Decyzja nr 126
Dyrektora Generalnego Lasów Państwowych
z dnia 6 sierpnia 2025 r.

w sprawie wprowadzania Polityki Bezpieczeństwa Informacji Dyrekcji Generalnej Lasów Państwowych

(znak: EI.0413.16.2025)

Na podstawie art. 33 ust. 1 ustawy z dnia 28 września 1991 r. o lasach (t.j. Dz. U. z 2025 r. poz. 567) oraz § 6 Statutu Państwowego Gospodarstwa Leśnego Lasy Państwowe, wprowadzonego zarządzeniem nr 50 Ministra Ochrony Środowiska, Zasobów Naturalnych i Leśnictwa z dnia 18 maja 1994 r. – w wykonaniu zadań Dyrektora Generalnego Lasów Państwowych, wynikających z realizacji jego uprawnienia określonego w § 8 ust. 1 pkt 6 ww. statutu, zarządzam, co następuje:

§ 1

Wprowadzam do stosowania Politykę Bezpieczeństwa Informacji Dyrekcji Generalnej Lasów Państwowych, stanowiącą załącznik do niniejszej decyzji.

§ 2

Decyzja wchodzi w życie z dniem podpisania

DYREKTOR GENERALNY
LASÓW PAŃSTWOWYCH
Adam Wasiak

Polityka Bezpieczeństwa Informacji Dyrekcji Generalnej Lasów Państwowych

Spis treści

I. Wprowadzenie

Bezpieczeństwo informacji oraz systemów, w których informacje są przetwarzane jest jednym z kluczowych elementów zapewniających realizację zadań Dyrekcji Generalnej Lasów Państwowych. Dyrekcja Generalna Lasów Państwowych zobowiązuje się do zapewnienia najwyższych standardów ochrony bezpieczeństwa informacji, w szczególności w zakresie zachowania jej poufności, integralności oraz dostępności.

Polityka Bezpieczeństwa Informacji (PBI) określa ramy dla funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji w Dyrekcji Generalnej Lasów Państwowych. PBI opisuje zasady ochrony informacji obowiązujące w DGLP, proces zarządzania ryzykiem, role i zadania osób uczestniczących w procesie przetwarzania informacji oraz zarządzania jej bezpieczeństwem, zgodne z przepisami obowiązującego prawa, regulacjami branżowymi oraz wypracowanymi własnymi standardami w zakresie funkcjonowania organizacji.

Kierownictwo DGLP jest w pełni zaangażowane i deklaruje pełne wsparcie dla podejmowanych działań zmierzających do zapewnienia bezpieczeństwa informacji, a także zapewnia niezbędne zasoby i czas na ich realizację.

Kwestie które dotyczą bezpieczeństwa informacji i wykraczają poza ramy niniejszej polityki, zostały szczegółowo uregulowane w odrębnych decyzjach i zarządzeniach Dyrektora Generalnego Lasów Państwowych.

II. Definicje

- **Audyt bezpieczeństwa** - proces systematycznego przeglądu i oceny skuteczności systemu zarządzania bezpieczeństwem informacji zgodnie z określonymi kryteriami.
- **Bezpieczeństwo informacji** - działania mające na celu ochronę informacji przetwarzanej w systemach teleinformatycznych przed nieuprawnionym dostępem, wykorzystaniem, ujawnieniem, zakłóceniem działania, modyfikacją lub zniszczeniem.
- **Incydent bezpieczeństwa** - każde zdarzenie, które narusza polityki bezpieczeństwa lub stwarza ryzyko dla poufności, integralności lub dostępności informacji.
- **Zagrożenie bezpieczeństwa danych** - potencjalna sytuacja lub zdarzenie, które może zagrozić bezpieczeństwu informacji przetwarzanych w systemach informatycznych.
- **Poufność** - cecha informacji która zapewnienia, że informacja jest udostępniana jedynie osobom upoważnionym.
- **Integralność** - cecha, która zapewnia, że dane i systemy jej przetwarzające są dokładne, spójne i niezmienione przez osoby nieupoważnione, w sposób przypadkowy lub celowy.
- **Dostępność** - cecha, która zapewnia, terminowy i niezawodny dostęp do informacji i ich wykorzystania w przypadku wystąpienia potrzeby takiego dostępu.
- **Ciągłość działania** - Zdolność organizacji do utrzymania kluczowych funkcji i usług na akceptowalnym poziomie w przypadku zakłóceń.
- **DGLP, Organizacja** - Dyrekcja Generalna Lasów Państwowych.
- **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, zgodnie z definicją zawartą w Rozporządzeniu Parlamentu

