danych biometrycznych określone przez organizację].

Zabezpieczenia powiązane: AC-7.

(13) ZARZĄDZANIE UWIERZYTELNIANIEM | PRZEDAWNIENIE BUFOROWANYCH ELEMENTÓW UWIERZYTELNIANIA

Zakazuj używania buforowanych elementów uwierzytelniania po [Realizacja: okres czasu zdefiniowany przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(14) ZARZĄDZANIE UWIERZYTELNIANIEM | ZARZĄDZANIE ZAWARTOŚCIĄ ZAUFANYCH MAGAZYNÓW INFRASTRUKTURY KLUCZA PUBLICZNEGO

W przypadku uwierzytelniania opartego na infrastrukturze klucza publicznego (PKI) należy zastosować obejmującą całą organizację metodologię zarządzania zawartością zaufanych magazynów infrastruktury klucza publicznego (PKI) zainstalowanych na wszystkich platformach, w tym w sieciach, systemach operacyjnych, przeglądarkach i aplikacjach.

Zabezpieczenia powiązane: nie dotyczy.

(15) ZARZĄDZANIE UWIERZYTELNIANIEM | PRODUKTY I USŁUGI

Do zarządzania tożsamością, poświadczeniami i dostępem używaj wyłącznie produktów i usług zapewniających zgodność z obowiązującymi regulacjami i standardami bezpieczeństwa.

Zabezpieczenia powiązane: nie dotyczy.

(16) ZARZĄDZANIE UWIERZYTELNIANIEM | OSOBISTY LUB ZAUFANY ZEWNĘTRZNY PODMIOT UWIERZYTELNIAJĄCY

Wymagaj, aby wydawanie [Realizacja: zdefiniowane przez organizację typy i/lub określone metody uwierzytelniania] odbywało się [Wybór: osobisty; przez zaufaną stronę zewnętrzną] przed [Realizacja:

organ rejestracyjny zdefiniowany przez organizację] z upoważnieniem [Realizacja: zdefiniowany przez organizację personel lub role].

Zabezpieczenia powiązane: IA-12.

(17) ZARZĄDZANIE UWIERZYTELNIANIEM | WYKRYWANIE ATAKÓW PREZENTACYJNYCH PRZY UWIERZYTELNIANIU BIOMETRYCZNYM

Wdrażaj mechanizmy wykrywania ataków prezentacyjnych w celu uwierzytelniania opartego na danych biometrycznych.

Zabezpieczenia powiązane: AC-7.

(18) ZARZĄDZANIE UWIERZYTELNIANIEM | MENEDŻER HASEŁ

(a) Zatrudniaj [Realizacja: menedżerów haseł zdefiniowanych przez organizację] do generowania i zarządzania hasłami;

(b) Chroń hasła, używając [Realizacja: kontroli zdefiniowanych przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

IA-6 INFORMACJA ZWROTNA UWIERZYTELNIANIA

Zabezpieczenie:

Ukryj informację zwrotną dotyczącą uwierzytelniania podczas procesu uwierzytelniania, aby chronić informacje przed możliwym wykorzystaniem i użyciem przez nieupoważnione osoby.

Zabezpieczenia powiązane: AC-3.

Zabezpieczenia rozszerzone: nie dotyczy.

IA-7 UWIERZYTELNIANIE MODUŁU KRYPTOGRAFICZNEGO

Zabezpieczenie:

Wprowadź mechanizmy uwierzytelniania do modułu kryptograficznego, które spełniają wymagania obowiązujących przepisów prawa, zarządzeń wykonawczych, dyrektyw, polityk, regulacji, standardów i wytycznych dotyczących takiego uwierzytelniania.

Zabezpieczenia powiązane: AC-3, IA-5, SA-4, SC-12, SC-13.

IA-8 IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY SPOZA ORGANIZACJI)

Jednoznaczna identyfikacja i uwierzytelnianie użytkowników spoza organizacji lub procesów działających w imieniu użytkowników spoza organizacji.

Zabezpieczenia powiązane: AC-2, AC-6, AC-14, AC-17, AC-18, AU-6, IA-2, IA-4, IA-5, IA-10, IA-11, MA-4, RA-3, SA-4, SC-8.

Zabezpieczenia rozszerzone:

(1) IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY SPOZA ORGANIZACJI) | AKCEPTACJA POŚWIADCZEŃ TOŻSAMOŚCI WYDANYCH PRZEZ INNE ORGANIZACJE

Akceptuj i elektronicznie weryfikuj poświadczenia zgodnie z procedurą weryfikacji tożsamości z innych organizacji.

Zabezpieczenia powiązane: WP-3.

(2) IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY SPOZA ORGANIZACJI) | AKCEPTACJA POŚWIADCZEŃ STRON TRZECICH

a. Akceptuj tylko poświadczeń stron trzecich zgodnych z krajowymi i unijnymi normami bezpieczeństwa;

b. Dokumentowanie i utrzymywanie listy zaakceptowanych poświadczeń stron trzecich.

Zabezpieczenia powiązane: nie dotyczy.

(3) IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY SPOZA ORGANIZACJI) | KORZYSTANIE Z PRODUKTÓW ZATWIERDZONYCH PRZEZ FICAM

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(4) IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY SPOZA ORGANIZACJI) WYKORZYSTANIE ZDEFINIOWANYCH PROFILI

Dostosuj e się do następujących profili zarządzania tożsamością [Realizacja: profile zarządzania tożsamością zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(5) IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY SPOZA ORGANIZACJI) | AKCEPTACJA POŚWIADCZEŃ

Akceptuj i zweryfikuj poświadczenia lub PKI, które spełniają [Realizacja: zasady zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(6) IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY SPOZA ORGANIZACJI) | ROZŁĄCZNOŚĆ

Wprowadź następujące środki zapewniające ochronę prywatności poprzez rozdzielenie informacji o użytkowniku między różnymi uczestnikami procesu uwierzytelniania (osobami, dostawcami usług uwierzytelniania i stronami zaufania): [Realizacja: środki zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

IA-9 IDENTYFIKACJA I UWIERZYTELNIANIE USŁUG

Zabezpieczenie:

Jednoznacznie identyfikuj i uwierzytelniaj [Realizacja: usługi i aplikacje systemowe zdefiniowane przez organizację] przed nawiązaniem komunikacji z urządzeniami, użytkownikami lub innymi usługami czy aplikacjami.

Zabezpieczenia powiązane: SC-8.

Zabezpieczenia rozszerzone:

(1) IDENTYFIKACJA I UWIERZYTELNIANIE USŁUG | WYMIANA INFORMACJI

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(2) IDENTYFIKACJA I UWIERZYTELNIANIE USŁUG | PRZESYŁANIE DECYZJI

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

IA-10 UWIERZYTELNIANIE ADAPTACYJNE

Zabezpieczenie:

Wymagaj, aby zatrudniane osoby uzyskiwały dostęp do systemu teleinformatycznego poprzez [Realizacja: zdefiniowane przez organizację dodatkowe techniki lub mechanizmy uwierzytelniania] w określonych [Realizacja: okoliczności lub sytuacje zdefiniowane przez organizację].

Zabezpieczenia powiązane: IA-2, IA-8.

Zabezpieczenia rozszerzone: nie dotyczy.

IA-11 PONOWNE UWIERZYTELNIANIE

Wymagaj od użytkowników ponownego uwierzytelnienia, gdy wystąpią [Realizacja: okoliczności lub sytuacje zdefiniowane przez organizację wymagające ponownego uwierzytelnienia].

Zabezpieczenia powiązane: AC-3, AC-11, IA-2, IA-3, IA-4, IA-8.

IA-12 WERYFIKACJA TOŻSAMOŚCI

Zabezpieczenie:

a. Weryfikuj tożsamości użytkowników wymagających kont dostępu do systemu w oparciu o odpowiednie wymagania poziomu pewności tożsamości określone w obowiązujących standardach i wytycznych;

b. Powiąż tożsamości użytkownika z konkretną osobą fizyczną;

c. Zbieraj, waliduj i weryfikuj dowody tożsamości.

Zabezpieczenia powiązane: AC-5, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-8.

Zabezpieczenia rozszerzone:

(1) WERYFIKACJA TOŻSAMOŚCI | AUTORYZACJA PRZEŁOŻONEGO

Wymagaj, aby proces rejestracji w celu otrzymania konta dostępu do systemu zawierał autoryzację przełożonego lub sponsora.

Zabezpieczenia powiązane: nie dotyczy.

(2) WERYFIKACJA TOŻSAMOŚCI | DOWÓD TOŻSAMOŚCI

Wymagaj przedstawienia dowodów potwierdzających tożsamość osoby.

Zabezpieczenia powiązane: nie dotyczy.

(3) WERYFIKACJA TOŻSAMOŚCI | WALIDACJA I WERYFIKACJA DOWODÓW TOŻSAMOŚCI

Wymagaj, aby przedstawione dowody tożsamości były walidowane i weryfikowane poprzez [Realizacja: metody walidacji i weryfikacji zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(4) WERYFIKACJA TOŻSAMOŚCI | WERYFIKACJA I WALIDACJA OSOBISTA

Wymagaj, aby walidacja i weryfikacja dowodów tożsamości była przeprowadzana osobiście.

Zabezpieczenia powiązane: nie dotyczy.

(5) WERYFIKACJA TOŻSAMOŚCI | POTWIERDZENIE ADRESU

Wymagaj, aby [*Wybór:* kod rejestracyjny; powiadomienie o weryfikacji] został dostarczony poprzez kanał alternatywny w celu weryfikacji adresu użytkownika (fizycznego lub cyfrowego).

Zabezpieczenia powiązane: IA-12.

(6) WERYFIKACJA TOŻSAMOŚCI | AKCEPTACJA TOŻSAMOŚCI ZWERYFIKOWANYCH ZEWNĘTRZNIE

Akceptuj tożsamości zweryfikowane zewnętrznie na [Realizacja: poziom pewności tożsamości zdefiniowany przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

KATEGORIA: IR – REAGOWANIE NA INCYDENTY

IR-1 POLITYKA I PROCEDURY

Zabezpieczenie:

a. Opracowuj, udokumentuj i rozpowszechnij wśród [Realizacja: personel lub role zdefiniowane w organizacji]:

   1. [Realizacja (jedno lub więcej): na poziomie organizacji, na poziomie misji/procesu biznesowego, na poziomie systemu] politykę reagowania na incydenty, która:

      (a) Dotyczy celu, zakresu, ról, obowiązków, zaangażowania kierownictwa, koordynacji między jednostkami organizacyjnymi i zgodności;

      (b) Jest zgodna z obowiązującymi przepisami prawa, rozporządzeniami wykonawczymi, dyrektywami, regulacjami, zasadami, normami i wytycznymi;

   2. Procedury ułatwiające wdrażanie polityki reagowania na incydenty i powiązanych z nią kontroli reagowania na incydenty;

b. Wyznacz [Realizacja: urzędnika określonego przez organizację] do zarządzania opracowywaniem, dokumentowaniem i rozpowszechnianiem polityki i procedur reagowania na incydenty;

c. Przejrzyj i zaktualizuj na bieżąco reakcję na incydent w:

   1. Polityce [Realizacja: częstotliwość zdefiniowana przez organizację] i następujące po niej [Realizacja: zdarzenia zdefiniowane przez organizację]; i

   2. Procedurach [Realizacja: częstotliwość zdefiniowana przez organizację] i następujące po nich [Realizacja: zdarzenia zdefiniowane przez organizację].

Zabezpieczenia powiązane: PM-9, PS-8, SI-12.

Zabezpieczenia rozszerzone: nie dotyczy.

IR-2 SZKOLENIE W ZAKRESIE REAGOWANIA NA INCYDENTY

Zabezpieczenie:

a. Zapewnij użytkownikom systemu szkolenie w zakresie reagowania na incydenty, zgodnie z przypisanymi rolami i obowiązkami:

    1. W ciągu [Realizacja: okres czasu określony przez organizację] od objęcia roli lub odpowiedzialności związanej z reagowaniem na incydenty lub uzyskania dostępu do systemu;

    2. W przypadku wystąpienia zmian w systemie;

    3. Cyklicznie [Realizacja: częstotliwość określona przez organizację];

b. Przejrzyj i zaktualizuj treści szkolenia dotyczącego reagowania na incydenty [Realizacja: częstotliwość zdefiniowana przez organizację] i wykonaj następujące czynności [Realizacja: zdarzenia zdefiniowane przez organizację].

Zabezpieczenia powiązane: AT-2, AT-3, AT-4, CP-3, IR-3, IR-4, IR-8, IR-9.

Zabezpieczenia rozszerzone:

(1) SZKOLENIE W ZAKRESIE REAGOWANIA NA INCYDENTY | SYMULOWANE WYDARZENIA

Włącz symulację zdarzeń do szkoleń w zakresie reagowania na incydenty w celu ułatwienia personelowi podjęcia odpowiednich działań w sytuacjach kryzysowych.

Zabezpieczenia powiązane: nie dotyczy.

(2) SZKOLENIE W ZAKRESIE REAGOWANIA NA INCYDENTY | ZAUTOMATYZOWANE ŚRODOWISKA SZKOLENIOWE

Zapewnij środowisko szkoleniowe w zakresie reagowania na incydenty, korzystając z [Realizacja: zautomatyzowane mechanizmy zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(3) SZKOLENIE W ZAKRESIE REAGOWANIA NA INCYDENTY | NARUSZENIE

Zapewnij szkolenie w zakresie reagowania na incydenty, obejmujące sposoby identyfikowania naruszeń i reagowania na nie, w tym procedurę zgłaszania naruszeń w organizacji.

Zabezpieczenia powiązane: nie dotyczy.

IR-3 TESTOWANIE REAKCJI NA INCYDENTY

Zabezpieczenie:

Przetestuj skuteczność możliwości reagowania na incydenty dla systemu [Realizacja: częstotliwość zdefiniowana przez organizację], korzystając z następujących testów: [Realizacja: testy zdefiniowane przez organizację].

Zabezpieczenia powiązane: CP-3, CP-4, IR-2, IR-4, IR-8, PM-14.

Zabezpieczenia rozszerzone:

(1) TESTOWANIE REAKCJI NA INCYDENTY | TESTOWANIE AUTOMATYCZNE

Przetestuj zdolność reagowania na incydenty, korzystając z [Realizacja: zautomatyzowane mechanizmy zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(2) TESTOWANIE REAKCJI NA INCYDENTY | KOORDYNACJA Z POWIĄZANYMI PLANAMI

Koordynuj testy reagowania na incydenty z elementami organizacji odpowiedzialnymi za powiązane plany.

Zabezpieczenia powiązane: nie dotyczy.

(3) TESTOWANIE REAKCJI NA INCYDENTY | CIĄGŁE DOSKONALENIE

Wykorzystuj dane jakościowe i ilościowe pochodzące z testów, aby: określić skuteczność procesów reagowania na incydenty; stale udoskonalać procesy reagowania na incydenty; oraz zapewnić dokładne, spójne i powtarzalne środki i wskaźniki reagowania na incydenty.

Zabezpieczenia powiązane: nie dotyczy.

IR-4 OBSŁUGA INCYDENTÓW

Zabezpieczenie:

a. Wdrażaj możliwość obsługi incydentów, która jest zgodna z planem reagowania na incydenty i obejmuje przygotowanie, wykrywanie i analizę, powstrzymywanie, eliminowanie i odzyskiwanie;

b. Koordynuj działania związane z obsługą incydentów z działaniami w zakresie planowania awaryjnego;

c. Wdrażaj wnioski wyciągnięte z bieżących działań związanych z obsługą incydentów w procedurach reagowania na incydenty, szkoleniach i testach oraz wynikające z nich zmiany;

d. Upewnij się, że rygor, intensywność, zakres i wyniki działań związanych z obsługą incydentów są porównywalne i przewidywalne w całej organizacji.

Zabezpieczenia powiązane: AC-19, AU-6, AU-7, CM-6, CP-2, CP-3, CP-4, IR-2, IR-3, IR-5, IR-6, IR-8, PE-6, PL-2, PM-12, SA-8, SC-5, SC-7, SI-3, SI-4, SI-7.

Zabezpieczenia rozszerzone:

(1) OBSŁUGA INCYDENTÓW | ZAUTOMATYZOWANE PROCESY OBSŁUGI INCYDENTÓW

Wspieraj proces obsługi incydentów przy użyciu [Realizacja: zautomatyzowane mechanizmy zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(2) OBSŁUGA INCYDENTÓW | DYNAMICZNA REKONFIGURACJA

Uwzględnij następujące typy dynamicznej rekonfiguracji dla [Realizacja: komponenty systemu zdefiniowane przez organizację] jako część możliwości reagowania na incydenty: [Realizacja: typy dynamicznej rekonfiguracji zdefiniowane przez organizację].

Zabezpieczenia powiązane: AC-2, AC-4, CM-2.

(3) OBSŁUGA INCYDENTÓW | CIĄGŁOŚĆ DZIAŁANIA

Zidentyfikuj [Realizacja: klasy incydentów zdefiniowane przez organizację] i podejmij następujące działania w odpowiedzi na te incydenty, aby zapewnić ciągłość misji organizacji i funkcji biznesowych: [Realizacja: działania zdefiniowane przez organizację w odpowiedzi na klasy incydentów].

Zabezpieczenia powiązane: nie dotyczy.

(4) OBSŁUGA INCYDENTÓW | KORELACJA INFORMACJI

Powiąż informacje o incydencie z indywidualnymi reakcjami na incydenty, aby uzyskać perspektywę całej organizacji w zakresie świadomości incydentów i reagowania na nie.

Zabezpieczenia powiązane: nie dotyczy.

(5) OBSŁUGA INCYDENTÓW | AUTOMATYCZNE WYŁĄCZANIE SYSTEMU

Zastosuj konfigurowalną funkcję umożliwiającą automatyczne wyłączenie systemu w przypadku wykrycia [Realizacja: naruszeń bezpieczeństwa zdefiniowanych przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(6) OBSŁUGA INCYDENTÓW | ZAGROŻENIA WEWNĘTRZNE

Zastosuj funkcję obsługi incydentów obejmujących zagrożenia wewnętrzne.

Zabezpieczenia powiązane: nie dotyczy.

(7) OBSŁUGA INCYDENTÓW | ZAGROŻENIA WEWNĘTRZNE – KOORDYNACJA WEWNĄTRZORGANIZACYJNA

Koordynuj możliwość obsługi incydentów związanych z zagrożeniami wewnętrznymi, w jednostkach wewnętrznych organizacji [Realizacja: jednostki zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(8) OBSŁUGA INCYDENTÓW | KORELACJA Z ORGANIZACJAMI ZEWNĘTRZNYMI

Współpracuj z [Realizacja: zewnętrzne organizacje zdefiniowane przez organizację] w celu korelowania i udostępniania [Realizacja: informacje o incydentach zdefiniowane przez organizację] w celu uzyskania perspektywy międzyorganizacyjnej w zakresie świadomości incydentów i skuteczniejszych reakcji na incydenty.

Zabezpieczenia powiązane: AU-16, PM-16.

(9) OBSŁUGA INCYDENTÓW | ZDOLNOŚĆ DO DYNAMICZNEJ REAKCJI

Zapewnij [Realizacja: dynamiczne zdolności reagowania zdefiniowane przez organizację] w celu reagowania na incydenty.

Zabezpieczenia powiązane: nie dotyczy.

(10) OBSŁUGA INCYDENTÓW | KOORDYNACJA ŁAŃCUCHA DOSTAW

Koordynuj działania związane z obsługą incydentów związanych z łańcuchem dostaw z innymi organizacjami zaangażowanymi w łańcuch dostaw.

Zabezpieczenia powiązane: CA-3, MA-2, SA-9, SR-8.

(11) OBSŁUGA INCYDENTÓW | ZINTEGROWANY ZESPÓŁ REAGOWANIA NA INCYDENTY

Utwórz i utrzymuj zintegrowany zespół reagowania na incydenty, który może zostać wysłany do dowolnej lokalizacji wskazanej przez organizację w [Realizacja: okres czasu określony przez organizację].

Zabezpieczenia powiązane: AT-3.

(12) OBSŁUGA INCYDENTÓW | ZŁOŚLIWY KOD I ANALIZA KRYMINALISTYCZNA

Przeprowadź analizę złośliwego kodu i/lub innych pozostałości w systemie po incydencie.

Zabezpieczenia powiązane: nie dotyczy.

(13) OBSŁUGA INCYDENTÓW | ANALIZA ZACHOWAŃ

Przeanalizuj nietypowe lub podejrzewane wrogie zachowania w [Realizacja: środowiskach lub zasobach zdefiniowanych przez organizację] lub w związku z nimi.

Zabezpieczenia powiązane: nie dotyczy.

(14) OBSŁUGA INCYDENTÓW | CENTRUM OPERACJI BEZPIECZEŃSTWA

Utwórz i utrzymuj centrum operacji bezpieczeństwa.

Zabezpieczenia powiązane: nie dotyczy.

(15) OBSŁUGA INCYDENTÓW | PUBLIC RELATIONS I NAPRAWA REPUTACJI

Zarządzaj relacjami publicznymi związanymi z incydentem oraz wdrażaj środki mające na celu naprawę reputacji organizacji.

Zabezpieczenia powiązane: nie dotyczy.

IR-5 MONITOROWANIE INCYDENTÓW

Zabezpieczenie:

Śledź i dokumentuj incydenty.

Zabezpieczenia powiązane: AU-6, AU-7, IR-4, IR-8, PE-6, PM-5, SC-5, SC-7, SI-3, SI-4, SI-7.

Zabezpieczenia rozszerzone:

(1) MONITOROWANIE INCYDENTÓW | AUTOMATYCZNE ŚLEDZENIE, ZBIERANIE DANYCH I ANALIZA

Śledź incydenty oraz zbieraj i analizuj informacje o incydentach, korzystając z [Realizacja: zautomatyzowanych mechanizmów zdefiniowanych przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

IR-6 RAPORTOWANIE INCYDENTÓW

Zabezpieczenie:

a. Wymagaj od personelu zgłaszania podejrzeń incydentów do działu reagowania na incydenty w organizacji w ciągu [Realizacja: okres czasu określony przez organizację];

b. Zgłoś informację o incydencie do [Realizacja: uprawnienia określone w organizacji].

Zabezpieczenia powiązane: CM-6, CP-2, IR-4, IR-5, IR-8, IR-9.

Zabezpieczenia rozszerzone:

(1) RAPORTOWANIE INCYDENTÓW | AUTOMATYCZNE RAPORTOWANIE

Zgłaszaj incydenty za pomocą [Realizacja: zautomatyzowane mechanizmy zdefiniowane przez organizację].

Zabezpieczenia powiązane: IR-7.

(2) RAPORTOWANIE INCYDENTÓW | PODATNOŚĆ NA INCYDENTY

Zgłaszaj luki w zabezpieczeniach systemu związane ze zgłoszonymi incydentami do [Realizacja: personel lub role zdefiniowane w organizacji].

Zabezpieczenia powiązane: nie dotyczy.

(3) RAPORTOWANIE INCYDENTÓW | KOORDYNACJA ŁAŃCUCHA DOSTAW

Przekaż informacje o incydencie dostawcy produktu lub usługi oraz innym organizacjom zaangażowanym w łańcuch dostaw lub zarządzanie łańcuchem dostaw w odniesieniu do systemów lub komponentów systemów, których dotyczy incydent.

Zabezpieczenia powiązane: SR-8.

IR-7 WSPARCIE REAGOWANIA NA INCYDENTY

Zabezpieczenie:

Zapewnij zasoby wsparcia w zakresie reagowania na incydenty, stanowiące integralną część zdolności reagowania na incydenty w organizacji, oferuj użytkownikom systemu porady i pomoc w zakresie obsługi i zgłaszania incydentów.

Zabezpieczenia powiązane: AT-2, AT-3, IR-4, IR-6, IR-8, PM-22, PM-26, SA-9, SI-18.

Zabezpieczenia rozszerzone:

(1) WSPARCIE REAGOWANIA NA INCYDENTY | AUTOMATYCZNE WSPARCIE DOSTĘPNOŚCI INFORMACJI / OBSŁUGI

Zwiększ dostępność informacji i wsparcia w zakresie reagowania na incydenty, korzystając z [Realizacja: zautomatyzowane mechanizmy zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(2): WSPARCIE REAGOWANIA NA INCYDENTY | KOORDYNACJA Z ZEWNĘTRZNYMI DOSTAWCAMI

a. Nawiąż bezpośrednią, opartą na współpracy relację pomiędzy zdolnością reagowania na incydenty a zewnętrznymi dostawcami zdolności ochrony systemu;

b. Wskaż zewnętrznym dostawcom członków zespołu reagowania na incydenty w organizacji.

Zabezpieczenia powiązane: nie dotyczy.

IR-8: PLAN REAGOWANIA NA INCYDENTY

Zabezpieczenie:

a. Opracuj plan reagowania na incydenty, który:

   1. Dostarcza organizacji plan działania w celu wdrożenia zdolności reagowania na incydenty;

2. Opisuje strukturę i organizację zdolności reagowania na incydenty;

3. Zapewnia ogólne podejście do tego, w jaki sposób zdolność reagowania na incydenty wpisuje się w strukturę całej organizacji;

4. Spełnia wyjątkowe wymagania organizacji związane z misją, wielkością, strukturą i funkcjami;

5. Definiuje incydenty podlegające zgłoszeniu;

6. Dostarcza metryk do pomiaru zdolności reagowania na incydenty w organizacji;

7. Definiuje zasoby i wsparcie kierownictwa potrzebne do efektywnego utrzymania i doskonalenia zdolności reagowania na incydenty;

8. Dotyczy udostępniania informacji o incydentach;

9. Został sprawdzony i zatwierdzony przez [Realizacja: personel lub role zdefiniowane przez organizację] [Realizacja: częstotliwość zdefiniowana przez organizację]; i

10. Wyraźnie wskazuje odpowiedzialność za reagowanie na incydenty na [Realizacja: podmioty, personel lub role zdefiniowane w organizacji].

b. Przekaż kopie planu reagowania na incydenty do [Realizacja: Określony przez organizację zespół reagowania na incydenty (określonemu według nazwiska i/lub roli) oraz jednostkom organizacyjnym];

c. Zaktualizuj plan reagowania na incydenty, aby uwzględnić zmiany systemowe i organizacyjne lub problemy napotkane podczas wdrażania, wykonywania lub testowania planu;

d. Przekaż zmiany w planie reagowania na incydenty do [Realizacja: Określony przez organizację zespół reagowania na incydenty (określonemu według nazwiska i/lub roli) oraz jednostkom organizacyjnym];

e. Chroń plan reagowania na incydenty przed nieautoryzowanym ujawnieniem i modyfikacją.

Zabezpieczenia powiązane: AC-2, CP-2, CP-4, IR-4, IR-7, IR-9, PE-6, PL-2, SA-15, SI-12, SR-8.

Zabezpieczenia rozszerzone:

(1) PLAN REAGOWANIA NA INCYDENTY | NARUSZENIA

W przypadku naruszeń obejmujących dane osobowe w Planie reagowania na incydenty uwzględnij następujące elementy:

a. Proces mający na celu ustalenie, czy konieczne jest powiadomienie osób fizycznych lub innych organizacji, w tym organizacji nadzorczych;

b. Proces oceny mający na celu określenie stopnia szkody, naruszenia prywatności, niedogodności lub niesprawiedliwego traktowania osób poszkodowanych w wyniku incydentu bezpieczeństwa oraz identyfikację mechanizmów mających na celu minimalizację takich skutków.

c. Identyfikację obowiązujących wymogów prywatności.

Zabezpieczenia powiązane: PT-1, PT-2, PT-3, PT-4, PT-5, PT-7.

IR-9: REAKCJA NA WYCIEK / UJAWNIENIE INFORMACJI

Zabezpieczenie:

Reaguj na wycieki informacji poprzez:

a. Przypisywanie [Realizacja: personelowi lub rolom zdefiniowanym przez organizację] odpowiedzialności za reagowanie na wycieki informacji;

b. Określenie konkretnych informacji mających związek z zanieczyszczeniem systemu;

c. Powiadomienie [Realizacja: personel lub role określone w organizacji] o wycieku informacji przy użyciu metody komunikacji niezwiązanej z wyciekiem;

d. Izolowanie zanieczyszczonego układu lub podzespołu układu;

e. Usuwanie informacji z zainfekowanego systemu lub komponentu;

f. Identyfikacja innych systemów lub podzespołów systemów, które mogły ulec późniejszemu zanieczyszczeniu; oraz

g. Wykonanie następujących dodatkowych czynności: [Realizacja: czynności zdefiniowane przez organizację].

Zabezpieczenia powiązane: AT-2, AT-3, CP-2, CP-3, IR-2, IR-6, PM-26, PM-27, PT-2, PT-3, PT-7, RA-7.

Zabezpieczenia rozszerzone:

(1) REAKCJA NA WYCIEK / UJAWNIENIE INFORMACJI | PERSONEL ODPOWIEDZIALNY

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(2) REAKCJA NA WYCIEK / UJAWNIENIE INFORMACJI | SZKOLENIE

Zapewnij szkolenie w zakresie reagowania na wyciek informacji [Realizacja: częstotliwość określona przez organizację].

Zabezpieczenia powiązane: AT-2, AT-3, CP-3, IR-2.

(3) REAKCJA NA WYCIEK / UJAWNIENIE INFORMACJI | OPERACJE PO WYCIEKU

Wprowadź procedury zapewniające, że personel organizacji, której dotyczy wyciek informacji, będzie mógł kontynuować wykonywanie przypisanych zadań, podczas gdy w zainfekowanych systemach będą podejmowane działania naprawcze: [Realizacja: procedury zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(4) REAKCJA NA WYCIEK / UJAWNIENIE INFORMACJI | NARAŻENIE NA KONTAKT Z NIEUPOWAŻNIONYM PERSONELEM

W przypadku personelu narażonego na dostęp do informacji nieobjętych przyznanymi uprawnieniami stosuj następujące środki kontroli: [Realizacja: środki kontroli zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

IR-10: ZESPÓŁ DS. ZINTEGROWANEJ ANALIZY BEZPIECZEŃSTWA INFORMACJI

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

KATEGORIA: MA - UTRZYMANIE I WSPARCIE

MA-1 POLITYKA I PROCEDURY

Zabezpieczenie:

a. Opracuj, udokumentuj i rozpowszechnij wśród [Realizacja: personel lub role zdefiniowane przez organizację]:

   1. [Wybór (jeden lub więcej): Poziom organizacji; Poziom misji/procesu biznesowego; Poziom systemu] politykę konserwacji, która:

      (a) dotyczy celu, zakresu, ról, obowiązków, zaangażowania kierownictwa, koordynacji między jednostkami organizacyjnymi i zgodności;

      (b) jest zgodna z obowiązującymi przepisami prawa, rozporządzeniami wykonawczymi, dyrektywami, regulacjami, politykami, standardami i wytycznymi;

   2. Procedury ułatwiające wdrażanie polityki konserwacji i powiązanych kontroli konserwacji;

b. Wyznacz [Realizacja: urzędnika zdefiniowanego przez organizację] do zarządzania rozwojem, dokumentowaniem i rozpowszechnianiem polityki i procedur konserwacji;

c. Przeglądaj i aktualizuj na bieżąco polityki konserwacji w:

   1. Polityce [Realizacja: częstotliwość zdefiniowana przez organizację] i następujących [Realizacja: zdarzenia zdefiniowane przez organizację];

   2. Procedurach [Realizacja: częstotliwość zdefiniowana przez organizację] i następujących [Realizacja: zdarzenia zdefiniowane przez organizację].

Zabezpieczenia powiązane: PM-9, PS-8, SI-12.

Zabezpieczenia rozszerzone: nie dotyczy.

MA-2 KONTROLOWANA KONSERWACJA

Zabezpieczenie:

a. Planuj, dokumentuj i przeglądaj zapisy konserwacji, napraw i wymiany podzespołów systemu zgodnie ze specyfikacjami producenta lub dostawcy i/lub wymogami organizacyjnymi;

b. Zatwierdzaj i monitoruj wszystkie czynności konserwacyjne, niezależnie od tego, czy są wykonywane na miejscu, czy zdalnie oraz niezależnie od tego, czy system lub podzespoły systemu są serwisowane na miejscu, czy też przenoszone do innej lokalizacji;

c. Wymagaj, aby [Realizacja: personel lub role zdefiniowane przez organizację] wyraźnie zatwierdzano usunięcie systemu lub podzespołów systemu z obiektów organizacyjnych w celu przeprowadzenia konserwacji, naprawy lub wymiany poza obiektem;

d. Kontroluj sprzęt mający na celu usunięcie następujących informacji z powiązanych nośników przed usunięciem z obiektów organizacyjnych w celu przeprowadzenia konserwacji, naprawy lub wymiany poza obiektem: [Realizacja: informacje zdefiniowane przez organizację];

e. Sprawdzaj wszystkie potencjalne naruszenia zabezpieczeń w celu zweryfikowania, czy nadal działają one prawidłowo po przeprowadzeniu czynności konserwacyjnych, naprawczych lub wymianie;

f. Dołączaj następujące informacje do rejestrów konserwacji organizacji: [Realizacja: informacje zdefiniowane przez organizację].

Zabezpieczenia powiązane: CM-2, CM-3, CM-4, CM-5, CM-8, MA-4, MP-6, PE-16, SI-2, SR-3, SR-4, SR-11.

Zabezpieczenia rozszerzone:

(1) KONTROLOWANA KONSERWACJA | ZAWARTOŚĆ REKORDU

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(2) KONTROLOWANA KONSERWACJA | ZAUTOMATYZOWANE DZIAŁANIA KONSERWACYJNE

a. Planuj, przeprowadzaj i dokumentuj działania konserwacyjne, naprawcze i wymiany systemu przy użyciu [Realizacja: zautomatyzowane mechanizmy zdefiniowane przez organizację];

b. Prowadź aktualne, dokładne i kompletne zapisy wszystkich zlecanych, zaplanowanych, trwających i zakończonych działań konserwacyjnych, naprawczych i wymian.

Zabezpieczenia powiązane: MA-3.

MA-3 NARZĘDZIA KONSERWACYJNE

Zabezpieczenie:

a. Zatwierdzaj, kontroluj i monitoruj korzystanie z narzędzi do konserwacji systemu;

b. Przeglądaj wcześniej zatwierdzone narzędzia do konserwacji systemu [Realizacja: częstotliwość zdefiniowana przez organizację].

Zabezpieczenia powiązane: MA-2, PE-16.

Zabezpieczenia rozszerzone:

(1) NARZĘDZIA KONSERWACYJNE | INSPEKCJA NARZĘDZI

Sprawdź, czy narzędzia konserwacyjne używane przez personel konserwacyjny nie zostały poddane niewłaściwym lub nieautoryzowanym modyfikacjom.

Zabezpieczenia powiązane: SI-7.

(2) NARZĘDZIA KONSERWACYJNE | INSPEKCJA NOŚNIKÓW

Sprawdź nośniki zawierające programy diagnostyczne i testowe pod kątem obecności złośliwego kodu przed ich użyciem w systemie.

Zabezpieczenia powiązane: SI-3.

(3) NARZĘDZIA KONSERWACYJNE | ZAPOBIEGAJ NIEAUTORYZOWANEMU USUWANIU

Zapobiegaj usuwaniu sprzętu konserwacyjnego zawierającego informacje organizacyjne poprzez:

a. sprawdzenie, czy na sprzęcie nie znajdują się żadne informacje organizacyjne;

b. kasowanie danych lub niszczenie sprzętu;

c. zachowanie sprzętu w obiekcie;

d. uzyskanie zwolnienia z [Realizacja: personel lub role określone przez organizację] wyraźnie upoważniającego do usunięcia sprzętu z obiektu.

Zabezpieczenia powiązane: MP-6.

(4) NARZĘDZIA KONSERWACYJNE | OGRANICZONE UŻYCIE NARZĘDZI

Zezwalaj na używanie narzędzi konserwacyjnych wyłącznie przez personel upoważniony.

Zabezpieczenia powiązane: AC-3, AC-5, AC-6.

(5) NARZĘDZIA KONSERWACYJNE | WYKONYWANIE Z UPRAWNIENIAMI

Monitoruj wykorzystanie narzędzi konserwacyjnych, które działają z większymi uprawnieniami.

Zabezpieczenia powiązane: AC-3, AC-6.

(6) NARZĘDZIA KONSERWACYJNE | AKTUALIZACJE OPROGRAMOWANIA I POPRAWKI

Sprawdź narzędzia konserwacyjne, aby upewnić się, że zainstalowano najnowsze aktualizacje i poprawki oprogramowania.

Zabezpieczenia powiązane: AC-3, AC-6.

MA-4 KONSERWACJA ZDALNA

Zabezpieczenie:

a. Zatwierdzaj i monitoruj zdalne działania konserwacyjne i diagnostyczne;

b. Zezwalaj na korzystanie ze zdalnych narzędzi konserwacyjnych i diagnostycznych wyłącznie zgodnie z polityką organizacji oraz udokumentowanych w planie bezpieczeństwa systemu;

c. Stosuj silne uwierzytelnianie podczas ustanawiania sesji konserwacyjnych i diagnostycznych spoza lokalizacji;

d. Dokumentuj zapisy działań konserwacyjnych i diagnostycznych spoza lokalizacji;

e. Kończ sesje i połączenia sieciowe po zakończeniu konserwacji spoza lokalizacji.

Zabezpieczenia powiązane: AC-2, AC-3, AC-6, AC-17, AU-2, AU-3, IA-2, IA-4, IA-5, IA-8, MA-2, MA-5, PL- 2, SC-7, SC-10.

Zabezpieczenia rozszerzone:

(1) KONSERWACJA ZDALNA | REJESTROWANIE I PRZEGLĄD

a. Rejestruj [Realizacja: zdarzenia audytu zdefiniowane przez organizację] dla sesji konserwacji i diagnostyki, które nie są lokalne;

b. Przejrzyj zapisy audytu sesji konserwacji i diagnostyki w celu wykrycia zachowań nietypowych.

Zabezpieczenia powiązane: AU-6, AU-12.

(2) KONSERWACJA ZDALNA | DOKUMENTOWANIE KONSERWACJI ZDALNEJ

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(3) KONSERWACJA ZDALNA | PORÓWNYWALNE ZABEZPIECZENIA I SANITYZACJA

a. Wymagaj, aby zdalne usługi konserwacyjne i diagnostyczne były wykonywane z systemu, który implementuje poziom zabezpieczeń porównywalny z serwisowanym systemem;

b. Przed wykonaniem usług konserwacyjnych lub diagnostycznych spoza systemu usuń z systemu komponent, który ma być serwisowany; oczyść komponent (z informacji organizacyjnych); a po

wykonaniu usługi, sprawdź i oczyść komponent (w celu wykrycia potencjalnie złośliwego oprogramowania) przed ponownym podłączeniem tego komponentu do systemu.

Zabezpieczenia powiązane: MP-6, SI-3, SI-7.

(4) KONSERWACJA ZDALNA | UWIERZYTELNIANIE I ROZDZIELANIE SESJI KONSERWACYJNYCH

Chroń zdalne sesje konserwacyjne poprzez:

a. Zastosowanie [Realizacja: zdefiniowanych przez organizację jednorazowych metod uwierzytelniania];

b. Oddzielenie sesji konserwacyjnych od innych sesji sieciowych w systemie poprzez:

   1. Fizycznie oddzielone ścieżki komunikacyjne;

   2. Logicznie oddzielone ścieżki komunikacyjne.

Zabezpieczenia powiązane: nie dotyczy.

(5) KONSERWACJA ZDALNA| ZATWIERDZENIA I POWIADOMIENIA

a. Wymagaj zatwierdzenia każdej zdalnej sesji konserwacji przez [Realizacja: personel lub role określone w organizacji];

b. Powiadamiaj personel lub właściwe grupy o dacie i godzinie planowanej konserwacji zdalnej: [Realizacja: personel lub role określone w organizacji].

Zabezpieczenia powiązane: nie dotyczy.

(6) KONSERWACJA ZDALNA | OCHRONA KRYPTOGRAFICZNA

Wprowadź następujące mechanizmy kryptograficzne w celu ochrony integralności i poufności zdalnej komunikacji konserwacyjnej i diagnostycznej z systemem lokalnym: [Realizacja: mechanizmy kryptograficzne zdefiniowane przez organizację].

Zabezpieczenia powiązane: SC-8, SC-12, SC-13.

(7) KONSERWACJA ZDALNA | WERYFIKACJA ROZŁĄCZENIA

Weryfikuj zakończenia sesji i połączenia sieciowe po zakończeniu sesji konserwacji i diagnostyki zdalnej.

Zabezpieczenia powiązane: AC-12.

MA-5 PERSONEL KONSERWACYJNY

Zabezpieczenie:

a. Wprowadź proces autoryzacji personelu konserwacyjnego i prowadź listę upoważnionych organizacji lub personelu konserwacyjnego;

b. Zweryfikuj, czy personel nieeskortowany wykonujący konserwację systemu posiada wymagane uprawnienia dostępu;

c. Wyznacz personel organizacyjny z wymaganymi uprawnieniami dostępu i kompetencjami technicznymi do nadzorowania działań konserwacyjnych personelu, który nie posiada wymaganych uprawnień dostępu.

Zabezpieczenia powiązane: AC-2, AC-3, AC-5, AC-6, IA-2, IA-8, MA-4, MP-2, PE-2, PE-3, PS-7, RA-3.

Zabezpieczenia rozszerzone:

(1) PERSONEL KONSERWACYJNY | OSOBY BEZ ODPOWIEDNIEGO DOSTĘPU

a. Wprowadź procedury dotyczące korzystania z personelu konserwacyjnego, który nie posiada odpowiednich uprawnień bezpieczeństwa lub nie jest obywatelem Polski, obejmujące następujące wymagania:

    1. Personel konserwacyjny, który nie posiada wymaganych upoważnień dostępu, uprawnień ani formalnych zatwierdzeń dostępu, jest eskortowany i nadzorowany podczas wykonywania czynności konserwacyjnych i diagnostycznych w systemie przez zatwierdzony personel organizacyjny, który posiada pełne uprawnienia, odpowiednie upoważnienia dostępu i kwalifikacje techniczne;

    2. Przed rozpoczęciem czynności konserwacyjnych lub diagnostycznych przez personel, który nie posiada wymaganych upoważnień dostępu, uprawnień ani formalnych zatwierdzeń dostępu, wszystkie komponenty ulotnej pamięci masowej w systemie są czyszczone, a wszystkie trwałe nośniki pamięci są usuwane lub fizycznie odłączane od systemu i zabezpieczane;

b. Opracuj i wprowadź [Realizacja: alternatywne kontrole zdefiniowane przez organizację] na wypadek, gdyby komponentu systemu nie można było oczyścić, usunąć lub odłączyć od systemu.

Zabezpieczenia powiązane: MP-6, PL-2.

(2) PERSONEL KONSERWACYJNY | UPRAWNIENIA BEZPIECZEŃSTWA DLA SYSTEMÓW NIEJAWNYCH

Sprawdzaj, czy personel wykonujący czynności konserwacyjne i diagnostyczne w systemie przetwarzającym, przechowującym lub przesyłającym informacje niejawne posiada odpowiednie poświadczenia bezpieczeństwa i formalne zezwolenia dostępu co najmniej do najwyższego poziomu tajności oraz do przedziałów informacji w systemie.

Zabezpieczenia powiązane: PS-3.

(3) PERSONEL KONSERWACYJNY | WYMAGANIA DOTYCZĄCE OBYWATELSTWA DLA SYSTEMÓW NIEJAWNYCH

Zweryfikuj, czy osoby wykonujące prace konserwacyjne i diagnostyczne na systemie przetwarzającym, przechowującym lub przesyłającym informacje niejawne są obywatelami Polski.

Zabezpieczenia powiązane: PS-3.

(4) PERSONEL KONSERWACYJNY | CUDZOZIEMCY

Zapewnij się, że:

a. obcokrajowcy posiadający odpowiednie uprawnienia bezpieczeństwa są zatrudniani do prowadzenia prac konserwacyjnych i diagnostycznych w systemach tajnych wyłącznie w przypadku, gdy systemy te są wspólną własnością Polski i rządów sojuszniczych innych państw lub są własnością i są obsługiwane wyłącznie przez rządy sojusznicze innych państw;

b. zgody, zezwolenia oraz szczegółowe warunki operacyjne dotyczące korzystania z obcokrajowców do prowadzenia prac konserwacyjnych i diagnostycznych w systemach niejawnych są w pełni udokumentowane w Porozumieniach Współpracy.

Zabezpieczenia powiązane: PS-3.

(5) PERSONEL KONSERWACYJNY | KONSERWACJA NIEZWIĄZANA Z UTRZYMANIEM SYSTEMU

Zapewnij, że personel bez eskorty, wykonujący czynności konserwacyjne niezwiązane bezpośrednio z systemem, ale znajdujący się w jego fizycznej bliskości, posiada wymagane uprawnienia dostępu.

Zabezpieczenia powiązane: nie dotyczy.

MA-6 TERMINOWA KONSERWACJA

Zabezpieczenie:

Zapewnij wsparcie i/lub części zamienne dla [Realizacja: komponenty systemu zdefiniowane przez organizację] w ciągu [Realizacja: okres czasu zdefiniowany przez organizację] od awarii.

Zabezpieczenia powiązane: CM-8, CP-2, CP-7, RA-7, SA-15, SI-13, SR-2, SR-3, SR-4.

