Zestawienie wymagań i dowodów na spełnienie kryteriów

Audyt bezpieczeństwa informacji – Krajowe Ramy Interoperacyjności (rozporządzenie KRI)

Wykaz dokumentów i dowodów, które jednostka audytowana powinna przedstawić dla wykazania zgodności z § 19 ust. 1 i 2 rozporządzenia KRI. Opracowanie: VALVEN Sp. z o.o.

Lp.	Obszar / podstawa prawna	Wymaganie (kryterium oceny)	Dokument (przykładowy dowód realizacji)
2.1. Dokumenty z zakresu bezpieczeństwa informacji			
1	**Dokumentacja SZBI** *§ 19 ust. 1 i 2 oraz ust. 2 pkt 1 KRI*	Dokumenty SZBI zatwierdzone przez kierownictwo, wdrożone do stosowania i podane do wiadomości pracownikom oraz właściwym stronom zewnętrznym.	• Polityka Bezpieczeństwa Informacji (PBI) z datą i podpisem kierownictwa, • Zarządzenie / decyzja wprowadzająca dokumentację SZBI do stosowania, • Procedury i instrukcje wykonawcze stanowiące SZBI, • Potwierdzenia zapoznania pracowników (lista / oświadczenia), • Wykaz aktywów informacyjnych wraz z właścicielami aktywów, • Zakres Systemu Zarządzania Bezpieczeństwem Informacji, • Potwierdzenie udostępnienia dokumentacji pracownikom (np. intranet, e-mail, system obiegu dokumentów).
2	**Przegląd i aktualizacja regulacji** *§ 19 ust. 2 pkt 1 KRI*	Regularny przegląd dokumentacji SZBI; aktualizacja jako konsekwencja wyników szacowania ryzyka i wniosków z incydentów.	• Protokoły / notatki z okresowego przeglądu dokumentacji (datowane), • Historia wersji dokumentów (metryka zmian), • Zarządzenia aktualizujące regulacje, • Powiązanie zmian z raportem z analizy ryzyka i rejestrem incydentów.
2.2. Inwentaryzacja sprzętu i oprogramowania informatycznego			
3	**Zarządzanie sprzętem i oprogramowaniem** *§ 19 ust. 2 pkt 2 KRI*	Określony sposób zarządzania sprzętem i oprogramowaniem (w tym licencjami) oraz funkcjonowanie rejestru zasobów (CMDB).	• Procedura / regulamin zarządzania zasobami IT i licencjami, • Wskazanie osoby / roli odpowiedzialnej za zarządzanie zasobami, • Ewidencja licencji na oprogramowanie.
4	**Rejestr zasobów teleinformatycznych** *§ 19 ust. 2 pkt 2 KRI*	Rejestr (CMDB) zawierający wszystkie aktywa IT: urządzenia, oprogramowanie, środki komunikacji, ich rodzaj, parametry, konfigurację, relacje i użytkownika.	• Rejestr / baza konfiguracji CMDB (plik lub system), • Wpisy obejmujące rodzaj, parametry, konfigurację i przypisanego użytkownika, • Powiązania między elementami konfiguracji.
5	**Aktualizacja rejestru zasobów** *§ 19 ust. 2 pkt 2 KRI*	Bieżąca aktualizacja rejestru wraz ze zmianą otoczenia i infrastruktury IT.	• Datowane wpisy / historia zmian w rejestrze, • Procedura aktualizacji rejestru (kto, kiedy, jak).
2.3. Analiza zagrożeń związanych z przetwarzaniem informacji			
6	**Podejście do szacowania ryzyka** *§ 19 ust. 2 pkt 3 KRI*	Wskazana metodyka szacowania ryzyka odpowiednia dla SZBI, uwzględniająca kontekst działalności oraz wymagania prawne i nadzoru.	• Dokument metodyki szacowania ryzyka, • Zdefiniowane kryteria akceptacji ryzyka, • Harmonogram / zasady cykliczności analizy (min. raz w roku).