Europejskiego i Rady (UE) 2016/679 oraz obowiązującą ustawą o ochronie danych osobowych.

- **Hasło** - sekretne słowo lub fraza używana do uwierzytelnienia użytkownika w systemie informatycznym.
- **Kontrola dostępu** - mechanizmy i procedury używane do zapewnienia, że dostęp do zasobów informatycznych jest udzielany tylko upoważnionym użytkownikom.
- **MFA (Multi-Factor Authentication), uwierzytelnianie wieloskładnikowe** - metoda uwierzytelniania użytkowników, która wymaga podania dwóch lub więcej niezależnych form weryfikacji tożsamości.
- **Polityka bezpieczeństwa informacji, PBI** - niniejszy dokument definiujący podejście organizacji do zarządzania bezpieczeństwem informacji, w tym cele, zasady i obowiązki.
- **Zasady ochrony informacji** - wszystkie ustanowione w LP zasady dotyczące bezpieczeństwa informacji.
- **Reagowanie na incydenty** - proces zarządzania i odpowiedzi na zdarzenia związane z bezpieczeństwem informacji w celu minimalizacji skutków.
- **System Informatyczny Lasów Państwowych, SILP** - zbiór elementów, którego funkcją jest przetwarzanie, przechowywanie i przesyłanie danych w PGL LP przy użyciu techniki komputerowej.
- **Użytkownik SILP** - pracownik DGLP, w okresie pozostawania w stosunku zatrudnienia lub inna osoba fizyczna wykonująca prace na podstawie umowy o dzieło, umowy zlecenia lub innej umowy cywilnoprawnej w okresie obowiązywania umowy.
- **Administrator SILP** - pracownicy Wydziału Informatyki DGLP którzy są odpowiedzialni za zasoby SILP.
- **Dane SILP stanowiące tajemnice przedsiębiorstwa** - dane stanowiące tajemnicę przedsiębiorstwa zgodnie z klasyfikacją danych określoną przez stosowne zarządzenie Dyrektora Generalnego Lasów Państwowych.
- **Przetwarzanie danych, przetwarzanie informacji** - operacja lub zestaw operacji wykonywanych na danych lub zestawach danych w sposób zautomatyzowany lub niezautomatyzowany, taką jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
- **System Zarządzania Bezpieczeństwem Informacji, SZBI** - zestaw zasad, procesów, procedur, struktur organizacyjnych i zasobów wykorzystywanych do ochrony informacji w organizacji.
- **VPN (Virtual Private Network)** - technologia umożliwiająca bezpieczne połączenie z siecią LP za pośrednictwem sieci publicznych przez zaszyfrowany tunel, co zapewnia poufność i integralność przesyłanych danych.
- **Zarządzanie ryzykiem** - proces identyfikacji, oceny i klasyfikacji ryzyk oraz wdrażania środków zaradczych w celu ich minimalizacji.
- **Zarządzanie tożsamością i dostępem** - procedury i technologie służące do zarządzania dostępem do zasobów informatycznych, w tym identyfikacja i uwierzytelnianie użytkowników.

- **ZCI, Zespół ds. Cyberbezpieczeństwa -** komórka organizacyjna w Wydziale Informatyki DGLP dedykowana do sprawa związanych z bezpieczeństwem informacji.
- **ZILP, Zakład Informatyki Lasów Państwowych** – jednostka w strukturze PGL LP, która utrzymuje składniki SILP służące do przetwarzania oraz prowadzi przetwarzanie danych na rzecz innych jednostek w tym DGLP.