Zabezpieczenia rozszerzone:

(1) TERMINOWA KONSERWACJA | KONSERWACJA ZAPOBIEGAWCZA

Wykonuj konserwację zapobiegawczą [Realizacja: komponenty systemu zdefiniowane przez organizację] w [Realizacja: odstępach czasu zdefiniowanych przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(2) TERMINOWA KONSERWACJA | KONSERWACJA PREDYKCYJNA

Wykonuj konserwację predykcyjną [Realizacja: komponenty systemu zdefiniowane przez organizację] w [Realizacja: odstępach czasu zdefiniowanych przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(3) TERMINOWA KONSERWACJA | ZAUTOMATYZOWANE WSPARCIE DLA KONSERWACJI PREDYKCYJNEJ

Przesyłaj dane dotyczące konserwacji predykcyjnej do systemu zarządzania konserwacją przy użyciu [Realizacja: zautomatyzowane mechanizmy zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

MA-7 KONSERWACJA W TERENIE

Zabezpieczenie:

Ogranicz lub zabroń przeprowadzania konserwacji w terenie na [Określone przez organizację systemy lub komponenty systemu] wyłącznie do [Określonych przez organizację zaufanych obiektów serwisowych].

Zabezpieczenia powiązane: MA-2, MA-4, MA-5.

Zabezpieczenia rozszerzone: nie dotyczy.

KATEGORIA: MP – OCHRONA NOŚNIKÓW DANYCH

MP-1 POLITYKA I PROCEDURY

Zabezpieczenie:

a. Opracowuj, udokumentuj i rozpowszechnij wśród [Realizacja: personel lub role zdefiniowane przez organizację]:

    1. [Wybór (jeden lub więcej): Poziom organizacji; Poziom misji/procesu biznesowego; Poziom systemu] polityki ochrony mediów, która:

        (a) dotyczy celu, zakresu, ról, obowiązków, zaangażowania kierownictwa, koordynacji między jednostkami organizacyjnymi i zgodności;

        (b) jest zgodna z obowiązującymi przepisami prawa, rozporządzeniami wykonawczymi, dyrektywami, regulacjami, politykami, standardami i wytycznymi;

    2. Procedur ułatwiających wdrażanie polityki ochrony nośników danych i powiązanych kontroli ochrony nośników danych;

b. Wyznacz [Realizacja: urzędnika zdefiniowanego przez organizację] do zarządzania opracowywaniem, dokumentowaniem i rozpowszechnianiem polityki i procedur ochrony nośników danych;

c. Przeglądaj i aktualizuj na bieżąco ochronę nośników danych w:

   1. Polityce [Realizacja: częstotliwość zdefiniowana przez organizację] i następujących [Realizacja: zdarzenia zdefiniowane przez organizację];

   2. Procedurach [Realizacja: częstotliwość zdefiniowana przez organizację] i następujących [Realizacja: zdarzenia zdefiniowane przez organizację].

Zabezpieczenia powiązane: PM-9, PS-8, SI-12.

Zabezpieczenia rozszerzone: nie dotyczy.

MP-2 DOSTĘP DO NOŚNIKÓW

Zabezpieczenie:

Ogranicz dostęp do [Realizacja: typy mediów cyfrowych i/lub nie cyfrowych zdefiniowane przez organizację] do [Realizacja: personel lub role zdefiniowane przez organizację].

Zabezpieczenia powiązane:

AC-19, AU-9, CP-2, CP-9, CP-10, MA-5, MP-4, MP-6, PE-2, PE-3, SC-12, SC-13, SC- 34, SI-12.

Zabezpieczenia rozszerzone:

(1) DOSTĘP DO NOŚNIKÓW | ZAUTOMATYZOWANY OGRANICZONY DOSTĘP

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(2) DOSTĘP DO NOŚNIKÓW | OCHRONA KRYPTOGRAFICZNA

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

MP-3 OZNAKOWANIE NOŚNIKÓW

Zabezpieczenie:

a. Oznacz nośniki systemowe, wskazując ograniczenia dystrybucji, zastrzeżenia dotyczące obsługi i stosowne oznaczenia bezpieczeństwa informacji (jeśli takie istnieją);

b. Zwolnij [Realizacja: typy nośników systemowych zdefiniowane przez organizację] z oznaczenia, jeśli nośniki pozostają w [Realizacja: obszary kontrolowane zdefiniowane przez organizację].

Zabezpieczenia powiązane: AC-16, CP-9, MP-5, PE-22, SI-12.

Zabezpieczenia rozszerzone: nie dotyczy.

MP-4 PRZECHOWYWANIE NOŚNIKÓW

Zabezpieczenie:

a. Fizycznie kontroluj i bezpiecznie przechowuj [Realizacja: typy nośników cyfrowych i/lub nie cyfrowych zdefiniowane przez organizację] w [Realizacja: obszary kontrolowane zdefiniowane przez organizację];

b. Chroń typy nośników systemowych zdefiniowane w MP-4a do momentu zniszczenia lub wykasowania nośników przy użyciu zatwierdzonego sprzętu, technik i procedur.

Zabezpieczenia powiązane: AC-19, CP-2, CP-6, CP-9, CP-10, MP-2, MP-7, PE-3, PL-2, SC-12, SC-13, SC-28, SC- 34, SI-12.

Zabezpieczenia rozszerzone:

(1) PRZECHOWYWANIE NOŚNIKÓW | OCHRONA KRYPTOGRAFICZNA

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(2) PRZECHOWYWANIE NOŚNIKÓW | ZAUTOMATYZOWANY OGRANICZONY DOSTĘP

Ogranicz dostęp do obszarów przechowywania multimediów i rejestruj próby dostępu oraz przyznane uprawnienia za pomocą [Realizacja: zautomatyzowane mechanizmy zdefiniowane przez organizację].

Zabezpieczenia powiązane: AC-3, AU-2, AU-6, AU-9, AU-12, PE-3.

MP-5 TRANSPORT MEDIÓW

Zabezpieczenie:

a. Chroń i kontroluj [Realizacja: typy nośników systemowych zdefiniowane przez organizację] podczas transportu poza obszary kontrolowane przy użyciu [Realizacja: kontrole zdefiniowane przez organizację];

b. Utrzymuj odpowiedzialność za nośniki systemowe podczas transportu poza obszary kontrolowane;

c. Dokumentuj działania związane z transportem nośników systemowych;

d. Ograniczaj działania związane z transportem nośników systemowych do upoważnionego personelu.

Zabezpieczenia powiązane: AC-7, AC-19, CP-2, CP-9, MP-3, MP-4, PE-16, PL-2, SC-12, SC-13, SC-28, SC-34.

Zabezpieczenia rozszerzone:

(1) TRANSPORT MEDIÓW | OCHRONA POZA OBSZARAMI KONTROLOWANYMI

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(2) TRANSPORT MEDIÓW | DOKUMENTACJA DZIAŁAŃ

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(3) TRANSPORT MEDIÓW | OPIEKUNOWIE

Wyznaczyć opiekunów na czas transportu nośników systemowych poza obszary kontrolowane.

Zabezpieczenia powiązane: nie dotyczy.

(4) TRANSPORT MEDIÓW | OCHRONA KRYPTOGRAFICZNA

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

MP-6 KASOWANIE NOŚNIKÓW

Zabezpieczenie:

a. Usuwaj dane z nośników [Realizacja: nośniki systemowe zdefiniowane przez organizację] przed utylizacją, wydaniem poza kontrolę organizacji lub wydaniem do ponownego użycia, stosując [Realizacja: techniki i procedury kasowania zdefiniowane przez organizację];

b. Zastosuj mechanizmy kasowania o sile i integralności współmiernej do kategorii bezpieczeństwa lub klasyfikacji informacji.

Zabezpieczenia powiązane: AC-3, AC-7, AU-11, MA-2, MA-3, MA-4, MA-5, PM-22, SI-12, SI-18, SI-19, SR-11.

Zabezpieczenia rozszerzone:

(1) KASOWANIE NOŚNIKÓW | PRZEGLĄDAĆ, ZATWIERDZAĆ, ŚLEDZIĆ, DOKUMENTOWAĆ I WERYFIKOWAĆ

Przeglądaj, zatwierdzaj, śledź, dokumentuj i weryfikuj czynności związane z kasowaniem i utylizacją nośników.

Zabezpieczenia powiązane: nie dotyczy.

(2) KASOWANIE NOŚNIKÓW | TESTOWANIE SPRZĘTU

Testuj sprzęt i procedury kasowania [Realizacja: częstotliwość określona przez organizację], aby zapewnić, że spełniono wymagania w zakresie kasowania.

Zabezpieczenia powiązane: nie dotyczy.

(3) KASOWANIE NOŚNIKÓW | TECHNIKI NIENISZCZĄCE

Zastosuj nieniszczące techniki kasowania przed podłączeniem przenośnych urządzeń pamięci masowej do systemu w następujących okolicznościach: [Realizacja: okoliczności określone przez organizację wymagające kasowania przenośnych urządzeń pamięci masowej].

Zabezpieczenia powiązane: nie dotyczy.

(4) KASOWANIE NOŚNIKÓW | KONTROLOWANE INFORMACJE JAWNE

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(5) KASOWANIE NOŚNIKÓW | INFORMACJE NIEJAWNE

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(6) KASOWANIE NOŚNIKÓW | NISZCZENIE NOŚNIKÓW

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(7) KASOWANIE NOŚNIKÓW | PODWÓJNA AUTORYZACJA

Wymagaj podwójnej autoryzacji w celu kasowania [Realizacja: nośniki systemowe zdefiniowane przez organizację].

Zabezpieczenia powiązane: AC-3, MP-2.

(8) KASOWANIE NOŚNIKÓW | ZDALNE USUWANIE LUB WYMAZYWANIE INFORMACJI

Zapewnij możliwość usuwania lub wymazywania informacji z [Realizacja: systemów zdefiniowanych przez organizację lub komponentów systemu] [Wybór: zdalnie; pod następującymi warunkami: [Realizacja: warunki zdefiniowane przez organizację]].

Zabezpieczenia powiązane: nie dotyczy.

MP-7 UŻYWANIE NOŚNIKÓW

Zabezpieczenie:

a. [Wybór: Ograniczyć; Zabronić] używania [Realizacja: typy nośników systemowych zdefiniowane przez organizację] w [Realizacja: systemy zdefiniowane przez organizację lub komponenty systemu] przy użyciu [Realizacja: elementy sterujące zdefiniowane przez organizację];

b. Zabroń używania przenośnych urządzeń pamięci masowej w systemach organizacyjnych, gdy takie urządzenia nie mają identyfikowalnego właściciela.

Zabezpieczenia powiązane: AC-19, AC-20, PL-4, PM-12, SC-34, SC-41.

Zabezpieczenia rozszerzone:

(1) UŻYWANIE NOŚNIKÓW | ZABROŃ UŻYWANIA BEZ WŁAŚCICIELA

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(2) UŻYWANIE NOŚNIKÓW | ZAKAZ STOSOWANIA NOŚNIKÓW ODPORNYCH NA KASOWANIE

Zakazać stosowania w systemach organizacyjnych nośników odpornych na usuwanie danych.

Zabezpieczenia powiązane: MP-6.

MP-8 DEKLASYFIKACJA NOŚNIKÓW

Zabezpieczenie:

a. Wprowadź [Realizacja: zdefiniowany przez organizację proces deklasyfikacji], który obejmuje stosowanie mechanizmów deklasyfikacji o sile i integralności współmiernej do kategorii bezpieczeństwa lub klasyfikacji informacji;

b. Zweryfikuj, czy proces deklasyfikacji jest współmierny do kategorii bezpieczeństwa i/lub poziomu klasyfikacji informacji, które mają zostać usunięte oraz uprawnień dostępu potencjalnych odbiorców zdeklasyfikowanych informacji;

c. Zidentyfikuj [Realizacja: zdefiniowany przez organizację systemowy nośnik wymagający deklasyfikacji];

d. Zdeklasyfikuj zidentyfikowany nośnik informacji przy użyciu ustalonego procesu.

Zabezpieczenia powiązane: nie dotyczy.

Zabezpieczenia rozszerzone:

(1) DEKLASYFIKACJA NOŚNIKÓW | DOKUMENTACJA PROCESU

Dokumentuj deklasyfikację nośnika systemowego.

Zabezpieczenia powiązane: nie dotyczy.

(2) DEKLASYFIKACJA NOŚNIKÓW | TESTOWANIE SPRZĘTU

Testuj sprzęt do deklasyfikacji i procedury [Realizacja: częstotliwość określona przez organizację], aby upewnić się, że działania deklasyfikacji są realizowane prawidłowo.

Zabezpieczenia powiązane: nie dotyczy.

(3) DEKLASYFIKACJA NOŚNIKÓW | KONTROLOWANE INFORMACJE JAWNE

Deklasyfikuj nośniki systemowe zawierające kontrolowane, jawne informacje przed ich publicznym udostępnieniem.

Zabezpieczenia powiązane: nie dotyczy.

(4) DEKLASYFIKACJA NOŚNIKÓW | INFORMACJE NIEJAWNE

Deklasyfikuj nośniki systemowe zawierające informacje niejawne przed udostępnieniem ich osobom niemającym wymaganych uprawnień dostępu.

Zabezpieczenia powiązane: nie dotyczy.

KATEGORIA: PE - OCHRONA FIZYCZNA I ŚRODOWISKOWA

PE-1 POLITYKA I PROCEDURY

Zabezpieczenie:

a. Opracowuje, udokumentuj i rozpowszechnij wśród [Realizacja: personel lub role zdefiniowane w organizacji]:

   1. [Wybór (jedno lub więcej): na poziomie organizacji, na poziomie misji/procesu biznesowego, na poziomie systemu] politykę ochrony fizycznej i środowiskowej, która:

      (a) Adresuje cel, zakres, role, obowiązki, zaangażowanie kierownictwa, koordynację między jednostkami organizacyjnymi i zgodności z przepisami;

      (b) Jest zgodna z obowiązującymi przepisami prawa, rozporządzeniami wykonawczymi, dyrektywami, regulacjami, zasadami, normami i wytycznymi;

   2. Procedury ułatwiające wdrażanie polityki ochrony fizycznej i środowiskowej oraz powiązanych zabezpieczeń w zakresie ochrony fizycznej i środowiskowej;

b. Wyznacz [Realizacja: osoba wyznaczona przez organizację] do zarządzania rozwojem, dokumentacją i rozpowszechnianiem polityki i procedur ochrony fizycznej i środowiskowej;

c. Przeglądaj i aktualizuj:

   1. Politykę ochrony fizycznej i środowiskowej z [Realizacja: częstotliwość określona przez organizację] i następujących [Realizacja: zdarzenia określone przez organizację];

   2. Procedury ochrony fizycznej i środowiskowej z [Realizacja: częstotliwość określona przez organizację] i następujących [Realizacja: zdarzenia określone przez organizację].

Zabezpieczenia powiązane: AT-3, PM-9, PS-8, SI-12.

Zabezpieczenia rozszerzone: nie dotyczy.

PE-2 ZEZWOLENIA NA DOSTĘP FIZYCZNY

Zabezpieczenie:

a. Opracowuj, zatwierdzaj i prowadź listę osób upoważnionych do dostępu do obiektu, w którym znajduje się system;

b. Nadawaj uprawnienia dostępu do obiektu;

c. Przeglądaj listy dostępu zawierające szczegółowe informacje na temat autoryzowanego dostępu do obiektu przez osoby fizyczne [Realizacja: częstotliwość określona przez organizację];

d. Aktualizuj listy osób posiadających dostęp do obiektu.

Zabezpieczenia powiązane: AT-3, AU-9, IA-4, MA-5, MP-2, PE-3, PE-4, PE-5, PE-8, PM-12, PS-3, PS-4, PS-5, PS-6.

Zabezpieczenia rozszerzone:

(1) ZEZWOLENIA NA DOSTĘP FIZYCZNY | DOSTĘP WEDŁUG STANOWISKA LUB ROLI

Zezwalaj na dostęp fizyczny do obiektu, w którym znajduje się system, w zależności od posiadanego stanowiska lub roli.

Zabezpieczenia powiązane: AC-2, AC-3, AC-6.

(2) ZEZWOLENIA NA DOSTĘP FIZYCZNY | PODWÓJNA IDENTYFIKACJA

Wymagaj podwójnej identyfikacji w celu uzyskania dostępu gości do obiektu, w którym znajduje się system: [Realizacja: lista dopuszczalnych form identyfikacji zdefiniowana przez organizację].

Zabezpieczenia powiązane: IA-2, IA-4, IA-5.

(3) ZEZWOLENIA NA DOSTĘP FIZYCZNY | OGRANICZENIE DOSTĘPU BEZ ASYSTY

Ogranicz dostęp bez asysty do obiektu, w którym znajduje się system, wyłącznie do personelu posiadającego [Wybór (jedno lub więcej): poświadczenia bezpieczeństwa dla wszystkich informacji zawartych w systemie, formalne upoważnienia dostępu do wszystkich informacji zawartych w systemie, uzasadnioną potrzebę dostępu do wszystkich informacji zawartych w systemie, [Realizacja: zdefiniowane przez organizację fizyczne upoważnienia dostępu]].

Zabezpieczenia powiązane: PS-2, PS-6.

PE-3 KONTROLA DOSTĘPU FIZYCZNEGO

Zabezpieczenie:

a. Egzekwuj fizyczne uprawnienia dostępu w [Realizacja: zdefiniowanych przez organizację punktach wejścia i wyjścia do obiektu, w którym znajduje się system] poprzez:

    1. Weryfikację indywidualnych zezwoleń na dostęp przed udzieleniem dostępu do obiektu;

2. Kontrolę wejścia i wyjścia do obiektu przy użyciu [Realizacja (jedno lub więcej): [Realizacja: zdefiniowane przez organizację systemy lub urządzenia kontroli dostępu fizycznego], ochrona];

b. Prowadź dzienniki kontroli dostępu fizycznego w [Realizacja: punkty wejścia lub wyjścia zdefiniowane przez organizację];

c. Zabezpiecz dostęp do obszarów w obiekcie wyznaczonych jako publicznie dostępne, wdrażając następujące zabezpieczenia: [Realizacja: określone przez organizację fizyczne zabezpieczenia dostępu];

d. Eskortuj gości i kontroluj ich aktywność [Realizacja: okoliczności określone przez organizację, wymagające eskortowania gości i kontroli ich aktywności];

e. Zabezpiecz klucze, kombinacje zamków szyfrowych i innych urządzeń umożliwiających dostęp fizyczny;

f. Inwentaryzuj [Realizacja: urządzenia dostępu fizycznego zdefiniowane przez organizację] co [Realizacja: częstotliwość zdefiniowana przez organizację];

g. Zmieniaj kombinacje zamków szyfrowych i kluczy z częstotliwością [Realizacja: częstotliwość określona przez organizację] i/lub w przypadku utraty kluczy, kompromitacji kombinacji lub przeniesienia lub zwolnienia osób posiadających klucze lub kombinacje.

Zabezpieczenia powiązane: AT-3, AU-2, AU-6, AU-9, AU-13, CP-10, IA-3, IA-8, MA-5, MP-2, MP-4, PE-2, PE-4, PE-5, PE-8, PS-2, PS-3, PS-6, PS-7, RA-3, SC-28, SI-4, SR-3.

Zabezpieczenia rozszerzone:

(1) KONTROLA DOSTĘPU FIZYCZNEGO | DOSTĘP DO SYSTEMU

Oprócz kontroli dostępu fizycznego do obiektu w [Realizacja: przestrzenie fizyczne zdefiniowane przez organizację zawierające jeden lub więcej komponentów systemu] wymuszaj uwierzytelnianie uprawnień dostępu fizycznego do systemu.

Zabezpieczenia powiązane: nie dotyczy.

(2) KONTROLA DOSTĘPU FIZYCZNEGO | OBIEKT / OBSZAR SYSTEMU

Przeprowadzaj kontrole bezpieczeństwa w zakresie dostępu do fizycznej strefy obiektu lub dostępu do systemu informatycznego w celu uniemożliwienia nieautoryzowanego upublicznienia informacji lub usunięcia komponentów systemu z [Realizacja: częstotliwość określona przez organizację]

Zabezpieczenia powiązane: AC-4, SC-7.

(3) KONTROLA DOSTĘPU FIZYCZNEGO | STAŁA OCHRONA FIZYCZNA

Zapewnij personel ochrony do monitorowania [Realizacja: zdefiniowane przez organizację punkty dostępu fizycznego] dostępu do obiektu, w którym znajduje się system przez 24 godziny na dobę, 7 dni w tygodniu.

Zabezpieczenia powiązane: CP-6, CP-7, PE-6.

(4) KONTROLA DOSTĘPU FIZYCZNEGO | ZAMYKANE OBUDOWY

Używaj zamykanych na klucz fizycznych obudów, do ochrony [Realizacja: komponenty systemu zdefiniowane przez organizację] przed nieautoryzowanym dostępem fizycznym.

Zabezpieczenia powiązane: nie dotyczy.

(5) KONTROLA DOSTĘPU FIZYCZNEGO | OCHRONA PRZED MANIPULACJĄ

Stosuj [Realizacja: technologie antysabotażowe zdefiniowane przez organizację] w celu [Wybór (jedno lub więcej): wykrywanie, zapobieganie] fizycznej manipulacji lub zmiany [Realizacja: komponenty sprzętowe zdefiniowane przez organizację] w systemie.

Zabezpieczenia powiązane: SA-16, SR-9, SR-11.

(6) KONTROLA DOSTĘPU FIZYCZNEGO | TESTY PENETRACYJNE OBIEKTU

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(7) KONTROLA DOSTĘPU FIZYCZNEGO | BARIERY FIZYCZNE

Ograniczaj dostęp fizyczny za pomocą barier fizycznych.

Zabezpieczenia powiązane: nie dotyczy.

(8) KONTROLA DOSTĘPU FIZYCZNEGO | ŚLUZY W KONTROLI DOSTĘPU

Stosuj przedsionki (śluzy) w kontroli dostępu w [Realizacja: lokalizacjach określonych przez organizację w obiekcie].

Zabezpieczenia powiązane: nie dotyczy.

PE-4 KONTROLA DOSTĘPU DO MEDIUM TRANSMISYJNEGO

Zabezpieczenie:

Zabezpiecz fizyczny dostęp do [Realizacja: linie dystrybucyjne i transmisyjne systemu zdefiniowane przez organizację] w obiektach organizacji, korzystając z [Realizacja: środki bezpieczeństwa zdefiniowane przez organizację].

Zabezpieczenia powiązane: AT-3, IA-4, MP-2, MP-4, PE-2, PE-3, PE-5, PE-9, SC-7, SC-8.

Zabezpieczenia rozszerzone: nie dotyczy.

PE-5 KONTROLA DOSTĘPU DO URZĄDZEŃ WEJŚCIA - WYJŚCIA

Zabezpieczenie:

Kontroluj fizyczny dostęp do urządzeń wejścia / wyjścia z [Realizacja: urządzenia wejścia / wyjścia zdefiniowane przez organizację], w celu uniemożliwienia osobom nieupoważnionym uzyskanie dostępu do wyników przetwarzania informacji.

Zabezpieczenia powiązane: PE-2, PE-3, PE-4, PE-18.

Zabezpieczenia rozszerzone:

(1) KONTROLA DOSTĘPU DO URZĄDZEŃ WEJŚCIA - WYJŚCIA | DOSTĘP UPOWAŻNIONYCH OSÓB DO URZĄDZEŃ

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(2) KONTROLA DOSTĘPU DO URZĄDZEŃ WEJŚCIA - WYJŚCIA | POWIĄZANIE Z TOŻSAMOŚCIĄ JEDNOSTKI

Powiąż tożsamość jednostki z udzielaniem dostępu do danych wejściowych / wyjściowych urządzenia.

Zabezpieczenia powiązane: nie dotyczy.

(3) KONTROLA DOSTĘPU DO URZĄDZEŃ WEJŚCIA - WYJŚCIA | OZNACZANIE URZĄDZEŃ WEJŚCIA - WYJŚCIA

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

PE-6 MONITOROWANIE DOSTĘPU FIZYCZNEGO

Zabezpieczenie:

a. Monitoruj dostęp fizyczny do obiektu, w którym znajduje się system, w celu wykrywania i reagowania na incydenty związane z bezpieczeństwem fizycznym;

b. Przeglądaj dzienniki dostępu fizycznego [Realizacja: częstotliwość określone przez organizację] i po wystąpieniu [Realizacja: zdarzenia określone przez organizację lub potencjalne wskazania zdarzeń];

c. Koordynuj wyniki analiz i dochodzeń z możliwościami reagowania na incydenty w organizacji.

Zabezpieczenia powiązane: AU-2, AU-6, AU-9, AU-12, CA-7, CP-10, IR-4, IR-8.

Zabezpieczenia rozszerzone:

(1) MONITOROWANIE DOSTĘPU FIZYCZNEGO | ALARMY ANTYWŁAMANIOWE I SPRZĘT MONITORUJĄCY

Monitoruj fizyczny dostęp do obiektu, w którym znajduje się system, za pomocą systemów antywłamaniowych i urządzeń nadzorujących.

Zabezpieczenia powiązane: nie dotyczy.

(2) MONITOROWANIE DOSTĘPU FIZYCZNEGO | AUTOMATYCZNE ROZPOZNAWANIE WŁAMAŃ I REAGOWANIE NA NIE

Rozpoznawaj [Realizacja: klasy lub typy włamań zdefiniowane przez organizację] i inicjuj [Realizacja: działania reagowania zdefiniowane przez organizację] przy użyciu [Realizacja: zautomatyzowane mechanizmy zdefiniowane przez organizację].

Zabezpieczenia powiązane: SI-4.

(3) MONITOROWANIE DOSTĘPU FIZYCZNEGO | MONITORING WIZYJNY

(a) Zastosuj nadzór wideo [Realizacja: obszary operacyjne zdefiniowane przez organizację];

(b) Przeglądaj nagrania wideo [Realizacja: częstotliwość określona przez organizację];

(c) Przechowuj nagrania wideo [Realizacja: okres czasu określony przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(4) MONITOROWANIE DOSTĘPU FIZYCZNEGO | MONITOROWANIE DOSTĘPU FIZYCZNEGO DO SYSTEMÓW

Monitoruj dostęp fizyczny do systemu w uzupełnieniu monitorowania dostępu fizycznego do obiektu w [Realizacja: przestrzenie fizyczne zdefiniowane przez organizację zawierające jeden lub więcej komponentów systemu].

Zabezpieczenia powiązane: nie dotyczy.

PE-7 KONTROLA GOŚCI

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

PE-8 REJESTRY DOSTĘPU GOŚCI

Zabezpieczenie:

a. Prowadź ewidencję dostępu gości do obiektu, w którym znajduje się system, przez [Realizacja: okres czasu określony przez organizację];

b. Przeglądaj zapisy dotyczące dostępu gości [Realizacja: częstotliwość zdefiniowana przez organizację];

c. Zgłaszaj nieprawidłowości w rejestrach dostępu gości do [Realizacja: personel zdefiniowany przez organizację].

Zabezpieczenia powiązane: PE-2, PE-3, PE-6.

Zabezpieczenia rozszerzone:

(1) REJESTRY DOSTĘPU GOŚCI | AUTOMATYCZNA REJESTRACJA / PRZEGLĄD

Utrzymuj i przeglądanie rejestrów dostępu gości przy użyciu [Realizacja: zautomatyzowane mechanizmy zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(2) REJESTRY DOSTĘPU GOŚCI | EWIDENCJA DOSTĘPU FIZYCZNEGO

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(3) REJESTRY DOSTĘPU GOŚCI | OGRANICZENIE ELEMENTÓW INFORMACJI UMOŻLIWIAJĄCYCH IDENTYFIKACJĘ OSOBY

Ogranicz informacje umożliwiające identyfikację osób zawartych w ewidencji dostępu gości do następujących elementów zidentyfikowanych w ocenie ryzyka dotyczącego prywatności: [Realizacja: elementy zdefiniowane przez organizację].

Zabezpieczenia powiązane: RA-3, SA-8.

PE-9 URZĄDZENIA ENERGETYCZNE I OKABLOWANIE

Zabezpieczenie:

Zabezpiecz urządzenia zasilające oraz okablowanie energetyczne systemu przed uszkodzeniem i zniszczeniem.

Zabezpieczenia powiązane: PE-4.

Zabezpieczenia rozszerzone:

(1) URZĄDZENIA ENERGETYCZNE I OKABLOWANIE | REDUNDANCJA OKABLOWANIA

Stosuj nadmiarowe tory okablowania zasilającego, które są fizycznie oddzielone od torów głównych [Realizacja: odległość zdefiniowana przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(2) URZĄDZENIA ENERGETYCZNE I OKABLOWANIE | AUTOMATYCZNA KONTROLA JAKOŚCI NAPIĘCIA

Stosuj automatyczną kontrolę napięcia dla [Realizacja: krytycznych komponentów systemu zdefiniowanych przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

PE-10 WYŁĄCZENIE AWARYJNE

Zabezpieczenie:

a. Zapewnij możliwości wyłączenia zasilania [Realizacja: system zdefiniowany przez organizację lub poszczególne komponenty systemu] w sytuacjach awaryjnych;

b. Umieszczaj wyłączniki awaryjne lub urządzenia wyłączania awaryjnego w [Realizacja: lokalizacja zdefiniowana przez organizację według systemu lub komponentu systemu], w sposób umożliwiający upoważnionemu personelowi bezpieczny i łatwy dostęp;

c. Zabezpieczenie wyłączników/urządzeń wyłączania awaryjnego przed nieuprawnioną aktywacją.

Zabezpieczenia powiązane: PE-15.

Zabezpieczenia rozszerzone:

(1) WYŁĄCZENIE AWARYJNE | PRZYPADKOWA I NIEAUTORYZOWANA AKTYWACJA

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

PE-11 ZASILANIE AWARYJNE

Zabezpieczenie:

Zapewnij gwarantowane zasilanie, w celu umożliwienia [Wybór: (jedno lub więcej): uporządkowanego wyłączenia systemu, przejścia systemu na długoterminowe źródło zasilania alternatywnego] w przypadku utraty podstawowego źródła zasilania.

Zabezpieczenia powiązane: AT-3, CP-2, CP-7.

Zabezpieczenia rozszerzone:

(1) ZASILANIE AWARYJNE | ALTERNATYWNE ŹRÓDŁO ZASILANIA – MINIMALNA ZDOLNOŚĆ OPERACYJNA

Zapewnij alternatywne źródła zasilania dla systemu, aktywowanego [Realizacja: ręcznie, automatycznie], które może utrzymać minimalną wymaganą zdolność operacyjną w przypadku długotrwałej utraty głównego źródła zasilania.

Zabezpieczenia powiązane: nie dotyczy.

(2) ZASILANIE AWARYJNE | ALTERNATYWNE ŹRÓDŁO ZASILANIA – AUTONOMICZNE

Zapewnij alternatywne źródło zasilania dla systemu, aktywowanego [Realizacja: ręcznie, automatycznie] i które jest:

(a) Samoobsługowe (autostart);

(b) Niezależne od zewnętrznego przyłącza energetycznego;

(c) Zdolne do utrzymania [Wybór: minimalna wymagana zdolność operacyjna; pełna zdolność operacyjna] w przypadku długotrwałej utraty dostępności podstawowego źródła zasilania.

Zabezpieczenia powiązane: nie dotyczy.

PE-12 OŚWIETLENIE AWARYJNE

Zabezpieczenie:

Zastosuj i utrzymuj automatyczne oświetlenie awaryjne w systemie, które uruchamia się w przypadku zaniku lub przerwy w dostawie prądu, a także obejmuje wyjścia ewakuacyjne i drogi ewakuacyjne na terenie obiekcie.

Zabezpieczenia powiązane: CP-2, CP-7.

Zabezpieczenia rozszerzone:

(1) OŚWIETLENIE AWARYJNE | ZASADNICZE DZIAŁANIA / FUNKCJE BIZNESOWE

Zapewnij oświetlenie awaryjne we wszystkich pomieszczeniach obiektu, wspierając realizację podstawowych zadań i funkcji biznesowych.

Zabezpieczenia powiązane: nie dotyczy.

PE-13 OCHRONA PRZECIWPOŻAROWA

Zabezpieczenie:

Stosuj i utrzymuj systemy wykrywania i gaszenia pożaru, które są zasilane niezależnym źródłem energii.

Zabezpieczenia powiązane: AT-3.

Zabezpieczenia rozszerzone:

(1) OCHRONA PRZECIWPOŻAROWA | SYSTEMY DETEKCJI – AUTOMATYCZNA AKTYWACJA I POWIADAMIANIE

Stosuj systemy wykrywania pożaru, które uruchamiają się automatycznie i powiadamiają [Realizacja: personel lub role określone przez organizację] oraz [Realizacja: służby ratownicze określone przez organizację] w przypadku pożaru.

Zabezpieczenia powiązane: nie dotyczy.

(2) OCHRONA PRZECIWPOŻAROWA | SYSTEMY TŁUMIENIA – AUTOMATYCZNA AKTYWACJA I POWIADAMIANIE

(a) Stosuj systemy gaszenia pożaru, które uruchamiają się automatycznie i powiadamiają [Realizacja: personel lub role określone przez organizację] oraz [Realizacja: służby ratownicze określone przez organizację];

(b) Stosuj automatyczne systemy gaszenia pożaru, gdy w obiekcie nie ma ciągłej obecności personelu.

Zabezpieczenia powiązane: nie dotyczy.

(3) OCHRONA PRZECIWPOŻAROWA | AUTOMATYCZNE GASZENIE POŻARU

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(4) OCHRONA PRZECIWPOŻAROWA | INSPEKCJE

Zapewnij, że obiekt jest poddawany [Realizacja: częstotliwość określona przez organizację] kontrolom przeciwpożarowym przeprowadzanym przez upoważnionych i wykwalifikowanych inspektorów, a zidentyfikowane niedociągnięcia są usuwane w [Realizacja: okres określony przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

PE-14 KONTROLE ŚRODOWISKOWE

Zabezpieczenie:

a. Utrzymuj [Wybór (jeden lub więcej): temperatura, wilgotność, ciśnienie, promieniowanie, [Realizacja: kontrola środowiskowa zdefiniowana przez organizację]] poziomy w obiekcie, w którym znajduje się system, na [Realizacja: akceptowalnych poziomach zdefiniowanych przez organizację];

b. Monitoruj poziomy zabezpieczeń środowiskowych [Realizacja: częstotliwość określona przez organizację].

Zabezpieczenia powiązane: AT-3, CP-2.

Zabezpieczenia rozszerzone:

(1) KONTROLE ŚRODOWISKOWE | STEROWANIE AUTOMATYCZNE

Stosuj następujące automatyczne zabezpieczenia środowiskowe w obiekcie, aby zapobiec potencjalnie szkodliwym dla systemu fluktuacjom: [Realizacja: automatyczne zabezpieczenia środowiskowe zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(2) KONTROLE ŚRODOWISKOWE | MONITOROWANIE, ALARMOWANIE I POWIADOMIANIE

Monitoruj zabezpieczenia środowiskowe zapewniając alarmowanie lub powiadomienie o zmianach potencjalnie szkodliwych dla personelu lub sprzętu dla [Realizacja: personel lub role określone przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

PE-15: OCHRONA PRZED ZALANIEM

Zabezpieczenie:

Zabezpiecz systemu przed uszkodzeniami spowodowanymi wyciekiem wody, zapewniając główne zawory odcinające lub separujące, które są łatwo dostępne, działają prawidłowo i są znane kluczowemu personelowi.

Zabezpieczenia powiązane: AT-3, PE-10.

Zabezpieczenia rozszerzone:

(1) OCHRONA PRZED ZALANIEM | AUTOMATYCZNE WYKRYWANIE

Wykrywaj obecność wody w pobliżu systemu i alarmuj [Realizacja: personel lub role zdefiniowane przez organizację] za pomocą [Realizacja: zautomatyzowane mechanizmy zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

PE-16 DOSTAWA I USUWANIE

Zabezpieczenie:

a. Autoryzuj i zabezpiecz [Realizacja: typy komponentów systemu zdefiniowane przez organizację] wchodzące i wychodzące z obiektu;

b. Prowadź ewidencję komponentów systemu.

Zabezpieczenia powiązane: CM-3, CM-8, MA-2, MA-3, MP-5, PE-20, SR-2, SR-3, SR-4, SR-6.

Zabezpieczenia rozszerzone: nie dotyczy.

PE-17 ZAPASOWE MIEJSCE PRACY

Zabezpieczenie:

a. Ustal i udokumentuj [Realizacja: alternatywne miejsca pracy określone przez organizację] wyznaczone do użytku przez pracowników;

b. Wprowadź [Realizacja: środki kontroli zdefiniowane przez organizację] w zapasowych miejscach pracy;

c. Oceniaj skuteczność zabezpieczeń w zapasowych miejscach pracy;

d. Zapewnij pracownikom możliwość komunikowania się z personelem odpowiedzialnym za bezpieczeństwo informacji i ochrony prywatność w razie wystąpienia incydentów.

Zabezpieczenia powiązane: AC-17, AC-18, CP-7.

Zabezpieczenia rozszerzone: nie dotyczy.

PE-18 LOKALIZACJA KOMPONENTÓW SYSTEMU

Zabezpieczenie:

Stosuj rozmieszczaj elementy systemu w obiekcie w taki sposób, aby zminimalizować potencjalne uszkodzenia spowodowane [Realizacja: zagrożenia fizyczne i środowiskowe zdefiniowane przez organizację] oraz zminimalizowania możliwość nieautoryzowanego dostępu.

Zabezpieczenia powiązane: CP-2, PE-5, PE-19, PE-20, RA-3.

Zabezpieczenia rozszerzone:

(1) LOKALIZACJA KOMPONENTÓW SYSTEMU | LOKALIZACJA OBIEKTU

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

PE-19 WYCIEK INFORMACJI

Zabezpieczenie:

Zabezpiecz system przed utratą informacji spowodowanym emisją sygnałów elektromagnetycznych.

Zabezpieczenia powiązane: AC-18, PE-18, PE-20.

Zabezpieczenia rozszerzone:

(1) WYCIEK INFORMACJI | KRAJOWE ZASADY I PROCEDURY DOTYCZĄCE EMISJI UJAWNIAJĄCEJ

Zabezpiecz komponenty systemu, powiązanej transmisji danych i sieci zgodnie z krajowymi zasadami i procedurami bezpieczeństwa emisji w oparciu o kategorię bezpieczeństwa lub klasyfikację informacji.

Zabezpieczenia powiązane: nie dotyczy.

PE-20 MONITOROWANIE I ŚLEDZENIE AKTYWÓW

Zabezpieczenie:

Stosuj [Realizacja: technologie lokalizacji aktywów zdefiniowane przez organizację] w celu śledzenia i monitorowania lokalizacji i ruchu [Realizacja: aktywa zdefiniowane przez organizację] w obrębie [Realizacja: kontrolowane obszary zdefiniowane przez organizację].

Zabezpieczenia powiązane: CM-8, PE-16, PM-8.

Zabezpieczenia rozszerzone: nie dotyczy.

PE-21 OCHRONA PRZED IMPULSAMI ELEKTROMAGNETYCZNYMI

Zabezpieczenie:

Stosuj [Realizacja: środki ochronne zdefiniowane przez organizację] chroniące przed uszkodzeniami spowodowanymi impulsem elektromagnetycznym dla [Realizacja: systemy i komponenty systemów zdefiniowane przez organizację].

Zabezpieczenia powiązane: PE-18, PE-19.

Zabezpieczenia rozszerzone: nie dotyczy.

PE-22 ZNAKOWANIE KOMPONENTÓW

Zabezpieczenie:

Znakuj [Realizacja: komponenty sprzętowe systemu zdefiniowane przez organizację], wskazujące poziom wpływu lub poziom klasyfikacji informacji, których przetwarzanie, przechowywanie lub przesyłanie jest dozwolone przez komponent sprzętowy.

Zabezpieczenia powiązane: AC-3, AC-4, AC-16, MP-3.

Zabezpieczenia rozszerzone: nie dotyczy.

PE-23 LOKALIZACJA OBIEKTU

Zabezpieczenie:

a. Planuj lokalizacje lub miejsca posadowienia obiektu, w którym znajduje się system, biorąc pod uwagę zagrożenia fizyczne i środowiskowe;

b. Uwzględniaj w strategii zarządzania ryzykiem organizacyjnym zagrożeń fizycznych i środowiskowych w odniesieniu do istniejących obiektów.

Zabezpieczenia powiązane: CP-2, PE-18, PE-19, PM-8, PM-9, RA-3.

Zabezpieczenia rozszerzone: nie dotyczy.

KATEGORIA: PL – PLANOWANIE

PL-1 POLITYKA I PROCEDURY

a. Opracuj, udokumentuj i rozpowszechnij wśród [Realizacja: personel lub role zdefiniowane w organizacji]:

    1. [Wybór (jedno lub więcej): na poziomie organizacji, na poziomie misji/procesu biznesowego, na poziomie systemu] politykę planowania, która:

        (a) Dotyczy celu, zakresu, ról, obowiązków, zaangażowania kierownictwa, koordynacji między jednostkami organizacyjnymi i zgodności;

        (b) Jest zgodna z obowiązującymi przepisami prawa, rozporządzeniami wykonawczymi, dyrektywami, regulacjami, zasadami, normami i wytycznymi;

    2. Procedury ułatwiające wdrażanie polityki planowania i powiązanych z nią kontroli planowania;

b. Wyznacz [Realizacja: urzędnika określonego przez organizację] do zarządzania opracowywaniem, dokumentowaniem i rozpowszechnianiem polityki i procedur planowania;

c. Przeglądaj i aktualizuj na bieżąco:

    1. Politykę [Realizacja: częstotliwość zdefiniowana przez organizację] i następujące po niej [Realizacja: zdarzenia określone przez organizację];

    2. Procedury planowania z [Realizacja: częstotliwość zdefiniowana przez organizację] i następujące [Realizacja: zdarzenia zdefiniowane przez organizację].

Zabezpieczenia powiązane: PM-9, PS-8, SI-12.

Zabezpieczenia rozszerzone: nie dotyczy.

PL-2 PLANY BEZPIECZEŃSTWA SYSTEMU I OCHRONY PRYWATNOŚCI

Zabezpieczenie:

a. Opracuj plany bezpieczeństwa i prywatności dla systemu, które:

    1. Są spójne z architekturą korporacyjną organizacji;

    2. Jednoznacznie określają składniki systemu;

    3. Opisują środowisko operacyjny systemu w kontekście misji i procesów biznesowych;

    4. Identyfikują osoby pełniące role i obowiązki w systemie;

    5. Identyfikują typy informacji przetwarzanych, przechowywanych i przesyłanych przez system;

    6. Zapewniają kategoryzację bezpieczeństwa systemu, łącznie z uzasadnieniem;

    7. Opisują wszelkie zagrożenia specyficzne dla systemu, które dotyczą organizacji;

    8. Zapewniają udostępnianie wyników oceny ryzyka prywatności dla systemów przetwarzających dane osobowe;

    9. Opisują środowisko operacyjne systemu oraz wszelkie zależności lub połączenia z innymi systemami lub komponentami systemu;

    10. Przedstawiają przegląd wymagań dotyczących bezpieczeństwa i ochrony prywatności systemu;

    11. Określają wszelkie istotne linie bazowe lub nakładki kontrolne, jeżeli ma to zastosowanie;

    12. Opisują istniejące lub planowane zabezpieczenia mające na celu spełnienie wymogów bezpieczeństwa i ochrony prywatności, w tym uzasadnienie wszelkich decyzji dotyczących dostosowywania zabezpieczeń;

    13. Zapewniają uwzględnianie określania ryzyka dla architektury i decyzji projektowych dotyczących bezpieczeństwa i prywatności;

    14. Obejmują działania związane z bezpieczeństwem i ochroną prywatności, mające wpływ na system, które wymagają planowania i koordynacji z [Realizacja: osoby lub grupy określone przez organizację];

    15. Są weryfikowane i zatwierdzane przez osobę autoryzującą lub wyznaczonego przedstawiciela przed wprowadzeniem w życie planu.

b. Dystrybuuj kopie planów i przekazywanie kolejnych zmian w planach personelowi [Realizacja: personel lub role określone przez organizację];

c. Przeglądaj planów [Realizacja: częstotliwość określona przez organizację];

d. Aktualizuj plany, w celu uwzględnienia zmian w systemie i środowisku działania lub problemów zidentyfikowanych podczas wdrażania planu lub oceny zabezpieczeń;

e. Chroń plany przed nieautoryzowanym ujawnieniem i modyfikacją.

Zabezpieczenia powiązane: AC-2, AC-6, AC-14, AC-17, AC-20, CA-2, CA-3, CA-7, CM-9, CM-13, CP-2, CP-4, IR- 4, IR-8, MA-4, MA-5, MP-4, MP-5, PL-7, PL-8, PL-10, PL-11, PM-1, PM-7, PM-8, PM-9, PM-10, PM-11, RA-3, RA-8, RA-9, SA-5, SA-17, SA-22, SI-12, SR-2, SR-4.

Zabezpieczenia rozszerzone:

(1) PLANY BEZPIECZEŃSTWA SYSTEMU I OCHRONY PRYWATNOŚCI | KONCEPCJA DZIAŁANIA

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(2) PLANY BEZPIECZEŃSTWA SYSTEMU I OCHRONY PRYWATNOŚCI | ARCHITEKTURA FUNKCJONALNA

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(3) PLANY BEZPIECZEŃSTWA SYSTEMU I OCHRONY PRYWATNOŚCI | PLANOWANIE / KOORDYNACJA Z INNYMI PODMIOTAMI ORGANIZACYJNYMI

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

PL-3 AKTUALIZACJA PLANU BEZPIECZEŃSTWA SYSTEMU

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

PL-4 ZASADY ZACHOWANIA

Zabezpieczenie:

a. Wprowadź i zapewnij osobom wymagającym dostępu do systemu zasady, które opisują ich obowiązki i oczekiwane zachowania w zakresie korzystania z informacji i systemu, bezpieczeństwa i ochrony prywatności;

b. Przed wydaniem zezwolenia na dostęp do informacji i systemu uzyskaj od tych osób udokumentowane potwierdzenie, że przeczytały, zrozumiały i zgadzają się przestrzegać ustanowione zasad postępowania;

c. Przeglądaj i aktualizuj zasady zachowania [Realizacja: częstotliwość określona przez organizację];

d. Wymagaj od osób, które zapoznały się z poprzednią wersją zasad zachowania, przeczytania, ponownego przeczytania i podpisania tych reguł [Wybór (jedna lub więcej)]: [Realizacja częstotliwość określona przez organizację], gdy zasady są zmieniane lub aktualizowane].