Lp.	Obszar / podstawa prawna	Wymaganie (kryterium oceny)	Dokument (przykładowy dowód realizacji)
7	**Szacowanie ryzyka** *§ 19 ust. 2 pkt 3 KRI*	Dokumentacja okresowej analizy ryzyka utraty integralności, poufności lub dostępności informacji wraz z rejestrem ryzyk i poziomami ryzyka.	• Raport z analizy ryzyka (datowany), • Rejestr ryzyk z poziomami (prawdopodobieństwo × skutek), • Rejestr ryzyk bezpieczeństwa informacji, • Protokół zatwierdzenia wyników analizy ryzyka przez kierownictwo, • Deklaracja stosowania zabezpieczeń (jeżeli została opracowana).
8	**Postępowanie z ryzykiem** *§ 19 ust. 2 pkt 3 KRI*	Proces wyboru i wdrażania środków modyfikujących ryzyko.	• Plan postępowania z ryzykiem (ryzyka, cele, zabezpieczenia), • Akceptacja ryzyka szczątkowego przez kierownictwo.
2.4. Zarządzanie uprawnieniami do pracy w systemach informatycznych			
9	**Zarządzanie uprawnieniami** *§ 19 ust. 2 pkt 4 i 5 KRI*	Uprawnienia adekwatne do zadań i obowiązków osób przetwarzających informacje; zmiana zadań skutkuje zmianą uprawnień.	• Procedura zarządzania uprawnieniami / kontroli dostępu, • Macierz / rejestr uprawnień do systemów, • Rozdzielenie uprawnień administracyjnych.
10	**Nadawanie, zmiana i odbieranie praw dostępu** *§ 19 ust. 2 pkt 4 i 5 KRI*	Poziom uprawnień adekwatny do upoważnień (w tym do przetwarzania danych osobowych); modyfikacja lub odebranie przy zmianie / zakończeniu stosunku pracy.	• Wnioski o nadanie / zmianę / odebranie uprawnień, • Upoważnienia do przetwarzania danych osobowych, • Dowody odebrania uprawnień przy odejściu / zmianie stanowiska.
2.5. Szkolenia pracowników zaangażowanych w proces przetwarzania informacji			
11	**Regulacje dotyczące szkoleń** *§ 19 ust. 2 pkt 6 KRI*	Regulacje wewnętrzne dotyczące przeprowadzania szkoleń użytkowników z bezpieczeństwa informacji.	• Procedura / regulamin szkoleń z bezpieczeństwa informacji, • Plan / harmonogram szkoleń (cykliczność).
12	**Realizacja szkoleń** *§ 19 ust. 2 pkt 6 KRI*	Wszyscy pracownicy oraz wskazani wykonawcy i strony trzecie przeszkoleni i regularnie informowani o aktualizacjach polityk i procedur.	• Listy obecności / zaświadczenia / certyfikaty ze szkoleń, • Materiały szkoleniowe i zakres tematyczny, • Dowody przeszkolenia / poinformowania stron trzecich.
2.6. Ochrona informacji przed kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami			
13	**Monitorowanie dostępu do informacji** *§ 19 ust. 2 pkt 7 KRI*	Środki techniczne i organizacyjne kontroli dostępu do informacji.	• Polityka kluczy i dostępu do pomieszczeń, • Monitoring wizyjny (regulamin + dowód funkcjonowania), • Rejestrowanie historii logowań i operacji na danych (logi).
14	**Wykrywanie nieautoryzowanych działań** *§ 19 ust. 2 pkt 7 KRI*	Środki do wykrywania nieautoryzowanych działań związanych z przetwarzaniem informacji.	• Konfiguracja blokady konta po nieudanych próbach logowania, • Systemy IDS / IPS / SIEM (jeśli stosowane), • Oprogramowanie antywirusowe; czujniki ruchu / system alarmowy.