III. Cel

Celem PBI jest zdefiniowanie i ustanowienie zasad właściwej ochrony i utrzymania bezpieczeństwa informacji przetwarzanych przez DGLP oraz zasad funkcjonowania SZBI w organizacji. Realizowane jest to poprzez wdrożenie odpowiednich działań i środków zarządzania, które minimalizują ryzyko związane z zagrożeniami wewnętrznymi i zewnętrznymi dla bezpieczeństwa informacji przetwarzanych przez DGLP. Dla osiągnięcia zamierzonego celu podjęte zostały następujące działania:

1. Zabezpieczenie informacji przed zagrożeniami wewnętrznymi i zewnętrznymi poprzez wdrożenie odpowiednich procedur organizacyjnych oraz systemów zabezpieczeń technicznych.
2. Dążenie do zapewnienia poufności (dostępność informacji jedynie dla uprawnionych osób), integralności (zapewnienie kompletności i dokładności danych) oraz dostępności informacji (zapewnienie ich dostępności w wymaganym czasie).
3. Wszystkie działania w zakresie zarządzania bezpieczeństwem informacji będą prowadzone zgodnie z obowiązującymi przepisami prawa oraz regulacjami wewnętrznymi organizacji.
4. Ustanowienie odpowiednich procedur organizacyjnych i utrzymanie środków technicznych, które tworzą sprawny System Zarządzania Bezpieczeństwem Informacji.
5. Wyznaczenie zadań i odpowiedzialności osób zaangażowanych w przetwarzanie informacji. Określenie ich zadań i odpowiedzialności związanych z ochroną informacji.
6. Identyfikacja właścicieli aktywów i zasobów informatycznych poprzez wyznaczenie właścicieli aktywów i zasobów informatycznych, którzy będą odpowiedzialni za zapewnienie zgodnego z PBI poziomu bezpieczeństwa przetwarzanych informacji.
7. Prowadzenie współpracy z podmiotami zewnętrznymi w sposób gwarantujący realizację zleconych przez DGLP zadań w zgodności z obowiązującą PBI.
8. Prowadzenie regularnego przeglądu i dostosowanie polityk, procedur oraz dokumentacji związanej z bezpieczeństwem informacji, mające na celu weryfikację i zapewnienie zgodności z bieżącymi wymogami.
9. Wdrażanie procedur reakcji na zagrożenia i incydenty związane z bezpieczeństwem informacji. Prowadzenie działań korygujących i minimalizujących skutki incydentu.
10. Prowadzenie regularnych działań podnoszących świadomość pracowników w zakresie bezpieczeństwa informacji, poprzez szkolenia i działania edukacyjne.
11. Stałe doskonalenie System Zarządzania Bezpieczeństwem Informacji zgodnie z wymaganiami prawnymi oraz uwagami wszystkich uczestniczących w procesie ochrony informacji stron, w celu optymalizacji poziomu ochrony danych.

IV. Role i odpowiedzialności uczestników procesu

Dyrektor Generalny Lasów Państwowych ustanawia i realizuje strategiczne cele Polityki Bezpieczeństwa Informacji, a właścicielem procesu zarządzania bezpieczeństwem informacji jest Kierownik Zespołu ds. Cyberbezpieczeństwa w Wydziale Informatyki DGLP.