Zabezpieczenia powiązane: AC-2, AC-6, AC-8, AC-9, AC-17, AC-18, AC-19, AC-20, AC-22, AT-2, AT-3, AU-13, CM-11, IA-2, IA- 4, IA-5, MP-7, PS-6, PS-8, SA-5, SI-12.

Zabezpieczenia rozszerzone:

(1) ZASADY ZACHOWANIA | ZASADY KORZYSTANIA Z MEDIÓW SPOŁECZNOŚCIOWYCH I ZEWNĘTRZNYCH STRON/APLIKACJI

Włącz do zasad zachowania ograniczenia:

a. Korzystania z mediów społecznościowych, portali społecznościowych i zewnętrznych stron/aplikacji;

b. Umieszczania informacji organizacyjnych na publicznych stronach internetowych;

c. Wykorzystywania identyfikatorów dostarczonych przez organizację (np. adresów e-mail) i sekretów uwierzytelniania (np. haseł) do tworzenia kont na zewnętrznych stronach/aplikacjach.

Zabezpieczenia powiązane: AC-22, AU-13.

PL-5 OCENA WPŁYWU NA PRYWATNOŚĆ

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

PL-6 PLANOWANIE DZIAŁALNOŚCI ZWIĄZANEJ Z BEZPIECZEŃSTWEM

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

PL-7 KONCEPCJA BEZPIECZEŃSTWA DZIAŁAŃ OPERACYJNYCH

Zabezpieczenie:

a. Opracowuj koncepcję działań operacyjnych (ang. concept of operations - CONOPS) opisującą sposób, w jaki organizacja zamierza obsługiwać system z punktu widzenia bezpieczeństwa informacji i ochrony prywatności;

b. Przeglądaj i aktualizuj CONOPS [Realizacja: częstotliwość określona przez organizację].

Zabezpieczenia powiązane: PL-2, SA-2, SI-12.

Zabezpieczenia rozszerzone: nie dotyczy.

PL-8 ARCHITEKTURA BEZPIECZEŃSTWA I OCHRONA PRYWATNOŚCI

Zabezpieczenie:

a. Opracuj architekturę bezpieczeństwa i ochrony prywatności dla systemu, która opisuje:

1. Wymagania i podejście, jakie należy zastosować w celu ochrony poufności, integralności i dostępności informacji organizacyjnych;

2. Wymagania i podejście, jakie należy przyjąć w odniesieniu do przetwarzania danych osobowych, aby zminimalizować zagrożenia dla prywatności osób;

3. Sposób, w jaki architektury te są zintegrowane z architekturą korporacyjną i ją wspierają;

4. Wszelkie założenia dotyczące systemów i usług oraz ich zależności;

b. Przeglądaj i aktualizuj architekturę bezpieczeństwa i ochrony prywatności [Realizacja: częstotliwość zdefiniowana przez organizację], w celu odzwierciedlenia zmian w architekturze korporacyjnej;

c. Odzwierciedlaj planowane zmiany w architekturze planów bezpieczeństwa i ochrony prywatności, koncepcji bezpieczeństwa operacji (CONOPS), analizach krytyczności, procedurach organizacyjnych oraz zamówieniach i zakupach organizacyjnych.

Zabezpieczenia powiązane: CM-2, CM-6, PL-2, PL-7, PL-9, PM-5, PM-7, RA-9, SA-3, SA-5, SA-8, SA-17, SC-2, SC-3, SC- 7, SC-29, SC-36, SR-3.

Zabezpieczenia rozszerzone:

(1) ARCHITEKTURA BEZPIECZEŃSTWA I OCHRONA PRYWATNOŚCI | ZABEZPIECZENIE WIELOSTOPNIOWE (OCHRONA WARSTWOWA)

Zaprojektuj architekturę bezpieczeństwa i ochrony prywatności dla systemu, stosując dogłębne podejście ochronne, które:

a. Przydziela [Realizacja: zabezpieczenie zdefiniowane przez organizację] do [Realizacja: zdefiniowane przez organizację i warstwy architektoniczne];

b. Zapewnia, że przydzielone zabezpieczenia działają w sposób skoordynowany i wzajemnie się uzupełniają.

Zabezpieczenia powiązane: SC-2, SC-3, SC-29, SC-36.

(2) ARCHITEKTURA BEZPIECZEŃSTWA I OCHRONA PRYWATNOŚCI | DYWERSYFIKACJA DOSTAWCY

Wymagaj, aby [Realizacja: określone przez organizację zabezpieczenia] przydzielone do [Realizacja: określone przez organizację lokalizacje i warstwy architektoniczne] były nabywane od różnych dostawców.

Zabezpieczenia powiązane: SC-29, SR-3.

PL-9 ZARZĄDZANIE CENTRALNE

Zabezpieczenie:

Zarządzaj centralnie zabezpieczeniami [Realizacja: zabezpieczenia zdefiniowane przez organizację i powiązane procesy].

Zabezpieczenia powiązane: PL-8, PM-9.

Zabezpieczenia rozszerzone: nie dotyczy.

PL-10 WYBÓR ZABEZPIECZEŃ BAZOWYCH

Zabezpieczenie:

Wyselekcjonuj zabezpieczenia bazowe systemu.

Zabezpieczenia powiązane: PL-2, PL-11, RA-2, RA-3, SA-8.

Zabezpieczenia rozszerzone: nie dotyczy.

PL-11 DOPASOWANIE BAZOWE

Zabezpieczenie:

Dostosuj wybrane zabezpieczenia bazowe poprzez zastosowanie określonych czynności dostosowania.

Zabezpieczenia powiązane: PL-10, RA-2, RA-3, RA-9, SA-8.

Zabezpieczenia rozszerzone: nie dotyczy.

KATEGORIA: PM - PROGRAMY BEZPIECZEŃSTWA INFORMACJI

PM-1 PLAN PROGRAMU BEZPIECZEŃSTWA INFORMACJI

Zabezpieczenie:

a. Opracuj i rozpowszechnij plan programu bezpieczeństwa informacji w całej organizacji, który:

    1. Zapewnia przegląd wymagań programu bezpieczeństwa i opis kontroli zarządzania tym programem bezpieczeństwa i wspólnych kontroli wdrożonych lub zaplanowanych w celu spełnienia tych wymagań;

    2. Obejmuje identyfikację i przypisanie ról, obowiązków, zaangażowania kierownictwa, koordynację między jednostkami organizacyjnymi i zgodność z przepisami;

3. Odzwierciedla koordynację między jednostkami organizacyjnymi odpowiedzialnymi za różne aspekty bezpieczeństwa informacji (tj. techniczne, fizyczne, osobowe, teleinformatyczne);

4. Jest zatwierdzony przez kierownika jednostki organizacyjnej lub osobę przez niego upoważnioną;

b. Dokonaj przeglądów i zaktualizuj plan programu bezpieczeństwa informacji w całej organizacji z częstotliwością [Realizacja: częstotliwość zdefiniowana przez organizację] i zgodnie z [Realizacja: zdarzenia zdefiniowane przez organizację];

c. Chroń plan programu bezpieczeństwa informacji przed nieautoryzowanym ujawnieniem i modyfikacją.

Zabezpieczenia powiązane: PL-2, PM-18, PM-30, RA-9, SI-12, SR-2.

Zabezpieczenia rozszerzone: nie dotyczy.

PM-2 OSOBA ODPOWIEDZIALNA ZA BEZPIECZEŃSTWO INFORMACJI (CSO)

Zabezpieczenie:

Wyznacz osobę odpowiedzialną za bezpieczeństwo informacji z misją i zadaniami w zakresie koordynowania, opracowywania, wdrażania i utrzymywania programu bezpieczeństwa informacji obejmującego całą organizację.

Zabezpieczenia powiązane: nie dotyczy.

Zabezpieczenia rozszerzone: nie dotyczy.

PM-3 ŚRODKI BEZPIECZEŃSTWA I PRYWATNOŚCI INFORMACJI

Zabezpieczenie:

a. Uwzględnij zasoby potrzebne do wdrożenia programów bezpieczeństwa informacji i prywatności w planowaniu kapitałowym i wnioskach inwestycyjnych oraz udokumentuj wszystkie wyjątki od tego wymogu;

b. Przygotuj dokumentację wymaganą do obsługi programów bezpieczeństwa informacji i prywatności w planowaniu budżetu i zasobów inwestycyjnych zgodnie z obowiązującymi przepisami prawa, rozporządzeniami wykonawczymi, dyrektywami, politykami, regulacjami, standardami;

c. Udostępnij na wydatki planowane zasoby bezpieczeństwa informacji i prywatności.

Zabezpieczenia powiązane: PM-4 i SA-2.

Zabezpieczenia rozszerzone: nie dotyczy.

PM-4 PLAN DZIAŁANIA I ETAPY WPROWADZANIA ZABEZPIECZEŃ

Zabezpieczenie:

a. Wdrażaj proces, aby zapewnić, że plany działania i etapy wprowadzania programu zarządzania ryzykiem w zakresie bezpieczeństwa informacji, prywatności i łańcucha dostaw oraz powiązanych systemów organizacyjnych:

    1. Są opracowywane i utrzymywane;

    2. Dokumentują działania naprawcze w zakresie bezpieczeństwa informacji, prywatności i zarządzania ryzykiem łańcucha dostaw w celu odpowiedniego reagowania na wystąpienie ryzyka związanego z operacjami organizacyjnymi i aktywami, osobami fizycznymi, innymi organizacjami i organami władzy państwowej;

    3. Są raportowane zgodnie z wymogami sprawozdawczości.

b. Przejrzyj plany działań i etapów wprowadzania pod kątem spójności ze strategią zarządzania ryzykiem organizacji i priorytetami w całej organizacji dla działań reagowania na ryzyko.

Zabezpieczenia powiązane: CA-5, CA-7, PM-3, RA-7, SI-12.

Zabezpieczenia rozszerzone: nie dotyczy.

PM-5 INWENTARYZACJA SYSTEMU

Zabezpieczenie:

Opracuj i aktualizuj [Realizacja: częstotliwość określona przez organizację] inwentaryzację systemów organizacyjnych.

Zabezpieczenia powiązane: nie dotyczy.

Zabezpieczenia rozszerzone:

(1) INWENTARYZACJA SYSTEMU | INWENTARYZACJA DANYCH OSOBOWYCH

Utwórz, utrzymuj i aktualizuj [Realizacja: częstotliwość określona przez organizację] spis wszystkich systemów, aplikacji i projektów, w których przetwarzane są dane osobowe.

Zabezpieczenia powiązane: AC-3, CM-8, CM-12, CM-13, PL-8, PM-22, PT-3, PT-5, SI-12, SI-18.

PM-6 MIARY WYDAJNOŚCI

Zabezpieczenie:

Opracuj, monitoruj i raportuj wyniki działań mających na celu zapewnienie bezpieczeństwa informacji i prywatności.

Zabezpieczenia powiązane: CA-7, PM-9.

Zabezpieczenia rozszerzone: nie dotyczy.

PM-7 STRUKTURA ORGANIZACYJNA

Zabezpieczenie:

Opracuj i utrzymuj struktury organizacyjne z uwzględnieniem aspektów bezpieczeństwa informacji, prywatności oraz wynikającego z tego ryzyka dla operacji i aktywów organizacji, osób fizycznych, innych organizacji i organów władzy państwowej.

Zabezpieczenia powiązane: AU-6, PL-2, PL-8, PM-11, RA-2, SA-3, SA-8, SA-17.

Zabezpieczenia rozszerzone:

(1) STRUKTURA ORGANIZACYJNA | ODCIĄŻANIE

Przenieś [Realizacja: zdefiniowane przez organizację funkcje lub usługi niebędące niezbędne] do innych systemów, komponentów systemu lub do zewnętrznego dostawcy.

Zabezpieczenia powiązane: SA-8.

PM-8 PLAN INFRASTRUKTURY KRYTYCZNEJ

Zabezpieczenie:

Uwzględnij kwestii bezpieczeństwa informacji i prywatności w opracowywaniu, dokumentowaniu i aktualizowaniu planu ochrony infrastruktury krytycznej i kluczowych zasobów.

Zabezpieczenia powiązane: CP-2, CP-4, PE-18, PL-2, PM-9, PM-11, PM-18, RA-3, SI-12.

Zabezpieczenie rozszerzone: Nie dotyczy.

PM-9 STRATEGIA ZARZĄDZANIA RYZYKIEM

Zabezpieczenie:

a. Opracuj kompleksową strategię zarządzania:

    1. ryzykiem bezpieczeństwa dla operacji i aktywów organizacji, osób fizycznych, innych organizacji i organów władzy państwowej związanych z obsługą i wykorzystaniem systemów organizacyjnych;

2. ryzykiem prywatności osób fizycznych wynikającym z autoryzowanego przetwarzania danych osobowych;

b. Wdrażaj strategię zarządzania ryzykiem w sposób spójny w całej organizacji;

c. Przeglądaj i aktualizuj strategię zarządzania ryzykiem z częstotliwością [Realizacja: częstotliwość zdefiniowana przez organizację] lub zgodnie z wymaganiami przepisów prawa, uwzględniając zmiany organizacyjne.

Zabezpieczenia powiązane: AC-1, AU-1, AT-1, CA-1, CA-2, CA-5, CA-6, CA-7, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PL-2, PM-2, PM-8, PM-18, PM-28, PM-30, PS-1, PT-1, PT-2, PT-3, RA-1, RA-3, RA-9, SA-1, SA-4, SC-1, SC-38, SI-1, SI-12, SR-1, SR-2.

Zabezpieczenia rozszerzone: nie dotyczy.

PM-10 PROCES AUTORYZACJI

Zabezpieczenie:

a. Zarządzaj stanem bezpieczeństwa i prywatności systemów informatycznych organizacji i środowiskami, w których systemy te działają, poprzez procesy autoryzacji;

b. Wyznaczaj osoby do wypełniania określonych ról i obowiązków w ramach procesu zarządzania ryzykiem organizacyjnym;

c. W pełni integruj procesy autoryzacji z programem zarządzania ryzykiem w całej organizacji.

Zabezpieczenia powiązane: CA-6, CA-7, PL-2.

Zabezpieczenia rozszerzone: nie dotyczy.

PM-11 DEFINICJA MISJI I PROCESÓW BIZNESOWYCH

Zabezpieczenie:

a. Zdefiniuj misję organizacyjną i procesy biznesowe z uwzględnieniem bezpieczeństwa informacji i prywatności oraz wynikającego z tego ryzyka dla operacji organizacyjnych, aktywów organizacyjnych, osób fizycznych, innych organizacji i organów władzy państwowej;

b. Określaj ochronę informacji i potrzeby przetwarzania danych osobowych wynikające z określonej misji i procesów biznesowych;

c. Przejrzyj i zrewiduj misję i procesy biznesowe [Realizacja: częstotliwość zdefiniowana przez organizację].

Zabezpieczenia powiązane: CP-2, PL-2, PM-7, PM-8, RA-2, RA-3, RA-9, SA-2.

Zabezpieczenia rozszerzone: nie dotyczy.

PM-12 ZAGROŻENIA WEWNĘTRZNE

Zabezpieczenie:

Wprowadź program dotyczący zagrożeń wewnętrznych, który obejmuje interdyscyplinarny zespół zajmujący się obsługą incydentów związanych z zagrożeniami wewnętrznymi.

Zabezpieczenia powiązane: AC-6, AT-2, AU-6, AU-7, AU-10, AU-12, AU-13, CA-7, IA-4, IR-4, MP-7, PE-2, PM- 16, PS-3, PS-4, PS-5, PS-7, PS-8, SC-7, SC-38, SI-4, PM-14.

Zabezpieczenia rozszerzone: nie dotyczy.

PM-13 PRACOWNICY DS. BEZPIECZEŃSTWA I PRYWATNOŚCI

Zabezpieczenie:

Wprowadź program rozwoju i doskonalenia personelu ds. bezpieczeństwa i prywatności.

Zabezpieczenia powiązane: AT-2, AT-3.

Zabezpieczenia rozszerzone: nie dotyczy.

PM-14 TESTOWANIE, SZKOLENIA I MONITOROWANIE

Zabezpieczenie:

a. Wprowadź proces zapewniający, że plany organizacyjne dotyczące przeprowadzania testów bezpieczeństwa i prywatności, szkoleń i działań monitorujących związanych z systemami organizacyjnymi:

    1. są opracowywane i utrzymywane;

    2. nadal są wykonywane;

b. Przeglądaj plany testowania, szkoleń i monitorowania pod kątem zgodności ze strategią zarządzania ryzykiem organizacji i priorytetami w całej organizacji dotyczącymi działań w zakresie reagowania na ryzyko.

Zabezpieczenia powiązane: AT-2, AT-3, CA-7, CP-4, IR-3, PM-12, SI-4.

Zabezpieczenie rozszerzone: nie dotyczy.

PM-15 GRUPY I STOWARZYSZENIA DS. BEZPIECZEŃSTWA I PRYWATNOŚCI

Zabezpieczenie:

Nawiązuj i instytucjonalizuj kontakty z wybranymi grupami i stowarzyszeniami w społecznościach zajmujących się bezpieczeństwem i prywatnością:

a. aby ułatwić ciągłą edukację i szkolenia w zakresie bezpieczeństwa i prywatności dla personelu organizacji;

b. aby utrzymywać aktualność zalecanych praktyk, technik i technologii dotyczących bezpieczeństwa i prywatności;

c. aby udostępniać bieżące informacje dotyczące bezpieczeństwa i prywatności, w tym o zagrożeniach, podatnościach i incydentach.

Zabezpieczenia powiązane: SA-11, SI-5.

Zabezpieczenia rozszerzone: nie dotyczy.

PM-16 OSTRZEGANIE O ZAGROŻENIACH

Zabezpieczenie:

Wprowadź program zapewniający podnoszenie świadomości o zagrożeniach, który obejmuje wymianę informacji między organizacjami na temat zagrożeń.

Zabezpieczenia powiązane: IR-4, PM-12.

Zabezpieczenia rozszerzone:

(1) OSTRZEGANIE O ZAGROŻENIACH | ZAUTOMATYZOWANE ŚRODKI UDOSTĘPNIANIA INFORMACJI O ZAGROŻENIACH

Wdrażaj zautomatyzowane mechanizmy, aby zmaksymalizować efektywność udostępniania informacji o zagrożeniach.

Zabezpieczenia powiązane: nie dotyczy.

PM-17 OCHRONA KONTROLOWANYCH INFORMACJI NIEJAWNYCH W SYSTEMACH ZEWNĘTRZNYCH

Zabezpieczenie:

a. Wprowadź zasady i procedury, które zapewnią, że wymagania dotyczące ochrony kontrolowanych informacji niejawnych, które są przetwarzane, przechowywane lub przesyłane w systemach

zewnętrznych, są wdrażane zgodnie z obowiązującymi przepisami prawa, rozporządzeniami wykonawczymi, dyrektywami, zasadami, regulacjami i standardami;

b. Przejrzyj i zaktualizuj zasady i procedury [Realizacja: częstotliwość zdefiniowana przez organizację].

Zabezpieczenia powiązane: CA-6 i PM-10.

Zabezpieczenia rozszerzone: nie dotyczy.

PM-18 PLAN PROGRAMU OCHRONY PRYWATNOŚCI

Zabezpieczenie:

a. Opracuj i rozpowszechnij plan programu prywatności w całej organizacji, który zapewnia przegląd programu prywatności:

    1. Obejmuje opis struktury programu prywatności i zasobów przeznaczonych na program prywatności;

    2. Zapewnia przegląd wymagań programu prywatności i opis kontroli zarządzania programem prywatności i wspólnych kontroli obowiązujących lub zaplanowanych w celu spełnienia tych wymagań;

    3. Obejmuje rolę kierownika/pełnomocnika ds. prywatności oraz identyfikuje i przypisuje role innym urzędnikom ds. prywatności i personelowi oraz ich obowiązki;

    4. Opisuje zaangażowanie kierownictwa, zgodność oraz strategiczne cele i zadania programu prywatności;

    5. Odzwierciedla koordynację między jednostkami organizacyjnymi odpowiedzialnymi za różne aspekty prywatności;

    6. Jest zatwierdzony przez kierownika/pełnomocnika odpowiedzialnego za ryzyko dla prywatności związane z operacjami organizacyjnymi (w tym misji, funkcji, wizerunku i reputacji), aktywów organizacyjnych, osób fizycznych, innych organizacji i organów władzy państwowej;

b. Aktualizuj plan [Realizacja: częstotliwość określona przez organizację] i uwzględniaj zmiany w przepisach i polityce prywatności oraz zmiany organizacyjne i problemy zidentyfikowane podczas wdrażania planu lub ocen kontroli prywatności.

Zabezpieczenia powiązane: PM-8, PM-9, PM-19.

Zabezpieczenia rozszerzone: nie dotyczy.

PM-19 ROLA KIEROWNICZA PROGRAMU OCHRONY PRYWATNOŚCI

Zabezpieczenie:

Wyznacz kierownika/pełnomocnika ds. prywatności, który będzie miał uprawnienia, misję, odpowiedzialność i zasoby niezbędne do koordynowania, opracowywania i wdrażania stosownych wymogów dotyczących prywatności oraz zarządzania ryzykiem związanym z prywatnością w ramach programu ochrony prywatności obejmującego całą organizację.

Zabezpieczenia powiązane: PM-18, PM-20, PM-23, PM-24, PM-27.

Zabezpieczenia rozszerzone: nie dotyczy.

PM-20 ROZPOWSZECHNIANIE INFORMACJI O PROGRAMIE OCHRONY PRYWATNOŚCI

Zabezpieczenie:

Utrzymuj centralną stronę internetową z zasobami na głównej publicznej stronie internetowej organizacji, która służy jako centralne źródło informacji o programie prywatności organizacji i która:

a. Zapewnia, że społeczeństwo ma dostęp do informacji o działaniach organizacji w zakresie prywatności i może zwrócić się do nadrzędnej jednostki organizacyjnej w sprawie prywatności;

b. Zapewnia, że praktyki i raporty dotyczące prywatności organizacji są publicznie dostępne;

c. Wykorzystuje publiczne adresy e-mail i/lub linie telefoniczne, aby umożliwić społeczeństwu przekazywanie opinii i/lub kierowanie pytań do biur ds. prywatności dotyczących praktyk prywatności.

Zabezpieczenia powiązane: AC-3, PM-19, PT-5, PT-6, PT-7, RA-8.

Zabezpieczenia rozszerzone:

(1) ROZPOWSZECHNIANIE INFORMACJI O PROGRAMIE OCHRONY PRYWATNOŚCI | ZASADY OCHRONY PRYWATNOŚCI W WITRYNACH INTERNETOWYCH, APLIKACJACH I USŁUGACH CYFROWYCH

Opracuj i publikuj zasady ochrony prywatności na wszystkich zewnętrznych stronach internetowych, w aplikacjach mobilnych i innych usługach cyfrowych, które:

a. są napisane prostym językiem i zorganizowane w sposób łatwy do zrozumienia i nawigacji;

b. zawierają informacje potrzebne opinii publicznej do podjęcia świadomej decyzji o tym, czy i jak wchodzić w interakcję z organizacją;

c. są aktualizowane za każdym razem, gdy organizacja wprowadza istotną zmianę w opisywanych praktykach, i zawierają znacznik czasu/daty informujący opinię publiczną o dacie ostatnich zmian.

Zabezpieczenia powiązane: nie dotyczy.

PM-21 ROZLICZANIE UDOSTĘPNIEŃ

Zabezpieczenie:

a. Opracuj i prowadź dokładny rejestr udostępnień danych osobowych, w tym:

    1. Datę, charakter i cel każdego udostępnienia;

    2. Nazwę i adres lub inne dane kontaktowe osoby lub organizacji, której udostępnienie zostało dokonane;

b. Przechowuj rejestr udostępnień przez okres przechowywania danych osobowych lub pięć lat po dokonaniu ujawnienia, w zależności od tego, który okres jest dłuższy;

c. Udostępniaj na żądanie, informacje z rejestru udostępnień osobie, której dotyczą dane osobowe.

Zabezpieczenia powiązane: AC-3, AU-2, PT-2.

Zabezpieczenia rozszerzone: nie dotyczy.

PM-22 ZARZĄDZANIE JAKOŚCIĄ INFORMACJI UMOŻLIWIAJĄCYCH IDENTYFIKACJĘ OSOBY

Zabezpieczenie:

Opracuj i udokumentuj zasady i procedury obowiązujące w całej organizacji w celu:

a. Przeglądu dokładności, trafności, aktualności i kompletności danych osobowych w całym cyklu życia informacji;

b. Poprawiania lub usuwania niedokładnych lub nieaktualnych danych osobowych;

c. Rozpowszechniania powiadomień o poprawionych lub usuniętych danych osobowych osobom fizycznym lub innym właściwym podmiotom;

d. Odwołań od niekorzystnych decyzji dotyczących wniosków o korektę lub usunięcie.

Zabezpieczenia powiązane: PM-23, SI-18.

Zabezpieczenia rozszerzone: nie dotyczy.

PM-23 ZARZĄDZANIE DANYMI

Zabezpieczenie:

Powołaj osobę/zespół zarządzający i nadzorujący ochronę danych składający się z [Realizacja: role określone przez organizację] z [Realizacja: obowiązki określone przez organizację].

Zabezpieczenia powiązane: AT-2, AT-3, PM-19, PM-22, PM-24, PT-7, SI-4, SI-19.

Zabezpieczenia rozszerzone: nie dotyczy.

PM-24 RADA DS. INTEGRALNOŚCI DANYCH

Zabezpieczenie:

Powołaj Radę/Zespół ds. Integralności Danych w celu:

a. Przeglądania propozycji przeprowadzenia lub uczestnictwa w programie dopasowania;

b. Przeprowadzania corocznego przeglądu wszystkich programów dopasowania, w których organizacja uczestniczyła.

Zabezpieczenia powiązane: AC-4, PM-19, PM-23, PT-2, PT-8.

Zabezpieczenia rozszerzone: nie dotyczy.

PM-25 MINIMALIZACJA DANYCH OSOBOWYCH WYKORZYSTYWANYCH W TESTACH, SZKOLENIACH I BADANIACH

Zabezpieczenie:

a. Opracowuj, dokumentuj i wdrażaj zasady i procedury dotyczące wykorzystania danych osobowych do wewnętrznych testów, szkoleń i badań;

b. Ograniczaj lub minimalizuj ilość danych osobowych wykorzystywanych do wewnętrznych testów, szkoleń i badań;

c. Autoryzuj wykorzystanie danych osobowych, gdy takie informacje są wymagane do wewnętrznych testów, szkoleń i badań;

d. Przeglądaj i aktualizuj zasady i procedury [Realizacja: częstotliwość zdefiniowana przez organizację].

Zabezpieczenia powiązane: PM-23, PT-3, SA-3, SA-8, SI-12.

Zabezpieczenia rozszerzone: nie dotyczy.

PM-26 ZARZĄDZANIE SKARGAMI

Zabezpieczenie:

Wprowadź proces przyjmowania i odpowiadania na skargi, obawy lub pytania od osób fizycznych dotyczące praktyk bezpieczeństwa i prywatności organizacji, który obejmuje:

a. Mechanizmy, które są łatwe w użyciu i łatwo dostępne dla opinii publicznej;

b. Wszystkie informacje niezbędne do skutecznego składania skarg;

c. Mechanizmy śledzenia w celu zapewnienia, że wszystkie otrzymane skargi są sprawdzane i rozpatrywane w [Realizacja: okres czasu określony przez organizację];

d. Potwierdzenie otrzymania skarg, obaw lub pytań od osób fizycznych w [Realizacja: okres czasu określony przez organizację];

e. Odpowiedź na skargi, obawy lub pytania od osób fizycznych w [Realizacja: okres czasu określony przez organizację].

Zabezpieczenia powiązane: IR-7, IR-9, PM-22 i SI-18.

Zabezpieczenia rozszerzone: nie dotyczy.

PM-27 RAPORTOWANIE PRYWATNOŚCI

Zabezpieczenie:

a. Opracuj [Realizacja: raporty dotyczące prywatności zdefiniowane przez organizację] i rozpowszechnij je:

   1. [Realizacja: organy nadzorcze zdefiniowane przez organizację] w celu wykazania odpowiedzialności za ustawowe, regulacyjne i polityczne nakazy dotyczące prywatności;

   2. [Realizacja: urzędnicy zdefiniowani przez organizację] i inny personel odpowiedzialny za monitorowanie zgodności z programem prywatności;

b. Przeglądaj i aktualizuj raporty dotyczące prywatności [Realizacja: częstotliwość zdefiniowana przez organizację].

Zabezpieczenia powiązane: IR-9, PM-19.

Zabezpieczenia rozszerzone: nie dotyczy.

PM-28 UJĘCIE RYZYKA

Zabezpieczenie:

a. Zidentyfikuj i udokumentuj:

   1. Założenia wpływające na ocenę ryzyka, reakcje na ryzyko i monitorowanie ryzyka;

   2. Ograniczenia wpływające na ocenę ryzyka, reakcje na ryzyko i monitorowanie ryzyka;

   3. Priorytety i kompromisy rozważane przez organizację w celu zarządzania ryzykiem;

4. Tolerancję ryzyka organizacyjnego;

b. Dystrybuuj wyniki działań związanych z określaniem ryzyka do [Realizacja: personel zdefiniowany przez organizację];

c. Przejrzyj i zaktualizuj rozważania dotyczące określania ryzyka [Realizacja: częstotliwość zdefiniowana przez organizację].

Zabezpieczenia powiązane: CA-7, PM-9, RA-3, RA-7.

Zabezpieczenia rozszerzone: nie dotyczy.

PM-29 ROLE KIEROWNICZE W PROGRAMIE ZARZĄDZANIA RYZYKIEM

Zabezpieczenie:

a. Wyznacz kierownika/pełnomocnika odpowiedzialnego za zarządzanie ryzykiem, aby dostosować procesy zarządzania bezpieczeństwem informacji i prywatnością organizacji do procesów planowania strategicznego, operacyjnego i budżetowego;

b. Powołaj Dyrektora ds. Ryzyka (funkcja), aby przeglądać i analizować ryzyko z perspektywy całej organizacji i zapewnić spójność zarządzania ryzykiem w całej organizacji.

Zabezpieczenia powiązane: PM2, PM19.

Zabezpieczenia rozszerzone: nie dotyczy.

PM-30 STRATEGIA ZARZĄDZANIA RYZYKIEM ŁAŃCUCHA DOSTAW

Zabezpieczenie:

a. Opracuj strategię zarządzania ryzykiem łańcucha dostaw w całej organizacji, związaną z rozwojem, nabywaniem, konserwacją i utylizacją systemów, komponentów systemu i usług systemowych;

b. Wdrażaj strategię zarządzania ryzykiem łańcucha dostaw w sposób spójny w całej organizacji;

c. Przeglądaj i zaktualizuj strategię zarządzania ryzykiem łańcucha dostaw w [Realizacja: częstotliwość określona przez organizację] lub w razie potrzeby, aby uwzględnić zmiany organizacyjne.

Zabezpieczenia powiązane: CM-10, PM-9, SR-1, SR-2, SR-3, SR-4, SR-5, SR-6, SR-7, SR-8, SR-9, SR-11.

Zabezpieczenia rozszerzone:

(1) STRATEGIA ZARZĄDZANIA RYZYKIEM ŁAŃCUCHA DOSTAW | DOSTAWCY ARTYKUŁÓW KRYTYCZNYCH LUB NIEZBĘDNYCH DO REALIZACJI MISJI

Identyfikuj, ustalaj priorytety i oceniaj dostawców technologii, produktów i usług o znaczeniu krytycznym lub niezbędnym dla realizacji misji.

Zabezpieczenia powiązane: RA-3, SR-6.

PM-31 STRATEGIA CIĄGŁEGO MONITOROWANIA

Zabezpieczenie:

Opracuj strategię ciągłego monitorowania w całej organizacji i wprowadź programy ciągłego monitorowania, które obejmują:

a. Ustalenie następujących metryk w całej organizacji, które mają być monitorowane: [Realizacja: metryki zdefiniowane przez organizację];

b. Ustalenie [Realizacja: częstotliwości zdefiniowane przez organizację] do monitorowania i [Realizacja: częstotliwości zdefiniowane przez organizację] do oceny skuteczności kontroli;

c. Ciągłe monitorowanie metryk zdefiniowanych przez organizację zgodnie ze strategią ciągłego monitorowania;

d. Korelację i analizę informacji generowanych przez oceny kontroli i monitorowanie;

e. Działania reagowania w celu rozwiązania wyników analizy informacji o ocenie kontroli i monitorowaniu;

f. Raportowanie stanu bezpieczeństwa i prywatności systemów organizacyjnych do [Realizacja: personel lub role zdefiniowane przez organizację] [Realizacja: częstotliwość zdefiniowana przez organizację].

Zabezpieczenia powiązane: AC-2, AC-6, AC-17, AT-4, AU-6, AU-13, CA-2, CA-5, CA-6, CA-7, CM-3, CM-4, CM-6, CM-11, IA-5, IR-5, MA-2, MA-3, MA-4, PE-3, PE-6, PE-14, PE-16, PE-20, PL-2, PM-4, PM-6, PM-9, PM-10, PM-12, PM-14, PM-23, PM-28, PS-7, PT-7, RA-3, RA-5, RA-7, SA-9, SA-11, SC-5, SC-7, SC-18, SC-38, SC-43, SI-3, SI-4, SI-12, SR-2, SR-4.

Zabezpieczenia rozszerzone: nie dotyczy.

PM-32 CELOWOŚĆ

Zabezpieczenie:

Przeprowadź analizę [Realizacja: systemy lub komponenty systemów zdefiniowane przez organizację] wspierającą istotne dla misji usługi lub funkcje, aby upewnić się, że zasoby informacyjne są wykorzystywane zgodnie z ich zamierzonym celem.

Zabezpieczenia powiązane: CA-7, PL-2, RA-3, RA-9.

Zabezpieczenia rozszerzone: nie dotyczy.

KATEGORIA: PS – BEZPIECZEŃSTWO OSOBOWE

PS-1 POLITYKA I PROCEDURY

Zabezpieczenie:

Opracowuj, dokumentuj i rozpowszechnij wśród [Realizacja: personel lub role określone przez organizację]:

a. [Wybór (jeden lub więcej): poziom organizacji; poziom misji/procesu biznesowego; poziom systemu] politykę bezpieczeństwa osobowego, która:

    (a) Adresuje cel, zakres, role, obowiązki, zaangażowanie kierownictwa, koordynację między jednostkami organizacyjnymi i zgodność z przepisami;

    (b) Jest zgodna z obowiązującym prawem, rozporządzeniami, dyrektywami, przepisami, zasadami, standardami i wytycznymi;

    2. Procedury ułatwiające wdrożenie polityki bezpieczeństwa osobowego oraz powiązanych zabezpieczeń w zakresie bezpieczeństwa osobowego;

b. Wyznacz [Realizacja: osoba wyznaczona przez organizację] do zarządzania rozwojem, dokumentacją i rozpowszechnianiem polityki i procedur bezpieczeństwa osobowego;

c. Przeglądaj i aktualizuj na bieżąco:

    1. Polityki bezpieczeństwa osobowego z [Realizacja: częstotliwość określona przez organizację] i następujące [Realizacja: zdarzenia określone przez organizację];

    2. Procedury bezpieczeństwa osobowego z [Realizacja: częstotliwość określona przez organizację] i następujące [Realizacja: zdarzenia określone przez organizację].

Zabezpieczenia powiązane: PM-9, PS-8, SI-12.

Zabezpieczenia rozszerzone: nie dotyczy.

PS-2 OKREŚLANIE RYZYKA DLA STANOWISKA PRACY

Zabezpieczenie:

a. Przypisz oznaczenia ryzyka do wszystkich stanowisk organizacyjnych;

b. Ustal kryteriów selekcji osób zajmujących te stanowiska;

c. Przeglądaj i aktualizuj oznaczenia ryzyka stanowisk [Realizacja: częstotliwość określona przez organizację].

Zabezpieczenia powiązane: AC-5, AT-3, PE-2, PE-3, PL-2, PS-3, PS-6, SA-5, SA 21, SI-12.

Zabezpieczenia rozszerzone: nie dotyczy.

PS-3 DOBÓR PERSONELU

Zabezpieczenie:

a. Przeprowadzaj postępowania sprawdzające osób przed autoryzowaniem dostępu do systemu;

b. Ponownie sprawdzaj osoby zgodnie z [Realizacja: warunki określone przez organizację, które wymagają ponownego sprawdzenia oraz w przypadku, gdy ponowne postępowanie sprawdzające jest wskazane, częstotliwość ponownego sprawdzenia].

Zabezpieczenia powiązane: AC-2, IA-4, MA-5, PE-2, PM-12, PS-2, PS-6, PS-7, SA-21.

Zabezpieczenia rozszerzone:

(1) DOBÓR PERSONELU | INFORMACJE NIEJAWNE

Sprawdzaj, czy osoby mające dostęp do systemu przetwarzającego, przechowującego lub przekazującego informacje niejawne posiadają poświadczenia bezpieczeństwa do najwyższego poziomu klasyfikacji informacji, do których mają dostęp w systemie.

Zabezpieczenia powiązane: AC-3, AC-4.

(2) DOBÓR PERSONELU | POSTĘPOWANIA SPRAWDZAJĄCE

Sprawdzaj, czy osoby mające dostęp do systemu przetwarzającego, przechowującego lub przekazującego informacje niejawne, podlegały, zgodnie z ustawą o ochronie informacji niejawnych, stosownemu postępowaniu sprawdzającemu.

Zabezpieczenia powiązane: AC-3, AC-4.

(3) DOBÓR PERSONELU | INFORMACJE WYMAGAJĄCE SZCZEGÓLNEJ OCHRONY

Sprawdzaj, czy osoby mające dostęp do systemu przetwarzającego, przechowującego lub przesyłającego informacje wymagające szczególnej ochrony:

a. Posiadają ważne poświadczenia bezpieczeństwa zezwalające na dostęp do informacji, których posiadanie jest wymagane w związku z powierzonymi im obowiązkami służbowymi;

b. Spełniają dodatkowe kryteria [Realizacja: zdefiniowane przez organizację dodatkowe kryteria selekcji personelu].

Zabezpieczenia powiązane: nie dotyczy.

(4) DOBÓR PERSONELU | WYMAGANIA DOTYCZĄCE OBYWATELSTWA

Sprawdzaj, czy osoby mające dostęp do systemu przetwarzającego, przechowującego lub przesyłającego [Realizacja: typy informacji określone przez organizację] spełniają [Realizacja: wymagania dotyczące obywatelstwa określone przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

PS-4 ZAKOŃCZENIE ZATRUDNIENIA

Zabezpieczenie:

Po zakończeniu indywidualnego zapewnij w organizacji:

a. Wyłączenie dostępu do systemu w ciągu [Realizacja: okres czasu określony przez organizację];

b. Zakończenie / odwołanie wszelkich pełnomocnictw / poświadczeń powiązanych z osobą;

c. Przeprowadź rozmowy końcowe, które obejmują omówienie tematów bezpieczeństwa [Realizacja: tematy związane z bezpieczeństwem informacji określone przez organizację];

d. Odbieraj wszystkie aktywa związane z bezpieczeństwem systemu wykorzystywane, przydzielone oraz wytworzone przez pracownika na danym stanowisku;

e. Zachowuj dostęp do informacji organizacyjnych i systemów nadzorowanych (użytkowanych) przez zwalnianą osobę.

Zabezpieczenia powiązane: AC-2, IA-4, PE-2, PM-12, PS-6, PS-7.

Zabezpieczenia rozszerzone:

(1) ZAKOŃCZENIE ZATRUDNIENIA | ZOBOWIĄZANIA PO ZAKOŃCZENIU ZATRUDNIENIA

a. Powiadamiaj osoby, z którymi rozwiązano stosunek pracy, o obowiązujących, prawnie wiążących wymogach dotyczących ochrony informacji organizacyjnych po ustaniu stosunku pracy;

b. Wymagaj podpisania przez zwalniane osoby oświadczenie w zakresie zachowania tajemnicy organizacji po okresie zatrudnienia.

Zabezpieczenia powiązane: nie dotyczy.

(2) ZAKOŃCZENIE ZATRUDNIENIA | AUTOMATYCZNE POWIADAMIANIE

Używaj [Realizacja: mechanizmy automatyczne zdefiniowane przez organizację] do [Wybór (jeden lub więcej): powiadomienia [Realizacja: personel lub role zdefiniowane przez organizację] o indywidualnym zakończeniu pracy przez daną osobę; wyłączenie dostępu do zasobów systemu].

Zabezpieczenia powiązane: nie dotyczy.

PS-5 OBSADZENIE LUB PRZENIESIENIE STANOWISKA

Zabezpieczenie:

a. Przeglądaj i potwierdzaj na bieżąco potrzeby operacyjne w zakresie aktualnych logicznych i fizycznych uprawnień dostępu do systemów i obiektów w przypadku zmiany przydziału lub przeniesienia osób na inne stanowiska w organizacji;

b. Inicjuj [Realizacja: zdefiniowane przez organizację działania przeniesienia lub ponownego obsadzenia stanowiska] w ciągu [Realizacja: zdefiniowane przez organizację okres po formalnym przeniesieniu / ponownym obsadzeniu];

c. Modyfikuj uprawnienia dostępu w zależności od potrzeb, tak aby odpowiadały one wszelkim zmianom potrzeb operacyjnych wynikających ze zmiany przydziału lub przeniesienia;

d. Powiadamiaj [Realizacja: personel lub role określone przez organizację] w ciągu [Realizacja: okres czasu określony przez organizację].

Zabezpieczenia powiązane: AC-2, IA-4, PE-2, PM-12, PS-4, PS-7.

Zabezpieczenia rozszerzone: nie dotyczy.

PS-6 UMOWY DOSTĘPU / WSPÓŁPRACY

Zabezpieczenie:

a. Opracowuj i dokumentuj umowy o dostępie do systemów organizacyjnych;

b. Przeglądaj i aktualizuj umowy o dostępie/współpracy [Realizacja: częstotliwość określona przez organizację];

c. Sprawdzaj, czy osoby wymagające dostępu do informacji i systemów organizacyjnych:

   1. Podpisały odpowiednie umowy o dostępie przed udzieleniem dostępu;

   2. Ponowne podpisały umowy o dostępie/współpracy w celu zachowania dostępu do systemów organizacyjnych po aktualizacji umów o dostępie lub z częstotliwością [Realizacja: częstotliwość określona przez organizację].

Zabezpieczenia powiązane: AC-17, PE-2, PL-4, PS-2, PS-3, PS-4, PS-6, PS-7, PS-8, SA-21, SI-12.

Zabezpieczenia rozszerzone:

(1) UMOWY DOSTEPU / WSPÓŁPRACY | INFORMACJE WYMAGAJĄCE SZCZEGÓLNEJ OCHRONY

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(2) UMOWY DOSTEPU / WSPÓŁPRACY | INFORMACJE NIEJAWNE WYMAGAJĄCE OCHRONY SPECJALNEJ

Sprawdzaj, czy dostęp do informacji niejawnych wymagających szczególnej ochrony jest udzielany wyłącznie osobom, które:

a. Posiadają ważne poświadczenia bezpieczeństwa, wydane przez krajową władzę bezpieczeństwa;

b. Spełniają kryteria bezpieczeństwa osobowego;

c. Przeczytały, zrozumiały i podpisały umowy o zachowaniu poufności.

Zabezpieczenia powiązane: nie dotyczy.

(3) UMOWY DOSTEPU / WSPÓŁPRACY | WYMOGI PO ZAKOŃCZENIU ZATRUDNIENIA

a. Powiadamiaj osoby o obowiązujących, prawnie wiążących wymogach dotyczących ochrony informacji organizacyjnych po zatrudnieniu;

b. Wymagaj od osób podpisania oświadczenia o zachowaniu tajemnicy informacji organizacyjnych.

Zabezpieczenia powiązane: PS-4.

PS-7 BEZPIECZEŃSTWO OSOBOWE STRON TRZECICH

Zabezpieczenie:

a. Ustanawiaj wymagania dotyczących bezpieczeństwa personelu, w tym ról i obowiązków dostawców zewnętrznych w zakresie bezpieczeństwa;

b. Wymagaj od dostawców zewnętrznych przestrzegania zasad i procedur bezpieczeństwa personelu ustanowionych przez organizację;

c. Dokumentuje wymagania bezpieczeństwa personelu;

d. Wymagaj od zewnętrznych usługodawców powiadamiania [Realizacja: personel lub role określone przez organizację] o każdym przeniesieniu lub zakończeniu pracy personelu zewnętrznego, który posiada poświadczenia i / lub identyfikatory organizacyjne lub posiada uprawnienia systemowe nie później niż do [Realizacja: okres czasu zdefiniowany przez organizację];

e. Monitoruj stosowanie przez dostawcę zasad i procedur bezpieczeństwa.

Zabezpieczenia powiązane: AT-2, AT-3, MA-5, PE-3, PS-2, PS-3, PS-4, PS-5, PS-6, SA-5, SA-9, SA-21.

Zabezpieczenia rozszerzone: nie dotyczy.

PS-8 SANKCJE PERSONALNE

Zabezpieczenie:

a. Stosuj formalne procedury sankcji organizacyjnych wobec osób, które nie przestrzegają ustalonych zasad i procedur dotyczących bezpieczeństwa informacji i ochrony prywatności;

b. Powiadamiaj [Realizacja: zdefiniowany przez organizację personel lub role] w ciągu [Realizacja: zdefiniowany przez organizację okres czasu] o rozpoczęciu formalnego procesu sankcji pracowniczych, określając osobę, na którą nałożono sankcje oraz powód nałożenia sankcji.