15	**Środki przeciw nieautoryzowanemu dostępowi (OS, sieć, aplikacje)** *§ 19 ust. 2 pkt 7 KRI*	Środki uniemożliwiające nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji.	• Wymóg logowania do systemów i aplikacji; polityka haseł, • Zabezpieczenie sieci Wi-Fi i blokada nieautoryzowanych urządzeń, • Firewall i system antywirusowy (konfiguracja).
2.7. Praca na odległość i mobilne przetwarzanie danych			
16	**Praca zdalna i przetwarzanie mobilne** *§ 19 ust. 2 pkt 8 KRI*	Formalna polityka i zabezpieczenia ograniczające ryzyko związane z przetwarzaniem mobilnym i pracą zdalną.	• Polityka / procedura pracy zdalnej i urządzeń mobilnych, • Szyfrowanie urządzeń mobilnych i połączenia VPN,

Lp.	Obszar / podstawa prawna	Wymaganie (kryterium oceny)	Dokument (przykładowy dowód realizacji)
			• Zasady korzystania z sieci ogólnodostępnych.
2.8. Zabezpieczenie informacji przed ujawnieniem, modyfikacją, usunięciem lub zniszczeniem			
17	**Zabezpieczenia informacji** *§ 19 ust. 2 pkt 9 KRI*	Zabezpieczenia minimalizujące ryzyko nieuprawnionego ujawnienia, modyfikacji, usunięcia lub zniszczenia informacji.	• Kontrola dostępu do pomieszczeń; szafy/szafki zamykane na klucz, • Odpowiednie usytuowanie komputerów; firewall, • Polityka silnych haseł; monitoring wizyjny.
2.9. Serwis sprzętu informatycznego i oprogramowania			
18	**Regulacje współpracy z podmiotami zewnętrznymi** *§ 19 ust. 2 pkt 10 KRI*	Zasady współpracy z podmiotami zewnętrznymi w zakresie serwisu i rozwoju systemów, w tym wymagane klauzule bezpieczeństwa.	• Procedura współpracy z dostawcami / serwisem IT, • Wzór wymaganych klauzul bezpieczeństwa informacji.
19	**Bezpieczeństwo informacji w umowach** *§ 19 ust. 2 pkt 10 KRI*	Umowy ze stronami trzecimi obejmujące wszystkie stosowane wymagania bezpieczeństwa.	• Umowy serwisowe / rozwojowe z klauzulami bezpieczeństwa, • Zapisy o prawie do kontroli dostawcy, • Umowy powierzenia / zobowiązania do poufności (NDA).
2.10. Zasady postępowania z informacjami minimalizujące ryzyko kradzieży			
20	**Zasady postępowania z informacjami** *§ 19 ust. 2 pkt 11 KRI*	Polityki / procedury zabezpieczania danych przed nieautoryzowanym dostępem, wynoszeniem nośników i postępowania z urządzeniami mobilnymi.	• Polityka czystego biurka / czystego ekranu, • Zasady nadzorowanego dostępu do pomieszczeń, • Zasady wynoszenia danych i nośników poza miejsce pracy, • Procedura postępowania z urządzeniami mobilnymi.
2.11. Zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych			
21	**Aktualizacja oprogramowania** *§ 19 ust. 2 pkt 12 KRI*	Automatyczne / regularne aktualizacje oprogramowania lub system zarządzania aktualizacjami.	• Konfiguracja automatycznych aktualizacji, • Dziennik / harmonogram aktualizacji, • System zarządzania poprawkami (patch management).
22	**Minimalizowanie ryzyka utraty informacji** *§ 19 ust. 2 pkt 12 KRI*	Mechanizmy minimalizujące ryzyko utraty informacji w wyniku awarii.	• Harmonogram i logi kopii zapasowych (backup), • Dowód testu odtworzenia danych, • Macierze RAID; gwarancje dostawcy chmury w zakresie odtworzenia danych.