Odpowiedzialności

Określenie odpowiedzialności związanych z bezpieczeństwem informacji to kluczowy element skutecznego zarządzania ochroną danych i zasobów informatycznych. Zostały zdefiniowane i określone podstawowe role i odpowiedzialności związane z procesem utrzymania bezpieczeństwem informacji w DGLP:

Dyrektor Generalny Lasów Państwowych:

1) Ustanawia Polityki Bezpieczeństwa Informacji, określa strategiczne cele dla bezpieczeństwa informacji.
2) Zapewnienia odpowiednie środki finansowe, osobowe i technologiczne dla działań związanych z bezpieczeństwem informacji.
3) Zatwierdza okresowe raporty dotyczące realizacji celów i skuteczności ustanowionych polityk bezpieczeństwa informacji.
4) Zarządza okresowe audyty oceniające skuteczności stosowanych w DGLP środków ochrony bezpieczeństwa informacji SILP.
5) Ustanawia wymagania odnośnie bezpieczeństwa SILP dla wszystkich jednostek PGL LP, w tym dla Dyrekcji Generalnej Lasów Państwowych oraz kontroluje ich realizację.

Zespół ds. Cyberbezpieczeństwa w Wydziale Informatyki DGLP:

1) Nadzoruje i monitoruje realizację Polityki Bezpieczeństwa Informacji.
2) Zapewnienia, że procesy wymagane w zarządzaniu bezpieczeństwem są ustanowione, wdrożone i utrzymywane.
3) Prowadzi nadzór nad dokumentacją dotyczącą bezpieczeństwa informacji w systemach informatycznych organizacji na etapach jej opracowywania, weryfikacji, aktualizacji, udostępniania i przechowywania.
4) Prowadzi analizy ryzyka dla bezpieczeństwa informacji w systemach teleinformatycznych organizacji.
5) Utrzymuje lub nadzoruje utrzymanie aktywa teleinformatyczne uczestniczące w przetwarzaniu informacji.
6) Implementuje lub nadzoruje implementacje polityk bezpieczeństwa informacji.
7) Opracowuje szczegółowe polityki bezpieczeństwa dla systemów teleinformatycznych Informatycznych.
8) Prowadzi nadzór nad bezpieczeństwem informacji systemów teleinformatycznych. Monitoruje i nadzoruje przestrzeganie ustanowionych zasad polityki bezpieczeństwa informacji.
9) Utrzymuje System Zarządzania Bezpieczeństwem Informacji. Prowadzi okresową ocenę skuteczności oraz działania korygujące i usprawniające jego działanie.

10) Koordynuje realizacje audytów w zakresie bezpieczeństwa informacji w systemach informatycznych.
11) Prowadzi audyt w jednostkach LP w zakresie bezpieczeństwa informacji w systemach teleinformatycznych.
12) Koordynuje lub organizuje przeglądy bezpieczeństwa systemów teleinformatycznych DGLP.
13) Prowadzi nadzór nad realizacją zaleceń wynikających z audytów i przeglądów.
14) Raportuje Dyrektorowi Generalnemu Lasów Państwowych o funkcjonowaniu procesu zarządzania bezpieczeństwem informacji oraz o informuje o realizacji jego celów i skuteczności.
15) Prowadzi i koordynuje organizacje szkoleń dotyczących bezpieczeństwa informacji w systemach informatycznych dla użytkowników SILP.
16) Analizuje raporty dotyczące zdarzeń i incydentów związanych z bezpieczeństwem systemów teleinformatycznych.
17) Informuje i ostrzega administratorów oraz użytkowników SILP o znanych zagrożeniach dla bezpieczeństwa informacji przetwarzanych w systemach teleinformatycznych.
18) Opracowuje, wprowadza i okresowo testuje plany ciągłości działania i planów awaryjnych dla systemów teleinformatycznych DGLP.
19) Prowadzi współpracę operacyjną z krajowymi Zespołami Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT GOV, CSIRT NASK, CSIRT MON).
20) Prowadzi okresową analizę podatności systemów teleinformatycznych na zagrożenia.
21) Prowadzi obsługę i reaguje na zgłoszenia dotyczące zagrożeń bezpieczeństwa informacji przetwarzanych w systemach teleinformatycznych.
22) Prowadzi wsparcie merytoryczne komórek organizacyjnych DGLP w działaniach, które mogą mieć wpływ na bezpieczeństwo informacji w systemach teleinformatycznych.
23) Prowadzi i aktualizuje rejestr podmiotów które dostarczają oprogramowanie, sprzęt lub usługi cyfrowe krytyczne dla ciągłości działania kluczowych procesów w organizacji.