Zabezpieczenia powiązane: AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PL-4, PM-1, PM-12, PS-1, PS-6, PT-1, RA-1, SA-1, SC-1, SI-1, SR-1.

Zabezpieczenia rozszerzone: nie dotyczy.

PS-9 OPISY STANOWISK PRACY

Zabezpieczenie:

Włącz role i obowiązki w zakresie bezpieczeństwa ochrony prywatności do opisów stanowisk organizacyjnych.

Zabezpieczenia powiązane: nie dotyczy.

Zabezpieczenia rozszerzone: nie dotyczy.

KATEGORIA: PT - PRZEJRZYSTOŚĆ PRZETWARZANIA DANYCH OSOBOWYCH

PT-1 POLITYKA I PROCEDURY

Zabezpieczenie:

a. Opracowuj, dokumentuj i rozpowszechnij wśród [Realizacja: personel lub role określone przez organizację]:

    1. [Wybór (jeden lub więcej): poziom organizacji; poziom misji/procesu biznesowego; poziom systemu] politykę przejrzystości przetwarzania danych osobowych, która:

(a) Adresuje cel, zakres, role, obowiązki, zaangażowanie kierownictwa, koordynację między jednostkami organizacyjnymi i zgodność z przepisami;

(b) Jest zgodna z obowiązującym prawem, rozporządzeniami, dyrektywami, przepisami, zasadami, standardami i wytycznymi;

2. Procedury ułatwiające wdrożenie polityki przejrzystości przetwarzania danych osobowych oraz powiązanych zabezpieczeń przejrzystości przetwarzania danych osobowych;

b. Wyznaczaj [Realizacja: osoba wyznaczona przez organizację] do zarządzania rozwojem, dokumentacją i rozpowszechnianiem polityki i procedur przejrzystości przetwarzania danych osobowych;

c. Przeglądaj i aktualizuj na bieżąco:

1. Politykę przejrzystości przetwarzania danych osobowych z [Realizacja: częstotliwość określona przez organizację] i następujące [Realizacja: zdarzenia określone przez organizację];

2. Procedury przejrzystości przetwarzania danych osobowych z [Realizacja: częstotliwość określona przez organizację] i następujące [Realizacja: zdarzenia określone przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

Zabezpieczenia rozszerzone: nie dotyczy.

PT 2 UPRAWNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

Zabezpieczenie:

a. Określ i udokumentuj [Realizacja: organ zdefiniowany przez organizację], który zezwala na [Realizacja: przetwarzanie zdefiniowane przez organizację] informacji umożliwiających identyfikację osób;

b. Ogranicz [Realizacja: zdefiniowane przez organizację przetwarzanie] informacji umożliwiających identyfikację osób do tych, które są autoryzowane.

Zabezpieczenia powiązane: AC-2, AC-3, CM-13, IR-9, PM-9, PM-24, PT-1, PT-3, PT-5, PT-6, RA-3, RA-8, SI-12, SI-18.

Zabezpieczenia rozszerzone:

(1) UPRAWNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH | OZNACZANIE DANYCH

Dołączaj znaczniki (tagów) danych zawierających [Realizacja: określone przez organizację autoryzowane przetwarzanie] do [Realizacja: zdefiniowane przez organizację elementy informacji umożliwiające identyfikację osoby].

Zabezpieczenia powiązane: AC-16, CA-6, CM-12, PM-5, PM-22, PT-4, SC-16, SC-43, SI-10, SI-15, SI-19.

(2) UPRAWNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH | AUTOMATYZACJA

Zarządzaj egzekwowaniem upoważnień do przetwarzania danych osobowych przy użyciu [Realizacja: zautomatyzowane mechanizmy zdefiniowane przez organizację].

Zabezpieczenia powiązane: CA-6, CM-12, PM-5, PM-22, PT-4, SC-16, SC-43, SI-10, SI-15, SI-19.

PT-3 CELE PRZETWARZANIA DANYCH OSOBOWYCH

Zabezpieczenie:

a. Zidentyfikuj i udokumentuj cele przetwarzania danych osobowych [Realizacja: cele zdefiniowane przez organizację];

b. Opisz cele przetwarzania danych osobowych w publicznie dostępnej informacji o prywatności i polityce organizacji;

c. Ogranicz [Realizacja: przetwarzane informacje zdefiniowane przez organizację] umożliwiających identyfikację osoby tylko do tych, które są zgodne ze zidentyfikowanymi celami;

d. Monitoruj zmiany w przetwarzaniu danych osobowych i wdrożenie [Realizacja: mechanizmy określone przez organizację] w celu zapewnienia, że wszelkie zmiany są dokonywane zgodnie z [Realizacja: wymagania określone przez organizację].

Zabezpieczenia powiązane: AC-2, AC-3, AT-3, CM-13, IR-9, PM-9, PM-25, PT-2, PT-5, PT-6, PT-7, RA-8, SC-43, SI-12, SI-18.

Zabezpieczenia rozszerzone:

(1) CELE PRZETWARZANIA DANYCH OSOBOWYCH | OZNACZANIE DANYCH

Dołącz do [Realizacja: zdefiniowane przez organizację elementy informacji umożliwiających identyfikację osoby] znaczniki danych zawierających następujące cele: [Realizacja: zdefiniowane przez organizację cele przetwarzania].

Zabezpieczenia powiązane: CA-6, CM-12, PM-5, PM-22, SC-16, SC-43, SI-10, SI-15, SI-19.

(2) CELE PRZETWARZANIA DANYCH OSOBOWYCH | AUTOMATYZACJA

Śledź cele przetwarzania danych osobowych przy użyciu [Realizacja: zautomatyzowane mechanizmy zdefiniowane przez organizację].

Zabezpieczenia powiązane: CA-6, CM-12, PM-5, PM-22, SC-16, SC-43, SI-10, SI-15, SI-19.

PT-4 ZGODY

Zabezpieczenie:

Wprowadź [Realizacja: zdefiniowane przez organizację narzędzia lub mechanizmy ułatwiające osobom podejmowanie świadomych decyzji] pozwalające osobom fizycznym na wyrażanie zgody na przetwarzanie ich danych osobowych przed ich zebraniem.

Zabezpieczenia powiązane: AC-16, PT-2, PT-5.

Zabezpieczenia rozszerzone:

(1) ZGODY | UPOWAŻNIENIE

Dostarcz [Realizacja: mechanizmy zdefiniowane przez organizację] umożliwiających osobom dostosowanie uprawnień do przetwarzania wybranych elementów danych osobowych.

Zabezpieczenia powiązane: PT-2.

(2) ZGODY | ZGODA TYPU „JUST-IN TIME"

Prezentuj [Realizacja: zdefiniowane przez organizację mechanizmy zgody] osobom z [Realizacja: zdefiniowana przez organizację częstotliwość] i w połączeniu z [Realizacja: zdefiniowane przez organizację przetwarzanie danych osobowych].

Zabezpieczenia powiązane: PT-2.

(3) ZGODY | WYCOFANIE ZGODY

Wprowadź [Realizacja: narzędzia lub mechanizmy określone przez organizację] umożliwiające osobom wycofanie zgody na przetwarzanie ich danych osobowych.

Zabezpieczenia powiązane: PT-2.

PT-5 INFORMACJA O OCHRONIE PRYWATNOŚCI

Zabezpieczenie:

Powiadamiaj o przetwarzaniu danych osobowych osoby, których dane dotyczą:

a. podczas pierwszego kontaktu z organizacją, a następnie [Realizacja: częstotliwość określona przez organizację];

b. w sposób jasny i łatwy do zrozumienia, przedstawiaj informacje o przetwarzaniu danych osobowych w prostym języku;

c. wskazując administratora danych osobowych;

d. określając cele, dla których dane osobowe mają być przetwarzane;

e. wskazując [Realizacja: informacje określone przez organizację].

Zabezpieczenia powiązane: PM-20, PM-22, PT-2, PT-3, PT-4, PT-7, RA-3, SC-42, SI-18.

Zabezpieczenia rozszerzone:

(1) INFORMACJA O OCHRONIE PRYWATNOŚCI | INFORMACJA NA ŻĄDANIE

Przedstawiaj osobom, których dane dotyczą powiadomienia o przetwarzaniu danych osobowych w czasie i miejscu, w którym osoba udostępnia informacje umożliwiające identyfikację, lub prowadzonych działaniach na danych, lub [Realizacja: częstotliwość określona przez organizację].

Zabezpieczenia powiązane: PM-21.

(2) INFORMACJA O OCHRONIE PRYWATNOŚCI | OŚWIADCZENIE O OCHRONIE PRYWATNOŚCI

Umieść klauzule informacyjne dotyczące ochrony danych osobowych na formularzach służących do zbierania informacji, które będą przechowywane w systemie rejestrów danych osobowych zgodnie z przepisami o ochronie danych, lub przekaż te klauzule na osobnych formularzach, które mogą zostać zachowane przez osoby, których dane dotyczą.

Zabezpieczenia powiązane: PT-6.

Zabezpieczenia rozszerzone: nie dotyczy.

PT-6 INFORMACJA O PROWADZONYCH REJESTRACH

Zabezpieczenie:

W przypadku systemów przetwarzających informacje, które będą przechowywane w prowadzonych rejestrach:

a. Sporządzaj zawiadomienia o systemie rejestrów zgodnie z przepisami prawa oraz przedkładaj nowe i znacząco zmodyfikowane zawiadomienia o prowadzonych rejestrach odpowiednim komisjom organizacyjnym celu dokonania wcześniejszego przeglądu;

b. Publikuj informacje o prowadzonych rejestrach;

c. Utrzymuj dokładność, aktualność i zakres informacji o prowadzonych rejestrach zgodnie z polityką.

Zabezpieczenia powiązane: AC-3, PM-20, PT-2, PT-3, PT-5.

Zabezpieczenia rozszerzone:

(1) POWIADOMIENIE O PROWADZONYCH REJESTRACH | RUTYNOWE ZASTOSOWANIA

Przeglądaj wszystkie rutynowe zastosowania opublikowanych w zawiadomieniu o prowadzonych rejestrach z [Realizacja: częstotliwość określona przez organizację] w celu zapewnienia nieprzerwanej zgodności z celem, dla którego informacja została zebrana.

Zabezpieczenia powiązane: nie dotyczy.

(2) POWIADOMIENIE O PROWADZONYCH REJESTRACH | ZASADY WYŁĄCZENIA

Przeglądaj wszystkie zwolnienia z ustawy o ochronie danych zgłoszonych do prowadzonych rejestrów [Realizacja: częstotliwość określona przez organizację] w celu zapewnienia, że pozostają one właściwe i niezbędne zgodnie z prawem, że zostały ogłoszone jako przepisy i że są dokładnie opisane w prowadzonych rejestrach.

Zabezpieczenia powiązane: nie dotyczy.

PT-7 SZCZEGÓLNE KATEGORIE DANYCH OSOBOWYCH

Zabezpieczenie:

Zastosuj [Realizacja: warunki przetwarzania określone przez organizację] dla określonych kategorii informacji umożliwiających identyfikację osób.

Zabezpieczenia powiązane: IR-9, PT-2, PT-3, RA-3.

Zabezpieczenia rozszerzone:

(1) SZCZEGÓLNE KATEGORIE DANYCH OSOBOWYCH | IDENTYFIKATOR OSOBY - NP. NUMER PESEL

Przy przetwarzaniu przez system numerów identyfikatorów osobowych zastosuj:

a. Wyeliminowanie zbędnego gromadzenia, utrzymywania i wykorzystywania identyfikatorów osobowych oraz zbadać alternatywy dla ich wykorzystywania jako identyfikatorów osobowych;

b. Nie odmawiaj żadnej osobie jakichkolwiek praw, korzyści lub przywilejów przewidzianych prawem z powodu odmowy ujawnienia numeru identyfikacji osobistej przez tę osobę;

c. Informuj każdą osobę, która jest proszona o ujawnienie swojego identyfikatora osobowego o tym, czy ujawnienie to jest obowiązkowe czy dobrowolne, na podstawie jakich przepisów ustawowych lub innych uprawnień taki identyfikator jest wymagany i w jaki sposób będzie wykorzystywany.

Zabezpieczenia powiązane: IA-4.

(2) SZCZEGÓLNE KATEGORIE DANYCH OSOBOWYCH | PRZETWARZANIE WRAŻLIWYCH DANYCH OSOBOWYCH

Zabraniaj przetwarzania informacji opisujących, korzystanie przez osobę z praw gwarantowanych przez Konstytucję RP, chyba że: jest to wyraźnie dozwolone przez ustawę, odbywa się to za zgodą osoby lub jeśli jest to istotne i mieści się w zakresie uprawnionej działalności organów ścigania.

Zabezpieczenia powiązane: nie dotyczy.

PT-8 WYMAGANIA DOTYCZĄCE ZGODNOŚCI PRZY AUTOMATYCZNYM PRZETWARZANIU DANYCH

Zabezpieczenie:

Gdy system lub organizacja przetwarza informacje w celu przeprowadzenia programu dopasowywania danych:

a. Uzyskaj zgodę Radę/Zespół ds. Integralności Danych na realizację programu dopasowywania danych;

b. Opracuj i zawrzyj umowę o dopasowywaniu komputerowym;

c. Opublikuj zawiadomienie o dopasowywaniu danych w Dzienniku Urzędowym;

d. Niezależnie zweryfikuj informacje uzyskane w wyniku programu dopasowywania danych przed podjęciem negatywnych działań wobec osoby, jeśli jest to wymagane;

e. Poinformuj osoby, których dane dotyczą, i zapewnij im możliwość odpowiedzi.

Zabezpieczenia powiązane: PM-24.

Zabezpieczenia rozszerzone: nie dotyczy.

KATEGORIA: RA - OCENA RYZYKA

RA-1 POLITYKA I PROCEDURY

Zabezpieczenie:

a. Opracuj, udokumentuj i rozpowszechnij do [Realizacja: personel lub role zdefiniowane przez organizację]:

    1. [Wybór (jeden lub więcej): poziom organizacji, poziom procesów misji/biznesu, poziom systemu] politykę oceny ryzyka, która:

        (a) Dotyczy celu, zakresu, ról, obowiązków, zaangażowania kierownictwa, koordynacji między jednostkami organizacyjnymi i zgodności;

        (b) Jest zgodna z obowiązującymi przepisami prawa, zarządzeniami wykonawczymi, dyrektywami, regulacjami, politykami, standardami i wytycznymi;

    2. Procedury ułatwiające wdrożenie polityki oceny ryzyka i powiązanych mechanizmów kontrolnych oceny ryzyka;

b. Wyznacz [Realizacja: urzędnika zdefiniowanego przez organizację] do zarządzania opracowywaniem, dokumentacją i rozpowszechnianiem polityki i procedur oceny ryzyka;

c. Przeglądaj i aktualizuj na bieżąco ocenę ryzyka w:

    1. Polityce [Realizacja: częstotliwość określona przez organizację] i następujących [Realizacja: zdarzenia określone przez organizację];

    2. Procedurach [Realizacja: częstotliwość określona przez organizację] i następujących [Realizacja: zdarzenia określone przez organizację].

Zabezpieczenia powiązane: PM-9, PS-8, SI-12.

Zabezpieczenia rozszerzone: nie dotyczy.

RA-2 KATEGORYZACJA BEZPIECZEŃSTWA

Zabezpieczenie:

a. Skategoryzuj system i informacje, które przetwarza, przechowuje i przesyła;

b. Udokumentuj wyniki kategoryzacji bezpieczeństwa wraz z uzasadnieniem w planie bezpieczeństwa systemu;

c. Zweryfikuj, czy administrator autoryzujący lub wyznaczony przedstawiciel administratora autoryzującego przegląda i zatwierdza decyzję o kategoryzacji bezpieczeństwa.

Zabezpieczenia powiązane: CM-8, MP-4, PL-2, PL-10, PL-11, PM-7, RA-3, RA-5, RA-7, RA-8, SA-8, SC-7, SC-38, SI-12.

Zabezpieczenia rozszerzone:

(1) KATEGORYZACJA BEZPIECZEŃSTWA | PRIORYTETYZACJA POZIOMÓW WPŁYWU

Przeprowadź priorytetyzację systemów organizacyjnych na podstawie poziomu oddziaływania, aby uzyskać dodatkową szczegółowość poziomów oddziaływania na system.

Zabezpieczenia powiązane: nie dotyczy.

RA-3 SZACOWANIE RYZYKA

Zabezpieczenie:

a. Przeprowadź szacowanie ryzyka, w tym:

    1. Identyfikację zagrożeń i podatności w systemie;

2. Określenie prawdopodobieństwa i skali szkód wynikających z nieuprawnionego dostępu, użycia, ujawnienia, zakłócenia, modyfikacji lub zniszczenia systemu, informacji, które przetwarza, przechowuje lub przesyła oraz wszelkich powiązanych informacji;

3. Określenie prawdopodobieństwa i wpływu negatywnych skutków na osoby wynikających z przetwarzania danych osobowych;

b. Zintegruj wyniki szacowania ryzyka i decyzje dotyczące zarządzania ryzykiem z perspektywy organizacji oraz misji lub procesów biznesowych z szacowaniem ryzyka na poziomie systemu;

c. Udokumentuj wyniki szacowania ryzyka [Wybór: plany bezpieczeństwa i ochrony danych, raport szacowania ryzyka, [Realizacja: dokument zdefiniowany przez organizację]];

d. Przeglądaj wyniki szacowania ryzyka [Realizacja: częstotliwość określona przez organizację];

e. Rozpowszechnij wyniki szacowania ryzyka do [Realizacja: personel lub role zdefiniowane przez organizację];

f. Aktualizuj szacowanie ryzyka [Realizacja: częstotliwość określona przez organizację] lub gdy występują znaczące zmiany w systemie, jego środowisku operacyjnym lub inne warunki, które mogą wpłynąć na stan bezpieczeństwa lub prywatności systemu.

Zabezpieczenia powiązane: AT-2, CA-3, CA-6, CM-4, CM-13, CP-6, CP-7, IA-8, MA-5, PE-3, PE-8, PE-18, PL-2, PL-10, PL-11, PM-8, PM-9, PM-17, PM-28, PM-30, PT-2, PT-7, RA-2, RA-5, RA-7, RA-9, SA-8, SA-9, SC-38, SI-12, SR-2.

Zabezpieczenia rozszerzone:

(1) SZACOWANIE RYZYKA | SZACOWANIE RYZYKA W ŁAŃCUCHU DOSTAW

a. Oceń ryzyka łańcucha dostaw związane z [Realizacja: systemy, komponenty systemu i usługi systemowe zdefiniowane przez organizację];

b. Aktualizuj szacowanie ryzyka łańcucha dostaw [Realizacja: częstotliwość określona przez organizację], gdy występują znaczące zmiany w odpowiednim łańcuchu dostaw lub gdy zmiany w systemie, środowiskach operacyjnych lub inne warunki mogą wymagać zmiany w łańcuchu dostaw.

Zabezpieczenia powiązane: RA-2, RA-9, PM-17, PM-30, SR-2.

(2) SZACOWANIE RYZYKA | WYKORZYSTANIE INFORMACJI ZE WSZYSTKICH ŹRÓDEŁ

Wykorzystaj informacje ze wszystkich źródeł, aby wspomóc analizę ryzyka.

Zabezpieczenia powiązane: nie dotyczy.

(3) SZACOWANIE RYZYKA | ŚWIADOMOŚĆ DYNAMICZNEGO ZAGROŻENIA

Określaj bieżące środowisko zagrożeń cybernetycznych w sposób ciągły przy użyciu [Realizacja: środki zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(4) SZACOWANIE RYZYKA | PREDYKCYJNA ANALITYKA CYBERBEZPIECZEŃSTWA

Zastosuj następujące zaawansowane możliwości automatyzacji i analityki do przewidywania i identyfikacji ryzyka dla [Realizacja: systemy lub komponenty systemu zdefiniowane przez organizację]: [Realizacja: zaawansowane możliwości automatyzacji i analityki zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

RA-4 AKTUALIZACJA OCENY RYZYKA

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

RA-5 MONITOROWANIE I SKANOWANIE PODATNOŚCI

Zabezpieczenie:

a. Monitoruj i skanuj pod kątem podatności w systemie i hostowanych aplikacjach [Realizacja: częstotliwość określona przez organizację i/lub losowo zgodnie z procesem zdefiniowanym przez organizację] oraz gdy zostaną zidentyfikowane i zgłoszone nowe podatności potencjalnie wpływające na system;

b. Stosuj narzędzia i techniki monitorowania podatności, które ułatwiają współdziałanie między narzędziami i automatyzują części procesu zarządzania podatnościami poprzez użycie standardów dla:

    1. Wyliczania platform, wad oprogramowania i nieprawidłowych konfiguracji;

    2. Formatowania list kontrolnych i procedur testowych;

    3. Mierzenia wpływu podatności;

c. Analizuj raporty ze skanowania podatności i wyniki z monitorowania podatności;

d. Naprawiaj uzasadnione podatności [Realizacja: czasy reakcji zdefiniowane przez organizację] zgodnie z organizacyjną oceną ryzyka;

e. Udostępniaj informacje uzyskane z procesu monitorowania podatności i ocen kontrolnych [Realizacja: personel lub role zdefiniowane przez organizację] aby pomóc wyeliminować podobne podatności w innych systemach;

f. Stosuj narzędzia monitorowania podatności, które obejmują możliwość łatwej aktualizacji skanowanych podatności.

Zabezpieczenia powiązane: CA-2, CA-7, CA-8, CM-2, CM-4, CM-6, CM-8, RA-2, RA-3, SA-11, SA-15, SC-38, SI-2, SI-3, SI-4, SI-7, SR-11.

Zabezpieczenia rozszerzone:

(1) MONITOROWANIE I SKANOWANIE PODATNOŚCI | AKTUALIZACJA NARZĘDZI

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(2) MONITOROWANIE I SKANOWANIE PODATNOŚCI | AKTUALIZACJA SKANOWANYCH PODATNOŚCI

Aktualizuj podatności systemu, które mają być skanowane [Wybór (jeden lub więcej): [Realizacja: częstotliwość określona przez organizację], przed nowym skanowaniem, gdy nowe podatności są identyfikowane i raportowane].

Zabezpieczenia powiązane: SI-5.

(3) MONITOROWANIE I SKANOWANIE PODATNOŚCI | ZAKRES I GŁĘBOKOŚĆ POKRYCIA

Zdefiniuj zakres i głębokość pokrycia skanowania podatności.

Zabezpieczenia powiązane: nie dotyczy.

(4) MONITOROWANIE I SKANOWANIE PODATNOŚCI | INFORMACJE MOŻLIWE DO ODKRYCIA

Określ informacje o systemie, które są możliwe do wykrycia i podejmij [Realizacja: działania naprawcze zdefiniowane przez organizację].

Zabezpieczenia powiązane: AU-13, SC-26.

(5) MONITOROWANIE I SKANOWANIE PODATNOŚCI | DOSTĘP UPRZYWILEJOWANY

Wprowadź autoryzację dostępu uprzywilejowanego do [Realizacja: komponenty systemu zdefiniowane przez organizację] dla [Realizacja: działania skanowania podatności zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(6) MONITOROWANIE I SKANOWANIE PODATNOŚCI | ZAUTOMATYZOWANE ANALIZY TRENDÓW

Porównuj wyniki wielu skanowań podatności przy użyciu [Realizacja: zautomatyzowane mechanizmy zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(7) MONITOROWANIE I SKANOWANIE PODATNOŚCI | AUTOMATYCZNE WYKRYWANIE I POWIADAMIANIE O NIEAUTORYZOWANYCH KOMPONENTACH

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(8) MONITOROWANIE I SKANOWANIE PODATNOŚCI | PRZEGLĄD HISTORYCZNYCH LOGÓW AUDYTU

Przeglądaj historyczne logi audytu, aby ustalić, czy podatność zidentyfikowana w [Realizacja: system zdefiniowany przez organizację] została wcześniej wykorzystana w [Realizacja: okres czasu zdefiniowany przez organizację].

Zabezpieczenia powiązane: AU-6, AU-11.

(9) MONITOROWANIE I SKANOWANIE PODATNOŚCI | TESTOWANIE PENETRACYJNE I ANALIZY

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(10) MONITOROWANIE I SKANOWANIE PODATNOŚCI | KORELACJA INFORMACJI ZE SKANOWANIA

Skoreluj dane wyjściowe z narzędzi skanowania podatności, aby określić obecność wektorów ataku wykorzystujących wiele podatności oraz wektorów ataku wieloetapowego.

Zabezpieczenia powiązane: nie dotyczy.

(11) MONITOROWANIE I SKANOWANIE PODATNOŚCI | PROGRAM UJAWNIANIA PUBLICZNEGO

Ustanów publiczny kanał raportowania do otrzymywania zgłoszeń o podatnościach w systemach organizacyjnych i komponentach systemu.

Zabezpieczenia powiązane: nie dotyczy.

RA-6 PRZEGLĄD ŚRODKÓW PRZECIWDZIAŁANIA INWIGILACJI TECHNICZNEJ

Zabezpieczenie:

Zastosuj przegląd środków przeciwdziałania inwigilacji technicznej w [Realizacja: lokalizacje zdefiniowane przez organizację] [Wybór (jeden lub więcej): [Realizacja: częstotliwość określona przez organizację], gdy wystąpią następujące zdarzenia lub wskaźniki: [Realizacja: zdarzenia lub wskaźniki zdefiniowane przez organizację]].

Zabezpieczenia powiązane: nie dotyczy.

Zabezpieczenia rozszerzone: nie dotyczy.

RA-7 ODPOWIEDŹ NA RYZYKO

Zabezpieczenie:

Reaguj na ustalenia z ocen bezpieczeństwa i prywatności, monitorowania i audytów zgodnie z tolerancją ryzyka organizacji.

Zabezpieczenia powiązane: CA-5, IR-9, PM-4, PM-28, RA-2, RA-3, SR-2.

Zabezpieczenia rozszerzone: nie dotyczy.

RA-8 OCENY WPŁYWU NA PRYWATNOŚĆ

Zabezpieczenie:

Przeprowadź ocenę wpływu na prywatność systemów, programów lub innych działań przed:

a. Rozwijaniem lub pozyskiwaniem technologii informacyjnej, która przetwarza dane osobowe;

b. Inicjowaniem nowego zbioru danych osobowych, który:

    1. Będzie przetwarzany przy użyciu technologii informacyjnej;

    2. Obejmuje dane osobowe umożliwiające fizyczny lub wirtualny (online) kontakt z konkretną osobą, jeśli identyczne pytania lub wymagania dotyczące raportowania zostały skierowane do co najmniej dziesięciu osób, z wyłączeniem instytucji rządowych lub pracowników administracji publicznej.

Zabezpieczenia powiązane: CM-4, CM-9, CM-13, PT-2, PT-3, PT-5, RA-1, RA-2, RA-3, RA-7.

Zabezpieczenia rozszerzone: nie dotyczy.

RA-9 ANALIZA KRYTYCZNOŚCI

Zabezpieczenie:

Zidentyfikuj krytyczne komponenty i funkcje systemu poprzez wykonanie analizy krytyczności dla [Realizacja: systemy, komponenty systemu lub usługi systemowe zdefiniowane przez organizację] w [Realizacja: punkty decyzyjne zdefiniowane przez organizację w cyklu życia rozwoju systemu].

Zabezpieczenia powiązane: CP-2, PL-2, PL-8, PL-11, PM-1, RA-2, SA-8, SA-15, SA-20, SR-5.

Zabezpieczenia rozszerzone: nie dotyczy.

RA-10 WYKRYWANIE ZAGROŻEŃ

Zabezpieczenie:

a. Ustanów i utrzymuj zdolność wykrywania zagrożeń cyberbezpieczeństwa w celu:

    1. Wyszukiwania wskaźników naruszenia bezpieczeństwa w systemach organizacji;

    2. Wykrywania, śledzenia i zakłócania zagrożeń, które wymykają się istniejącym mechanizmom kontroli;

b. Wykorzystuj zdolność wykrywania zagrożeń [Realizacja: częstotliwość określona przez organizację].

Zabezpieczenia powiązane: CA-2, CA-7, CA-8, RA-3, RA-5, RA-6, SI-4.

Zabezpieczenia rozszerzone: nie dotyczy.

KATEGORIA: SA – NABYWANIE SYSTEMU I USŁUG

SA-1 POLITYKA I PROCEDURY

Zabezpieczenie:

a. Opracuj, udokumentuj i rozpowszechnij do [*Realizacja:* personel lub role zdefiniowane przez organizację]:

    1. [Wybór (jeden lub więcej): poziom organizacji, poziom procesów misji/biznesu, poziom systemu] politykę nabywania systemów i usług, która:

        (a) Określa cel, zakres, role, obowiązki, zaangażowanie kierownictwa, koordynację między jednostkami organizacyjnymi oraz zgodność z przepisami.

        (b) Jest zgodna z obowiązującymi przepisami prawa, zarządzeniami wykonawczymi, dyrektywami, regulacjami, politykami, standardami i wytycznymi;

    2. Procedury ułatwiające wdrożenie polityki nabywania systemów i usług oraz powiązanych mechanizmów kontrolnych nabywania systemów i usług;

b. Wyznacz [*Realizacja:* urzędnika zdefiniowanego przez organizację] do zarządzania opracowywaniem, dokumentacją i rozpowszechnianiem polityki i procedur dotyczących nabywania systemów i usług;

c. Przeglądaj i aktualizuj bieżące regulacje nabywania systemów i usług:

    1. Politykę [Realizacja: częstotliwość określona przez organizację] i po [Zadanie: zdarzenia określone przez organizację];

    2. Procedury [Realizacja: częstotliwość określona przez organizację] i po [Zadanie: zdarzenia określone przez organizację].

Zabezpieczenia powiązane: PM-9, PS-8, SA-8, SI-12.

Zabezpieczenia rozszerzone: nie dotyczy.

SA-2 ALOKACJA ZASOBÓW

Zabezpieczenie:

a. Określ wysokopoziomowe wymagania bezpieczeństwa informacji i prywatności dla systemu lub usługi systemowej w planowaniu misji i procesów biznesowych;

b. Określ, udokumentuj i przydziel zasoby wymagane do ochrony systemu lub usługi systemowej jako część organizacyjnego procesu planowania i kontroli inwestycji;

c. Ustanów oddzielną pozycję dla bezpieczeństwa informacji i prywatności w dokumentacji programowej i budżetowej organizacji.

Zabezpieczenia powiązane: PL-7, PM-3, PM-11, SA-9, SR-3, SR-5.

Zabezpieczenia rozszerzone: nie dotyczy.

SA-3 CYKL ŻYCIA SYSTEMU

Zabezpieczenie:

a. Pozyskuj, rozwijaj i zarządzaj systemem używając [Realizacja: cykl życia systemu zdefiniowany przez organizację], który uwzględnia aspekty bezpieczeństwa informacji i prywatności;

b. Zdefiniuj i udokumentuj role i obowiązki w zakresie bezpieczeństwa informacji i prywatności w całym cyklu życia systemu;

c. Zidentyfikuj osoby posiadające role i obowiązki w zakresie bezpieczeństwa informacji i prywatności;

d. Zintegruj organizacyjny proces zarządzania ryzykiem bezpieczeństwa informacji i prywatności w organizacji cyklem życia systemu.

Zabezpieczenia powiązane: AT-3, CM-2, CM-4, MA-6, PL-8, PM-7, PM-25, RA-3, RA-9, SA-4, SA-5, SA-8, SA-11, SA-15, SA-17, SA-22, SR-3, SR-4, SR- 5, SR-9

Zabezpieczenia rozszerzone:

(1) CYKL ŻYCIA SYSTEMU | ZARZĄDZANIE ŚRODOWISKIEM PRZEDPRODUKCYJNYM

Chroń środowiska przedprodukcyjne systemu współmiernie do ryzyka w całym cyklu życia systemu, komponentu systemu lub usługi systemowej.

Zabezpieczenia powiązane: CM-2, CM-4, RA-3, RA-9, SA-4.

Zabezpieczenia rozszerzone: nie dotyczy

(2) CYKL ŻYCIA SYSTEMU | WYKORZYSTANIE DANYCH PRODUKCYJNYCH BIEŻĄCYCH LUB OPERACYJNYCH

a. Zatwierdź, udokumentuj i kontroluj wykorzystanie danych produkcyjnych w środowiskach przedprodukcyjnych dla systemu, komponentu systemu lub usługi systemowej;

b. Chroń środowiska przedprodukcyjne dla systemu, komponentu systemu lub usługi systemowej na tym samym poziomie wpływu lub klasyfikacji co jakiekolwiek dane produkcyjne używane w środowiskach przedprodukcyjnych.

Zabezpieczenia powiązane: PM-25, RA-3.

Zabezpieczenia rozszerzone: nie dotyczy.

(3) CYKL ŻYCIA SYSTEMU | ODŚWIEŻANIE TECHNOLOGII

Zaplanuj i wdrażaj harmonogram odświeżania technologii dla systemu w całym cyklu życia systemu.

Zabezpieczenia powiązane: MA-6.

Zabezpieczenia rozszerzone: nie dotyczy.

SA-4 PROCES NABYWANIA

Zabezpieczenie:

Uwzględnij następujące wymagania, opisy i kryteria, bezpośrednio lub przez odniesienie, używając [Wybór (jeden lub więcej): ustandaryzowanego języka umów, [Realizacja: język umów zdefiniowany przez organizację]] w umowie pozyskania dla systemu, komponentu systemu lub usługi systemowej:

a. Wymagania dotyczące funkcji bezpieczeństwa i prywatności;

b. Wymagania dotyczące siły mechanizmów zabezpieczeń;

c. Wymagania dotyczące zapewnienia bezpieczeństwa i prywatności;

d. Kontrole niezbędne do spełnienia wymagań bezpieczeństwa i prywatności;

e. Wymagania dotyczące dokumentacji bezpieczeństwa i prywatności;

f. Wymagania dotyczące ochrony dokumentacji związanej z bezpieczeństwem i prywatnością;

g. Opis środowiska tworzenia systemu oraz środowiska, w którym system ma działać;

h. Podział odpowiedzialności lub wskazanie stron odpowiedzialnych za bezpieczeństwo informacji, ochronę prywatności oraz zarządzanie ryzykiem łańcucha dostaw;

i. Kryteria akceptacji.

Zabezpieczenia powiązane: CM-6, CM-8, PS-7, SA-3, SA-5, SA-8, SA-11, SA-15, SA-16, SA-17, SA-21, SR-3, SR-5.

Zabezpieczenia rozszerzone:

(1) PROCES NABYWANIA | WŁAŚCIWOŚCI FUNKCJONALNE MECHANIZMÓW KONTROLNYCH

Wymagaj od developera systemu, komponentu systemu lub usługi systemowej dostarczenia opisu funkcjonalnych właściwości mechanizmów kontrolnych, które mają zostać zaimplementowane.

Zabezpieczenia powiązane: nie dotyczy.

(2) PROCES NABYWANIA | PROJEKTOWANIE I IMPLEMENTACJA MECHANIZMÓW KONTROLNYCH

Wymagaj od twórcy systemu, komponentu systemu lub usługi systemowej dostarczenia informacji o projekcie i implementacji mechanizmów kontrolnych, które obejmują: [Wybór (jeden lub więcej): zewnętrzne interfejsy systemu istotne dla bezpieczeństwa, projekt wysokopoziomowy, konstrukcja niskopoziomowa, kod źródłowy lub schematy sprzętowe, [Realizacja: informacje o projekcie i implementacji zdefiniowane przez organizację]] na [Realizacja: poziom szczegółowości zdefiniowany przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(3) PROCES NABYWANIA | METODY ROZWOJU, TECHNIKI I PRAKTYKI

Wymagaj od twórcy systemu, komponentu systemu lub usługi systemowej zademonstrowania wykorzystania procesu cyklu życia rozwoju systemu, który obejmuje:

a. [Realizacja: metody inżynierii systemów zdefiniowane przez organizację];

b. [Wybór (jeden lub więcej): metody inżynierii bezpieczeństwa systemów, inżynierii prywatności] zdefiniowane przez organizację;

c. [Realizacja: metody rozwoju oprogramowania, metody testowania, ewaluacji, oceny, weryfikacji i walidacji oraz procesy kontroli jakości zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(4) PROCES NABYWANIA | PRZYPISANIE KOMPONENTÓW DO SYSTEMÓW

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(5) PROCES NABYWANIA | KONFIGURACJA SYSTEMU, KOMPONENTU I USŁUGI

Wymagaj od twórcy systemu, komponentu systemu lub usługi systemowej, aby:

a. Dostarczył system, komponent lub usługę z wdrożonymi [Realizacja: konfiguracje bezpieczeństwa zdefiniowane przez organizację];

b. Używał tych konfiguracji jako domyślnych przy każdej kolejnej reinstalacji lub aktualizacji systemu, komponentu lub usługi.

Zabezpieczenia powiązane: Nie dotyczy

(6) PROCES NABYWANIA | UŻYWANIE PRODUKTÓW ZAPEWNIAJĄCYCH BEZPIECZEŃSTWO INFORMACJI

a. Używaj wyłącznie dostępnych na rynku lub opracowanych przez administrację publiczną produktów informatycznych zapewniających bezpieczeństwo informacji lub wyposażonych w funkcje ochrony informacji, które tworzą rozwiązanie zatwierdzone przez instytucję odpowiedzialną za cyberbezpieczeństwo kraju, w celu ochrony informacji niejawnych, gdy sieci używane do ich transmisji mają niższy poziom klasyfikacji niż przesyłane informacje;

b. Upewnij się, że te produkty zostały ocenione i/lub zatwierdzone przez instytucję odpowiedzialną za cyberbezpieczeństwo kraju lub zgodnie z zatwierdzonymi przez nią procedurami.

Zabezpieczenia powiązane: SC-8, SC-12, SC-13.

(7) PROCES NABYWANIA | ZATWIERDZONE PROFILE OCHRONY

a. Korzystaj z komercyjnych produktów technologii teleinformatycznych, które zostały pomyślnie ocenione przez krajowy organ bezpieczeństwa zgodnie z obowiązującymi przepisami.;

b. Wymagaj, aby moduł kryptograficzny stosowany w systemie teleinformatycznym został zatwierdzony przez krajowy organ bezpieczeństwa zgodnie z obowiązującymi przepisami.

Zabezpieczenia powiązane: IA-7, SC-12, SC-13.

(8) PROCES NABYWANIA | PLAN CIĄGŁEGO MONITOROWANIA MECHANIZMÓW KONTROLNYCH

Wymagaj od twórcy systemu, komponentu systemu lub usługi systemowej opracowania planu ciągłego monitorowania skuteczności mechanizmów kontrolnych, który jest zgodny z programem ciągłego monitorowania organizacji.

Zabezpieczenia powiązane: CA-7.

(9) PROCES NABYWANIA | FUNKCJE, PORTY, PROTOKOŁY I USŁUGI W UŻYCIU

Wymagaj od twórcy systemu, komponentu systemu lub usługi systemowej zidentyfikowania funkcji, portów, protokołów i usług przeznaczonych do użytku organizacyjnego.

Zabezpieczenia powiązane: CM-7, SA-9.

(10) PROCES NABYWANIA | WYKORZYSTANIE ZATWIERDZONYCH PRODUKTÓW

Używaj wyłącznie produktów technologii informacyjnej posiadające certyfikaty interoperacyjności zgodne z krajowymi przepisami prawa do obsługi funkcji weryfikacji tożsamości osobistej (PIV) wdrożonej w systemach organizacyjnych.

Zabezpieczenia powiązane: IA-2, IA-8, PM-9.

(11) PROCES NABYWANIA | SYSTEM REJESTRÓW

W umowie zakupu dotyczącej obsługi systemu rejestrów w imieniu organizacji w celu realizacji jej misji lub funkcji uwzględnij [Realizacja: wymagania ustawy o ochronie prywatności określone przez organizację].

Zabezpieczenia powiązane: PT-6.

(12) PROCES NABYWANIA | WŁASNOŚĆ DANYCH

a. Uwzględnij w umowie zakupu wymagania organizacyjne dotyczące własności danych;

b. Wymagaj usunięcia wszystkich danych z systemu wykonawcy i zwrotu do organizacji w ciągu [Realizacja: ramy czasowe zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

SA-5 DOKUMENTACJA SYSTEMU

Zabezpieczenie:

a. Uzyskaj lub opracuj dokumentację administratora dla systemu, komponentu systemu lub usługi systemowej, która opisuje:

   1. Bezpieczną konfigurację, instalację i działanie systemu, komponentu lub usługi;

   2. Efektywne wykorzystanie i utrzymanie funkcji i mechanizmów bezpieczeństwa i prywatności;

   3. Znane podatności dotyczące konfiguracji i korzystania z funkcji administracyjnych lub uprzywilejowanych;

b. Uzyskaj lub opracuj dokumentację użytkownika dla systemu, komponentu systemu lub usługi systemowej, która opisuje:

   1. Dostępne dla użytkownika funkcje i mechanizmy bezpieczeństwa i prywatności oraz sposoby skutecznego korzystania z tych funkcji i mechanizmów;

   2. Metody interakcji użytkownika, które umożliwiają osobom korzystanie z systemu, komponentu lub usługi w bardziej bezpieczny sposób i ochronę prywatności indywidualnej;

   3. Metody interakcji użytkownika umożliwiające bezpieczniejsze korzystanie z systemu, komponentu lub usługi oraz ochronę prywatności użytkownika;

c. Dokumentuj próby uzyskania dokumentacji systemu, komponentu systemu lub usługi systemowej, gdy taka dokumentacja jest niedostępna lub nie istnieje, podejmij [Realizacja: działania zdefiniowane przez organizację] w odpowiedzi;

d. Rozpowszechnij dokumentację do [*Zadanie:* personel lub role zdefiniowane przez organizację].

Zabezpieczenia powiązane: CM-4, CM-6, CM-7, CM-8, PL-2, PL-4, PL-8, PS-2, SA-3, SA-4, SA-8, SA-9, SA- 10, SA-11, SA-15, SA-16, SA-17, SI-12, SR-3.

Zabezpieczenia rozszerzone:

(1) DOKUMENTACJA SYSTEMU | FUNKCJONALNE WŁAŚCIWOŚCI ŚRODKÓW BEZPIECZEŃSTWA

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(2) DOKUMENTACJA SYSTEMU | BEZPIECZEŃSTWO INTERFEJSÓW SYSTEMU ZEWNĘTRZNEGO

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(3) DOKUMENTACJA SYSTEMU | PROJEKTOWANIE WYSOKOPOZIOMOWE

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(4) DOKUMENTACJA SYSTEMU | PROJEKTOWANIE NISKOPOZIOMOWE

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(5) DOKUMENTACJA SYSTEMU | KOD ŹRÓDŁOWY

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

SA-6 OGRANICZENIA W UŻYCIU OPROGRAMOWANIA

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

SA-7 OPROGRAMOWANIE INSTALOWANE PRZEZ UŻYTKOWNIKA

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

SA-8 ZASADY INŻYNIERII BEZPIECZEŃSTWA I PRYWATNOŚCI

Zabezpieczenie:

Określaj następujące zasady inżynierii bezpieczeństwa systemów i prywatności w specyfikacji, projekcie oraz podczas rozwoju, implementacji i modyfikacji systemu i komponentów systemu: [Realizacja: zasady inżynierii bezpieczeństwa systemów i prywatności zdefiniowane przez organizację].

Zabezpieczenia powiązane: PL-8, PM-7, RA-2, RA-3, RA-9, SA-3, SA-4, SA-15, SA-17, SA-20, SC-2, SC-3, SC-32, SC-39, SR-2, SR-3, SR-4, SR-5.

Zabezpieczenia rozszerzone:

(1) ZASADY INŻYNIERII BEZPIECZEŃSTWA I PRYWATNOŚCI | PRZEJRZYSTOŚĆ INTERFEJSÓW/UKRYWANIE INFORMACJI

Wdrażaj zasady projektowania bezpieczeństwa polegające na przejrzystych i klarownych interfejsach (ukrywaniu informacji).

Zabezpieczenia powiązane: nie dotyczy.

(2) ZASADY INŻYNIERII BEZPIECZEŃSTWA I PRYWATNOŚCI | MINIMALNY WSPÓŁDZIELONY MECHANIZM

Wdrażaj zasady projektowania zabezpieczeń polegające na zastosowaniu minimalnego współdzielony mechanizm w [Realizacja: systemy zdefiniowane przez organizację lub komponenty systemu].

Zabezpieczenia powiązane: nie dotyczy.

(3) ZASADY INŻYNIERII BEZPIECZEŃSTWA I PRYWATNOŚCI | MODUŁOWOŚĆ I WARSTWOWOŚĆ

Wdrażaj zasady projektowania bezpieczeństwa polegające na modułowości i warstwowości w [Realizacja: systemy lub komponenty systemu zdefiniowane przez organizację].

Zabezpieczenia powiązane: SC-2, SC-3.

(4) ZASADY INŻYNIERII BEZPIECZEŃSTWA I PRYWATNOŚCI | CZĘŚCIOWO UPORZĄDKOWANE ZALEŻNOŚCI

Wdrażaj zasady projektowania bezpieczeństwa polegające na uwzględnieniu zasady zastosowaniu minimalnego współdzielonego mechanizmu w [Realizacja: systemy zdefiniowane przez organizację lub komponenty systemu].

Zabezpieczenia powiązane: nie dotyczy.

(5) ZASADY INŻYNIERII BEZPIECZEŃSTWA I PRYWATNOŚCI | EFEKTYWNIE KONTROLOWANY DOSTĘP

Wdrażaj zasady projektowania bezpieczeństwa polegające na efektywnie kontrolowanym dostępie w [Określonych przez organizację systemach lub komponentach systemów].

Zabezpieczenia powiązane: AC-25.