23	**Ochrona przed błędami, utratą, nieuprawnioną modyfikacją** *§ 19 ust. 2 pkt 12 (zw. z pkt 9) KRI*	Zabezpieczenia minimalizujące ryzyko nieuprawnionego ujawnienia, modyfikacji, usunięcia lub zniszczenia informacji.	• Kontrola dostępu do pomieszczeń; szafy zamykane na klucz, • Firewall; polityka silnych haseł; monitoring wizyjny.
24	**Mechanizmy kryptograficzne** *§ 19 ust. 2 pkt 12 KRI*	Szyfrowanie adekwatne do zagrożeń lub wymogów prawa.	• Szyfrowanie dysków i nośników informacji, • Szyfrowanie komunikacji (poczta elektroniczna), • Szyfrowanie połączeń zdalnych (VPN).
25	**Bezpieczeństwo plików systemowych** *§ 19 ust. 2 pkt 12 KRI*	Konta użytkowników bez uprawnień administratora; ograniczenie instalacji oprogramowania i uruchamiania plików wykonywalnych.	• Konfiguracja kont bez uprawnień administratora, • Ograniczenie instalacji oprogramowania przez użytkowników,

Lp.	Obszar / podstawa prawna	Wymaganie (kryterium oceny)	Dokument (przykładowy dowód realizacji)
			• Blokada uruchamiania plików .exe/.bat/.dll/.com.
26	**Redukcja podatności technicznych** *§ 19 ust. 2 pkt 12 KRI*	Redukcja ryzyk wynikających z opublikowanych podatności technicznych.	• Oprogramowanie do skanowania podatności + raporty skanów, • Automatyczne aktualizacje oprogramowania i systemów, • Systemy typu IPS / IDS.
27	**Reakcja na nieujawnione podatności** *§ 19 ust. 2 pkt 12 KRI*	Skuteczny system identyfikacji, zgłaszania i reagowania na nieujawnione podatności systemów IT.	• Procedura zarządzania podatnościami, • Dowody podjętych działań po wykryciu podatności.
28	**Kontrola zgodności z normami i politykami** *§ 19 ust. 2 pkt 12 KRI*	Polityki / instrukcje w zakresie standardów bezpieczeństwa systemów oraz osoby odpowiedzialne za ich kontrolę i stosowanie.	• Polityki / standardy bezpieczeństwa systemów IT, • Wyznaczenie osób odpowiedzialnych za kontrolę, • Raporty / protokoły z kontroli zgodności.
2.12. Zarządzanie incydentami związanymi z bezpieczeństwem informacji			
29	**Odpowiedzialność i procedury** *§ 19 ust. 2 pkt 13 KRI*	Odpowiedzialność kierownictwa oraz procedury zapewniające szybką i uporządkowaną reakcję na incydenty.	• Procedura zarządzania incydentami bezpieczeństwa informacji, • Przypisana odpowiedzialność kierownictwa / wyznaczonych osób.
30	**Zgłaszanie i postępowanie z incydentami** *§ 19 ust. 2 pkt 13 KRI*	Mechanizmy liczenia i monitorowania rodzajów, rozmiarów i kosztów incydentów.	• Rejestr incydentów bezpieczeństwa informacji, • Formularz zgłoszenia incydentu, • Mechanizm monitorowania liczby i skutków incydentów.
2.13. Audyt wewnętrzny z zakresu bezpieczeństwa informacji			
31	**Wykonywanie audytu** *§ 19 ust. 2 pkt 14 KRI*	Staranne planowanie i uzgadnianie wymagań audytu oraz sprawdzeń eksploatowanych systemów, by zminimalizować zakłócenia.	• Plan audytu / harmonogram audytów wewnętrznych, • Uzgodnienia zakresu i terminów audytu.
32	**Sprawozdania i działania korygujące** *§ 19 ust. 2 pkt 14 KRI*	Sprawozdania z audytu wewnętrznego w zakresie bezpieczeństwa informacji (nie rzadziej niż raz na rok).	• Sprawozdanie z audytu wewnętrznego (datowane, min. raz na rok), • Plan działań korygujących / realizacja zaleceń poaudytowych.