Administratorzy SILP w Wydziale Informatyki DGLP:

1) Implementują w zarządzanych systemach polityki i procedury bezpieczeństwa informacji.
2) Zarządzają dostępem do systemów zapewniając, że dostępy są przyznawane jedynie uprawnionym użytkownikom z zachowaniem zasady najmniejszych uprawnień.
3) Monitorują aktywności utrzymywanych systemów, identyfikują anomalie, reagują i niezwłocznie raportują do Zespołu ds. Cyberbezpieczeństwa o wykrytych incydentach.
4) Współpracują w zakresie realizacji zadań związanych z bezpieczeństwem informacji oraz realizuje wytyczne Zespołu ds. Cyberbezpieczeństwa.
5) Na bieżąco instalują aktualizacje krytyczne i bezpieczeństwa w utrzymywanych systemach w celu eliminacji ich podatności.
6) Zabezpieczają dowody i tworzy dokumentacje dla wykrytych incydentów.
7) Tworzą lub gwarantują tworzenie kopii zapasowych dla utrzymywanych systemów teleinformatycznych.
8) Regularnie weryfikują poprawność tworzonych kopii zapasowych.
9) Tworzą procedury odzyskiwania zarządzanych systemów teleinformatycznych z kopii zapasowych.

10) Tworzą procedury awaryjnego dostępu administracyjnego do zarządzanych systemów dla pozostałych administratorów.
11) Zapewniają, że wszystkie prowadzone działania administracyjne są zgodne z polityką bezpieczeństwa informacji oraz regulacjami wewnętrznymi organizacji.
12) Identyfikują ryzyka dla systemów i uczestniczą w prowadzonym procesie analizy ryzyka.

Kierownicy komórek organizacyjnych DGLP:

1) Wnioskują do kierownictwa DGLP o nadanie, zmianę lub odebranie uprawnień do danych SILP dla podległych pracowników w zakresie działań podległej komórki organizacyjnej.
2) Informują pracowników o obowiązkach związanych z ochroną informacji na stanowiskach pracy.
3) Egzekwują przestrzeganie zasad ochrony informacji przetwarzanych w systemach teleinformatycznych przez podległych pracowników.
4) Informują Zespół ds. Cyberbezpieczeństwa w Wydziale Informatyki DGLP o prowadzonych działaniach, które mogą mieć wpływ na bezpieczeństwo informacji w systemach teleinformatycznych.
5) Informują Zespół ds. Cyberbezpieczeństwa o zidentyfikowanych zagrożeniach dla bezpieczeństwa informacji w obszarze działania nadzorowanej komórki organizacyjnej.

Użytkownicy SILP w DGLP

1) Przestrzegają zasad ochrony informacji przetwarzanych w SILP.
2) Informują kierownika własnej komórki lub bezpośrednio pracowników Wydziału Informatyki DGLP o zidentyfikowanych incydentach, zagrożeniach dla bezpieczeństwa informacji oraz nieprawidłowościach w pracy systemów informatycznych.
3) Współpracują z pracownikami Wydziału Informatyki DGLP w celu identyfikacji i dokumentowania zagrożeń dla bezpieczeństwa informacji SILP.
4) Dbają o poprawności merytoryczną wprowadzanych za pomocą systemów informatycznych danych.
5) Stosują złożone i unikalne hasła dostępu, zgodnie z zasadami bezpieczeństwa.
6) Dbają o bezpieczeństwo fizyczne powierzonych środków przetwarzania danych, w szczególności w przypadku ich wynoszenia poza siedzibę organizacji.