(6) ZASADY INŻYNIERII BEZPIECZEŃSTWA I PRYWATNOŚCI | MINIMALIZACJA WSPÓŁDZIELENIA

Wdrażaj zasady projektowania bezpieczeństwa polegające na minimalizacji współdzielenia w [Realizacja: systemy lub komponenty systemu zdefiniowane przez organizację].

Zabezpieczenia powiązane: SC-31.

(7) ZASADY INŻYNIERII BEZPIECZEŃSTWA I PRYWATNOŚCI | ZMNIEJSZONA ZŁOŻONOŚĆ

Wdrażaj zasady projektowania bezpieczeństwa polegające na zredukowaniu złożoności w [Realizacja: systemy zdefiniowane przez organizację lub komponenty systemu].

Zabezpieczenia powiązane: nie dotyczy.

(8) ZASADY INŻYNIERII BEZPIECZEŃSTWA I PRYWATNOŚCI | BEZPIECZNA ZDOLNOŚĆ DO STOPNIOWEGO ROZWOJU

Wdrażaj zasady projektowania zabezpieczeń polegające na bezpiecznej zdolności do stopniowego rozwoju w [Realizacja: systemy lub komponenty systemu zdefiniowane przez organizację].

Zabezpieczenia powiązane: CM-3.

(9) ZASADY INŻYNIERII BEZPIECZEŃSTWA I PRYWATNOŚCI | ZAUFANE KOMPONENTY

Wdrażaj zasady projektowania bezpieczeństwa polegające na zaufanych komponentach w [Realizacja: systemy lub komponenty systemu zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(10) ZASADY INŻYNIERII BEZPIECZEŃSTWA I PRYWATNOŚCI | HIERARCHICZNE ZAUFANIE

Wdrażaj zasady projektowania bezpieczeństwa polegające na hierarchicznym zaufaniu w [Realizacja: systemy lub komponenty systemu zdefiniowane przez organizację].

Zabezpieczenia powiązane: CM-3.

Zabezpieczenia rozszerzone: nie dotyczy.

(11) ZASADY INŻYNIERII BEZPIECZEŃSTWA I PRYWATNOŚCI | ODWROTNY PRÓG MODYFIKACJI

Wdrażaj zasady projektowania bezpieczeństwa polegające na odwrotnym progu modyfikacji w [Określonych przez organizację systemach lub komponentach systemów].

Zabezpieczenia powiązane: nie dotyczy.

(12) ZASADY INŻYNIERII BEZPIECZEŃSTWA I PRYWATNOŚCI | OCHRONA HIERARCHICZNA

Wdrażaj zasady projektowania bezpieczeństwa polegające na ochronie hierarchicznej w [Realizacja: systemy lub komponenty systemu zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(13) ZASADY INŻYNIERII BEZPIECZEŃSTWA I PRYWATNOŚCI | ZMINIMALIZOWANE ELEMENTY BEZPIECZEŃSTWA

Wdrażaj zasady projektowania bezpieczeństwa polegające na zminimalizowanych elementach bezpieczeństwa w [Realizacja: systemy lub komponenty systemu zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(14) ZASADY INŻYNIERII BEZPIECZEŃSTWA I PRYWATNOŚCI | NAJMNIEJSZE UPRAWNIENIA

Wdrażaj zasady projektowania bezpieczeństwa polegające na najmniejszych uprawnieniach w [Realizacja: systemy lub komponenty systemu zdefiniowane przez organizację].

Zabezpieczenia powiązane: AC-6, CM-7.

(15) ZASADY INŻYNIERII BEZPIECZEŃSTWA I PRYWATNOŚCI | UPRAWNIENIA WARUNKOWE

Wdrażaj zasady projektowania bezpieczeństwa polegające na uprawnieniach warunkowych w [Realizacja: systemy lub komponenty systemu zdefiniowane przez organizację].

Zabezpieczenia powiązane: AC-5.

(16) ZASADY INŻYNIERII BEZPIECZEŃSTWA I PRYWATNOŚCI | SAMODZIELNA WIARYGODNOŚĆ

Wdrażaj zasady projektowania bezpieczeństwa polegające na samodzielnej wiarygodności w [Określonych przez organizację systemach lub komponentach systemów].

Zabezpieczenia powiązane: nie dotyczy.

(17) ZASADY INŻYNIERII BEZPIECZEŃSTWA I PRYWATNOŚCI | BEZPIECZNA ROZPROSZONA KOMPOZYCJA

Wdrażaj zasady projektowania bezpieczeństwa polegające na bezpiecznej rozproszonej kompozycji w [Realizacja: systemy lub komponenty systemu zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(18) ZASADY INŻYNIERII BEZPIECZEŃSTWA I PRYWATNOŚCI | ZAUFANE KANAŁY KOMUNIKACYJNE

Wdrażaj zasady projektowania bezpieczeństwa polegające na zaufanych kanałach komunikacyjnych w [Realizacja: systemy lub komponenty systemu zdefiniowane przez organizację].

Zabezpieczenia powiązane: SC-8, S-12, SC-13.

(19) ZASADY INŻYNIERII BEZPIECZEŃSTWA I PRYWATNOŚCI | OCHRONA CIĄGŁA

Wdrażaj zasady projektowania bezpieczeństwa polegające na ochronie ciągłej w [Realizacja: systemy lub komponenty systemu zdefiniowane przez organizację].

Zabezpieczenia powiązane: AC-25.

(20) ZASADY INŻYNIERII BEZPIECZEŃSTWA I PRYWATNOŚCI | BEZPIECZNE ZARZĄDZANIE METADANYMI

Wdrażaj zasady projektowania bezpieczeństwa polegające na bezpiecznym zarządzaniu metadanymi w [Realizacja: systemy lub komponenty systemu zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(21) ZASADY INŻYNIERII BEZPIECZEŃSTWA I PRYWATNOŚCI | SAMOOCENA

Wdrażaj zasady projektowania bezpieczeństwa polegające na samoanalizie w [Realizacja: systemy lub komponenty systemu zdefiniowane przez organizację].

Zabezpieczenia powiązane: CA-7.

(22) ZASADY INŻYNIERII BEZPIECZEŃSTWA I PRYWATNOŚCI | ODPOWIEDZIALNOŚĆ I MOŻLIWOŚĆ ŚLEDZENIA

Wdrażaj zasady projektowania zabezpieczeń dotyczącej odpowiedzialności i identyfikowalności w [Realizacja: systemy zdefiniowane przez organizację lub komponenty systemu].

Zabezpieczenia powiązane: AC-6, AU-2, AU-3, AU-6, AU-9, AU-10, AU-12, IA-2, IR-4.

(23) ZASADY INŻYNIERII BEZPIECZEŃSTWA I PRYWATNOŚCI | BEZPIECZNE USTAWIENIA DOMYŚLNE

Wdrażaj zasady projektowania bezpieczeństwa polegające na bezpiecznych ustawieniach domyślnych w [Realizacja: systemy lub komponenty systemu zdefiniowane przez organizację].

Zabezpieczenia powiązane: CM-1, CM-6, SA-4.

(24) ZASADY INŻYNIERII BEZPIECZEŃSTWA I PRYWATNOŚCI | KOPIA BEZPIECZEŃSTWA I ODZYSKIWANIE DANYCH

Wdrażaj zasady projektowania bezpieczeństwa polegające na wykonaniu kopii bezpieczeństwa i odzyskiwaniu danych w [Określonych przez organizację systemach lub komponentach systemów].

Zabezpieczenia powiązane: CP-10, CP-12, SC-7, SC-8, SC-24, SI-13

(25) ZASADY INŻYNIERII BEZPIECZEŃSTWA I PRYWATNOŚCI | BEZPIECZEŃSTWO EKONOMICZNE

Wdrażaj zasady projektowania bezpieczeństwa polegające na bezpieczeństwie ekonomicznym w [*Realizacja:* systemy lub komponenty systemu zdefiniowane przez organizację].

Zabezpieczenia powiązane: RA-3.

(26) ZASADY INŻYNIERII BEZPIECZEŃSTWA I PRYWATNOŚCI | BEZPIECZEŃSTWO WYDAJNOŚCIOWE

Wdrażaj zasady projektowania bezpieczeństwa polegające na bezpieczeństwie wydajnościowym w [*Realizacja:* systemy lub komponenty systemu zdefiniowane przez organizację].

Zabezpieczenia powiązane: SC-12, SC-13, SI-2, SI-7.

(27) ZASADY INŻYNIERII BEZPIECZEŃSTWA I PRYWATNOŚCI | BEZPIECZEŃSTWO UWZGLĘDNIAJĄCE CZYNNIK LUDZKI

Wdrażaj zasady projektowania bezpieczeństwa polegające na bezpieczeństwie uwzględniającym czynnik ludzki w [Realizacja: systemy lub komponenty systemu zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy

(28) ZASADY INŻYNIERII BEZPIECZEŃSTWA I PRYWATNOŚCI | AKCEPTOWALNE BEZPIECZEŃSTWO

Wdrażaj zasady projektowania bezpieczeństwa polegające na akceptowalnym bezpieczeństwie w [Realizacja: systemy lub komponenty systemu zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(29) ZASADY INŻYNIERII BEZPIECZEŃSTWA I PRYWATNOŚCI | POWTARZALNE I UDOKUMENTOWANE PROCEDURY

Wdrażaj zasady projektowania bezpieczeństwa polegające na powtarzalnych i udokumentowanych procedurach w [Realizacja: systemy lub komponenty systemu zdefiniowane przez organizację].

Zabezpieczenia powiązane: CM-1, SA-1, SA-10, SA-11, SA-15, SA-17, SC-1, SI-1.

(30) ZASADY INŻYNIERII BEZPIECZEŃSTWA I PRYWATNOŚCI | RYGOR PROCEDURALNY

Wdrażaj zasady projektowania zabezpieczeń zgodnie z rygorami proceduralnymi [Realizacja: systemy lub komponenty systemu zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(31) ZASADY INŻYNIERII BEZPIECZEŃSTWA I PRYWATNOŚCI | BEZPIECZNA MODYFIKACJA SYSTEMU

Wdrażaj zasady projektowania bezpieczeństwa polegające na bezpiecznej modyfikacji systemu w [Realizacja: systemy lub komponenty systemu zdefiniowane przez organizację].

Zabezpieczenia powiązane: CM-3, CM-4.

(32) ZASADY INŻYNIERII BEZPIECZEŃSTWA I PRYWATNOŚCI | WYSTARCZAJĄCA DOKUMENTACJA

Wdrażaj zasady projektowania bezpieczeństwa polegające na wystarczającej dokumentacji w [*Realizacja:* systemy lub komponenty systemu zdefiniowane przez organizację].

Zabezpieczenia powiązane: AT-2, AT-3, SA-5.

(33) ZASADY INŻYNIERII BEZPIECZEŃSTWA I PRYWATNOŚCI | MINIMALIZACJA

Wdrażaj zasady prywatności polegające na minimalizacji przy użyciu [*Realizacja:* procesy zdefiniowane przez organizację].

Zabezpieczenia powiązane: PE-8, PM-25, SC-42, SI12.

SA-9 USŁUGI SYSTEMU ZEWNĘTRZNEGO

Zabezpieczenie:

a. Wymagaj, aby dostawcy usług systemów zewnętrznych przestrzegali organizacyjnych wymagań bezpieczeństwa i prywatności oraz stosowali następujące mechanizmy kontrolne: [Realizacja: mechanizmy kontrolne zdefiniowane przez organizację];

b. Zdefiniuj i udokumentuj nadzór organizacyjny oraz role i odpowiedzialności użytkowników w odniesieniu do usług systemów zewnętrznych;

c. Wykorzystuj następujące procesy, metody i techniki do ciągłego monitorowania zgodności kontrolnej przez zewnętrznych dostawców usług: [Realizacja: procesy, metody i techniki zdefiniowane przez organizację].

Zabezpieczenia powiązane: AC-20, CA-3, CP-2, IR-4, IR-7, PL-10, PL-11, PS-7, SA-2, SA-4, SR-3, SR-5.

Zabezpieczenia rozszerzone:

(1) USŁUGI SYSTEMU ZEWNĘTRZNEGO | OCENY RYZYKA I ZATWIERDZENIA ORGANIZACYJNE

a. Przeprowadź ocenę ryzyka organizacyjnego przed nabyciem lub zleceniem wykonania usług bezpieczeństwa informacji;

b. Weryfikuj, czy nabycie lub zlecenie wykonania dedykowanych usług bezpieczeństwa informacji jest zatwierdzone przez [Realizacja: personel lub role zdefiniowane przez organizację]

Zabezpieczenia powiązane: CA-6, RA-3, RA-8.

(2) USŁUGI SYSTEMU ZEWNĘTRZNEGO | IDENTYFIKACJA FUNKCJI, PORTÓW, PROTOKOŁÓW I USŁUG

Wymagaj od dostawców następujących usług systemów zewnętrznych identyfikacji funkcji, portów, protokołów i innych usług wymaganych do korzystania z tych usług: [Realizacja: usługi systemów zewnętrznych zdefiniowane przez organizację].

Zabezpieczenia powiązane: CM-6, CM-7.

(3) USŁUGI SYSTEMU ZEWNĘTRZNEGO | USTANOWIENIE I UTRZYMANIE RELACJI ZAUFANIA Z DOSTAWCAMI

Ustanawiaj, udokumentuj i utrzymuj relacje zaufania z zewnętrznymi dostawcami usług w oparciu o następujące wymagania, właściwości, czynniki lub warunki: [Realizacja: wymagania bezpieczeństwa i prywatności, właściwości, czynniki lub warunki zdefiniowane przez organizację określające akceptowalne relacje zaufania].

Zabezpieczenia powiązane: SR-2.

(4) USŁUGI SYSTEMU ZEWNĘTRZNEGO | ZGODNOŚĆ INTERESÓW KONSUMENTÓW I DOSTAWCÓW

Podejmuj następujące działania w celu weryfikacji, czy interesy [Realizacja: zewnętrzni dostawcy usług zdefiniowani przez organizację] są spójne i odzwierciedlają interesy organizacyjne: [Realizacja: działania zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(5) USŁUGI SYSTEMU ZEWNĘTRZNEGO | OBSZAR PROCESOWANIA, PRZECHOWYWANIA I OBSŁUGI TECHNICZNEJ

Ogranicz lokalizację [Wybór (jeden lub więcej): przetwarzania informacji, informacji lub danych, usług systemowych] do [Realizacja: lokalizacje zdefiniowane przez organizację] w oparciu o [Realizacja: wymagania lub warunki zdefiniowane przez organizację].

Zabezpieczenia powiązane: SA-5, SR-4.

(6) USŁUGI SYSTEMU ZEWNĘTRZNEGO | KLUCZE KRYPTOGRAFICZNE KONTROLOWANE PRZEZ ORGANIZACJĘ

Utrzymuj wyłączną kontrolę nad kluczami kryptograficznymi dla zaszyfrowanych materiałów przechowywanych lub przesyłanych przez system zewnętrzny.

Zabezpieczenia powiązane: SC-12, SC-13, SI-4.

(7) USŁUGI SYSTEMU ZEWNĘTRZNEGO | KONTROLA INTEGRALNOŚCI KONTROLOWANA PRZEZ ORGANIZACJĘ

Zapewnij możliwość sprawdzania integralności informacji podczas ich przechowywania w systemie zewnętrznym.

Zabezpieczenia powiązane: SI-7.

(8) USŁUGI SYSTEMU ZEWNĘTRZNEGO | LOKALIZACJA PRZETWARZANIA I PRZECHOWYWANIA

Ogranicz geograficznie lokalizację przetwarzania informacji i przechowywania danych do obiektów znajdujących się w granicach EOG.

Zabezpieczenia powiązane: SA-5, SR-4.

SA-10 ZARZĄDZANIE KONFIGURACJĄ OPROGRAMOWANIA

Zabezpieczenie:

Wymagaj od twórcy systemu, komponentu systemu lub usługi systemowej:

a. Wykonywania zarządzania konfiguracją podczas [Wybór (jeden lub więcej): projektowania, rozwoju, wdrażania, działania, wycofywania] systemu, komponentu lub usługi;

b. Dokumentowania, zarządzania i kontrolowania integralności zmian w [Realizacja: elementy konfiguracji zdefiniowane przez organizację podlegające zarządzaniu konfiguracją];

c. Wdrażania wyłącznie zmian zatwierdzonych przez organizację w systemie, komponencie lub usłudze;

d. Dokumentowania zatwierdzonych zmian w systemie, komponencie lub usłudze oraz potencjalnych wpływów takich zmian na bezpieczeństwo i prywatność;

e. Śledzenia luk w zabezpieczeniach i ich rozwiązywania w systemie, komponencie lub usłudze oraz raportowania ustaleń do [Realizacja: personel zdefiniowany przez organizację].

Zabezpieczenia powiązane: CM-2, CM-3, CM-4, CM-7, CM-9, SA-4, SA-5, SA-8, SA-15, SI-2, SI-7, SR-3, SR-4, SR-5, SR-6, SR-11

Zabezpieczenia rozszerzone:

(1) ZARZĄDZANIE KONFIGURACJĄ OPROGRAMOWANIA | WERYFIKACJA INTEGRALNOŚCI OPROGRAMOWANIA I FIRMWARE

Wymagaj od dewelopera systemu, komponentu systemu lub usługi systemowej umożliwienia weryfikacji integralności komponentów oprogramowania i oprogramowania układowego.

Zabezpieczenia powiązane: SI-7, SR-11.

(2) ZARZĄDZANIE KONFIGURACJĄ OPROGRAMOWANIA | ALTERNATYWNE PROCESY ZARZĄDZANIA KONFIGURACJĄ

Zapewnij alternatywny proces zarządzania konfiguracją przy użyciu personelu organizacji w przypadku braku dedykowanego zespołu ds. zarządzania konfigurację.

Zabezpieczenia powiązane: nie dotyczy.

(3) ZARZĄDZANIE KONFIGURACJĄ OPROGRAMOWANIA | WERYFIKACJA INTEGRALNOŚCI SPRZĘTU

Wymagaj od twórcy systemu, komponentu systemu lub usługi systemowej umożliwienia weryfikacji integralności komponentów sprzętowych.

Zabezpieczenia powiązane: SI-7.

(4) ZARZĄDZANIE KONFIGURACJĄ OPROGRAMOWANIA | ZAUFANA GENERACJA

Wymagaj od twórcy systemu, komponentu systemu lub usługi systemowej wykorzystania narzędzi do porównywania nowo generowanych wersji opisów sprzętu związanych z bezpieczeństwem, kodu źródłowego i kodu wynikowego z poprzednimi wersjami.

Zabezpieczenia powiązane: nie dotyczy.

(5) ZARZĄDZANIE KONFIGURACJĄ OPROGRAMOWANIA | INTEGRALNOŚĆ MAPOWANIA KONTROLI WERSJI

Wymaganie od twórcy systemu, komponentu systemu lub usługi systemowej utrzymania integralności mapowania między danymi kompilacji głównej opisującymi aktualną wersję sprzętu, oprogramowania i oprogramowania układowego związanego z bezpieczeństwem oraz zaktualizowaną kopią głównej wersji danych.

Zabezpieczenia powiązane: nie dotyczy.

(6) ZARZĄDZANIE KONFIGURACJĄ OPROGRAMOWANIA | ZAUFANA DYSTRYBUCJA

Wymagaj od dewelopera systemu, komponentu systemu lub usługi systemowej realizacji procedur zapewniających, że aktualizacje sprzętu, oprogramowania i firmware'u istotne dla bezpieczeństwa, dystrybuowane do organizacji, są zgodne z oryginalnymi kopiami wzorcowymi (Master copies).

Zabezpieczenia powiązane: nie dotyczy.

(7) ZARZĄDZANIE KONFIGURACJĄ OPROGRAMOWANIA | PRZEDSTAWICIELE DS. BEZPIECZEŃSTWA I PRYWATNOŚCI

Wymagaj włączenia [Realizacja: przedstawiciele ds. bezpieczeństwa i prywatności zdefiniowani przez organizację] do [Realizacja: proces zarządzania i kontroli zmian konfiguracji zdefiniowany przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

SA-11 TESTOWANIE I OCENA OPROGRAMOWANIA

Zabezpieczenie:

Wymagaj od twórcy systemu, komponentu systemu lub usługi systemowej, na wszystkich etapach po projektowych cyklu życia systemu:

a. Opracowania i wdrożenia planu bieżących ocen bezpieczeństwa i prywatności;

b. Wykonywania testów/oceny [Wybór (jeden lub więcej): jednostkowych, integracyjnych, systemowych, regresyjnych] z [Realizacja: częstotliwość określona przez organizację] na [Realizacja: głębokość i zakres zdefiniowane przez organizację];

c. Dostarczenia dowodów wykonania planu oceny oraz wyników testów i oceny;

d. Wdrożenia weryfikowalnego procesu usuwania usterek;

e. Poprawiania usterek zidentyfikowanych podczas testowania i oceny.

Zabezpieczenia powiązane: CA-2, CA-7, CM-4, SA-3, SA-4, SA-5, SA-8, SA-15, SA-17, SI-2, SR-5, SR-6, SR-7.

Zabezpieczenia rozszerzone:

(1) TESTOWANIE I OCENA OPROGRAMOWANIA | ANALIZA KODU STATYCZNEGO

Wymagaj od twórcy systemu, komponentu systemu lub usługi systemowej wykorzystania narzędzi do analizy statycznej kodu w celu identyfikacji typowych usterek i udokumentowania wyników analizy.

Zabezpieczenia powiązane: nie dotyczy.

(2) TESTOWANIE I OCENA OPROGRAMOWANIA | MODELOWANIE ZAGROŻEŃ I ANALIZY PODATNOŚCI

Wymagaj od twórcy systemu, komponentu systemu lub usługi systemowej wykonania modelowania zagrożeń i analiz podatności podczas rozwoju oraz późniejszego testowania i oceny systemu, komponentu lub usługi, które:

a. Wykorzystują następujące informacje kontekstowe: [Realizacja: informacje zdefiniowane przez organizację dotyczące wpływu, środowiska działania, znanych lub zakładanych zagrożeń oraz akceptowalnych poziomów ryzyka];

b. Stosują następujące narzędzia i metody: [Realizacja: narzędzia i metody zdefiniowane przez organizację];

c. Przeprowadzają modelowanie i analizy na następującym poziomie rygoru: [Realizacja: zakres i głębokość modelowania i analiz zdefiniowane przez organizację];

d. Dostarczają dowody spełniające następujące kryteria akceptacji: [Realizacja: kryteria akceptacji zdefiniowane przez organizację].

Zabezpieczenia powiązane: PM-15, RA-3, RA-5.

(3) TESTOWANIE I OCENA OPROGRAMOWANIA | NIEZALEŻNA WERYFIKACJA PLANÓW OCENY I EWIDENCJI

a. Wymagaj od niezależnego podmiotu spełniającego [Realizacja: kryteria niezależności zdefiniowane przez organizację] weryfikacji prawidłowego wdrożenia planów oceny bezpieczeństwa i prywatności przez dewelopera oraz dowodów wytworzonych podczas testowania i oceny;

b. Weryfikuj czy niezależny podmiot otrzymuje wystarczające informacje do przeprowadzenia procesu weryfikacji lub ma przyznane uprawnienia do uzyskania takich informacji.

Zabezpieczenia powiązane: AT-3, RA-5.

(4) TESTOWANIE I OCENA OPROGRAMOWANIA | MANUALNY PRZEGLĄD KODU

Wymagaj od twórcy systemu, komponentu systemu lub usługi systemowej wykonania ręcznego przeglądu kodu [*Realizacja:* określony kod zdefiniowany przez organizację] przy użyciu następujących procesów, procedur i/lub technik: [*Realizacja:* procesy, procedury i/lub techniki zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(5) TESTOWANIE I OCENA OPROGRAMOWANIA | TESTY PENETRACYJNE

Wymagaj od twórcy systemu, komponentu systemu lub usługi systemowej przeprowadzenia testów penetracyjnych:

a. Na następującym poziomie rygoru: [Realizacja: zakres i głębokość testowania zdefiniowane przez organizację];

b. Przy następujących ograniczeniach: [Realizacja: ograniczenia zdefiniowane przez organizację].

Zabezpieczenia powiązane: CA-8, PM-14, PM-25, PT-2, SA-3, SI-2, SI-6.

(6) TESTOWANIE I OCENA OPROGRAMOWANIA | PRZEGLĄD PŁASZCZYZNY ATAKU

Wymagaj od twórcy systemu, komponentu systemu lub usługi systemowej wykonania przeglądów płaszczyzny ataku.

Zabezpieczenia powiązane: SA-15.

(7) TESTOWANIE I OCENA OPROGRAMOWANIA | WERYFIKACJA ZAKRESU TESTÓW I OCENY

Wymagaj od twórcy systemu, komponentu systemu lub usługi systemowej weryfikacji, że zakres testów i oceny zapewnia pełne pokrycie wymaganych mechanizmów kontrolnych na następującym poziomie rygoru: [Realizacja: zakres i głębokość testów i oceny zdefiniowane przez organizację].

Zabezpieczenia powiązane: SA-15

(8) TESTOWANIE I OCENA OPROGRAMOWANIA | ANALIZA DYNAMICZNA KODU

Wymagaj od dewelopera systemu, komponentu systemu lub usługi systemowej wykorzystania narzędzi do analizy dynamicznej kodu w celu identyfikacji typowych usterek i udokumentowania wyników analizy.

Zabezpieczenia powiązane: nie dotyczy.

(9) TESTOWANIE I OCENA OPROGRAMOWANIA | INTERAKTYWNE TESTOWANIE BEZPIECZEŃSTWA APLIKACJI

Wymagaj od dewelopera systemu, komponentu systemu lub usługi systemowej wykorzystania narzędzi do interaktywnego testowania bezpieczeństwa aplikacji w celu identyfikacji usterek i udokumentowania wyników.

Zabezpieczenia powiązane: nie dotyczy.

SA-12 BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

Zabezpieczenia rozszerzone:

(1) BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW | STRATEGIE / NARZĘDZIA / METODY POZYSKIWANIA

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(2) BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW | PRZEGLĄDY DOSTAWCÓW

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(3) BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW | ZAUFANA WYSYŁKA I MAGAZYNOWANIE

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(4) BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW | RÓŻNORODNOŚĆ DOSTAWCÓW

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(5) BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW | OGRANICZENIE SZKÓD

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(6) BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW | MINIMALIZACJA CZASU

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(7) BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW | OCENY PRZED WYBOREM / AKCEPTACJĄ / AKTUALIZACJĄ

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(8) BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW | WYKORZYSTANIE INFORMACJI ZE WSZYSTKICH ŹRÓDEŁ

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(9) OCHRONA ŁAŃCUCHA DOSTAW | BEZPIECZEŃSTWO OPERACJI

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(10) BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW | WALIDACJA AUTENTYCZNOŚCI I NIEZMIENNOŚCI

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(11) BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW | TESTY PENETRACYJNE / ANALIZA ELEMENTÓW, PROCESÓW I PODMIOTÓW

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(12) BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW | POROZUMIENIA MIĘDZYORGANIZACYJNE

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(13) BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW | KRYTYCZNE KOMPONENTY SYSTEMU INFORMACYJNEGO

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(14) BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW | TOŻSAMOŚĆ I IDENTYFIKOWALNOŚĆ

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(15) BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW | PROCESY DOTYCZĄCE SŁABOŚCI LUB NIEDOCIĄGNIĘĆ

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

SA-13 WIARYGODNOŚĆ

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

SA-14 ANALIZA KRYTYCZNOŚCI

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

Zabezpieczenia rozszerzone:

(1) ANALIZA KRYTYCZNOŚCI | KOMPONENTY KRYTYCZNE BEZ ALTERNATYWNYCH ŹRÓDEŁ POZYSKANIA

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

SA-15 PROCES ROZWOJU, STANDARDY I NARZĘDZIA

Zabezpieczenie:

a. Wymagaj od twórcy systemu, komponentu systemu lub usługi systemowej przestrzegania udokumentowanego procesu rozwoju, który:

    1. Jednoznacznie odnosi się do wymagań bezpieczeństwa i prywatności;

    2. Określa standardy i narzędzia używane w procesie rozwoju;

    3. Dokumentuje konkretne opcje narzędzi i konfiguracje narzędzi używane w procesie rozwoju;

    4. Dokumentuje, zarządza i zapewnia integralność zmian w procesie i/lub narzędziach używanych w rozwoju;

b. Przeglądaj proces rozwoju, standardów, narzędzi, opcji i konfiguracji narzędzi [Realizacja: częstotliwość określona przez organizację] w celu określenia, czy wybrany i zastosowany proces, standardy, narzędzia, opcje narzędzi i konfiguracje mogą spełnić następujące wymagania bezpieczeństwa i prywatności: [Realizacja: wymagania bezpieczeństwa i prywatności zdefiniowane przez organizację].

Zabezpieczenia powiązane: MA-6, SA-3, SA-4, SA-8, SA-10, SA-11, SR-3, SR-4, SR-5, SR-6, SR-9

Zabezpieczenia rozszerzone:

(1) PROCESY ROZWOJU, STANDARDY I NARZĘDZIA | METRYKI JAKOŚCI

Wymagaj od twórca systemu, komponentu systemu lub usługi systemowej:

a. Zdefiniowania metryk jakości na początku procesu rozwoju;

b. Dostarczaj dowody spełnienia metryk jakości [Wybór (jeden lub więcej): [Realizacja: częstotliwość określona przez organizację], [Realizacja: kamienie milowe przeglądu programu zdefiniowane przez organizację], przy dostawie]

Zabezpieczenia powiązane: nie dotyczy.

(2) PROCESY ROZWOJU, STANDARDY I NARZĘDZIA | NARZĘDZIA ŚLEDZENIA BEZPIECZEŃSTWA I PRYWATNOŚCI

Wymagaj od dewelopera systemu, komponentu systemu lub usługi systemowej wyboru i wykorzystania narzędzi śledzenia bezpieczeństwa i prywatności podczas procesu rozwoju.

Zabezpieczenia powiązane: SA-11.

(3) PROCESY ROZWOJU, STANDARDY I NARZĘDZIA | ANALIZA KRYTYCZNOŚCI

Wymagaj od dewelopera systemu, komponentu systemu lub usługi systemowej przeprowadzenia analizy krytyczności:

a. W następujących punktach decyzyjnych cyklu życia systemu: [Realizacja: punkty decyzyjne w cyklu życia systemu zdefiniowane przez organizację];

b. Na następującym poziomie rygoru: [Realizacja: zakres i głębokość analizy krytyczności zdefiniowane przez organizację].

Zabezpieczenia powiązane: RA-9.

(4) PROCESY ROZWOJU, STANDARDY I NARZĘDZIA | MODELOWANIE ZAGROŻEŃ I ANALIZA PODATNOŚCI

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(5) PROCESY ROZWOJU, STANDARDY I NARZĘDZIA | OGRANICZENIE PŁASZCZYZNY ATAKU

Wymagaj od dewelopera systemu, komponentu systemu lub usługi systemowej zredukowania płaszczyzny ataku do [*Realizacja:* progi zdefiniowane przez organizację].

Zabezpieczenia powiązane: AC-6, CM-7, RA-3, SA-11.

(6) PROCESY ROZWOJU, STANDARDY I NARZĘDZIA | CIĄGŁE DOSKONALENIE

Wymagaj od dewelopera systemu, komponentu systemu lub usługi systemowej wdrożenia jawnego procesu ciągłego doskonalenia procesu rozwoju.

Zabezpieczenia powiązane: nie dotyczy.

(7) PROCESY ROZWOJU, STANDARDY I NARZĘDZIA | ATOMATYCZNA ANALIZA PODATNOŚCI

Wymagaj od dewelopera systemu, komponentu systemu lub usługi systemowej [Realizacja: częstotliwość określona przez organizację]:

a. Wykonaj zautomatyzowaną analizę podatności przy użyciu [Realizacja: narzędzia zdefiniowane przez organizację];

b. Określ potencjał wykorzystania wykrytych podatności;

c. Określ potencjalne metody ograniczenia ryzyka dla dostarczonych podatności;

d. Dostarcz wyniki działania narzędzi i rezultatów analizy do [Realizacja: personel lub role zdefiniowane przez organizację].

Zabezpieczenia powiązane: RA-5, SA-11.

(8) PROCESY ROZWOJU, STANDARDY I NARZĘDZIA | PONOWNE UŻYCIE INFORMACJI O ZAGROŻENIACH I PODATNOŚCIACH

Wymagaj od dewelopera systemu, komponentu systemu lub usługi systemowej wykorzystania modelowania zagrożeń i analiz podatności z podobnych systemów, komponentów lub usług w celu usprawnienia bieżącego procesu rozwoju.

Zabezpieczenia powiązane: nie dotyczy.

(9) PROCESY ROZWOJU, STANDARDY I NARZĘDZIA | KREATYWNE WYKORZYSTANIE DANYCH

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(10) PROCESY ROZWOJU, STANDARDY I NARZĘDZIA | PLAN REAGOWANIA NA INCYDENTY

Wymagaj od dewelopera systemu, komponentu systemu lub usługi systemowej dostarczenia, wdrożenia i przetestowania planu reagowania na incydenty.

Zabezpieczenia powiązane: nie dotyczy.

(11) PROCESY ROZWOJU, STANDARDY I NARZĘDZIA | ARCHIWIZACJA SYSTEMU LUB KOMPONENTU

Wymagaj od dewelopera systemu lub komponentu systemu archiwizacji systemu lub komponentu przeznaczonego do wydania lub dostarczenia wraz z odpowiednimi dowodami wspierającymi końcowy przegląd bezpieczeństwa i prywatności.

Zabezpieczenia powiązane: nie dotyczy.

(12) PROCESY ROZWOJU, STANDARDY I NARZĘDZIA | MINIMALIZACJA DANYCH OSOBOWYCH

Wymagaj od dewelopera systemu lub komponentu systemu minimalizacji wykorzystania danych osobowych w środowiskach rozwojowych i testowych.

Zabezpieczenia powiązane: PM-25, SA-3, SA-8

SA-16 SZKOLENIA DOSTARCZANE PRZEZ DEWELOPERA

Zabezpieczenie:

Wymagaj od dewelopera systemu, komponentu systemu lub usługi systemowej zapewnienia następujących szkoleń w zakresie prawidłowego użytkowania i działania wdrożonych funkcji, mechanizmów kontrolnych i/lub mechanizmów bezpieczeństwa i prywatności: [Realizacja: szkolenia zdefiniowane przez organizację].

Zabezpieczenia powiązane: AT-2, AT-3, PE-3, SA-4, SA-5.

Zabezpieczenia rozszerzone: nie dotyczy.

SA-17 ARCHITEKTURA I PROJEKT BEZPIECZEŃSTWA I PRYWATNOŚCI OPROGRAMOWANIA

Zabezpieczenie:

Wymagaj od twórcy systemu, komponentu systemu lub usługi systemowej opracowania specyfikacji projektowej oraz architektury bezpieczeństwa i prywatności, która:

a. Jest zgodna z architekturą bezpieczeństwa i prywatności organizacji, która jest integralną częścią architektury korporacyjnej organizacji;

b. Dokładnie i kompletnie opisuje wymaganą funkcjonalność bezpieczeństwa i prywatność oraz alokację mechanizmów kontrolnych między komponenty fizyczne i logiczne;

c. Wyraża, jak poszczególne funkcje, mechanizmy i usługi bezpieczeństwa i prywatności współpracują ze sobą, aby zapewnić wymagane możliwości bezpieczeństwa i prywatności oraz jednolite podejście do ochrony.

Zabezpieczenia powiązane: PL-2, PL-8, PM-7, SA-3, SA-4, SA-8, SC-7.

Zabezpieczenia rozszerzone:

(1) ARCHITEKTURA I PROJEKTY BEZPIECZEŃSTWA I PRYWATNOŚCI OPROGRAMOWANIA | FORMALNY MODEL POLITYKI

Wymagaj od twórcy systemu, komponentu systemu lub usługi systemowej:

a. Stworzenia, jako integralnej części procesu rozwoju, formalnego modelu polityki opisującego [Realizacja: elementy organizacyjnej polityki bezpieczeństwa i prywatności zdefiniowane przez organizację], który ma być egzekwowany;

b. Udowodnienia, że formalny model polityki jest wewnętrznie spójny i wystarczający do egzekwowania zdefiniowanych elementów organizacyjnej polityki bezpieczeństwa i prywatności po wdrożeniu.

Zabezpieczenia powiązane: AC-3, AC-4, AC-25.

(2) ARCHITEKTURA I PROJEKTY BEZPIECZEŃSTWA I PRYWATNOŚCI OPROGRAMOWANIA | KOMPONENTY ISTOTNE DLA BEZPIECZEŃSTWA

Wymagaj od twórcy systemu, komponentu systemu lub usługi systemowej:

a. Zdefiniowania sprzętu, oprogramowania i oprogramowania sprzętowego istotnego dla bezpieczeństwa;

b. Dostarczenia uzasadnienia, że definicja sprzętu, oprogramowania i oprogramowania sprzętowego istotnego dla bezpieczeństwa jest kompletna.

Zabezpieczenia powiązane: AC-25, SA-5.

(3) ARCHITEKTURA I PROJEKTY BEZPIECZEŃSTWA I PRYWATNOŚCI OPROGRAMOWANIA | FORMALNA ZGODNOŚĆ

Wymagaj od twórcy systemu, komponentu systemu lub usługi systemowej:

a. Opracowania, jako integralne części procesu rozwoju, formalnej specyfikacji wysokiego poziomu, która określa interfejsy do sprzętu, oprogramowania i oprogramowania sprzętowego istotnego dla bezpieczeństwa w zakresie wyjątków, komunikatów o błędach i efektów;

b. Wykazania poprzez dowód, w zakresie wykonalnym z dodatkową nieformalną demonstracją w razie potrzeby, że formalna specyfikacja wysokiego poziomu jest zgodna z formalnym modelem polityki;

c. Wykazania poprzez nieformalną demonstrację, że formalna specyfikacja wysokiego poziomu całkowicie obejmuje interfejsy do sprzętu, oprogramowania i oprogramowania sprzętowego istotnego dla bezpieczeństwa;

d. Wykazania, że formalna specyfikacja wysokiego poziomu jest dokładnym opisem wdrożonego sprzętu, oprogramowania i oprogramowania sprzętowego istotnego dla bezpieczeństwa;

e. Opisania mechanizmów sprzętu, oprogramowania i oprogramowania sprzętowego istotnych dla bezpieczeństwa, które nie są ujęte w formalnej specyfikacji wysokiego poziomu, ale są ściśle wewnętrzne dla sprzętu, oprogramowania i oprogramowania sprzętowego istotnego dla bezpieczeństwa.

Zabezpieczenia powiązane: AC-3, AC-4, AC-25, SA-4, SA-5.

(4) ARCHITEKTURA I PROJEKTY BEZPIECZEŃSTWA I PRYWATNOŚCI OPROGRAMOWANIA | NIEFORMALNA ZGODNOŚĆ

Wymagaj od twórcy systemu, komponentu systemu lub usługi systemowej:

a. Opracowania, jako integralne części procesu rozwoju, nieformalnej opisowej specyfikacji najwyższego poziomu, która określa interfejsy do sprzętu, oprogramowania i oprogramowania sprzętowego istotnego dla bezpieczeństwa w zakresie wyjątków, komunikatów o błędach i efektów;

b. Wykazania poprzez [Zadanie: nieformalną demonstrację, przekonującą argumentację z metodami formalnymi w miarę możliwości], że opisowa specyfikacja najwyższego poziomu jest zgodna z formalnym modelem polityki;

c. Wykazania poprzez nieformalną demonstrację, że opisowa specyfikacja najwyższego poziomu całkowicie obejmuje interfejsy do sprzętu, oprogramowania i oprogramowania sprzętowego istotnego dla bezpieczeństwa;

d. Wykazania, że opisowa specyfikacja najwyższego poziomu jest dokładnym opisem interfejsów do sprzętu, oprogramowania i oprogramowania sprzętowego istotnego dla bezpieczeństwa;

e. Opisania mechanizmów sprzętu, oprogramowania i oprogramowania sprzętowego istotnych dla bezpieczeństwa, które nie są ujęte w opisowej specyfikacji najwyższego poziomu, ale są ściśle wewnętrzne dla sprzętu, oprogramowania i oprogramowania sprzętowego istotnego dla bezpieczeństwa.

Zabezpieczenia powiązane: AC-3, AC-4, AC-25, SA-4, SA-5.

(5) ARCHITEKTURA I PROJEKTY BEZPIECZEŃSTWA I PRYWATNOŚCI OPROGRAMOWANIA | PROSTY KONCEPCYJNIE PROJEKT

Wymagaj od twórcy systemu, komponentu systemu lub usługi systemowej:

a. Zaprojektowania i ustrukturyzowania sprzętu, oprogramowania i oprogramowania sprzętowego istotnego dla bezpieczeństwa w celu wykorzystania kompletnego, koncepcyjnie prostego mechanizmu ochrony z precyzyjnie zdefiniowaną semantyką;

b. Wewnętrznego ustrukturyzowania sprzętu, oprogramowania i oprogramowania sprzętowego istotnego dla bezpieczeństwa ze szczególnym uwzględnieniem tego mechanizmu.

Zabezpieczenia powiązane: AC-25, SA-8, SC-3.

(6) ARCHITEKTURA I PROJEKTY BEZPIECZEŃSTWA I PRYWATNOŚCI OPROGRAMOWANIA | STRUKTURA TESTOWANIA

Wymagaj od twórcy systemu, komponentu systemu lub usługi systemowej ustrukturyzowania sprzętu, oprogramowania i oprogramowania sprzętowego istotnego dla bezpieczeństwa w sposób ułatwiający testowanie.

Zabezpieczenia powiązane: SA-5, SA-11.

(7) ARCHITEKTURA I PROJEKTY BEZPIECZEŃSTWA I PRYWATNOŚCI OPROGRAMOWANIA | STRUKTURA DLA NAJNIŻSZYCH UPRAWNIEŃ

Wymagaj od dewelopera systemu, komponentu systemu lub usługi systemowej ustrukturyzowania sprzętu, oprogramowania i oprogramowania sprzętowego istotnego dla bezpieczeństwa w sposób ułatwiający kontrolowanie dostępu z najniższymi uprawnieniami.

Zabezpieczenia powiązane: AC-5, AC-6, SA-8.

(8) ARCHITEKTURA I PROJEKTY BEZPIECZEŃSTWA I PRYWATNOŚCI OPROGRAMOWANIA | ORKIESTRACJA

Zaprojektuj [Określone przez organizację krytyczne systemy lub komponenty systemowe] z skoordynowanym zachowaniem w celu wdrożenia następujących funkcjonalności: [Określone przez organizację funkcjonalności, przypisane do systemu lub komponentu].

Zabezpieczenia powiązane: nie dotyczy.

(9) ARCHITEKTURA I PROJEKTY BEZPIECZEŃSTWA I PRYWATNOŚCI OPROGRAMOWANIA | RÓŻNORODNOŚĆ PROJEKTÓW

Użyj różnych projektów dla [Realizacja: systemy krytyczne zdefiniowane przez organizację] w celu spełnienia wspólnego zestawu wymagań lub zapewnienia równoważnej funkcjonalności.

Zabezpieczenia powiązane: nie dotyczy.

SA-18 ODPORNOŚĆ NA SABOTAŻ I WYKRYWANIE MANIPULACJI

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

Zabezpieczenia rozszerzone:

(1) ODPORNOŚĆ NA SABOTAŻ I WYKRYWANIE MANIPULACJI | WIELOFAZOWOŚĆ CYKLU ŻYCIA SYSTEMU

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(2) ODPORNOŚĆ NA SABOTAŻ I WYKRYWANIE MANIPULACJI | KONTROLA SYSTEMÓW LUB KOMPONENTÓW

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

SA-19 AUTENTYCZNOŚĆ KOMPONENTÓW

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

Zabezpieczenia rozszerzone:

(1) AUTENTYCZNOŚĆ KOMPONENTÓW | SZKOLENIE / ROZPOZNAWANIE AUTENTYCZNOŚCI

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(2) AUTENTYCZNOŚĆ KOMPONENTÓW | KONTROLA KONFIGURACJI NA POTRZEBY SERWISOWANIA / NAPRAWY KOMPONENTÓW

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(3) AUTENTYCZNOŚĆ KOMPONENTÓW | UTYLIZACJA KOMPONENTÓW

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(4) AUTENTYCZNOŚĆ KOMPONENTÓW | SKANOWANIE AUTENTYCZNOŚCI

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

SA-20 DEDYKOWANE TWORZENIE KRYTYCZNYCH KOMPONENTÓW

Zabezpieczenie:

Ponownie zaimplementuj lub stwórz na zamówienie następujące krytyczne komponenty systemowe: [Określone przez organizację krytyczne komponenty systemowe].

Zabezpieczenia powiązane: CP-2, RA-9, SA-8.

Zabezpieczenia rozszerzone: nie dotyczy.

SA-21 KONTROLA PROGRAMISTY

Zabezpieczenie:

Wymagaj, aby twórca [Realizacja: system, komponenty systemu lub usługa systemowa zdefiniowane przez organizację]:

a. Posiadał odpowiednie upoważnienia dostępu określone przez przydzielone [Realizacja: oficjalne obowiązki rządowe zdefiniowane przez organizację];

b. Spełniał następujące dodatkowe kryteria weryfikacji personelu: [Realizacja: dodatkowe kryteria weryfikacji personelu zdefiniowane przez organizację].

Zabezpieczenia powiązane: PS-2, PS-3, PS-6, PS-7, SA-4, SR-6.

Zabezpieczenia rozszerzone:

(1) KONTROLA PROGRAMISTY | OCENA PRZEGLĄDU

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

SA-22 KOMPONENTY SYSTEMU BEZ WSPARCIA

Zabezpieczenie:

a. Wymieniaj komponenty systemu, gdy wsparcie dla komponentów nie jest już dostępne od dewelopera, dostawcy lub producenta;

b. Zapewnij następujące opcje alternatywnych źródeł dla ciągłego wsparcia niewspieranych komponentów [Wybór (jeden lub więcej): wsparcie wewnętrzne, [Realizacja: wsparcie od zewnętrznych dostawców zdefiniowane przez organizację]].