Komórka organizacyjna właściwa ds. administracji;

1) Opracowuje i wdraża zasady kontroli dostępu do biura DGLP.
2) Zapewnienia, że dostęp do wydzielonych stref w biurze mają wyłącznie osoby upoważnione.
3) Prowadzi wewnętrzny i zewnętrzny monitoring wizyjny budynku DGLP.
4) Organizuje ochronę fizyczną biura DGLP poprzez personel ochrony fizycznej i monitoring wizyjny.
5) Prowadzi monitoring wejść i wyjść oraz ważnych obszarów za pomocą kamer i innych systemów bezpieczeństwa.
6) Prowadzi rejestr zdarzeń związanych z naruszeniem lub próbami naruszeń fizycznego bezpieczeństwa.
7) Utrzymuje systemy doprowadzenia zasilania podstawowego i awaryjnego do serwerowni w biurze DGLP.

Komórka organizacyjna właściwa ds. ochrony danych osobowych, w której skład wchodzi Inspektor Ochrony Danych;

1) Opracowuje, wdraża i nadzoruje realizację polityki bezpieczeństwa danych osobowych w DGLP, zapewniając zgodność z przepisami Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 oraz przepisami krajowymi.
2) Wspiera Inspektora Ochrony Danych (IOD) w wykonywaniu jego zadań oraz zapewnia mu niezbędne zasoby i warunki pracy.
3) Informuje Administratora danych oraz pracowników i współpracowników o ich obowiązkach wynikających z RODO oraz innych przepisów dotyczących ochrony danych osobowych, a także udziela im doradztwa w tych sprawach.
4) Monitoruje przestrzeganie przepisów RODO i wewnętrznych regulacji dotyczących ochrony danych osobowych przez osoby upoważnione do ich przetwarzania.
5) Prowadzi działania podnoszące świadomość oraz organizuje szkolenia dla osób uczestniczących w operacjach przetwarzania danych osobowych w DGLP.
6) Współpracuje z organem nadzorczym do spraw ochrony danych osobowych — Prezesem Urzędu Ochrony Danych Osobowych i pełni funkcję punktu kontaktowego dla organu nadzorczego w kwestiach związanych z ochroną danych osobowych.
7) Pełni funkcję punktu kontaktowego dla osób, których dane są przetwarzane, w zakresie realizacji ich praw określonych w RODO.
8) Koordynuje oraz współuczestniczy w opracowywaniu, aktualizowaniu i opiniowaniu wewnętrznych aktów prawnych oraz procedur, odnoszących się do ochrony danych osobowych.
9) Zapewnia obsługę dedykowanego adresu e-mail: dane.osobowe@lasy.gov.pl.
10) Identyfikuje zagrożenia oraz przeprowadza analizę ryzyka związanego z przetwarzaniem danych osobowych, w tym – w przypadkach wymaganych przepisami prawa – dokonuje oceny skutków dla ochrony danych (DPIA).Analizuje sytuacje i przyczyny naruszeń bezpieczeństwa danych oraz zarządza procesem reagowania na naruszenia, w tym ich zgłaszaniem organowi nadzorczemu oraz informowaniem osób, których dane dotyczą. Wnioskuje do Dyrektora Generalnego o wdrożenie adekwatnych zabezpieczeń dostosowanych do poziomu ryzyka.
11) Zapewnia bieżące wsparcie merytoryczne dla wszystkich komórek organizacyjnych DGLP w zakresie ochrony danych osobowych.
12) Nadzoruje oraz koordynuje sprawy dotyczące ochrony danych osobowych w LP.
13) Prowadzi audyty mające na celu ocenę skuteczności stosowanych środków ochrony danych osobowych oraz aktualności dokumentacji związanej z przetwarzaniem danych.
14) Inicjuje oraz realizuje działania doskonalące system ochrony danych osobowych w DGLP.

Komórka organizacyjna właściwa ds. informacji niejawnych;

1) Prowadzi nadzór nad ochroną informacji niejawnych w DGLP
2) Prowadzi kancelarię tajną DGLP oraz zapewnia ochronę informacji niejawnych.