Zabezpieczenia powiązane: PL-2, SA-3.

Zabezpieczenia rozszerzone:

(1) KOMPONENTY SYSTEMU BEZ WSPARCIA | ALTERNATYWNE ŹRÓDŁA STAŁEGO WSPARCIA

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

SA-23 SPECJALIZACJA

Zabezpieczenie:

Zastosuj [Wybór (jeden lub więcej): modyfikacji projektu, rozszerzenia, rekonfiguracji] na [Realizacja: systemy lub komponenty systemu zdefiniowane przez organizację] wspierających podstawowe usługi lub funkcje misji w celu zwiększenia wiarygodności tych systemów lub komponentów.

Zabezpieczenia powiązane: RA-9, SA-8.

Zabezpieczenia rozszerzone: nie dotyczy.

KATEGORIA: SC - OCHRONA SYSTEMÓW I KOMUNIKACJI

SC-1 POLITYKA I PROCEDURY

Zabezpieczenie:

a. Opracuj, udokumentuj i rozpowszechnij wśród [Realizacja: personel lub role zdefiniowane przez organizację]:

    1. [Wybór (jeden lub więcej): Poziom organizacji; Poziom misji/procesu biznesowego; Poziom systemu] politykę ochrony systemu i komunikacji, która:

        (a) dotyczy celu, zakresu, ról, obowiązków, zaangażowania kierownictwa, koordynacji między jednostkami organizacyjnymi i zgodności;

        (b) jest zgodna z obowiązującymi przepisami prawa, rozporządzeniami wykonawczymi, dyrektywami, regulacjami, politykami, standardami i wytycznymi;

    2. Procedury ułatwiające wdrożenie polityki ochrony systemu i komunikacji oraz powiązanych kontroli ochrony systemu i komunikacji;

b. Wyznacz [Realizacja: urzędnika zdefiniowanego przez organizację] do zarządzania opracowaniem, dokumentowaniem i rozpowszechnianiem polityki i procedur ochrony systemu i komunikacji;

c. Przeglądaj i aktualizuj na bieżąco ochronę systemu i komunikacji w:

1. Polityce [Realizacja: częstotliwość zdefiniowana przez organizację] i następujących [Realizacja: zdarzenia zdefiniowane przez organizację];

2. Procedurach [Realizacja: częstotliwość zdefiniowana przez organizację] i następujących po nich [Realizacja: zdarzenia zdefiniowane przez organizację].

Zabezpieczenia powiązane: PM-9, PS-8, SA-8, SI-12.

Zabezpieczenia rozszerzone: nie dotyczy.

SC-2 SEPARACJA

Zabezpieczenie:

Oddzielaj funkcjonalności użytkownika, w tym usług interfejsu użytkownika, od funkcjonalności zarządzania systemem.

Zabezpieczenia powiązane: AC-6, SA-4, SA-8, SC-3, SC-7, SC-22, SC-32, SC-39.

Zabezpieczenia rozszerzone:

(1) SEPARACJA | INTERFEJSY DLA UŻYTKOWNIKÓW NIEUPRZYWILEJOWANYCH

Zapobiegaj udostępnianiu funkcjonalności zarządzania systemem na interfejsach użytkownikom nieuprawnionym.

Zabezpieczenia powiązane: AC-3.

(2) SEPARACJA | ROZŁĄCZENIE

Przechowuj oddzielnie informacje o stanie aplikacji i oprogramowania.

Zabezpieczenia powiązane: nie dotyczy.

SC-3 IZOLACJA FUNKCJI BEZPIECZEŃSTWA

Zabezpieczenie:

Odizoluj funkcje bezpieczeństwa od funkcji niebędących funkcjami bezpieczeństwa.

Zabezpieczenia powiązane: AC-3, AC-6, AC-25, CM-2, CM-4, SA-4, SA-5, SA-8, SA-15, SA-17, SC-2, SC-7, SC-32, SC-39, SI-16.

Zabezpieczenia rozszerzone:

(1) IZOLACJA FUNKCJI BEZPIECZEŃSTWA | SEPARACJA SPRZĘTOWA

Wdrażaj mechanizmy separacji sprzętowej w celu wdrożenia izolacji funkcji bezpieczeństwa.

Zabezpieczenia powiązane: nie dotyczy.

(2) IZOLACJA FUNKCJI BEZPIECZEŃSTWA | FUNKCJE KONTROLI DOSTĘPU I PRZEPŁYWU

Odizoluj funkcje bezpieczeństwa wymuszające kontrolę dostępu i przepływu informacji od funkcji niezwiązanych z bezpieczeństwem i od innych funkcji bezpieczeństwa.

Zabezpieczenia powiązane: nie dotyczy.

(3) IZOLACJA FUNKCJI BEZPIECZEŃSTWA | MINIMALIZACJA FUNKCJONALNOŚCI NIEBĘDĄCYCH FUNKCJAMI BEZPIECZEŃSTWA

Zminimalizuj liczbę funkcji niebędących funkcjami zabezpieczającymi, zawartych w granicy izolacji obejmującej funkcje zabezpieczające.

Zabezpieczenia powiązane: nie dotyczy.

(4) IZOLACJA FUNKCJI BEZPIECZEŃSTWA | SPRZĘGANIE I SPÓJNOŚĆ MODUŁÓW

Wdrażaj funkcje bezpieczeństwa jako w dużej mierze niezależne moduły, które maksymalizują wewnętrzną spójność w ramach modułów i minimalizują powiązania między nimi.

Zabezpieczenia powiązane: nie dotyczy.

(5) IZOLACJA FUNKCJI BEZPIECZEŃSTWA | STRUKTURY WARSTWOWE

Wdrażaj funkcje bezpieczeństwa jako strukturę warstwową, minimalizując interakcje między warstwami projektu i unikając jakiejkolwiek zależności niższych warstw od funkcjonalności lub poprawności wyższych warstw.

Zabezpieczenia powiązane: nie dotyczy.

SC-4 INFORMACJE W ZASOBACH WSPÓŁDZIELONEGO SYSTEMU

Zabezpieczenie:

Zapobiegaj nieautoryzowanemu i niezamierzonemu przesyłaniu informacji za pośrednictwem współdzielonych zasobów systemowych.

Zabezpieczenia powiązane: AC-3, AC-4, SA-8.

Zabezpieczenia rozszerzone:

(1) INFORMACJE W ZASOBACH WSPÓŁDZIELONEGO SYSTEMU | POZIOMY BEZPIECZEŃSTWA

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(2) INFORMACJE W ZASOBACH WSPÓŁDZIELONEGO SYSTEMU | PRZETWARZANIE WIELOPOZIOMOWE LUB OKRESOWE

Zapobiegaj nieautoryzowanemu transferowi informacji za pośrednictwem współdzielonych zasobów zgodnie z [Realizacja: procedury zdefiniowane przez organizację], gdy przetwarzanie w systemie wyraźnie przełącza się między różnymi poziomami klasyfikacji informacji lub kategoriami bezpieczeństwa.

Zabezpieczenia powiązane: nie dotyczy.

SC-5 OCHRONA PRZED ODMOWĄ USŁUGI

Zabezpieczenie:

a. [Wybór: Ochrona przed; Ograniczenie] skutków następujących typów zdarzeń odmowy usługi: [Realizacja: typy zdarzeń odmowy usługi zdefiniowane przez organizację];

b. Zastosuj następujące kontrole, aby osiągnąć cel odmowy usługi: [Realizacja: kontrolki zdefiniowane przez organizację według typu zdarzenia odmowy usługi].

Zabezpieczenia powiązane: CP-2, IR-4, SC-6, SC-7, SC-40.

Zabezpieczenia rozszerzone:

(1) OCHRONA PRZED ODMOWĄ USŁUGI | OGRANICZENIE MOŻLIWOŚCI ATAKOWANIA INNYCH SYSTEMÓW

Ogranicz możliwość przeprowadzania przez jednostki następujących ataków typu „odmowa usługi” na inne systemy: [Realizacja: ataki typu „odmowa usługi” zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(2) OCHRONA PRZED ODMOWĄ USŁUGI | POJEMNOŚĆ, PRZEPUSTOWOŚĆ I REDUNDANCJA

Zarządzaj pojemnością, przepustowością i innymi nadmiarowościami, aby ograniczyć skutki ataków typu „odmowa usługi” zalewających sieć.

Zabezpieczenia powiązane: nie dotyczy.

(3) OCHRONA PRZED ODMOWĄ USŁUGI | WYKRYWANIE I MONITOROWANIE

a. Zastosuj następujące narzędzia monitorujące w celu wykrycia wskaźników ataków typu „odmowa usługi” skierowanych przeciwko systemowi lub uruchamianych z niego: [Realizacja: narzędzia monitorujące zdefiniowane przez organizację];

b. Monitoruj następujące zasoby systemu w celu ustalenia, czy istnieją wystarczające zasoby, aby zapobiec skutecznym atakom typu „odmowa usługi”: [Realizacja: zasoby systemu zdefiniowane przez organizację].

Zabezpieczenia powiązane: CA-7, SI-4.

SC-6 DOSTĘPNOŚĆ ZASOBÓW

Zabezpieczenie:

Chroń dostępność zasobów, przydzielając [Realizacja: zasoby zdefiniowane przez organizację] według [Wybór (jeden lub więcej): priorytet; kwota; [Realizacja: elementy sterujące zdefiniowane przez organizację]].

Zabezpieczenia powiązane: SC-5.

Zabezpieczenia rozszerzone: nie dotyczy.

SC-7 OCHRONA POŁĄCZEŃ BRZEGOWYCH

Zabezpieczenie:

a. Monitoruj i kontroluj komunikację na zewnętrznych zarządzanych interfejsach do systemu i na kluczowych wewnętrznych zarządzanych interfejsach w systemie;

b. Implementuj podsieci dla publicznie dostępnych komponentów systemu, które są [Wybór: fizycznie; logicznie] oddzielone od wewnętrznych sieci organizacyjnych;

c. Łącz się z zewnętrznymi sieciami lub systemami tylko za pośrednictwem zarządzanych interfejsów składających się z urządzeń ochrony granic ułożonych zgodnie z architekturą bezpieczeństwa i prywatności organizacji.

Zabezpieczenia powiązane: AC-4, AC-17, AC-18, AC-19, AC-20, AU-13, CA-3, CM-2, CM-4, CM-7, CM-10, CP-8, CP-10, IR-4, MA-4, PE-3, PL-8, PM-12, SA-8, SA-17, SC-5, SC-26, SC-32, SC-35, SC-43.

Zabezpieczenia rozszerzone:

(1) OCHRONA POŁĄCZEŃ BRZEGOWYCH | PODSIECI FIZYCZNIE WYDZIELONE

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

Zabezpieczenia powiązane: nie dotyczy.

(2) OCHRONA POŁĄCZEŃ BRZEGOWYCH | DOSTĘP PUBLICZNY

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

Zabezpieczenia powiązane: nie dotyczy.

(3) OCHRONA POŁĄCZEŃ BRZEGOWYCH | PUNKTY DOSTĘPU

Ogranicz liczbę zewnętrznych połączeń sieciowych do systemu.

Zabezpieczenia powiązane: nie dotyczy.

(4) OCHRONA POŁĄCZEŃ BRZEGOWYCH | ZEWNĘTRZNE USŁUGI TELEKOMUNIKACYJNE

a. Wprowadź zarządzany interfejs dla każdej zewnętrznej usługi telekomunikacyjnej;

b. Ustanów politykę przepływu ruchu dla każdego zarządzanego interfejsu;

c. Chroń poufność i integralność informacji przesyłanych przez każdy interfejs;

d. Dokumentuj każdy wyjątek od polityki przepływu ruchu wraz z misją pomocniczą lub potrzebą biznesową i czasem trwania tej potrzeby;

e. Przejrzyj wyjątki od polityki przepływu ruchu [Realizacja: częstotliwość zdefiniowana przez organizację] i usunąć wyjątki, które nie są już obsługiwane przez wyraźną misję lub potrzebę biznesową;

f. Zapobiegaj nieautoryzowanej wymianie ruchu płaszczyzny sterowania z sieciami zewnętrznymi;

g. Publikuj informacje umożliwiające zdalnym sieciom wykrywanie nieautoryzowanego ruchu płaszczyzny sterowania z sieci wewnętrznych;

h. Filtruj nieautoryzowany ruch płaszczyzny sterowania z sieci zewnętrznych.

Zabezpieczenia powiązane: AC-3, SC-8, SC-20, SC-21, SC-22.

(5) OCHRONA POŁĄCZEŃ BRZEGOWYCH | ODMÓW DOMYŚLNIE — ZEZWÓL NA ZASADZIE WYJĄTKU

Domyślnie zabroń ruchu komunikacji sieciowej i zezwól na ruch komunikacji sieciowej na mocy wyjątku [Wybór (jeden lub więcej): na zarządzanych interfejsach; dla [Realizacja: systemy zdefiniowane przez organizację]].

Zabezpieczenia powiązane: nie dotyczy.

(6) OCHRONA POŁĄCZEŃ BRZEGOWYCH | REAKCJA NA WYKRYTE AWARIE

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(7) OCHRONA POŁĄCZEŃ BRZEGOWYCH | TUNELOWANIE DZIELONE DLA URZĄDZEŃ ZDALNYCH

Zapobiegaj dzieleniu tunelowania dla urządzeń zdalnych łączących się z systemami organizacji, chyba że podzielony tunel jest bezpiecznie skonfigurowany przy użyciu [Realizacja: zabezpieczenia zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(8) OCHRONA POŁĄCZEŃ BRZEGOWYCH | KIEROWANIE RUCHU DO UWIERZYTELNIONYCH SERWERÓW PROXY

Trasa [Realizacja: ruch komunikacji wewnętrznej zdefiniowany przez organizację] do [Realizacja: sieci zewnętrznych zdefiniowanych przez organizację] poprzez uwierzytelnione serwery proxy na zarządzanych interfejsach.

Zabezpieczenia powiązane: AC-3.

(9) OCHRONA POŁĄCZEŃ BRZEGOWYCH | OGRANICZANIE ZAGRAŻAJĄCEGO RUCHU KOMUNIKACYJNEGO WYCHODZĄCEGO

a. Wykrywaj i blokuj ruch wychodzący, który stwarza zagrożenie dla systemów zewnętrznych;

b. Audytuj tożsamości użytkowników wewnętrznych powiązanych z zablokowaną komunikacją.

Zabezpieczenia powiązane: AU-2, AU-6, SC-5, SC-38, SC-44, SI-3, SI-4.

(10) OCHRONA POŁĄCZEŃ BRZEGOWYCH | ZAPOBIEGANIE EKSFILTRACJI

a. Zapobiegaj wykradaniu informacji;

b. Przeprowadzać testy eksfiltracji [Realizacja: częstotliwość określona przez organizację].

Zabezpieczenia powiązane: AC-2, CA-8, SI-3.

(11) OCHRONA POŁĄCZEŃ BRZEGOWYCH | OGRANICZENIE RUCHU PRZYCHODZĄCEGO

Zezwalaj na kierowanie komunikacji przychodzącej tylko ze źródeł [Realizacja: autoryzowanych źródeł zdefiniowanych przez organizację] do [Realizacja: autoryzowanych miejsc docelowych zdefiniowanych przez organizację].

Zabezpieczenia powiązane: AC-3.

(12) OCHRONA POŁĄCZEŃ BRZEGOWYCH | OCHRONA OPARTA NA HOŚCIE

Wdrażaj [Realizacja: mechanizmy ochrony granic oparte na hoście zdefiniowane przez organizację] w [Realizacja: komponenty systemu zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(13) OCHRONA POŁĄCZEŃ BRZEGOWYCH | IZOLACJA NARZĘDZI BEZPIECZEŃSTWA, MECHANIZMÓW I KOMPONENTÓW POMOCNICZYCH

Izoluj [Realizacja: narzędzia, mechanizmy i komponenty wsparcia bezpieczeństwa informacji zdefiniowane przez organizację] od innych wewnętrznych komponentów systemu poprzez wdrożenie fizycznie oddzielnych podsieci z zarządzanymi interfejsami do innych komponentów systemu.

Zabezpieczenia powiązane: SC-2, SC-3.

(14) OCHRONA POŁĄCZEŃ BRZEGOWYCH | OCHRONA PRZED NIEAUTORYZOWANYMI POŁĄCZENIAMI FIZYCZNYMI

Zabezpiecz się przed nieautoryzowanymi połączeniami fizycznymi w [Realizacja: interfejsy zarządzane zdefiniowane przez organizację].

Zabezpieczenia powiązane: PE-4, PE-19.

(15) OCHRONA POŁĄCZEŃ BRZEGOWYCH | SIECIOWE UPRZYWILEJOWANE DOSTĘPY

Przekierowywanie uprzywilejowanych dostępów w ramach sieci poprzez dedykowany, zarządzany interfejs w celu kontroli dostępu i audytu.

Zabezpieczenia powiązane: AC-2, AC-3, AU-2, SI-4.

(16) OCHRONA POŁĄCZEŃ BRZEGOWYCH | ZAPOBIEGANIE WYKRYWANIU SKŁADNIKÓW SYSTEMU

Zapobiegaj wykrywaniu określonych komponentów systemu, które reprezentują zarządzany interfejs.

Zabezpieczenia powiązane: nie dotyczy.

(17) OCHRONA POŁĄCZEŃ BRZEGOWYCH | AUTOMATYCZNE EGZEKWOWANIE FORMATÓW PROTOKOŁÓW

Wymuszaj przestrzeganie formatów protokołów.

Zabezpieczenia powiązane: SC-4.

(18) OCHRONA POŁĄCZEŃ BRZEGOWYCH | FAIL SECURE

Zapobiegaj przechodzeniu systemów w stan niezabezpieczony w przypadku awarii urządzenia ochrony granicznej.

Zabezpieczenia powiązane: CP-2, CP-12, SC-24.

(19) OCHRONA POŁĄCZEŃ BRZEGOWYCH | BLOKOWANIE KOMUNIKACJI Z HOSTÓW NIESKONFIGUROWANYCH ORGANIZACYJNIE

Blokuj ruch komunikacyjny przychodzący i wychodzący między [Realizacja: klientami komunikacji zdefiniowanymi przez organizację], które są niezależnie konfigurowane przez użytkowników końcowych i zewnętrznych dostawców usług.

Zabezpieczenia powiązane: nie dotyczy.

(20) OCHRONA POŁĄCZEŃ BRZEGOWYCH | DYNAMICZNA IZOLACJA I SEPARACJA

Umożliwiaj dynamiczną izolację [Realizacja: zdefiniowane przez organizację komponenty systemu] od innych komponentów systemu.

Zabezpieczenia powiązane: nie dotyczy.

(21) OCHRONA POŁĄCZEŃ BRZEGOWYCH | IZOLACJA KOMPONENTÓW SYSTEMU

Wdrażaj mechanizmy ochrony granic, aby odizolować [Realizacja: komponenty systemu zdefiniowane przez organizację] wspierające [Realizacja: misje i/lub funkcje biznesowe zdefiniowane przez organizację].

Zabezpieczenia powiązane: CA-9.

(22) OCHRONA POŁĄCZEŃ BRZEGOWYCH | ODDZIELNE PODSIECI DO ŁĄCZENIA SIĘ Z RÓŻNYMI DOMENAMI ZABEZPIECZEŃ

Wprowadź oddzielne adresy sieciowe w celu połączenia z systemami w różnych domenach zabezpieczeń.

Zabezpieczenia powiązane: nie dotyczy.

(23) OCHRONA POŁĄCZEŃ BRZEGOWYCH | WYŁĄCZ INFORMACJE ZWROTNE NADAWCY O NIEPOWODZENIU WALIDACJI PROTOKOŁU

Wyłącz informowanie nadawców o niepowodzeniu weryfikacji formatu protokołu.

Zabezpieczenia powiązane: nie dotyczy.

(24) OCHRONA POŁĄCZEŃ BRZEGOWYCH | INFORMACJE UMOŻLIWIAJĄCE IDENTYFIKACJĘ OSOBY

W przypadku systemów przetwarzających dane osobowe:

a. Zastosuj następujące reguły przetwarzania do elementów danych zawierających dane osobowe: [Realizacja: reguły przetwarzania zdefiniowane przez organizację];

b. Monitoruj dozwolone przetwarzanie na zewnętrznych interfejsach systemu i na kluczowych granicach wewnętrznych w systemie;

c. Dokumentuj każdy wyjątek przetwarzania;

d. Przejrzyj i usuń wyjątki, które nie są już obsługiwane.

Zabezpieczenia powiązane: PT-2, SI-15.

(25) OCHRONA POŁĄCZEŃ BRZEGOWYCH | POŁĄCZENIA Z SYSTEMAMI PAŃSTWOWYMI PRZETWARZAJĄCYMI INFORMACJE JAWNE

Zabroń bezpośredniego podłączania [Realizacja: zdefiniowany przez organizację jawny system bezpieczeństwa narodowego] do sieci zewnętrznej bez użycia [Realizacja: zdefiniowane przez organizację urządzenie ochrony połączeń brzegowych].

Zabezpieczenia powiązane: nie dotyczy.

(26) OCHRONA POŁĄCZEŃ BRZEGOWYCH | POŁĄCZENIA Z SYSTEMAMI PAŃSTWOWYMI PRZETWARZAJĄCYMI INFORMACJE NIEJAWNE

Zabroń bezpośredniego połączenia systemu teleinformatycznego przetwarzającego informacje niejawne z siecią zewnętrzną bez zastosowania [Przypis: określonego przez organizację urządzenia ochrony połączeń brzegowych].

Zabezpieczenia powiązane: nie dotyczy.

(27) OCHRONA POŁĄCZEŃ BRZEGOWYCH | POŁĄCZENIA Z JAWNYMI SYSTEMAMI NIEMAJĄCYMI ZNACZENIA DLA BEZPIECZEŃSTWA NARODOWEGO

Zabroń bezpośredniego podłączania [Realizacja: zdefiniowany przez organizację niejawny system bezpieczeństwa narodowego] do sieci zewnętrznej bez użycia [Realizacja: zdefiniowane przez organizację urządzenie połączeń brzegowych].

Zabezpieczenia powiązane: nie dotyczy.

(28) OCHRONA POŁĄCZEŃ BRZEGOWYCH | POŁĄCZENIA Z SIECIAMI PUBLICZNYMI

Zabroń bezpośredniego połączenia [Realizacja: system zdefiniowany przez organizację] z siecią publiczną.

Zabezpieczenia powiązane: nie dotyczy.

(29) OCHRONA POŁĄCZEŃ BRZEGOWYCH | ODDZIELNE PODSIECI W CELU ODIZOLOWANIA FUNKCJI

Wprowadź [Wybór: fizycznie; logicznie] oddzielnych podsieci w celu odizolowania następujących krytycznych komponentów i funkcji systemu: [Realizacja: zdefiniowane przez organizację krytyczne komponenty i funkcje systemu].

Zabezpieczenia powiązane: nie dotyczy.

SC-8 POUFNOŚĆ I INTEGRALNOŚĆ TRANSMISJI

Zabezpieczenie:

Chroń [Wybór (jednego lub więcej): poufność; integralność] przesyłanych informacji.

Zabezpieczenia powiązane: AC-17, AC-18, AU-10, IA-3, IA-8, IA-9, MA-4, PE-4, SA-4, SA-8, SC-7, SC-16, SC- 20, SC-23, SC-28.

Zabezpieczenia rozszerzone:

(1) POUFNOŚĆ I INTEGRALNOŚĆ TRANSMISJI | OCHRONA KRYPTOGRAFICZNA

Wprowadź mechanizmy kryptograficzne w celu [Wybór (jednego lub więcej): zapobiegania nieautoryzowanemu ujawnieniu informacji; wykrywania zmian w informacjach] podczas transmisji.

Zabezpieczenia powiązane: SC-12, SC-13.

(2) POUFNOŚĆ I INTEGRALNOŚĆ TRANSMISJI | POSTĘPOWANIE PRZED I PO TRANSMISJI

Zachowaj [Wybór (jednego lub więcej): poufność; integralność] informacji podczas przygotowywania ich do transmisji oraz podczas odbioru.

Zabezpieczenia powiązane: nie dotyczy.

(3) POUFNOŚĆ I INTEGRALNOŚĆ TRANSMISJI | OCHRONA KRYPTOGRAFICZNA ZEWNĘTRZNYCH ELEMENTÓW WIADOMOŚCI

Wprowadź mechanizmy kryptograficzne w celu ochrony treści wiadomości zewnętrznych, chyba że są one chronione w inny sposób przez [Realizacja: alternatywne kontrole fizyczne zdefiniowane przez organizację].

Zabezpieczenia powiązane: SC-12, SC-13.

(4) POUFNOŚĆ I INTEGRALNOŚĆ TRANSMISJI | UKRYWANIE LUB LOSOWE ŁĄCZENIE KOMUNIKATÓW

Wprowadź mechanizmy kryptograficzne w celu ukrycia lub losowego określenia wzorców komunikacji, chyba że są one chronione przez [Realizacja: alternatywne kontrole fizyczne zdefiniowane przez organizację].

Zabezpieczenia powiązane: SC-12, SC-13.

(5) POUFNOŚĆ I INTEGRALNOŚĆ TRANSMISJI | CHRONIONY SYSTEM DYSTRYBUCJI

Wprowadź [Realizacja: zdefiniowany przez organizację chroniony system dystrybucji] w celu [Wybór (jeden lub więcej): zapobiegania nieautoryzowanemu ujawnieniu informacji; wykrywania zmian w informacjach] podczas transmisji.

Zabezpieczenia powiązane: nie dotyczy.

SC-9 POUFNOŚĆ TRANSMISJI

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

SC-10 ROZŁĄCZENIE SIECI

Zabezpieczenie:

Zakończ połączenie sieciowe związane z sesją komunikacyjną po zakończeniu sesji lub po [Realizacja: okres czasu zdefiniowany przez organizację] braku aktywności.

Zabezpieczenia powiązane: AC-17 i SC-23.

Zabezpieczenia rozszerzone: nie dotyczy.

SC-11 ZAUFANA ŚCIEŻKA

Zabezpieczenie:

a. Zapewnij [Wybór: fizycznie; logicznie] odizolowaną zaufaną ścieżkę komunikacyjną do komunikacji między użytkownikiem a zaufanymi komponentami systemu;

b. Zezwól użytkownikom na wywoływanie zaufanej ścieżki komunikacyjnej do komunikacji między użytkownikiem a następującymi funkcjami bezpieczeństwa systemu, w tym co najmniej uwierzytelnianie i ponowne uwierzytelnianie: [Realizacja: funkcje bezpieczeństwa zdefiniowane przez organizację].

Zabezpieczenia powiązane: AC-16, AC-25, SC-12, SC-23.

Zabezpieczenia rozszerzone:

(1) ZAUFANA ŚCIEŻKA | NIEPODWAŻALNA ŚCIEŻKA KOMUNIKACJI

Zabezpieczenie:

a. Zapewnij zaufaną ścieżkę komunikacji, która będzie jednoznacznie odróżniać się od innych ścieżek komunikacji;

b. Zainicjuj zaufaną ścieżkę komunikacji dla komunikacji pomiędzy [Realizacja: funkcje bezpieczeństwa zdefiniowane przez organizację] systemu a użytkownikiem.

Zabezpieczenia powiązane: nie dotyczy.

SC-12 USTANAWIANIE I ZARZĄDZANIE KLUCZAMI KRYPTOGRAFICZNYMI

Zabezpieczenie:

Ustanów i zarządzaj kluczami kryptograficznymi, gdy w systemie stosowana jest kryptografia, zgodnie z następującymi wymogami zarządzania kluczami: [Realizacja: wymagania organizacji dotyczące generowania, dystrybucji, przechowywania, dostępu i niszczenia kluczy].

Zabezpieczenia powiązane: AC-17, AU-9, AU-10, CM-3, IA-3, IA-7, SA-4, SA-8, SA-9, SC-8, SC-11, SC-12, SC- 13, SC-17, SC-20, SC-37, SC-40, SI-3, SI-7.

Zabezpieczenia rozszerzone:

(1) USTANAWIANIE I ZARZĄDZANIE KLUCZAMI KRYPTOGRAFICZNYMI | DOSTĘPNOŚĆ

Utrzymuj dostępność informacji na wypadek utraty kluczy kryptograficznych przez użytkowników.

Zabezpieczenia powiązane: nie dotyczy.

(2) USTANAWIANIE I ZARZĄDZANIE KLUCZAMI KRYPTOGRAFICZNYMI | KLUCZE SYMETRYCZNE

Generuj, zarządzaj i dystrybuuj symetryczne klucze kryptograficzne przy użyciu technologii i procesów zarządzania kluczami zgodnych z [Wybór: zatwierdzonymi przez polskie normy kryptograficzne; zatwierdzonymi przez odpowiednie krajowe organy ds. bezpieczeństwa].

Zabezpieczenia powiązane: nie dotyczy.

(3) USTANAWIANIE I ZARZĄDZANIE KLUCZAMI KRYPTOGRAFICZNYMI | KLUCZE ASYMETRYCZNE

Generuj, zarządzaj i dystrybuuj asymetryczne klucze kryptograficzne przy użyciu [Wybór: zatwierdzonych przez krajowe organy ds. bezpieczeństwa technologii i procesów zarządzania kluczami; certyfikatów PKI o średnim poziomie zaufania zatwierdzonych lub wydanych przez odpowiednie organy państwowe; certyfikatów PKI o średnim poziomie zaufania związanych ze sprzętem oraz sprzętowych tokenów bezpieczeństwa chroniących klucz prywatny użytkownika; certyfikatów wydanych zgodnie z wymaganiami określonymi przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(4) USTANAWIANIE I ZARZĄDZANIE KLUCZAMI KRYPTOGRAFICZNYMI | CERTYFIKATY PKI

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(5) USTANAWIANIE I ZARZĄDZANIE KLUCZAMI KRYPTOGRAFICZNYMI | CERTYFIKATY PKI / TOKENY SPRZĘTOWE

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(6) USTANAWIANIE I ZARZĄDZANIE KLUCZAMI KRYPTOGRAFICZNYMI | KONTROLA FIZYCZNA KLUCZY

Zachowaj fizyczną kontrolę nad kluczami kryptograficznymi, gdy przechowywane informacje są szyfrowane przez zewnętrznych dostawców usług.

Zabezpieczenia powiązane: nie dotyczy.

SC-13 OCHRONA KRYPTOGRAFICZNA

Zabezpieczenie:

a. Określ [Realizacja: zdefiniowane przez organizację zastosowania kryptograficzne];

b. Wdróż następujące typy kryptografii wymagane dla każdego określonego zastosowania kryptograficznego: [Realizacja: zdefiniowane przez organizację typy kryptografii dla każdego określonego zastosowania kryptograficznego].

Zabezpieczenia powiązane: AC-2, AC-3, AC-7, AC-17, AC-18, AC-19, AU-9, AU-10, CM-11, CP-9, IA-3, IA-5, IA- 7, MA-4, MP-2, MP-4, MP-5, SA-4, SA-8, SA-9, SC-8, SC-12, SC-20, SC-23, SC-28, SC-40, SI-3, SI-7.

Zabezpieczenia rozszerzone:

(1) OCHRONA KRYPTOGRAFICZNA | KRYPTOGRAFIA ZGODNA Z FIPS

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(2) OCHRONA KRYPTOGRAFICZNA | KRYPTOGRAFIA ZATWIERDZONA PRZEZ NSA

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(3) OCHRONA KRYPTOGRAFICZNA | OSOBY INDYWIDUALNE BEZ FORMALNYCH ZATWIERDZEŃ NA DOSTĘP

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(4) OCHRONA KRYPTOGRAFICZNA | PODPISY CYFROWE

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

SC-14 OCHRONA DOSTĘPU PUBLICZNEGO

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

SC-15 WSPÓŁPRACUJĄCE URZĄDZENIA KOMPUTEROWE

Zabezpieczenie:

a. Zabroń zdalnej aktywacji urządzeń i aplikacji do obliczeń grupowych z następującymi wyjątkami: [Realizacja: wyjątki zdefiniowane przez organizację, w których zdalna aktywacja ma być dozwolona];

b. Zapewnij wyraźne wskazanie użytkowania użytkownikom fizycznie obecnym przy urządzeniach.

Zabezpieczenia powiązane: AC-21 i SC-42.

Zabezpieczenia rozszerzone:

(1) WSPÓŁPRACUJĄCE URZĄDZENIA KOMPUTEROWE| ROZŁĄCZENIE FIZYCZNE LUB LOGICZNE

Zapewnij [Wybór (jeden lub więcej): fizyczny; logiczny] rozłączenie urządzeń do pracy grupowej w sposób ułatwiający użytkowanie.

Zabezpieczenia powiązane: nie dotyczy.

(2) WSPÓŁPRACUJĄCE URZĄDZENIA KOMPUTEROWE | BLOKOWANIE RUCHU WEJŚCIOWEGO/WYJŚCIOWEGO

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(3) WSPÓŁPRACUJĄCE URZĄDZENIA KOMPUTEROWE | WYŁĄCZANIE I USUWANIE W BEZPIECZNYCH OBSZARACH ROBOCZYCH

Wyłącz lub usuń urządzenia i aplikacje do pracy grupowej z [Realizacja: systemów lub komponentów systemu zdefiniowanych przez organizację] w [Realizacja: bezpiecznych obszarach roboczych zdefiniowanych przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(4) WSPÓŁPRACUJĄCE URZĄDZENIA KOMPUTEROWE | WYRAŹNIE WSKAŻ BIEŻĄCYCH UCZESTNIKÓW

Podaj wyraźne wskazanie aktualnych uczestników [Realizacja: spotkania online i telekonferencje zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

SC-16 PRZESYŁANIE ATRYBUTÓW BEZPIECZEŃSTWA I PRYWATNOŚCI

Zabezpieczenie:

Powiąż [Realizacja: atrybuty bezpieczeństwa i prywatności zdefiniowane przez organizację] z informacjami wymienianymi pomiędzy systemami i pomiędzy komponentami systemu.

Zabezpieczenia powiązane: AC-3, AC-4, AC-16.

Zabezpieczenia rozszerzone:

(1) PRZESYŁANIE ATRYBUTÓW BEZPIECZEŃSTWA I PRYWATNOŚCI | WERYFIKACJA INTEGRALNOŚCI

Sprawdź integralność przekazywanych atrybutów bezpieczeństwa i prywatności.

Zabezpieczenia powiązane: AU-10, SC-8.

(2) PRZESYŁANIE ATRYBUTÓW BEZPIECZEŃSTWA I PRYWATNOŚCI | MECHANIZMY ANTYSPOOFINGOWE

Wprowadź mechanizmy zapobiegające podszywaniu się, aby uniemożliwić atakującym fałszowanie atrybutów bezpieczeństwa wskazujących na pomyślne zastosowanie procesu bezpieczeństwa.

Zabezpieczenia powiązane: SI-3, SI-4, SI-7.

(3) PRZESYŁANIE ATRYBUTÓW BEZPIECZEŃSTWA I PRYWATNOŚCI | KRYPTOGRAFICZNE WIĄZANIE

Wprowadź [Realizacja: mechanizmy lub techniki zdefiniowane przez organizację] w celu powiązania atrybutów bezpieczeństwa i prywatności z przesyłanymi informacjami.

Zabezpieczenia powiązane: AC-16, SC-12, SC-13.

SC-17 CERTYFIKATY INFRASTRUKTURY KLUCZA PUBLICZNEGO

Zabezpieczenie:

a. Wydawaj certyfikaty klucza publicznego zgodnie z [Realizacja: polityka certyfikatów zdefiniowana przez organizację] lub uzyskuj certyfikaty klucza publicznego od zatwierdzonego dostawcy usług;

b. Uwzględniaj tylko zatwierdzone kotwice zaufania w magazynach zaufania lub magazynach certyfikatów zarządzanych przez organizację.

Zabezpieczenia powiązane: AU-10, IA-5, SC-12.

Zabezpieczenia rozszerzone: nie dotyczy.

SC-18 KOD MOBILNY

Zabezpieczenie:

a. Zdefiniuj akceptowalny i nieakceptowalny kod mobilny i technologie kodu mobilnego;

b. Autoryzuj, monitoruj i kontroluj użycie kodu mobilnego w systemie.

Zabezpieczenia powiązane: AU-2, AU-12, CM-2, CM-6, SI-3.

Zabezpieczenia rozszerzone:

(1) KOD MOBILNY | IDENTYFIKUJ NIEDOPUSZCZALNY KOD I PODEJMUJ DZIAŁANIA NAPRAWCZE

Zidentyfikuj [Realizacja: niedopuszczalny kod mobilny zdefiniowany przez organizację] i podejmij [Realizacja: działania naprawcze zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(2) KOD MOBILNY | NABYWANIE, ROZWÓJ I UŻYTKOWANIE

Sprawdź, czy pozyskiwanie, opracowywanie i używanie kodu mobilnego, który ma zostać wdrożony w systemie, spełnia [Realizacja: wymagania dotyczące kodu mobilnego zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(3) KOD MOBILNY | ZAPOBIEGAJ POBIERANIU I WYKONYWANIU

Zapobiegaj pobieraniu i wykonywaniu [Realizacja: niedopuszczalny kod mobilny zdefiniowany przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(4) KOD MOBILNY | ZAPOBIEGAJ AUTOMATYCZNEMU WYKONYWANIU

Zapobiegaj automatycznemu wykonywaniu kodu mobilnego w [Realizacja: aplikacje oprogramowania zdefiniowane przez organizację] i wymuszaj [Realizacja: działania zdefiniowane przez organizację] przed wykonaniem kodu.

Zabezpieczenia powiązane: nie dotyczy.

(5) KOD MOBILNY | ZEZWALAJ NA WYKONYWANIE TYLKO W OGRANICZONYCH ŚRODOWISKACH

Zezwalaj na wykonywanie dozwolonego kodu mobilnego wyłącznie w ograniczonych środowiskach maszyn wirtualnych.

Zabezpieczenia powiązane: SC-44, SI-7.

SC-19 VOIP

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

SC-20 USŁUGA BEZPIECZNEGO ROZPOZNAWANIA NAZW/ADRESÓW (ŹRÓDŁO WIARYGODNE)

Zabezpieczenie:

a. Zapewnij dodatkowe artefakty uwierzytelniania pochodzenia danych i weryfikacji integralności wraz z autorytatywnymi danymi rozwiązywania nazw, które system zwraca w odpowiedzi na zewnętrzne zapytania dotyczące rozwiązywania nazw/adresów;

b. Zapewnij środki do wskazywania statusu bezpieczeństwa stref podrzędnych i (jeśli strefa podrzędna obsługuje usługi bezpiecznego rozwiązywania) umożliwienie weryfikacji łańcucha zaufania między domenami nadrzędnymi i podrzędnymi, podczas działania jako część rozproszonej, hierarchicznej przestrzeni nazw.

Zabezpieczenia powiązane: AU-10, SC-8, SC-12, SC-13, SC-21, SC-22.

Zabezpieczenia rozszerzone:

(1) USŁUGA BEZPIECZNEGO ROZPOZNAWANIA NAZW/ADRESÓW | PODOBSZARY PODRZĘDNE

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(2) USŁUGA BEZPIECZNEGO ROZPOZNAWANIA NAZW/ADRESÓW (ŹRÓDŁO WIARYGODNE) | POCHODZENIE I INTEGRALNOŚĆ DANYCH

Zapewnij artefakty ochrony pochodzenia i integralności danych dla wewnętrznych zapytań dotyczących rozwiązywania nazw/adresów.

Zabezpieczenia powiązane: nie dotyczy.

SC-21 USŁUGA BEZPIECZNEGO ROZPOZNAWANIA NAZW/ADRESÓW (REKURENCYJNA LUB BUFORUJĄCA)

Zabezpieczenie:

Żądaj i przeprowadzaj uwierzytelnianie źródła danych oraz weryfikację integralności danych w odpowiedziach dotyczących rozwiązywania nazw/adresów, które system otrzymuje z wiarygodnych źródeł.

Zabezpieczenia powiązane: SC-20, SC-22.

Zabezpieczenia rozszerzone:

(1) USŁUGA BEZPIECZNEGO ROZPOZNAWANIA NAZW/ADRESÓW | POCHODZENIE I INTEGRALNOŚĆ DANYCH

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

SC-22 ARCHITEKTURA I DOSTARCZANIE USŁUG ROZPOZNAWANIA NAZW/ADRESÓW

Zabezpieczenie:

Upewnij się, że systemy, które wspólnie zapewniają usługę rozpoznawania nazw/adresów w organizacji, są odporne na błędy i wdrażają wewnętrzny i zewnętrzny podział ról.

Zabezpieczenia powiązane: SC-2, SC-20, SC-21, SC-24.

Zabezpieczenia rozszerzone: nie dotyczy.

SC-23 AUTENTYCZNOŚĆ SESJI

Zabezpieczenie:

Chroń autentyczność sesji komunikacyjnych.

Zabezpieczenia powiązane: AU-10, SC-8, SC-10, SC-11.

Zabezpieczenia rozszerzone:

(1) AUTENTYCZNOŚĆ SESJI | UNIEWAŻNIJ IDENTYFIKATORY SESJI PRZY WYLOGOWANIU

Unieważnij identyfikatory sesji po wylogowaniu użytkownika lub innym zakończeniu sesji.

Zabezpieczenia powiązane: nie dotyczy.

(2) AUTENTYCZNOŚĆ SESJI | WYLOGOWANIA INICJOWANE PRZEZ UŻYTKOWNIKA I WYŚWIETLANIE KOMUNIKATÓW

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(3) AUTENTYCZNOŚĆ SESJI | UNIKALNE IDENTYFIKATORY SESJI GENEROWANE PRZEZ SYSTEM

Wygeneruj unikatowy identyfikator sesji dla każdej sesji za pomocą [Realizacja: wymagania dotyczące losowości zdefiniowane przez organizację] i rozpoznaj tylko identyfikatory sesji generowane przez system.

Zabezpieczenia powiązane: AC-10, SC-12, SC-13.

(4) AUTENTYCZNOŚĆ SESJI | UNIKALNE IDENTYFIKATORY SESJI Z RANDOMIZACJĄ

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(5) AUTENTYCZNOŚĆ SESJI | DOZWOLONE CENTRA CERTYFIKACJI

Zezwalaj na używanie [Realizacja: centrów certyfikacji zdefiniowanych przez organizację] wyłącznie w celu weryfikacji ustanowienia chronionych sesji.

Zabezpieczenia powiązane: SC-12, SC-13.

SC-24 PRZEJŚCIE DO OKREŚLONEGO STANU SYSTEMU PO BŁĘDZIE

Zabezpieczenie:

Zapewnij, aby w przypadku wystąpienia awarii: [Realizacja: lista typów awarii systemu zdefiniowanych przez organizację] w [Realizacja: komponenty systemu zdefiniowane przez organizację], system powinien przejść do [Realizacja: znany stan systemu zdefiniowany przez organizację], przy jednoczesnym zachowaniu [Realizacja: informacje o stanie systemu zdefiniowanego przez organizację]

Zabezpieczenia powiązane: CP-2, CP-4, CP-10, CP-12, SA-8, SC-7, SC-22, SI-13.

Zabezpieczenia rozszerzone: nie dotyczy.

SC-25 THIN NODES / TERMINALOWE STACJE ROBOCZE

Zabezpieczenie:

Wprowadź minimalną funkcjonalność i przechowywanie informacji w następujących komponentach systemu: [Realizacja: komponenty systemu zdefiniowane przez organizację].

Zabezpieczenia powiązane: SC-30, SC-44.

Zabezpieczenia rozszerzone: nie dotyczy.

SC-26 HONEYPOTS

Zabezpieczenie:

Uwzględnij w systemach organizacyjnych komponenty specjalnie zaprojektowane tak, aby były celem złośliwych ataków, w celu wykrywania, odpierania i analizowania takich ataków.

Zabezpieczenia powiązane: RA-5, SC-7, SC-30, SC-35, SC-44, SI-3, SI-4.

Zabezpieczenia rozszerzone:

(1) HONEYPOTS | WYKRYWANIE ZŁOŚLIWEGO KODU

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

SC-27 APLIKACJE NIEZALEŻNE OD PLATFORMY

Zabezpieczenie:

W systemach organizacyjnych uwzględnij następujące aplikacje niezależne od platformy: [Realizacja: aplikacje niezależne od platformy zdefiniowane przez organizację].

Zabezpieczenia powiązane: SC-29.

Zabezpieczenia rozszerzone: nie dotyczy.

SC-28 OCHRONA INFORMACJI W SPOCZYNKU

Zabezpieczenie:

Chroń [Wybór (jednego lub więcej): poufność; integralność] następujących informacji w spoczynku: [Realizacja: zdefiniowane przez organizację informacje w spoczynku].

Zabezpieczenia powiązane: AC-3, AC-4, AC-6, AC-19, CA-7, CM-3, CM-5, CM-6, CP-9, MP-4, MP-5, PE-3, SC-8, SC-12, SC-13, SC-34, SI-3, SI-7, SI-16.

Zabezpieczenia rozszerzone:

(1) OCHRONA INFORMACJI W SPOCZYNKU | OCHRONA KRYPTOGRAFICZNA

Wprowadź mechanizmy kryptograficzne w celu zapobiegania nieautoryzowanemu ujawnieniu i modyfikacji następujących informacji przechowywanych w [Realizacja: komponenty systemu lub nośniki zdefiniowane przez organizację]: [Realizacja: informacje zdefiniowane przez organizację].

Zabezpieczenia powiązane: AC-19, SC-12, SC-13.

(2) OCHRONA INFORMACJI W SPOCZYNKU | PRZECHOWYWANIE OFFLINE

Usuń następujące informacje z pamięci online i przechowuj je w trybie offline w bezpiecznej lokalizacji: [Realizacja: informacje zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(3) OCHRONA INFORMACJI W SPOCZYNKU | KLUCZE KRYPTOGRAFICZNE

Zapewnij bezpieczne miejsce do przechowywania kluczy kryptograficznych [Wybór: [Realizacja: zabezpieczenia zdefiniowane przez organizację]; sprzętowo chroniony magazyn kluczy].

Zabezpieczenia powiązane: SC-12, SC-13.

SC-29 HETEROGENICZNOŚĆ SYSTEMU

Zastosuj zróżnicowany zestaw technologii informatycznych dla następujących komponentów systemu podczas wdrażania systemu: [Realizacja: komponenty systemu zdefiniowane przez organizację].

Zabezpieczenia powiązane: AU-9, PL-8, SC-27, SC-30, SR-3.

Zabezpieczenia rozszerzone:

(1) HETEROGENICZNOŚĆ SYSTEMU | TECHNIKI WIRTUALIZACJI

Wdrażaj techniki wirtualizacji w celu obsługi wdrażania różnorodnych systemów operacyjnych i aplikacji, które są zmieniane [Realizacja: częstotliwość zdefiniowana przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

SC-30 MASKOWANIE I DEZINFORMACJA

Zastosuj następujące techniki ukrywania i wprowadzania w błąd dla [Realizacja: systemy zdefiniowane przez organizację] w [Realizacja: okresy czasu zdefiniowane przez organizację], aby zdezorientować i

wprowadzić przeciwników w błąd: [Realizacja: techniki ukrywania i wprowadzania w błąd zdefiniowane przez organizację].

Zabezpieczenia powiązane: AC-6, SC-25, SC-26, SC-29, SC-44, SI-14.

Zabezpieczenia rozszerzone:

(1) MASKOWANIE I DEZINFORMACJA | TECHNIKI WIRTUALIZACJI

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(2) MASKOWANIE I DEZINFORMACJA | LOSOWOŚĆ

Zastosuj [Realizacja: techniki zdefiniowane przez organizację], aby wprowadzić losowość do operacji i aktywów organizacji.

Zabezpieczenia powiązane: nie dotyczy.

(3) MASKOWANIE I DEZINFORMACJA | ZMIANA LOKALIZACJI PRZETWARZANIA I PRZECHOWYWANIA

Zmień lokalizację [Realizacja: przetwarzanie i/lub przechowywanie zdefiniowane przez organizację] [Wybór: [Realizacja: częstotliwość czasu zdefiniowana przez organizację]; w losowych odstępach czasu]].

Zabezpieczenia powiązane: nie dotyczy.

(4) MASKOWANIE I DEZINFORMACJA | INFORMACJE WPROWADZAJĄCE W BŁĄD

W [Realizacja: komponenty systemu zdefiniowane przez organizację] stosuj realistyczne, ale wprowadzające w błąd informacje na temat stanu lub postawy bezpieczeństwa.

Zabezpieczenia powiązane: nie dotyczy.

(5) MASKOWANIE I DEZINFORMACJA | UKRYWANIE KOMPONENTÓW SYSTEMU

Zastosuj następujące techniki w celu ukrycia lub zamaskowania [Realizacja: komponenty systemu zdefiniowane przez organizację]: [Realizacja: techniki zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

SC-31 ANALIZA UKRYTEGO KANAŁU KOMUNIKACJI

Zabezpieczenie:

a. Wykonaj analizę kanałów ukrytych, aby zidentyfikować te aspekty komunikacji w systemie, które są potencjalnymi drogami dla kanałów ukrytych [Wybór (jeden lub więcej): przechowywanie; czas];

b. Oszacuj maksymalną przepustowość tych kanałów.

Zabezpieczenia powiązane: Przykłady: AC-3, AC-4, SA-8, SI-11.

Zabezpieczenia rozszerzone:

(1) ANALIZA UKRYTEGO KANAŁU KOMUNIKACJI | TESTOWANIE KANAŁÓW UKRYTYCH POD KĄTEM PODATNOŚCI NA WYKORZYSTANIE

Przetestuj podzbiór zidentyfikowanych kanałów tajnych, aby określić, które z nich nadają się do wykorzystania.

Zabezpieczenia powiązane: nie dotyczy.

(2) ANALIZA UKRYTEGO KANAŁU KOMUNIKACJI | MAKSYMALNA PRZEPUSTOWOŚĆ

Zmniejsz maksymalną przepustowość dla zidentyfikowanych kanałów ukrytych [Wybór (jeden lub więcej): magazyn; czas] do [Przypisanie: wartości zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(3) ANALIZA UKRYTEGO KANAŁU KOMUNIKACJI | POMIAR PRZEPUSTOWOŚCI W ŚRODOWISKACH OPERACYJNYCH

Zmierz przepustowość [Realizacja: podzbiór zidentyfikowanych kanałów ukrytych zdefiniowany przez organizację] w środowisku operacyjnym systemu.

Zabezpieczenia powiązane: nie dotyczy.

SC-32 PARTYCJONOWANIE SYSTEMU

Zabezpieczenie:

Podziel system na [Realizacja: komponenty systemu zdefiniowane przez organizację] znajdujące się w oddzielnych [Wybór: fizyczny; logiczny] domenach lub środowiskach na podstawie [Realizacja: okoliczności zdefiniowane przez organizację dotyczące fizycznego lub logicznego oddzielenia komponentów].

Zabezpieczenia powiązane: AC-4, AC-6, SA-8, SC-2, SC-3, SC-7, SC-36.

Zabezpieczenia rozszerzone:

(1) PARTYCJONOWANIE SYSTEMU | ODDZIELNE DOMENY FIZYCZNE DLA FUNKCJI UPRZYWILEJOWANYCH

Podziel funkcje uprzywilejowane na oddzielne domeny fizyczne.

Zabezpieczenia powiązane: nie dotyczy.

SC-33 INTEGRALNOŚĆ TRANSMISJI

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

SC-34 NIEMODYFIKOWALNE PROGRAMY WYKONYWALNE

Zabezpieczenie:

W przypadku [Zadania: zdefiniowane przez organizację komponenty systemu] załaduj i wykonaj:

a. Środowisko operacyjne z wymuszonego sprzętowo, tylko do odczytu nośnika;

b. Następujące aplikacje z wymuszonego sprzętowo, tylko do odczytu nośnika: [Realizacja: zdefiniowane przez organizację aplikacje].

Zabezpieczenia powiązane: AC-3, SI-7, SI-14.

Zabezpieczenia rozszerzone:

(1) NIEMODYFIKOWALNE PROGRAMY WYKONYWALNE | BRAK MOŻLIWOŚCI ZAPISU W PAMIĘCI MASOWEJ

Zastosuj [Realizacja: zdefiniowane przez organizację komponenty systemu] bez pamięci masowej z możliwością zapisu, która jest trwała po ponownym uruchomieniu komponentu lub włączeniu/wyłączeniu zasilania.

Zabezpieczenia powiązane: AC-19 i MP-7.

(2) NIEMODYFIKOWALNE PROGRAMY WYKONYWALNE | OCHRONA INTEGRALNOŚCI NA NOŚNIKACH TYLKO DO ODCZYTU

Chroń integralność informacji przed ich zapisaniem na nośniku tylko do odczytu i kontroluj nośnik po zapisaniu na nim informacji.

Zabezpieczenia powiązane: CM-3, CM-5, CM-9, MP-2, MP-4, MP-5, SC-28, SI-3.

(3) NIEMODYFIKOWALNE PROGRAMY WYKONYWALNE | OCHRONA SPRZĘTOWA

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

SC-35 IDENTYFIKACJA ZEWNĘTRZNEGO ZŁOŚLIWEGO KODU (HONEYCLIENTS)

Zabezpieczenie:

Uwzględnij komponenty systemu, które proaktywnie starają się identyfikować złośliwy kod w sieci lub złośliwe witryny internetowe.

Zabezpieczenia powiązane: SC-7, SC-26, SC-44, SI-3, SI-4.

Zabezpieczenia rozszerzone: nie dotyczy.

SC-36 ROZPROSZONE PRZETWARZANIE I PRZECHOWYWANIE

Zabezpieczenie:

Rozłóż następujące komponenty przetwarzania i przechowywania w wielu [Wybór: lokalizacje fizyczne, domeny logiczne]: [Realizacja: komponenty przetwarzania i przechowywania zdefiniowane przez organizację].

Zabezpieczenia powiązane: CP-6, CP-7, PL-8, SC-32.

Zabezpieczenia rozszerzone:

(1) ROZPROSZONE PRZETWARZANIE I PRZECHOWYWANIE | TECHNIKI SONDOWANIA

Zabezpieczenie:

a. Zastosuj techniki sondowania w celu zidentyfikowania potencjalnych usterek, błędów lub naruszeń następujących komponentów przetwarzania i przechowywania danych: [Realizacja: komponenty rozproszonego przetwarzania i przechowywania danych zdefiniowane przez organizację]; oraz

b. Podejmij następujące działania w odpowiedzi na zidentyfikowane usterki, błędy lub naruszeń: [Realizacja: działania zdefiniowane przez organizację].

Zabezpieczenia powiązane: SI-4.

(2) ROZPROSZONE PRZETWARZANIE I PRZECHOWYWANIE | SYNCHRONIZACJA

Zsynchronizuj następujące zduplikowane systemy lub komponenty systemu: [Realizacja: zduplikowane systemy lub komponenty systemu zdefiniowane przez organizację].

Zabezpieczenia powiązane: CP-9.

SC-37 KANAŁY POZAPASMOWE

Zastosuj następujące kanały poza pasmem do fizycznego dostarczania lub elektronicznej transmisji [Realizacja: informacje zdefiniowane przez organizację, komponenty systemu lub urządzenia] do [Realizacja: osoby lub systemy zdefiniowane przez organizację]: [Realizacja: kanały poza pasmem zdefiniowane przez organizację].

Zabezpieczenia powiązane: AC-2, CM-3, CM-5, CM-7, IA-2, IA-4, IA-5, MA-4, SC-12, SI-3, SI-4, SI-7.

Zabezpieczenia rozszerzone:

(1) KANAŁY POZA PASMEM | ZAPEWNIJ DOSTARCZANIE I TRANSMISJĘ

Zastosuj [Realizacja: elementy sterujące zdefiniowane przez organizację], aby mieć pewność, że tylko [Realizacja: osoby lub systemy zdefiniowane przez organizację] otrzymają następujące informacje, komponenty systemu lub urządzenia: [Realizacja: informacje, komponenty systemu lub urządzenia zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

SC-38 BEZPIECZEŃSTWO OPERACYJNE

Zabezpieczenie:

Wdrażaj następujące kontrole bezpieczeństwa operacji, aby chronić kluczowe informacje organizacji przez cały cykl życia rozwoju systemu: [Realizacja: kontrole bezpieczeństwa operacji zdefiniowane przez organizację].

Zabezpieczenia powiązane: CA-2, CA-7, PL-1, PM-9, PM-12, RA-2, RA-3, RA-5, SC-7, SR-3, SR-7.

Zabezpieczenia rozszerzone: nie dotyczy.

SC-39 IZOLACJA PROCESU

Zabezpieczenie:

Utrzymuj oddzielną domenę wykonywania dla każdego wykonywanego procesu systemowego.

Zabezpieczenia powiązane: AC-3, AC-4, AC-6, AC-25, SA-8, SC-2, SC-3, SI-16.

Zabezpieczenia rozszerzone:

(1) IZOLACJA PROCESU | SEPARACJA SPRZĘTOWA

Wprowadź mechanizmy separacji sprzętowej w celu ułatwienia izolacji procesów.

Zabezpieczenia powiązane: nie dotyczy.

(2) IZOLACJA PROCESÓW | ODDZIELNA DOMENA WYKONANIA NA WĄTEK

Utrzymuj oddzielną domenę wykonywania dla każdego wątku w [Realizacja: przetwarzanie wielowątkowe zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

SC-40 OCHRONA ŁĄCZA BEZPRZEWODOWEGO

Zabezpieczenie:

Chroń zewnętrzne i wewnętrzne [Realizacja: łącza bezprzewodowe zdefiniowane przez organizację] przed następującymi atakami na parametry sygnału: [Realizacja: typy ataków na parametry sygnału zdefiniowane przez organizację lub odwołania do źródeł takich ataków].

Zabezpieczenia powiązane: AC-18, SC-5.

Zabezpieczenia rozszerzone:

(1) OCHRONA ŁĄCZA BEZPRZEWODOWEGO | ZAKŁÓCENIA ELEKTROMAGNETYCZNE

Wprowadź mechanizmy kryptograficzne, które zapewnią [Realizacja: poziom ochrony zdefiniowany przez organizację] przed skutkami celowych zakłóceń elektromagnetycznych.

Zabezpieczenia powiązane: PE-21, SC-12, SC-13.

(2) OCHRONA ŁĄCZA BEZPRZEWODOWEGO | ZMNIEJSZENIE POTENCJAŁU WYKRYWANIA

Wprowadź mechanizmy kryptograficzne w celu zmniejszenia możliwości wykrycia łączy bezprzewodowych do [Realizacja: poziom redukcji określony przez organizację].

Zabezpieczenia powiązane: SC-12, SC-13.

(3) OCHRONA ŁĄCZA BEZPRZEWODOWEGO | OSZUSTWO KOMUNIKACYJNE IMITACYJNE LUB MANIPULACYJNE

Wprowadź mechanizmy kryptograficzne w celu identyfikacji i odrzucania transmisji bezprzewodowych stanowiących celowe próby imitacji lub manipulacji komunikatami opartymi na parametrach sygnału.

Zabezpieczenia powiązane: SC-12, SC-13, SI-4.

(4) OCHRONA ŁĄCZA BEZPRZEWODOWEGO | IDENTYFIKACJA PARAMETRÓW SYGNAŁU

Wprowadź mechanizmy kryptograficzne w celu uniemożliwienia identyfikacji [Realizacja: nadajniki bezprzewodowe zdefiniowane przez organizację] przy użyciu parametrów sygnału nadajnika.

Zabezpieczenia powiązane: SC-12, SC-13.

SC-41 DOSTĘP DO PORTU I URZĄDZENIA WEJŚCIA / WYJŚCIA

Zabezpieczenie:

[Wybór: Fizycznie; Logicznie] wyłącz lub usuń [Realizacja: zdefiniowane przez organizację porty połączeń lub urządzenia wejścia/wyjścia] w następujących systemach lub komponentach systemu: [Realizacja: zdefiniowane przez organizację systemy lub komponenty systemu].

Zabezpieczenia powiązane: AC-20, MP-7.

Zabezpieczenia rozszerzone: nie dotyczy.

SC-42 FUNKCJONALNOŚCI I DANE CZUJNIKÓW

Zabezpieczenie:

a. Zabroń [Wybór (jednego lub więcej): używania urządzeń posiadających [Realizacja: zdefiniowane przez organizację zdolności wykrywania środowiska] w [Realizacja: zdefiniowane przez organizację obiekty, obszary lub systemy]; zdalnej aktywacji zdolności wykrywania środowiska w systemach organizacyjnych lub komponentach systemu z następującymi wyjątkami: [Realizacja: zdefiniowane przez organizację wyjątki, w których zdalna aktywacja czujników jest dozwolona]]; i

b. Zapewnij wyraźne wskazanie użycia czujnika dla [Realizacja: zdefiniowanej przez organizację grupy użytkowników].

Zabezpieczenia powiązane: SC-15.

Zabezpieczenia rozszerzone:

(1) FUNKCJONALNOŚCI I DANE CZUJNIKÓW | RAPORTOWANIE DO UPOWAŻNIONYCH OSÓB LUB RÓL

Sprawdź, czy system jest skonfigurowany w taki sposób, że dane lub informacje zbierane przez [Realizacja: czujniki zdefiniowane przez organizację] są przekazywane wyłącznie upoważnionym osobom lub rolom.

Zabezpieczenia powiązane: nie dotyczy.

(2) FUNKCJONALNOŚCI I DANE CZUJNIKÓW | AUTORYZOWANE UŻYCIE

Należy zastosować następujące środki, aby dane lub informacje zbierane przez [Realizacja: czujniki zdefiniowane przez organizację] były wykorzystywane wyłącznie do autoryzowanych celów: [Realizacja: środki zdefiniowane przez organizację].

Zabezpieczenia powiązane: PT-2.

(3) FUNKCJONALNOŚCI I DANE CZUJNIKÓW | ZAKAZ UŻYWANIA URZĄDZEŃ

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(4) FUNKCJONALNOŚCI I DANE CZUJNIKÓW | POWIADOMIENIE O GROMADZENIU

Zastosuj następujące środki, aby ułatwić danej osobie uświadomienie sobie, że dane identyfikujące ją są gromadzone przez [Realizacja: czujniki zdefiniowane przez organizację]: [Realizacja: środki zdefiniowane przez organizację].

Zabezpieczenia powiązane: PT-1, PT-4, PT-5.

(5) FUNKCJONALNOŚCI I DANE CZUJNIKÓW | MINIMALIZACJA GROMADZENIA DANYCH

Zastosuj [Realizacja: czujniki zdefiniowane przez organizację] skonfigurowane w taki sposób, aby zminimalizować gromadzenie niepotrzebnych informacji o osobach.

Zabezpieczenia powiązane: SA-8, SI-12.

SC-43 OGRANICZENIA UŻYTKOWANIA

Zabezpieczenie:

a. Wprowadź ograniczenia użytkowania i wytyczne dotyczące wdrażania dla następujących komponentów systemu: [Realizacja: komponenty systemu zdefiniowane przez organizację]; i

b. Autoryzuj, monitoruj i kontroluj użytkowanie takich komponentów w systemie.

Zabezpieczenia powiązane: AC-18, AC-19, CM-6, SC-7, SC-18.

Zabezpieczenia rozszerzone: nie dotyczy.

SC-44 KOMORY DETONACYJNE

Zabezpieczenie:

Zastosuj komorę detonacyjną w [Realizacja: system zdefiniowany przez organizację, komponent systemu lub lokalizacja].

Zabezpieczenia powiązane: SC-7, SC-18, SC-25, SC-26, SC-30, SC-35, SC-39, SI-3, SI-7.

Zabezpieczenia rozszerzone: nie dotyczy.

SC-45 SYNCHRONIZACJA CZASU SYSTEMOWEGO

Zabezpieczenie:

Synchronizacja zegarów systemowych w obrębie systemów i pomiędzy systemami oraz ich komponentami.

Zabezpieczenia powiązane: AC-3, AU-8, IA-2, IA-8.

Zabezpieczenia rozszerzone:

(1) SYNCHRONIZACJA CZASU SYSTEMOWEGO | SYNCHRONIZACJA Z AUTORYTATYWNYM ŹRÓDŁEM CZASU

a. Porównaj wewnętrzne zegary systemowe [Realizacja: częstotliwość zdefiniowana przez organizację] z [Realizacja: źródło czasu zdefiniowane przez organizację]; i

b. Zsynchronizuj wewnętrzne zegary systemowe z autorytatywnym źródłem czasu, gdy różnica czasu jest większa niż [Realizacja: okres czasu zdefiniowany przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(2) SYNCHRONIZACJA CZASU SYSTEMOWEGO | DRUGORZĘDNE AUTORYTATYWNE ŹRÓDŁO CZASU

a. Zidentyfikuj drugorzędne wiarygodne źródło czasu, które znajduje się w innym regionie geograficznym niż główne wiarygodne źródło czasu;

b. Zsynchronizuj wewnętrzne zegary systemowe z drugorzędnym wiarygodnym źródłem czasu, jeśli główne wiarygodne źródło czasu jest niedostępne.

Zabezpieczenia powiązane: nie dotyczy.

SC-46 EGZEKWOWANIE POLITYKI MIĘDZY DOMENAMI

Zabezpieczenie:

Wprowadź mechanizm egzekwowania zasad [Wybór: fizycznie; logicznie] pomiędzy interfejsami fizycznymi i/lub sieciowymi dla łączących się domen zabezpieczeń.

Zabezpieczenia powiązane: AC-4, SC-7.

Zabezpieczenia rozszerzone: nie dotyczy.

SC-47 ALTERNATYWNE ŚCIEŻKI KOMUNIKACJI

Zabezpieczenie:

Wprowadź [Realizacja: alternatywne ścieżki komunikacji zdefiniowane przez organizację] w celu zapewnienia dowodzenia i kontroli organizacyjnej nad operacjami systemowymi.

Zabezpieczenia powiązane: CP-2, CP-8.

Zabezpieczenia rozszerzone: nie dotyczy.

SC-48 PRZENIESIENIE CZUJNIKA

Zabezpieczenie:

Przenieś [Realizacja: czujniki i możliwości monitorowania zdefiniowane przez organizację] do [Realizacja: lokalizacje zdefiniowane przez organizację] w następujących warunkach lub okolicznościach: [Realizacja: warunki lub okoliczności zdefiniowane przez organizację].

Zabezpieczenia powiązane: AU-2, SC-7, SI-4.

Zabezpieczenia rozszerzone:

(1) PRZENIESIENIE CZUJNIKA | DYNAMICZNE PRZENOSZENIE CZUJNIKÓW LUB MOŻLIWOŚCI MONITOROWANIA

Dynamicznie przenieś [Realizacja: czujniki i możliwości monitorowania zdefiniowane przez organizację] do [Realizacja: lokalizacje zdefiniowane przez organizację] w następujących warunkach lub okolicznościach: [Realizacja: warunki lub okoliczności zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

SC-49 SEPARACJA WYMUSZONA SPRZĘTOWO I EGZEKWOWANIE ZASAD

Zabezpieczenie:

Wprowadź mechanizmy separacji wymuszanych sprzętowo i egzekwowania zasad pomiędzy [Realizacja: domenami zabezpieczeń zdefiniowanymi przez organizację].

Zabezpieczenia powiązane: AC-4, SA-8, SC-50.

Zabezpieczenia rozszerzone: nie dotyczy.

SC-50 SEPARACJA WYMUSZANA PROGRAMOWO I EGZEKWOWANIE ZASAD

Zabezpieczenie:

Wprowadź mechanizmy separacji wymuszane programowo i egzekwowania zasad pomiędzy [Realizacja: domenami bezpieczeństwa zdefiniowanymi przez organizację].

Zabezpieczenia powiązane: AC-3, AC-4, SA-8, SC-2, SC-3, SC-49.

Zabezpieczenia rozszerzone: nie dotyczy.

SC-51 OCHRONA OPARTA NA SPRZĘCIE

Zabezpieczenie:

a. Zastosuj sprzętową ochronę zapisu dla [Realizacja: zdefiniowane przez organizację komponenty oprogramowania układowego];

b. Wprowadź określone procedury dla [Realizacja: zdefiniowane przez organizację upoważnione osoby], aby ręcznie wyłączyć sprzętową ochronę zapisu dla modyfikacji oprogramowania układowego i ponownie włączyć ochronę zapisu przed powrotem do trybu operacyjnego.

Zabezpieczenia powiązane: nie dotyczy.

Zabezpieczenia rozszerzone: nie dotyczy.

KATEGORIA: SI - INTEGRALNOŚĆ SYSTEMU I INFORMACJI

SI-1 POLITYKA I PROCEDURY

Zabezpieczenie:

a. Opracuj, udokumentuj i rozpowszechnij wśród [Realizacja: personel lub role zdefiniowane przez organizację]:

    1. [Wybór (jeden lub więcej): Poziom organizacji; Poziom misji/procesu biznesowego; Poziom systemu] politykę integralności systemu i informacji, która:

        (a) dotyczy celu, zakresu, ról, obowiązków, zaangażowania kierownictwa, koordynacji między jednostkami organizacyjnymi i zgodności;

        (b) jest zgodna z obowiązującymi przepisami prawa, rozporządzeniami wykonawczymi, dyrektywami, regulacjami, politykami, standardami i wytycznymi;

    2. Procedury ułatwiające wdrażanie polityki integralności systemu i informacji oraz powiązanych kontroli integralności systemu i informacji;

b. Wyznacz [Realizacja: urzędnika zdefiniowanego przez organizację] do zarządzania opracowywaniem, dokumentowaniem i rozpowszechnianiem polityki i procedur integralności systemu i informacji;

c. Przeglądaj i aktualizuj na bieżąco integralność systemu i informacji w:

    1. Polityce [Realizacja: częstotliwość zdefiniowana przez organizację] i następujących [Realizacja: zdarzenia zdefiniowane przez organizację];

2. Procedurach [Realizacja: częstotliwość zdefiniowana przez organizację] i następujących po nich [Realizacja: zdarzenia zdefiniowane przez organizację].

Zabezpieczenia powiązane: PM-9, PS-8, SA-8, SI-12.

Zabezpieczenia rozszerzone: nie dotyczy.

SI-2 NAPRAWA USTEREK

Zabezpieczenie:

a. Identyfikuj, zgłaszaj i koryguj wady systemu;

b. Testuj aktualizacje oprogramowania i oprogramowania sprzętowego związane z usuwaniem wad pod kątem skuteczności i potencjalnych skutków ubocznych przed instalacją;

c. Instaluj istotne dla bezpieczeństwa aktualizacje oprogramowania i oprogramowania sprzętowego w ciągu [Realizacja: okres czasu zdefiniowany przez organizację] od wydania aktualizacji;

d. Włącz usuwanie wad do procesu zarządzania konfiguracją organizacji.

Zabezpieczenia powiązane: CA-5, CM-3, CM-4, CM-5, CM-6, CM-8, MA-2, RA-5, SA-8, SA-10, SA-11, SI-3, SI-5, SI-7, SI-11.

Zabezpieczenia rozszerzone:

(1) NAPRAWA USTEREK | CENTRALNE ZARZĄDZANIE

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(2) NAPRAWA USTEREK | ZAUTOMATYZOWANY STATUS NAPRAWY USTEREK

Określ, czy w komponentach systemu zainstalowano odpowiednie aktualizacje oprogramowania i oprogramowania sprzętowego związane z bezpieczeństwem, korzystając z [Realizacja: zautomatyzowane mechanizmy zdefiniowane przez organizację] [Realizacja: częstotliwość zdefiniowana przez organizację].

Zabezpieczenia powiązane: CA-7, SI-4.

(3) NAPRAWA USTEREK | CZAS NA NAPRAWĘ USTEREK I PUNKTY ODNIESIENIA DLA DZIAŁAŃ KORYGUJĄCYCH

(a) Zmierz czas między wykryciem wady a jej usunięciem;

(b) Ustal następujące punkty odniesienia dla podejmowania działań korygujących: [Realizacja: punkty odniesienia zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(4) NAPRAWA USTEREK | ZAUTOMATYZOWANE NARZĘDZIA DO ZARZĄDZANIA POPRAWKAMI

Wdrażaj zautomatyzowane narzędzia do zarządzania poprawkami, aby ułatwić usuwanie usterek w następujących komponentach systemu: [Realizacja: komponenty systemu zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(5) NAPRAWA USTEREK | AUTOMATYCZNE AKTUALIZACJE OPROGRAMOWANIA I OPROGRAMOWANIA SPRZĘTOWEGO

Zainstaluj [Realizacja: zdefiniowane przez organizację aktualizacje oprogramowania i oprogramowania sprzętowego istotne z punktu widzenia bezpieczeństwa] automatycznie w [Realizacja: zdefiniowane przez organizację komponenty systemu].

Zabezpieczenia powiązane: nie dotyczy.

(6) NAPRAWA USTEREK | USUWANIE POPRZEDNICH WERSJI OPROGRAMOWANIA I OPROGRAMOWANIA SPRZĘTOWEGO

Usuń poprzednie wersje [Realizacja: zdefiniowane przez organizację komponenty oprogramowania i oprogramowania sprzętowego] po zainstalowaniu zaktualizowanych wersji.

Zabezpieczenia powiązane: nie dotyczy.

SI-3 OCHRONA PRZED ZŁOŚLIWYM KODEM

Zabezpieczenie:

a. Wprowadź [Wybór (jeden lub więcej): oparty na sygnaturach; nieoparty na sygnaturach] mechanizm ochrony przed złośliwym kodem w punktach wejścia i wyjścia systemu w celu wykrywania i eliminowania złośliwego kodu;

b. Automatycznie aktualizuj mechanizmy ochrony przed złośliwym kodem w miarę dostępności nowych wersji zgodnie z polityką i procedurami zarządzania konfiguracją organizacji;

c. Skonfiguruj mechanizmy ochrony przed złośliwym kodem w celu:

    1. Przeprowadzać okresowe skany systemu [Realizacja: częstotliwość zdefiniowana przez organizację] i skanowania plików ze źródeł zewnętrznych w czasie rzeczywistym w [Wybór (jeden lub więcej): punkcie końcowym; punktach wejścia i wyjścia sieci], gdy pliki są pobierane, otwierane lub wykonywane zgodnie z polityką organizacji;

    2. [Wybór (jeden lub więcej): blokowanie złośliwego kodu; kwarantanny złośliwego kodu; podejmowanie [Realizacja: działania zdefiniowanego przez organizację]]; i wysyłanie alertów do [Realizacja: personelu lub ról zdefiniowanych przez organizację] w odpowiedzi na wykrycie złośliwego kodu;

d. Rozwiąż problem otrzymywania fałszywych alarmów podczas wykrywania i eliminowania złośliwego kodu oraz wynikającego z tego potencjalnego wpływu na dostępność systemu.

Zabezpieczenia powiązane: AC-4, AC-19, CM-3, CM-8, IR-4, MA-3, MA-4, PL-9, RA-5, SC-7, SC-23, SC-26, SC-28, SC-44, SI-2, SI-4, SI-7, SI-8, SI-15.

Zabezpieczenia rozszerzone:

(1) OCHRONA PRZED ZŁOŚLIWYM KODEM | CENTRALNE ZARZĄDZANIE

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(2) OCHRONA PRZED ZŁOŚLIWYM KODEM | AUTOMATYCZNE AKTUALIZACJE

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(3) OCHRONA PRZED ZŁOŚLIWYM KODEM | UŻYTKOWNICY BEZ UPRAWNIEŃ

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(4) OCHRONA PRZED ZŁOŚLIWYM KODEM | AKTUALIZACJE TYLKO DLA UŻYTKOWNIKÓW UPRZYWILEJOWANYCH

Aktualizuj mechanizmy ochrony przed złośliwym kodem wyłącznie na polecenie uprawnionego użytkownika.

Zabezpieczenia powiązane: CM-5.

(5) OCHRONA PRZED ZŁOŚLIWYM KODEM | URZĄDZENIA PAMIĘCI MASOWEJ PRZENOŚNEJ

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(6) OCHRONA PRZED ZŁOŚLIWYM KODEM | TESTOWANIE I WERYFIKACJA

(a) Przetestuj mechanizmy ochrony przed złośliwym kodem [Realizacja: częstotliwość określona przez organizację], wprowadzając do systemu znany, łagodny kod;

(b) Zweryfikuj, czy wykrycie kodu i zgłoszenie powiązanego incydentu nastąpiło.

Zabezpieczenia powiązane: CA-2, CA-7, RA-5.

(7) OCHRONA PRZED ZŁOŚLIWYM KODEM | WYKRYWANIE NIEOPARTE NA SYGNATURACH

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(8) OCHRONA PRZED ZŁOŚLIWYM KODEM | WYKRYWANIE NIEAUTORYZOWANYCH POLECEŃ

a. Wykryj następujące nieautoryzowane polecenia systemu operacyjnego za pomocą interfejsu programowania aplikacji jądra na [Realizacja: zdefiniowane przez organizację komponenty sprzętowe systemu]: [Realizacja: zdefiniowane przez organizację nieautoryzowane polecenia systemu operacyjnego];

b. [Wybór (jednego lub więcej): wyświetl ostrzeżenie; sprawdź wykonanie polecenia; zapobiegnij wykonaniu polecenia].

Zabezpieczenia powiązane: AU-2, AU-6, AU-12.

(9) OCHRONA PRZED ZŁOŚLIWYM KODEM | UWIERZYTELNIANIE POLECEŃ ZDALNYCH

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(10) OCHRONA PRZED ZŁOŚLIWYM KODEM | ANALIZA ZŁOŚLIWEGO KODU

a. Zastosuj następujące narzędzia i techniki w celu analizy cech i zachowania złośliwego kodu: [Realizacja: narzędzia i techniki zdefiniowane przez organizację];

b. Włącz wyniki analizy złośliwego kodu do procesów reagowania na incydenty i usuwania wad w organizacji.

Zabezpieczenia powiązane: nie dotyczy.

SI-4 MONITOROWANIE SYSTEMU

Zabezpieczenie:

a. Monitoruj system w celu wykrycia:

    1. Ataków i wskaźników potencjalnych ataków zgodnie z następującymi celami monitorowania: [Realizacja: cele monitorowania zdefiniowane przez organizację];

    2. Nieautoryzowanych połączeń lokalnych, sieciowych i zdalnych;

b. Identyfikuj nieautoryzowane użycie systemu za pomocą następujących technik i metod: [Realizacja: techniki i metody zdefiniowane przez organizację];

c. Wywołuj wewnętrzne możliwości monitorowania lub wdrażaj urządzenia monitorujące:

    1. Strategicznie w systemie w celu zbierania istotnych informacji określonych przez organizację;

    2. W doraźnych lokalizacjach w systemie w celu śledzenia określonych typów transakcji interesujących organizację;

d. Analizuj wykryte zdarzenia i anomalie;

e. Dostosowuj poziom aktywności monitorowania systemu w przypadku zmiany ryzyka dla operacji i aktywów organizacji, osób, innych organizacji lub Państwa;

f. Uzyskaj opinię prawną dotyczącą działań monitorowania systemu;

g. Przekaż [Realizacja: informacje o monitorowaniu systemu zdefiniowane przez organizację] [Realizacja: personel lub role zdefiniowane przez organizację] [Wybór (jeden lub więcej): w razie potrzeby; [Realizacja: częstotliwość zdefiniowana przez organizację]].

Zabezpieczenia powiązane: AC-2, AC-3, AC-4, AC-8, AC-17, AU-2, AU-6, AU-7, AU-9, AU-12, AU-13, AU-14, CA-7, CM-3, CM-6, CM-8, CM-11, IA-10, IR-4, MA-3, MA-4, PL-9, PM-12, RA-5, RA-10, SC-5, SC-7, SC-18, SC-26, SC-31, SC-35, SC-36, SC-37, SC-43, SI-3, SI-6, SI-7, SR-9, SR-10.

Zabezpieczenia rozszerzone:

(1) MONITOROWANIE SYSTEMU | SYSTEM WYKRYWANIA WŁAMAŃ W CAŁYM SYSTEMIE

Połącz i skonfiguruj poszczególne narzędzia do wykrywania włamań, tworząc system wykrywania włamań obejmujący cały system.

Zabezpieczenia powiązane: nie dotyczy.

(2) MONITOROWANIE SYSTEMU | ZAUTOMATYZOWANE NARZĘDZIA I MECHANIZMY DO ANALIZY W CZASIE RZECZYWISTYM

Stosuj zautomatyzowane narzędzia i mechanizmy wspomagające analizę zdarzeń w czasie zbliżonym do rzeczywistego.

Zabezpieczenia powiązane: PM-23, PM-25.

(3) MONITOROWANIE SYSTEMU | ZAUTOMATYZOWANA INTEGRACJA NARZĘDZI I MECHANIZMÓW

Wdrażaj zautomatyzowane narzędzia i mechanizmy w celu zintegrowania narzędzi i mechanizmów wykrywania włamań z mechanizmami kontroli dostępu i kontroli przepływu.

Zabezpieczenia powiązane: PM-23, PM-25.

(4) MONITOROWANIE SYSTEMU | RUCH KOMUNIKACYJNY PRZYCHODZĄCY I WYCHODZĄCY

(a) Określ kryteria nietypowych lub nieautoryzowanych działań lub warunków dla ruchu komunikacyjnego przychodzącego i wychodzącego;

(b) Monitoruj ruch komunikacyjny przychodzący i wychodzący [Realizacja: częstotliwość zdefiniowana przez organizację] pod kątem [Realizacja: nietypowych lub nieautoryzowanych działań lub warunków zdefiniowanych przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(5) MONITOROWANIE SYSTEMU | ALERTY GENEROWANE PRZEZ SYSTEM

Wyślij alert [Realizacja: personel lub role zdefiniowane w organizacji], gdy wystąpią następujące wygenerowane przez system wskazania zagrożenia lub potencjalnego zagrożenia: [Realizacja: wskaźniki zagrożenia zdefiniowane w organizacji].

Zabezpieczenia powiązane: AU-4, AU-5, PE-6.

(6) MONITOROWANIE SYSTEMU | OGRANICZANIE UŻYTKOWNIKÓW BEZ UPRAWNIEŃ

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(7) MONITOROWANIE SYSTEMU | AUTOMATYCZNA REAKCJA NA PODEJRZANE ZDARZENIA

(a) Powiadom [Realizacja: personel reagowania na incydenty określony przez organizację (określony według nazwiska i/lub roli)] o wykrytych podejrzanych zdarzeniach;

(b) Podejmij następujące działania po wykryciu: [Realizacja: działania najmniej zakłócające określone przez organizację w celu zakończenia podejrzanych zdarzeń].

Zabezpieczenia powiązane: nie dotyczy.

(8) MONITOROWANIE SYSTEMU | OCHRONA INFORMACJI MONITOROWANYCH

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(9) MONITOROWANIE SYSTEMU | TESTOWANIE NARZĘDZI I MECHANIZMÓW MONITORUJĄCYCH

Przetestuj narzędzia i mechanizmy monitorowania włamań [Realizacja: częstotliwość określona przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(10) MONITOROWANIE SYSTEMU | WIDOCZNOŚĆ SZYFROWANEJ KOMUNIKACJI

Podejmij działania, aby [Realizacja: zaszyfrowany ruch komunikacyjny zdefiniowany przez organizację] był widoczny dla [Realizacja: narzędzia i mechanizmy monitorowania systemu zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(11) MONITOROWANIE SYSTEMU | ANALIZA ANOMALII RUCHU KOMUNIKACYJNEGO

Przeanalizuj ruch komunikacji wychodzącej na interfejsach zewnętrznych systemu i wybranych [Realizacja: zdefiniowane przez organizację punkty wewnętrzne w systemie] w celu wykrycia anomalii.

Zabezpieczenia powiązane: nie dotyczy.

(12) MONITOROWANIE SYSTEMU | AUTOMATYCZNE ALERTY GENEROWANE PRZEZ ORGANIZACJĘ

Wyślij alert [Realizacja: personel lub role zdefiniowane przez organizację] za pomocą [Realizacja: zautomatyzowane mechanizmy zdefiniowane przez organizację], gdy wystąpią następujące oznaki niewłaściwych lub nietypowych działań mających wpływ na bezpieczeństwo lub prywatność: [Realizacja: działania zdefiniowane przez organizację, które wyzwalają alerty].

Zabezpieczenia powiązane: nie dotyczy.

(13) MONITOROWANIE SYSTEMU | ANALIZA WZORCÓW RUCHU I ZDARZEŃ

a. Analizuj ruch komunikacyjny i wzorce zdarzeń dla systemu;

b. Twórz profile reprezentujące typowe wzorce ruchu i zdarzeń;

c. Wykorzystaj profile ruchu i zdarzeń do dostrajania urządzeń monitorujących system.

Zabezpieczenia powiązane: nie dotyczy.

(14) MONITOROWANIE SYSTEMU | WYKRYWANIE WŁAMAŃ BEZPRZEWODOWYCH

Wdróż bezprzewodowy system wykrywania włamań w celu identyfikacji nieautoryzowanych urządzeń bezprzewodowych i wykrywania prób ataków oraz potencjalnych naruszeń bezpieczeństwa systemu.

Zabezpieczenia powiązane: AC-18, IA-3.

(15) MONITOROWANIE SYSTEMU | KOMUNIKACJA BEZPRZEWODOWA DO PRZEWODOWEJ

Wprowadź system wykrywania włamań w celu monitorowania ruchu komunikacji bezprzewodowej w trakcie jego przekazywania z sieci bezprzewodowych do przewodowych.

Zabezpieczenia powiązane: AC-18.

(16) MONITOROWANIE SYSTEMU | POWIĄZANIE INFORMACJI O MONITOROWANIU

Porównuj informacje pochodzące z narzędzi monitorujących i mechanizmów stosowanych w całym systemie.

Zabezpieczenia powiązane: AU-6.

(17) MONITOROWANIE SYSTEMU | ZINTEGROWANA ŚWIADOMOŚĆ SYTUACYJNA

Powiąż informacje pochodzące z monitoringu aktywności fizycznej, cyfrowych i łańcucha dostaw, aby uzyskać zintegrowaną świadomość sytuacyjną w całej organizacji.

Zabezpieczenia powiązane: AU-16, PE-6, SR-2, SR-4, SR-6.

(18) MONITOROWANIE SYSTEMU | ANALIZA RUCHU I UKRYTEJ EKSFILTRACJI

Przeprowadź analizę ruchu komunikacji wychodzącej na zewnętrznych interfejsach systemu oraz w następujących punktach wewnętrznych w celu wykrycia ukrytego wycieku informacji: [Realizacja: zdefiniowane przez organizację punkty wewnętrzne w systemie].

Zabezpieczenia powiązane: nie dotyczy.

(19) MONITOROWANIE SYSTEMU | RYZYKO DLA OSÓB FIZYCZNYCH

Wyróżnij [Realizacja: dodatkowy monitoring zdefiniowany przez organizację] osoby, które zostały zidentyfikowane przez [Realizacja: źródła zdefiniowane przez organizację] jako osoby stwarzające zwiększony poziom ryzyka.

Zabezpieczenia powiązane: nie dotyczy.

(20) MONITOROWANIE SYSTEMU | UŻYTKOWNICY UPRZYWILEJOWANI

Wprowadź następujące dodatkowe monitorowanie użytkowników uprzywilejowanych: [Realizacja: dodatkowe monitorowanie zdefiniowane przez organizację].

Zabezpieczenia powiązane: AC-18.

(21) MONITOROWANIE SYSTEMU | OKRESY PRÓBNE

Wprowadź następujące dodatkowe monitorowania osób w trakcie [Realizacja: okres próbny określony przez organizację]: [Realizacja: dodatkowy monitoring określony przez organizację].

Zabezpieczenia powiązane: AC-18.

(22) MONITOROWANIE SYSTEMU | NIEAUTORYZOWANE USŁUGI SIECIOWE

a. Wykryj usługi sieciowe, które nie zostały autoryzowane lub zatwierdzone przez [Realizacja: zdefiniowane przez organizację procesy autoryzacji lub zatwierdzania];

b. [Wybór (jeden lub więcej): Audyt; Alert [Realizacja: zdefiniowany przez organizację personel lub role]] w przypadku wykrycia.

Zabezpieczenia powiązane: CM-7.

(23) MONITOROWANIE SYSTEMU | URZĄDZENIA HOSTOWE

Wdróż następujące mechanizmy monitorowania hostów w [Realizacja: komponenty systemu zdefiniowane przez organizację]: [Realizacja: mechanizmy monitorowania hostów zdefiniowane przez organizację].

Zabezpieczenia powiązane: AC-18, AC-19.

(24) MONITOROWANIE SYSTEMU | WSKAŹNIKI ZAGROŻENIA

Zidentyfikuj, zbierz i przekaż [Realizacja: personelowi lub rolom zdefiniowanym przez organizację] wskaźniki zagrożenia dostarczone przez [Realizacja: źródła zdefiniowane przez organizację].

Zabezpieczenia powiązane: AC-18.

(25) MONITOROWANIE SYSTEMU | OPTYMALIZACJA ANALIZY RUCHU SIECIOWEGO

Zapewnij widoczność ruchu sieciowego na zewnętrznych i kluczowych wewnętrznych interfejsach systemowych, aby zoptymalizować skuteczność urządzeń monitorujących.

Zabezpieczenia powiązane: nie dotyczy.

SI-5 ALERTY BEZPIECZEŃSTWA, PORADY I DYREKTYWY

Zabezpieczenie:

a. Otrzymuj alerty bezpieczeństwa systemu, porady i dyrektywy od [Realizacja: zewnętrzne organizacje zdefiniowane przez organizację] na bieżąco;

b. Generuj wewnętrzne alerty bezpieczeństwa, porady i dyrektywy, jeśli uznasz to za konieczne;

c. Rozsyłaj alerty bezpieczeństwa, porady i dyrektywy do: [Wybór (jeden lub więcej): [Realizacja: personel lub role zdefiniowane przez organizację]; [Realizacja: elementy zdefiniowane przez organizację w organizacji]; [Realizacja: zewnętrzne organizacje zdefiniowane przez organizację]];

d. Wdrażaj dyrektywy bezpieczeństwa zgodnie z ustalonymi ramami czasowymi lub powiadamiaj organizację wydającą o stopniu niezgodności.

Zabezpieczenia powiązane: PM-15, RA-5, SI-2.

Zabezpieczenia rozszerzone:

(1) ALERTY BEZPIECZEŃSTWA, PORADY I DYREKTYWY | AUTOMATYCZNE ALERTY I PORADY

Rozsyłaj alerty bezpieczeństwa i informacje doradcze w całej organizacji, korzystając z [Realizacja: zautomatyzowane mechanizmy zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

SI-6 WERYFIKACJA FUNKCJI BEZPIECZEŃSTWA I PRYWATNOŚCI

Zabezpieczenie:

a. Zweryfikuj prawidłowe działanie [Realizacja: funkcje bezpieczeństwa i prywatności zdefiniowane przez organizację];

b. Przeprowadź weryfikację funkcji określonych w SI-6a [Wybór (jeden lub więcej): [Realizacja: stany przejściowe systemu zdefiniowane przez organizację]; na polecenie użytkownika z odpowiednimi uprawnieniami; [Realizacja: częstotliwość zdefiniowana przez organizację]];

c. Powiadom [Realizacja: personel lub role zdefiniowane przez organizację] o nieudanych testach weryfikacji bezpieczeństwa i prywatności;

d. [Wybór (jeden lub więcej): Zamknij system; Uruchom ponownie system; [Realizacja: alternatywne działania zdefiniowane przez organizację]] w przypadku wykrycia anomalii.