V. Zakres i sposób postępowania

Zakres

Polityka reguluje wszystkie aspekty bezpieczeństwa informacji w Dyrekcji Generalnej Lasów Państwowych, w szczególności dotyczące informacji przetwarzanych w systemach teleinformatycznych z wykluczeniem danych osobowych i niejawnych, które są uregulowane w osobnych dokumentach.

Zaangażowanie kierownictwa

Kierownictwo DGLP przywiązuje szczególną wagę do ochrony informacji przetwarzanych przez organizację. Inicjuje i nadzoruje działania zmierzające do zapewnienia odpowiedniego poziomu bezpieczeństwa oraz aktywnie wspiera realizację procesów ochrony. Zapewnia niezbędne zasoby i czas na realizacje działań zmierzających do uzyskania odpowiedniego poziomu bezpieczeństwa informacji ze szczególnym uwzględnieniem wymagań wobec ich poufności, dostępności oraz integralności.

Kierownictwo DGLP ustanawia SZBI i wprowadza zasady jego funkcjonowania oraz deklaruje, że wdrożony SZBI, którego elementem jest niniejsza PBI, będzie podlegał regularnym przeglądom i doskonaleniu.

VI. System Zarządzania Bezpieczeństwem Informacji

System Zarządzania Bezpieczeństwem Informacji w DGLP stanowi zintegrowany zbiór polityk, procedur, procesów i środków technologicznych, których celem jest zapewnienie odpowiedniego poziomu ochrony przetwarzanych danych. SZBI opiera się na podejściu systemowym, które pozwala na identyfikowanie, ocenę i minimalizowanie ryzyka związanego z zagrożeniami bezpieczeństwa informacji, jednocześnie uwzględniając realizację strategicznych celów organizacji. Kluczowym celem SZBI jest dążenie do utrzymania poufności, integralności i dostępności danych, co przekłada się na ochronę interesów organizacji, jej klientów oraz partnerów biznesowych.

SZBI definiuje ramy operacyjne, w których działa DGLP, określając jakie środki techniczne i organizacyjne należy zastosować, aby spełnić wymagania prawne, regulacyjne i branżowe. Umożliwia wdrażanie i egzekwowanie zasad bezpieczeństwa w sposób spójny i efektywny. SZBI wspiera również budowanie świadomości pracowników w zakresie ochrony informacji poprzez szkolenia, audyty oraz monitorowanie zgodności z polityką.

Dzięki SZBI DGLP chroni swoje zasoby i może sprawnie reagować na incydenty bezpieczeństwa, stale doskonalić swoje procedury i zwiększać odporność na potencjalne zagrożenia.

1. Zarządzanie aktywami

1.1. Identyfikacja aktywów

Wszystkie aktywa służące do przetwarzania informacji muszę być zidentyfikowane i zinwentaryzowane w zakresie obejmującym co najmniej:

1) Opis urządzenia/systemu
2) Przypisanie do zasobu jego użytkownika lub odpowiedzialnego administratora.
3) Informacje o klasyfikacji przetwarzanych danych

1.2. Klasyfikacja informacji

Informacje przetwarzane w SILP są sklasyfikowane zgodnie z ich wartością, krytycznością oraz wrażliwością. Informacje klasyfikowane są do grup:

1) Dane SILP stanowiące tajemnicę przedsiębiorstwa i inne dane, które mogą mieć wpływ na działanie i bezpieczeństwo PGL LP
2) Pozostałe dane SILP
3) Dane osobowe
4) Informacje niejawne

2. Kontrola dostępu

2.1. Zasada najmniejszych uprawnień

Dostęp do informacji i systemów informatycznych jest przyznawany wyłącznie na podstawie zasadzie najmniejszych uprawnień, co oznacza, że użytkownicy mają dostęp tylko do tych zasobów, które są niezbędne do wykonywania ich obowiązków.

Podstawową metodą uwierzytelnienia użytkownika i administratorów w systemach wewnętrznych jest uwierzytelnienie przy pomocy kraty kryptograficznej i certyfikatu korporacyjnego PKI LP lub haseł jednorazowych do sieci SILP.