Zabezpieczenia powiązane:

Przykłady zastosowań: CA-7, CM-4, CM-6, SI-7.

Zabezpieczenia rozszerzone:

(1) WERYFIKACJA FUNKCJI BEZPIECZEŃSTWA I PRYWATNOŚCI | POWIADOMIENIE O NIEUDANYCH TESTACH BEZPIECZEŃSTWA

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(2) WERYFIKACJA FUNKCJI BEZPIECZEŃSTWA I PRYWATNOŚCI | OBSŁUGA AUTOMATYZACJI DLA ROZPROSZONYCH TESTÓW

Wprowadź zautomatyzowane mechanizmy wspomagające zarządzanie rozproszonym testowaniem funkcji bezpieczeństwa i prywatności.

Zabezpieczenia powiązane: SI-2.

(3) WERYFIKACJA FUNKCJI BEZPIECZEŃSTWA I PRYWATNOŚCI | RAPORTUJ WYNIKI WERYFIKACJI

Zgłoś wyniki weryfikacji funkcji bezpieczeństwa i prywatności do [Realizacja: personel lub role zdefiniowane w organizacji].

Zabezpieczenia powiązane: SI-4, SR-4, SR-5.

SI-7 OPROGRAMOWANIE, OPROGRAMOWANIE SPRZĘTOWE I INTEGRALNOŚĆ INFORMACJI

Zabezpieczenie:

a. Stosuj narzędzia weryfikacji integralności w celu wykrywania nieautoryzowanych zmian w następującym oprogramowaniu, oprogramowaniu sprzętowym i informacjach: [Realizacja: oprogramowanie, oprogramowanie sprzętowe i informacje zdefiniowane przez organizację];

b. Podejmuj następujące działania w przypadku wykrycia nieautoryzowanych zmian w oprogramowaniu, oprogramowaniu sprzętowym i informacjach: [Realizacja: działania zdefiniowane przez organizację].

Zabezpieczenia powiązane: AC-4, CM-3, CM-7, CM-8, MA-3, MA-4, RA-5, SA-8, SA-9, SA-10, SC-8, SC-12, SC-13, SC-28, SC-37, SI-3, SR-3, SR-4, SR-5, SR-6, SR-9, SR-10, SR-11.

Zabezpieczenia rozszerzone:

(1) OPROGRAMOWANIE, OPROGRAMOWANIE SPRZĘTOWE I INTEGRALNOŚĆ INFORMACJI | KONTROLE INTEGRALNOŚCI

Wykonaj kontrolę integralności [Realizacja: zdefiniowane przez organizację oprogramowanie, oprogramowanie sprzętowe i informacje] [Wybór (jeden lub więcej): podczas uruchamiania; w [Realizacja: zdefiniowane przez organizację stany przejściowe lub zdarzenia istotne z punktu widzenia bezpieczeństwa]; [Realizacja: częstotliwość zdefiniowana przez organizację]].

Zabezpieczenia powiązane: nie dotyczy.

(2) OPROGRAMOWANIE, OPROGRAMOWANIE SPRZĘTOWE I INTEGRALNOŚĆ INFORMACJI | AUTOMATYCZNE POWIADOMIENIA O NARUSZENIACH INTEGRALNOŚCI

Zastosuj zautomatyzowane narzędzia, które powiadamiają [Realizacja: personel lub role zdefiniowane w organizacji] w przypadku wykrycia nieprawidłowości podczas weryfikacji integralności.

Zabezpieczenia powiązane: nie dotyczy.

(3) OPROGRAMOWANIE, OPROGRAMOWANIE SPRZĘTOWE I INTEGRALNOŚĆ INFORMACJI | CENTRALNIE ZARZĄDZANE NARZĘDZIA DO ZAPEWNIANIA INTEGRALNOŚCI

Stosuj centralnie zarządzane narzędzia weryfikacji integralności.

Zabezpieczenia powiązane: AU-3, SI-2, SI-8.

(4) OPROGRAMOWANIE, OPROGRAMOWANIE SPRZĘTOWE I INTEGRALNOŚĆ INFORMACJI | OPAKOWANIE ZABEZPIECZAJĄCE PRZED MANIPULACJĄ

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(5) OPROGRAMOWANIE, OPROGRAMOWANIE SPRZĘTOWE I INTEGRALNOŚĆ INFORMACJI | AUTOMATYCZNA ODPOWIEDŹ NA NARUSZENIA INTEGRALNOŚCI

Automatycznie [Wybór (jeden lub więcej): wyłączenie systemu; ponowne uruchomienie systemu; wdrażaj [Realizacja: kontrole zdefiniowane przez organizację]] w przypadku wykrycia naruszeń integralności.

Zabezpieczenia powiązane: nie dotyczy.

(6) OPROGRAMOWANIE, OPROGRAMOWANIE SPRZĘTOWE I INTEGRALNOŚĆ INFORMACJI | OCHRONA KRYPTOGRAFICZNA

Wprowadź mechanizmy kryptograficzne w celu wykrywania nieautoryzowanych zmian w oprogramowaniu, oprogramowaniu sprzętowym i informacjach.

Zabezpieczenia powiązane: SC-12, SC-13.

(7) OPROGRAMOWANIE, OPROGRAMOWANIE SPRZĘTOWE I INTEGRALNOŚĆ INFORMACJI | INTEGRACJA WYKRYWANIA I REAGOWANIA

Wprowadź wykrywanie następujących nieautoryzowanych zmian do możliwości reagowania na incydenty w organizacji: [Realizacja: zmiany w systemie istotne z punktu widzenia bezpieczeństwa zdefiniowane przez organizację].

Zabezpieczenia powiązane: AU-2, AU-6, IR-4, IR-5, SI-4.

(8) OPROGRAMOWANIE, OPROGRAMOWANIE SPRZĘTOWE I INTEGRALNOŚĆ INFORMACJI | MOŻLIWOŚĆ AUDYTU ISTOTNYCH ZDARZEŃ

Po wykryciu potencjalnego naruszenia integralności zapewnij możliwość przeprowadzenia audytu zdarzenia i zainicjowania następujących działań: [Wybór (jeden lub więcej): wygenerowanie rekordu audytu; powiadomienie bieżącego użytkownika; powiadomienie [Realizacja: personel lub role zdefiniowane przez organizację]; [Realizacja: inne działania zdefiniowane przez organizację]].

Zabezpieczenia powiązane: AU-2, AU-6, AU-12.

(9) OPROGRAMOWANIE, OPROGRAMOWANIE SPRZĘTOWE I INTEGRALNOŚĆ INFORMACJI | WERYFIKACJA PROCESU ROZRUCHU

Sprawdź integralność procesu rozruchu następujących komponentów systemu: [Realizacja: komponenty systemu zdefiniowane przez organizację].

Zabezpieczenia powiązane: SI-6.

(10) OPROGRAMOWANIE, OPROGRAMOWANIE SPRZĘTOWE I INTEGRALNOŚĆ INFORMACJI | OCHRONA OPROGRAMOWANIA SPRZĘTOWEGO ROZRUCHOWEGO

Wprowadź następujące mechanizmy w celu ochrony integralności oprogramowania układowego rozruchowego w [Realizacja: komponenty systemu zdefiniowane przez organizację]: [Realizacja: mechanizmy zdefiniowane przez organizację].

Zabezpieczenia powiązane: SI-6.

(11) OPROGRAMOWANIE, OPROGRAMOWANIE SPRZĘTOWE I INTEGRALNOŚĆ INFORMACJI | ŚRODOWISKA ZAMKNIĘTE Z OGRANICZONYMI UPRAWNIENIAMI

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(12) OPROGRAMOWANIE, OPROGRAMOWANIE SPRZĘTOWE I INTEGRALNOŚĆ INFORMACJI | WERYFIKACJA INTEGRALNOŚCI

Wymagaj weryfikacji integralności następującego oprogramowania zainstalowanego przez użytkownika przed wykonaniem: [Realizacja: oprogramowanie zainstalowane przez użytkownika zdefiniowane przez organizację].

Zabezpieczenia powiązane: CM-11.

(13) OPROGRAMOWANIE, OPROGRAMOWANIE SPRZĘTOWE I INTEGRALNOŚĆ INFORMACJI | WYKONYWANIE KODU W ŚRODOWISKACH CHRONIONYCH

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(14) OPROGRAMOWANIE, OPROGRAMOWANIE SPRZĘTOWE I INTEGRALNOŚĆ INFORMACJI | KOD WYKONYWALNY BINARNY LUB MASZYNOWY

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(15) OPROGRAMOWANIE, OPROGRAMOWANIE SPRZĘTOWE I INTEGRALNOŚĆ INFORMACJI | UWIERZYTELNIANIE KODEM

Wprowadź mechanizmy kryptograficzne w celu uwierzytelnienia następujących komponentów oprogramowania lub oprogramowania sprzętowego przed instalacją: [Realizacja: komponenty oprogramowania lub oprogramowania sprzętowego zdefiniowane przez organizację].

Zabezpieczenia powiązane: CM-5, SC-12, SC-13.

(16) OPROGRAMOWANIE, OPROGRAMOWANIE SPRZĘTOWE I INTEGRALNOŚĆ INFORMACJI | OGRANICZENIE CZASOWE WYKONYWANIA PROCESÓW BEZ NADZORU

Zabroń wykonywania procesów bez nadzoru przez okres dłuższy niż [Realizacja: okres czasu określony przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(17) OPROGRAMOWANIE, OPROGRAMOWANIE SPRZĘTOWE I INTEGRALNOŚĆ INFORMACJI | SAMODZIELNA OCHRONA APLIKACJI W CZASIE WYKONYWANIA

Wprowadź [Realizacja: kontrole zdefiniowane przez organizację] w celu zapewnienia samodzielnej ochrony aplikacji w czasie wykonywania.

Zabezpieczenia powiązane: SI-16.

SI-8 OCHRONA PRZED SPAMEM

Zabezpieczenie:

a. Stosuj mechanizmy ochrony przed spamem w punktach wejścia i wyjścia systemu, aby wykrywać niechciane wiadomości i reagować na nie;
b. Aktualizuj mechanizmy ochrony przed spamem, gdy dostępne są nowe wersje zgodnie z polityką i procedurami zarządzania konfiguracją organizacji.

Zabezpieczenia powiązane: PL-9, SC-5, SC-7, SC-38, SI-3, SI-4.

Zabezpieczenia rozszerzone:

(1) OCHRONA PRZED SPAMEM | CENTRALNE ZARZĄDZANIE

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(2) OCHRONA PRZED SPAMEM | AUTOMATYCZNE AKTUALIZACJE

Automatycznie aktualizuj mechanizmy ochrony przed spamem [Realizacja: częstotliwość zdefiniowana przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(3) OCHRONA PRZED SPAMEM | MOŻLIWOŚĆ CIĄGŁEGO UCZENIA SIĘ

Wprowadź mechanizmy ochrony przed spamem z możliwością uczenia się w celu skuteczniejszej identyfikacji legalnego ruchu komunikacyjnego.

Zabezpieczenia powiązane: nie dotyczy.

SI-9 OGRANICZENIA WPROWADZANIA INFORMACJI

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

SI-10 WALIDACJA WPROWADZANYCH INFORMACJI

Zabezpieczenie:

Sprawdź poprawność następujących danych wejściowych: [Realizacja: dane wejściowe informacji zdefiniowane przez organizację w systemie].

Zabezpieczenia powiązane: nie dotyczy.

Zabezpieczenia rozszerzone:

(1) WALIDACJA WPROWADZANYCH INFORMACJI | MOŻLIWOŚĆ RĘCZNEGO NADPISYWANIA

a. Zapewnij możliwość ręcznego obejścia w celu walidacji danych wejściowych następujących danych wejściowych: [Realizacja: dane wejściowe zdefiniowane przez organizację zdefiniowane w kontroli bazowej (SI-10)];

b. Ogranicz korzystanie z możliwości ręcznego obejścia wyłącznie do [Realizacja: upoważnione osoby zdefiniowane przez organizację];

c. Przeprowadź audyt korzystania z możliwości ręcznego obejścia.

Zabezpieczenia powiązane: Dostępne są następujące modele: AC-3, AU-2, AU-12.

(2) WALIDACJA WPROWADZANYCH INFORMACJI | PRZEGLĄDANIE I ROZWIĄZYWANIE BŁĘDÓW

Przejrzyj i rozwiąż błędy walidacji danych wejściowych w [Realizacja: okres czasu określony przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(3) WALIDACJA WPROWADZANYCH INFORMACJI | PRZEWIDYWALNE ZACHOWANIE

Sprawdź, czy system zachowuje się w przewidywalny i udokumentowany sposób w przypadku otrzymania nieprawidłowych danych wejściowych.

Zabezpieczenia powiązane: nie dotyczy.

(4) WALIDACJA WPROWADZANYCH INFORMACJI | INTERAKCJE CZASOWE

Weź pod uwagę interakcje czasowe między komponentami systemu podczas określania właściwych reakcji na nieprawidłowe dane wejściowe.

Zabezpieczenia powiązane: nie dotyczy.

(5) WALIDACJA WPROWADZANYCH INFORMACJI | OGRANICZANIE DANYCH WEJŚCIOWYCH DO ZAUFANYCH ŹRÓDEŁ I ZATWIERDZONYCH FORMATÓW

Ogranicz użycie danych wejściowych do [Realizacja: zaufanych źródeł zdefiniowanych przez organizację] i/lub [Realizacja: formatów zdefiniowanych przez organizację].

Zabezpieczenia powiązane: AC-3, AC-6.

(6) WALIDACJA WPROWADZANYCH INFORMACJI | ZAPOBIEGANIE INIEKCJI

Zapobiegaj iniekcji niezaufanych danych.

Zabezpieczenia powiązane: AC-3, AC-6.

SI-11 OBSŁUGA BŁĘDÓW

Zabezpieczenie:

a. Generuj komunikaty o błędach, które dostarczają informacji niezbędnych do działań osób naprawiających błędy bez ujawniania informacji, które mogą być wykorzystane do ataku;

b. Ujawniaj komunikaty o błędach tylko [Realizacja: personel lub role zdefiniowane przez organizację].

Zabezpieczenia powiązane: AU-2, AU-3, SC-31, SI-2, SI-15.

Zabezpieczenia rozszerzone: nie dotyczy.

SI-12 ZARZĄDZANIE INFORMACJĄ I JEJ PRZECHOWYWANIE

Zabezpieczenie:

Zarządzaj informacjami w systemie i przechowuj informacje wyjściowe z systemu zgodnie z obowiązującymi przepisami prawa, rozporządzeniami wykonawczymi, dyrektywami, regulacjami, zasadami, standardami, wytycznymi i wymogami operacyjnymi.

Zabezpieczenia powiązane: AC-16, AU-5, AU-11, CA-2, CA-3, CA-5, CA-6, CA-7, CA-9, CM-5, CM-9, CP-2, IR-8, MP-2, MP-3, MP-4, MP-6, PL-2, PL-4, PM-4, PM-8, PM-9, PS-2, PS-6, PT-2, PT-3, RA-2, RA-3, SA-5, SA-8, SR-2.

Zabezpieczenia rozszerzone:

(1) ZARZĄDZANIE INFORMACJĄ I JEJ PRZECHOWYWANIE | OGRANICZANIE ELEMENTÓW INFORMACJI UMOŻLIWIAJĄCYCH IDENTYFIKACJĘ OSOBY

Ogranicz dane identyfikujące osobę przetwarzane w cyklu życia informacji do następujących elementów danych identyfikujących osobę: [Realizacja: elementy danych identyfikujących osobę zdefiniowane przez organizację].

Zabezpieczenia powiązane: PM-25.

(2) ZARZĄDZANIE INFORMACJĄ I JEJ PRZECHOWYWANIE | MINIMALIZOWANIE DANYCH OSOBOWYCH PODCZAS TESTÓW, SZKOLEŃ I BADAŃ

Stosuj następujące techniki, aby zminimalizować wykorzystanie danych osobowych do celów badawczych, testowych lub szkoleniowych: [Realizacja: techniki zdefiniowane przez organizację].

Zabezpieczenia powiązane: PM-22, PM-25, SI-19.

(3) ZARZĄDZANIE INFORMACJĄ I JEJ PRZECHOWYWANIE | USUWANIE INFORMACJI

Aby pozbyć się, zniszczyć lub wymazać informacje po upływie okresu przechowywania, należy zastosować następujące techniki: [Realizacja: techniki zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

SI-13 PRZEWIDYWALNE ZAPOBIEGANIE AWARIOM

Zabezpieczenie:

a. Określ średni czas do awarii (MTTF) dla następujących komponentów systemu w określonych środowiskach operacyjnych: [Realizacja: komponenty systemu zdefiniowane przez organizację];

b. Zapewnij zastępcze komponenty systemu i sposób wymiany aktywnych i zapasowych komponentów zgodnie z następującymi kryteriami: [Realizacja: kryteria substytucji MTTF zdefiniowane przez organizację].

Zabezpieczenia powiązane: CP-2, CP-10, CP-13, MA-2, MA-6, SA-8, SC-6.

Zabezpieczenia rozszerzone:

(1) PRZEWIDYWALNE ZAPOBIEGANIE AWARIOM | PRZENOSZENIE ODPOWIEDZIALNOŚCI ZA KOMPONENTY

Wycofaj z eksploatacji komponenty systemu, przenosząc odpowiedzialność za komponenty na komponenty zastępcze nie później niż [Realizacja: ułamek lub procent określony przez organizację] średniego czasu do awarii.

Zabezpieczenia powiązane: nie dotyczy.

(2) PRZEWIDYWALNE ZAPOBIEGANIE AWARIOM | LIMIT CZASU NA WYKONANIE PROCESU BEZ NADZORU

[Wycofane: włączone / przeniesione do innego zabezpieczenia, patrz: TABELA 5-2]

(3) PRZEWIDYWALNE ZAPOBIEGANIE AWARIOM | RĘCZNE PRZESYŁANIE MIĘDZY KOMPONENTAMI

Ręcznie inicjuj transfery między aktywnymi i zapasowymi komponentami systemu, gdy wykorzystanie aktywnego komponentu osiągnie [Realizacja: zdefiniowany przez organizację procent] średniego czasu do awarii.

Zabezpieczenia powiązane: nie dotyczy.

(4) PRZEWIDYWALNE ZAPOBIEGANIE AWARIOM | INSTALACJA I POWIADAMIANIE O KOMPONENTACH W TRYBIE GOTOWOŚCI

W przypadku wykrycia awarii komponentów systemu:

a. Upewnij się, że komponenty zapasowe zostały pomyślnie i przejrzyście zainstalowane w ciągu [Realizacja: okres czasu zdefiniowany przez organizację];

b. [Wybór (jeden lub więcej): Aktywuj [Realizacja: alarm zdefiniowany przez organizację]; Automatycznie wyłącz system; [Realizacja: działanie zdefiniowane przez organizację]].

Zabezpieczenia powiązane: nie dotyczy.

(5) PRZEWIDYWALNE ZAPOBIEGANIE AWARIOM | MOŻLIWOŚĆ PRZEŁĄCZANIA AWARYJNEGO

Zapewnij [Wybór: w czasie rzeczywistym; niemal w czasie rzeczywistym] [Realizacja: zdefiniowana przez organizację możliwość przełączania awaryjnego] dla systemu.

Zabezpieczenia powiązane: CP-6, CP-7, CP-9.

SI-14 NIETRWAŁOŚĆ

Zabezpieczenie:

Wdrażaj nietrwałe [Realizacja: zdefiniowane przez organizację komponenty i usługi systemu], które są inicjowane w znanym stanie i kończone [Wybór (jeden lub więcej): po zakończeniu sesji użytkowania; okresowo z [Realizacja: częstotliwość zdefiniowana przez organizację]].

Zabezpieczenia powiązane: SC-30, SC-34, SI-21.

Zabezpieczenia rozszerzone:

(1) NIETRWAŁOŚĆ | ODŚWIEŻ Z ZAUFANYCH ŹRÓDEŁ

Uzyskaj oprogramowanie i dane wykorzystywane podczas odświeżania komponentów systemu i usług z następujących zaufanych źródeł: [Realizacja: zaufane źródła zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(2) NIETRWAŁOŚĆ | INFORMACJE NIETRWAŁE

a. [Wybór: Odśwież [Realizacja: informacje zdefiniowane przez organizację] [Realizacja: częstotliwość zdefiniowana przez organizację]; Generuj [Realizacja: informacje zdefiniowane przez organizację] na żądanie];

b. Usuń informacje, gdy nie są już potrzebne.

Zabezpieczenia powiązane: nie dotyczy.

(3) NIETRWAŁOŚĆ | NIETRWAŁA ŁĄCZNOŚĆ

Nawiązuj połączenia z systemem na żądanie i kończ połączenia po [Wybór: zrealizowanie żądania; okres nieużywania].

Zabezpieczenia powiązane: SC-10.

SI-15 FILTROWANIE DANYCH WYJŚCIOWYCH

Zabezpieczenie:

Sprawdź poprawność informacji wyjściowych z następujących programów i/lub aplikacji, aby upewnić się, że informacje te są zgodne z oczekiwaną zawartością: [Realizacja: programy i/lub aplikacje zdefiniowane przez organizację].

Zabezpieczenia powiązane: SI-3, SI-4, SI-11.

Zabezpieczenia rozszerzone: nie dotyczy.

SI-16 OCHRONA PAMIĘCI

Zabezpieczenie:

Wprowadź następujące kontrole w celu ochrony pamięci systemowej przed nieautoryzowanym wykonaniem kodu: [Realizacja: kontrole zdefiniowane przez organizację].

Zabezpieczenia powiązane: AC-25, SC-3, SI-7.

Zabezpieczenia rozszerzone: nie dotyczy.

SI-17 PROCEDURY BEZPIECZEŃSTWA

Zabezpieczenie:

Wprowadź wskazane procedury bezpieczeństwa w przypadku wystąpienia wskazanych awarii: [Realizacja: lista warunków awarii zdefiniowana przez organizację i powiązane procedury bezpieczeństwa].

Zabezpieczenia powiązane: CP-12, CP-13, SC-24, SI-13.

Zabezpieczenia rozszerzone: nie dotyczy.

SI-18 OPERACJE ZWIĄZANE Z JAKOŚCIĄ DANYCH OSOBOWYCH

Zabezpieczenie:

a. Sprawdź dokładność, trafność, aktualność i kompletność danych osobowych w całym cyklu życia informacji [Realizacja: częstotliwość zdefiniowana przez organizację];

b. Poprawiaj lub usuwaj niedokładne lub nieaktualne dane osobowe.

Zabezpieczenia powiązane: PM-22, PM-24, PT-2, SI-4.

Zabezpieczenia rozszerzone:

(1) OPERACJE ZWIĄZANE Z JAKOŚCIĄ DANYCH OSOBOWYCH| WSPARCIE AUTOMATYZACJI

Popraw lub usuń dane osobowe, które są niedokładne lub nieaktualne, nieprawidłowo określone pod względem wpływu lub nieprawidłowo zanonimizowane, korzystając z [Realizacja: zautomatyzowane mechanizmy zdefiniowane przez organizację].

Zabezpieczenia powiązane: PM-18, RA-8.

(2) OPERACJE ZWIĄZANE Z JAKOŚCIĄ DANYCH OSOBOWYCH| ZNACZNIKI DANYCH

Stosuj tagi danych w celu zautomatyzowania korygowania lub usuwania danych osobowych w całym cyklu życia informacji w systemach organizacyjnych.

Zabezpieczenia powiązane: AC-3, AC-16, SC-16.

(3) OPERACJE ZWIĄZANE Z JAKOŚCIĄ DANYCH OSOBOWYCH| GROMADZENIE

Zbieraj dane identyfikujące bezpośrednio od danej osoby.

Zabezpieczenia powiązane: nie dotyczy.

(4) OPERACJE ZWIĄZANE Z JAKOŚCIĄ DANYCH OSOBOWYCH| INDYWIDUALNE ŻĄDANIA

Na żądanie osób fizycznych lub wyznaczonych przez nie przedstawicieli można poprawić lub usunąć dane umożliwiające identyfikację osoby.

Zabezpieczenia powiązane: nie dotyczy.

(5) OPERACJE ZWIĄZANE Z JAKOŚCIĄ DANYCH OSOBOWYCH| POWIADOMIENIE O KOREKCIE LUB USUNIĘCIU

Powiadom [Realizacja: odbiorcy danych osobowych zdefiniowani przez organizację] oraz osoby fizyczne, że dane osobowe zostały poprawione lub usunięte.

Zabezpieczenia powiązane: nie dotyczy.

SI-19 DE-IDENTYFIKACJA

Zabezpieczenie:

a. Usuń następujące elementy danych osobowych z zestawów danych: [Realizacja: elementy danych osobowych zdefiniowane przez organizację];

b. Oceń [Realizacja: częstotliwość zdefiniowana przez organizację] pod kątem skuteczności anonimizacji.

Zabezpieczenia powiązane: MP-6, PM-22, PM-23, PM-24, RA-2, SI-12.

Zabezpieczenia rozszerzone:

(1) DE-IDENTYFIKACJA | KOLEKCJA

W momencie gromadzenia zestawu danych uniemożliwiaj identyfikację użytkownika, nie zbierając informacji umożliwiających identyfikację osoby.

Zabezpieczenia powiązane: nie dotyczy.

(2) DE-IDENTYFIKACJA | ARCHIWIZACJA

Zabroń archiwizowania elementów informacji identyfikujących osobę, jeśli elementy te w zestawie danych nie będą potrzebne po archiwizacji zestawu danych.

Zabezpieczenia powiązane: nie dotyczy.

(3) DE-IDENTYFIKACJA | WYDANIE

Usuń elementy informacji umożliwiających identyfikację osoby ze zbioru danych przed jego udostępnieniem, jeśli elementy te nie muszą stanowić części udostępnianych danych.

Zabezpieczenia powiązane: nie dotyczy.

(4) DE-IDENTYFIKACJA | USUWANIE, MASKOWANIE, SZYFROWANIE, HASZOWANIE LUB ZASTĘPOWANIE BEZPOŚREDNICH IDENTYFIKATORÓW

Usuń, zamaskuj, zaszyfruj, haszuj lub zamień bezpośrednie identyfikatory w zestawie danych.

Zabezpieczenia powiązane: SC-12, SC-13.

(5) DE-IDENTYFIKACJA | KONTROLA UJAWNIANIA DANYCH STATYSTYCZNYCH

Manipuluj danymi liczbowymi, tabelami kontyngencji i wynikami statystycznymi w taki sposób, aby w wynikach analizy nie można było zidentyfikować żadnej osoby ani organizacji.

Zabezpieczenia powiązane: nie dotyczy.

(6) DE-IDENTYFIKACJA | RÓŻNICOWA PRYWATNOŚĆ

Zapobiegaj ujawnianiu informacji umożliwiających identyfikację osoby poprzez dodawanie niedeterministycznego szumu do wyników działań matematycznych przed ich zgłoszeniem.

Zabezpieczenia powiązane: SC-12, SC-13.

(7) DE-IDENTYFIKACJA | ZWERYFIKOWANE ALGORYTMY I OPROGRAMOWANIE

Przeprowadź anonimizację przy użyciu sprawdzonych algorytmów i oprogramowania, które zostało sprawdzone pod kątem implementacji algorytmów.

Zabezpieczenia powiązane: nie dotyczy.

(8) DE-IDENTYFIKACJA | TEST „ZMOTYWOWANEGO INTRUZA”

Przeprowadź test „zmotywowanego intruza” na zanonimizowanym zestawie danych, aby ustalić, czy zidentyfikowane dane pozostały, czy też zanonimizowane dane można ponownie zidentyfikować.

Zabezpieczenia powiązane: nie dotyczy.

SI-20 OZNACZANIE DANYCH

Zabezpieczenie:

Wprowadź dane lub funkcje w następujących systemach lub komponentach systemu, aby ustalić, czy dane organizacyjne zostały wykradzione lub nieprawidłowo usunięte z organizacji: [Realizacja: systemy lub komponenty systemu zdefiniowane przez organizację].

Zabezpieczenia powiązane: AU-13.

Zabezpieczenia rozszerzone: nie dotyczy.

SI-21 ODŚWIEŻANIE INFORMACJI

Zabezpieczenie:

Odśwież [Realizacja: informacje zdefiniowane przez organizację] z [Realizacja: częstotliwości zdefiniowane przez organizację] lub wygeneruj informacje na żądanie i usuń je, gdy nie będą już potrzebne.

Zabezpieczenia powiązane: SI-14.

Zabezpieczenia rozszerzone: nie dotyczy.

SI-22 RÓŻNORODNOŚĆ INFORMACJI

Zabezpieczenie:

a. Zidentyfikuj następujące alternatywne źródła informacji dla [Realizacja: podstawowe funkcje i usługi zdefiniowane przez organizację]: [Realizacja: alternatywne źródła informacji zdefiniowane przez organizację];

b. Użyj alternatywnego źródła informacji do wykonania podstawowych funkcji lub usług w [Realizacja: systemy zdefiniowane przez organizację lub komponenty systemu], gdy główne źródło informacji jest uszkodzone lub niedostępne.

Zabezpieczenia powiązane: nie dotyczy.

Zabezpieczenia rozszerzone: nie dotyczy.

SI-23 FRAGMENTACJA INFORMACJI

Zabezpieczenie:

Na podstawie [Realizacja: okoliczności zdefiniowane przez organizację]:

a. Podziel następujące informacje na fragmenty: [Realizacja: informacje zdefiniowane przez organizację];

b. Rozprowadź pofragmentowane informacje w następujących systemach lub komponentach systemu: [Realizacja: systemy lub komponenty systemu zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

Zabezpieczenia rozszerzone: nie dotyczy.

KATEGORIA: SR – ZARZĄDZANIE RYZYKIEM W ŁAŃCUCHU DOSTAW

SR-1 POLITYKA I PROCEDURY

Zabezpieczenie:

a. Opracuj, dokumentuj i rozpowszechnij wśród [Realizacja: personel lub role określone przez organizację]:

   1. [Wybór (jeden lub więcej): poziom organizacji; poziom misji/procesu biznesowego; poziom systemu] politykę zarządzania ryzykiem w łańcuchu dostaw, która:

      (a) Adresuje cel, zakres, role, obowiązki, zaangażowanie kierownictwa, koordynację między jednostkami organizacyjnymi i zgodność z przepisami; oraz

      (b) Jest zgodna z obowiązującym prawem, rozporządzeniami, dyrektywami, przepisami, zasadami, standardami i wytycznymi; oraz

   2. Procedury ułatwiające wdrożenie polityki zarządzania ryzykiem w łańcuchu dostaw oraz powiązanych zabezpieczeń w zakresie zarządzania ryzykiem w łańcuchu dostaw;

b. Wyznacz [Realizacja: osoba wyznaczona przez organizację] do zarządzania rozwojem, dokumentacją i rozpowszechnianiem polityki i procedur zarządzania ryzykiem w łańcuchu dostaw; oraz

c. Przeglądaj i aktualizuj na bieżąco:

   1. Polityki zarządzania ryzykiem w łańcuchu dostaw z [Realizacja: częstotliwość określona przez organizację] i następujących [Realizacja: zdarzenia określone przez organizację]; oraz

   2. Procedury zarządzania ryzykiem w łańcuchu dostaw z [Realizacja: częstotliwość określona przez organizację] i następujących [Realizacja: zdarzenia określone przez organizację].

Zabezpieczenia powiązane: PM-9, PM-30, PS-8, SI-12.

Zabezpieczenia rozszerzone: nie dotyczy.

SR-2 PLAN ZARZĄDZANIA RYZYKIEM W ŁAŃCUCHU DOSTAW

Zabezpieczenie:

a. Opracuj plan zarządzania ryzykiem związanym z łańcuchem dostaw w zakresie badań i rozwoju, projektowania, produkcji, nabywania, dostarczania, integracji, eksploatacji i konserwacji oraz utylizacji następujących systemów, komponentów systemu lub usług systemowych: [Realizacja: określone przez organizację systemy, komponenty systemu lub usługi systemowe];

b. Przeglądaj i aktualizuj plan zarządzania ryzykiem w łańcuchu dostaw [Realizacja: częstotliwość określona przez organizację] lub w razie potrzeby w celu uwzględnienia zagrożeń, zmian organizacyjnych lub środowiskowych; oraz

c. Zabezpiecz plan zarządzania ryzykiem w łańcuchu dostaw przed nieautoryzowanym ujawnieniem i modyfikacją.

Zabezpieczenia powiązane: CA-2, CP-4, IR-4, MA-2, MA-6, PE-16, PL-2, PM-9, PM-30, RA-3, RA-7, SA-8, SI-4.

Zabezpieczenia rozszerzone:

(1) PLAN ZARZĄDZANIA RYZYKIEM W ŁAŃCUCHU DOSTAW | POWOŁANIE ZESPOŁU ZARZĄDZANIA RYZYKIEM W ŁAŃCUCHU DOSTAW

Powołaj zespół zarządzania ryzykiem w łańcuchu dostaw składający się z [Realizacja: określony przez organizację personel, role i obowiązki], który będzie prowadził i wspierał następujące działania związane z zarządzaniem ryzykiem w łańcuchu dostaw (SCRM): [Realizacja: działania w zakresie zarządzania ryzykiem w łańcuchu dostaw określone przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

SR-3 ZABEZPIECZENIA I PROCESY W ŁAŃCUCHU DOSTAW

Zabezpieczenie:

a. Wprowadź procesy służące do identyfikacji i eliminacji słabych punktów lub braków w elementach i procesach łańcucha dostaw [Realizacja: zdefiniowany przez organizację system lub komponent systemu] w koordynacji z [Realizacja: zdefiniowany przez organizację personel łańcucha dostaw];

b. Stosuj następujące zabezpieczenia w celu ochrony przed ryzykiem powiązanym z łańcuchem dostaw systemu, komponentem systemu lub usługi systemowej oraz w celu ograniczenia szkód lub konsekwencji wynikających ze zdarzeń związanych z łańcuchem dostaw: [Realizacja: określone przez organizację zabezpieczenia łańcucha dostaw]; oraz

c. Dokumentuj wybrane i wdrożone procesy i zabezpieczenia łańcucha dostaw w [Wybór: plan bezpieczeństwa i ochrony prywatności; plan zarządzania ryzykiem w łańcuchu dostaw; [Realizacja: dokument zdefiniowany przez organizację].

Zabezpieczenia powiązane: CA-2, MA-2, MA-6, PE-3, PE-16, PL-8, PM-30, SA-2, SA-3, SA-4, SA-5, SA-8, SA-9, SA-10, SA-15, SC-7, SC-29, SC-30, SC-38, SI-7, SR-5, SR-6, SR-8, SR-9, SR-11.

Zabezpieczenia rozszerzone:

(1) ZABEZPIECZENIA I PROCESY W ŁAŃCUCHU DOSTAW | ZRÓŻNICOWANA BAZA DOSTAW

Wykorzystuj zróżnicowane źródła dostaw następujących komponentów systemu i usług: [Realizacja: zdefiniowane przez organizację komponenty systemu i usługi].

Zabezpieczenia powiązane: nie dotyczy.

(2) ZABEZPIECZENIA I PROCESY W ŁAŃCUCHU DOSTAW | OGRANICZANIE SZKODY

Stosuj następujące zabezpieczenia w celu ograniczenia szkód wyrządzanych przez potencjalnych przeciwników, którzy identyfikują i ukierunkowują łańcuch dostaw organizacji: [Realizacja: zabezpieczenia zdefiniowane przez organizację].

Zabezpieczenia powiązane: nie dotyczy.

(3) ZABEZPIECZENIA I PROCESY W ŁAŃCUCHU DOSTAW | PODWYKONAWCY

Zapewnij, że zabezpieczenia zawarte w umowach z głównymi wykonawcami są również zawarte w umowach z podwykonawcami.

Zabezpieczenia powiązane: SR-5, SR-8.

SR-4 POCHODZENIE

Zabezpieczenie:

Dokumentuj, monitorowanie i utrzymywanie autentyczności pochodzenia następujących systemów, komponentów systemu i związanych z nimi danych: [Realizacja: określone przez organizację systemy, komponenty systemu i związane z nimi dane].

Zabezpieczenia powiązane: AT-3, CM-8, IA-2, IA-2, IA-8, MA-2, MA-6, PE-16, PL-2, RA-3, RA-9, SA-3, SA-8, SI-4, SR-9, SR-10, SR-11.

Zabezpieczenia rozszerzone:

(1) POCHODZENIE |TOŻSAMOŚĆ

Wprowadź i utrzymuj unikalną identyfikację następujących elementów łańcucha dostaw, procesów i personelu związanego ze zidentyfikowanym systemem i krytycznymi elementami systemu: [Realizacja: zdefiniowane przez organizację elementy łańcucha dostaw, procesy i personel związany ze zdefiniowanymi przez organizację systemami i krytycznymi elementami systemu.

Zabezpieczenia powiązane: IA-2, IA-8, PE-16.

(2) POCHODZENIE | ŚLEDZENIE PRZESYŁEK

Wprowadź i utrzymuj unikalną identyfikację następujących systemów i krytycznych elementów systemu w celu śledzenia ich w całym łańcuchu dostaw: [Realizacja: określone przez organizację systemy i krytyczne komponenty systemu].

Zabezpieczenia powiązane: IA-2, IA-8, PE-16, PL-2.

(3) POCHODZENIE |POTWIERDZANIE AUTENTYCZNOŚCI I NIEZMIENNOŚCI

Stosuj następujące zabezpieczenia w celu potwierdzenia, że otrzymany system lub element systemu jest autentyczny i nie został zmieniony, [Realizacja: zabezpieczenia zdefiniowane przez organizację].

Zabezpieczenia powiązane: AT-3, SR-9, SR-10, SR-11.

(4) POCHODZENIE | INTEGRALNOŚĆ ŁAŃCUCHA DOSTAW - POCHODZENIE

Stosuj [Realizacja: zdefiniowane przez organizację zabezpieczenia] i prowadź [Realizacja: zdefiniowana przez organizację analiza] w celu zapewnienia integralności systemu i jego komponentów poprzez walidację wewnętrznego składu i pochodzenia krytycznych lub istotnych technologii, produktów i usług.

Zabezpieczenia powiązane: RA-3.

SR-5 STRATEGIE, NARZĘDZIA I METODY NABYCIA

Zabezpieczenie:

Stosowanie następujących strategii pozyskiwania, narzędzi zawierania umów i metod zaopatrzenia w celu ochrony przed ryzykiem związanym z łańcuchem dostaw, jego identyfikacji i ograniczania: [Realizacja: określone przez organizację strategie nabywania, narzędzia kontraktowe i metody zaopatrzenia].

Zabezpieczenia powiązane: AT-3, CA-8, RA-5, RA-9, SA-2, SA-3, SA-4, SA-5, SA-8, SA-9, SA-10, SA-11, SA-15, SI-7, SR- 6, SR-9, SR-10, SR-11.

Zabezpieczenia rozszerzone:

(1) STRATEGIE, NARZĘDZIA I METODY NABYCIA | ODPOWIEDNIE ZAOPATRZENIE

Stosuj następujące środki bezpieczeństwa w celu zapewnienia odpowiedniego zaopatrzenia [Realizacja: zdefiniowane przez organizację krytyczne komponenty systemu]: [Realizacja: środki bezpieczeństwa zdefiniowane przez organizację].

Zabezpieczenia powiązane: RA-9.

(2) STRATEGIE, NARZĘDZIA I METODY NABYCIA | OCENY PRZED WYBOREM AKCEPTACJĄ, MODYFIKACJĄ LUB AKTUALIZACJĄ

Dokonuj ocen systemu, komponentów systemu lub usługi systemowej przed jego wyborem, akceptacją, modyfikacją lub aktualizacją.

Zabezpieczenia powiązane: CA-8, RA-5, SA-11, SI-7, SR-9.

SR-6 OCENY I RECENZJE DOSTAWCÓW

Zabezpieczenie:

Oceniaj i przeglądaj ryzyka związane z łańcuchem dostaw, dotyczące dostawców lub wykonawców oraz dostarczanego przez nich systemu, komponentu systemu lub usługi systemowej [Realizacja: częstotliwość określona przez organizację].

Zabezpieczenia powiązane: CA-8, SI-4, SR-3, SR-5.

Zabezpieczenia rozszerzone:

(1) OCENY I RECENZJE DOSTAWCÓW | BADANIA I ANALIZY

Stosuj [Wybór (jeden lub więcej): analiza organizacyjna; niezależna analiza zewnętrzna; testy organizacyjne; niezależne testy zewnętrzne] następujących elementów łańcucha dostaw, procesów i podmiotów związanych z systemem, komponentem systemu lub usługą systemową: [Realizacja: zdefiniowane przez organizację elementy, procesy i podmioty łańcucha dostaw].

Zabezpieczenia powiązane: CA-8, SI-4.

SR-7 BEZPIECZEŃSTWO OPERACJI W RAMACH ŁAŃCUCHA DOSTAW

Zabezpieczenie:

Stosuj następujące środki bezpieczeństwa operacyjnego (ang. Operations Security - OPSEC) w celu ochrony informacji powiązanych z łańcuchem dostaw systemu, komponentu systemu lub usługi systemowej: [Realizacja: określone przez organizację zabezpieczenia w zakresie bezpieczeństwa operacyjnego (OPSEC)].

Zabezpieczenia powiązane: SC-38.

Zabezpieczenia rozszerzone: nie dotyczy.

SR-8 UMOWY DOTYCZĄCE POWIADOMIEŃ

Zabezpieczenie:

Ustal umowy i procedury z podmiotami uczestniczącymi w łańcuchu dostaw systemu, komponentu systemu lub usługi systemowej w celu przekazywania [Wybór (jeden lub więcej): zawiadomienie o naruszeniach w łańcuchu dostaw; wyniki oceny lub audytu; [Realizacja: informacje określone przez organizację]].

Zabezpieczenia powiązane: IR-4, IR-6, IR-8.

Zabezpieczenia rozszerzone: nie dotyczy.

SR-9 ODPORNOŚĆ NA MANIPULACJE I WYKRYWANIE SABOTAŻU

Zabezpieczenie:

Wprowadź program zabezpieczający przed manipulacją przy systemie, komponencie systemu lub usłudze systemowej.

Zabezpieczenia powiązane: PE-3, PM-30, SA-3, SA-15, SI-4, SI-7, SR-3, SR-4, SR-5, SR-10, SR-11.

Zabezpieczenia rozszerzone:

(1) ODPORNOŚĆ NA MANIPULACJE I WYKRYWANIE SABOTAŻU | WIELOETAPOWY CYKL ŻYCIA SYSTEMU

Stosuj technologie, narzędzia i techniki antysabotażowe przez cały cykl życia systemu.

Zabezpieczenia powiązane: SA-3.

SR-10 KONTROLA SYSTEMÓW / KOMPONENTÓW

Zabezpieczenie:

Kontroluj [Wybór (jeden lub więcej): losowo; z [Realizacja: częstotliwość zdefiniowana przez organizację] następujących systemów lub komponentów systemu po wystąpieniu [Realizacja: zdefiniowane przez organizację przesłanki przeprowadzenia inspekcji]] w celu wykrycia ingerencji w: [Realizacja: systemy lub części składowe systemu określone przez organizację].

Zabezpieczenia powiązane: AT-3, PM-30, SI-4, SI-7, SR-3, SR-4, SR-5, SR-9, SR-11.

SR-11 AUTENTYCZNOŚĆ KOMPONENTU

Zabezpieczenie:

a. Opracuj i wprowadź polityki i procedury walki z fałszerstwami, które obejmują środki wykrywania i zapobiegania wprowadzaniu podrabianych komponentów do systemu;

b. Zgłaszaj podrobione elementy systemu do [Wybór (jeden lub więcej): źródło podrobionego elementu; [Realizacja: zdefiniowane przez organizację zewnętrzne organizacje zajmujące się sporządzaniem raportów]; [Realizacja: zdefiniowany przez organizację personel lub role].

Zabezpieczenia powiązane: AT-3, CM-3, MA-2, MA-4, PE-3, RA-5, SA-4, SA-10, SI-7, SR-9, SR-10.

Zabezpieczenia rozszerzone:

(1) AUTENTYCZNOŚĆ KOMPONENTU | SZKOLENIE Z ZAKRESU ZAPOBIEGANIA FAŁSZERSTWOM

Przeprowadzaj szkolenia [Realizacja: personel lub role zdefiniowane przez organizację] w zakresie wykrywania podrobionych elementów systemu (w tym sprzętu, oprogramowania i oprogramowania układowego).

Zabezpieczenia powiązane: AT-3.

(2) AUTENTYCZNOŚĆ KOMPONENTU | ZABEZPIECZENIE KONFIGURACJI SERWISOWANYCH I NAPRAWIANYCH KOMPONENTÓW

Utrzymuj kontrolę konfiguracji następujących komponentów systemu oczekujących na serwis lub naprawę oraz komponentów serwisowanych lub naprawianych oczekujących na powrót do eksploatacji: [Realizacja: komponenty systemu zdefiniowane przez organizację].

Zabezpieczenia powiązane: CM-3, MA-2, MA-4, SA-10.

(3) AUTENTYCZNOŚĆ KOMPONENTU | SKANOWANIE ANTYFAŁSZERSKIE

Skanowanie w poszukiwaniu fałszywych komponentów systemu [Realizacja: częstotliwość zdefiniowana przez organizację].

Zabezpieczenia powiązane: RA-5.

SR-12 USUWANIE KOMPONENTÓW

Zabezpieczenie:

Usuwanie [Realizacja: dane zdefiniowane przez organizację, dokumentacja, narzędzia lub komponenty systemu] przy użyciu następujących technik i metod: [Realizacja: techniki i metody określone przez organizację].

Zabezpieczenia powiązane: MP-6.

Zabezpieczenia rozszerzone: nie dotyczy.