2.2. Uwierzytelnianie wieloskładnikowe (MFA)

W celu podniesienie poziomu bezpieczeństwa, dostęp użytkowników do zasobów SILP w standardowym trybie realizowany jest z wykorzystaniem uwierzytelniania wieloskładnikowego (MFA). Każdy użytkownik łączący się z SILP, musi przejść proces autoryzacji z użyciem co najmniej dwóch niezależnych składników uwierzytelniających.

2.3. Ochrona przed nieautoryzowanym dostępem

Wszystkie systemy o ile to technicznie możliwe muszą posiadać blokady konta po kilku nieudanych próbach logowania oraz regularne monitorowanie logowań i wykrywanie podejrzanej aktywności.

2.4. Monitorowanie dostępu

Wszystkie próby dostępu do systemów informatycznych LP muszą być logowane i regularnie monitorowane w celu wykrywania i reagowania na nieautoryzowane próby dostępu.

2.5. Przeglądy dostępu

Wykonywane są regularne przeglądy uprawnień dostępu do systemów informatycznych w celu zapewnienia, że dostęp jest zgodny z aktualnymi potrzebami użytkowników.

2.6. Złożoność haseł i numerów PIN

Hasła i numery PIN uwierzytelniające dostępy do SILP musza mieć określone i weryfikowane minimalne wymagania dla złożoności.

2.7. Dostępy administratorów do systemów

Zabroniony jest dostęp administracyjny do systemów w celach innych niż prace związane z administracją, utrzymaniem lub diagnostyką działania systemów.

2.8. Zapamiętywanie haseł w przeglądarkach

Zabronione jest używanie przeglądarek internetowych z włączoną funkcją zapamiętywania identyfikatorów i haseł.

3. Cykl funkcjonowania systemów informatycznych w DGLP

3.1. Bezpieczeństwo w cyklu życia systemu

W celu zapewnienia skutecznej ochrony informacji oraz zgodności z obowiązującymi regulacjami, organizacja zobowiązuje się do uwzględniania aspektów bezpieczeństwa informacji na każdym etapie projektowania, wdrażania, testowania, utrzymania i wycofania z eksploatacji systemów IT.

3.2. Bezpieczeństwo na etapie projektowania

Każdy wdrażany system informatyczny oraz każda znacząca modernizacja istniejących rozwiązań muszą być poprzedzone analizą ryzyka, mającą na celu identyfikację potencjalnych zagrożeń, podatności oraz ocenę wpływu na poufność, integralność i dostępność przetwarzanych danych. Wymagane jest uwzględnienie odpowiednich środków technicznych i organizacyjnych, takich jak kontrola dostępu, szyfrowanie, monitorowanie oraz mechanizmy reagowania na incydenty, już na etapie projektowania systemów - zasada „security by design and default".

3.3. Testowanie bezpieczeństwa

Wdrażane systemy informatyczne, a także istotne modyfikacje w istniejących systemach, które mogą mieć wpływ na bezpieczeństwo informacji, muszą być poddane testom bezpieczeństwa przed ich dopuszczeniem do eksploatacji. Testy te powinny obejmować zarówno analizę potencjalnych podatności, jak i ocenę skuteczności zastosowanych mechanizmów ochronnych.

W przypadku wykrycia jakichkolwiek nieprawidłowości dotyczących funkcjonowania systemu po wprowadzeniu zmian, należy niezwłocznie wycofać wprowadzone modyfikacje oraz podjąć działania mające na celu usunięcie wszystkich stwierdzonych nieprawidłowości. Dodatkowo, przed ponownym wdrożeniem zmian, konieczne jest przeprowadzenie powtórnych testów bezpieczeństwa w celu potwierdzenia, że wszystkie

problemy zostały skutecznie wyeliminowane i system spełnia wymagane standardy bezpieczeństwa informacji.

3.4. Likwidacja aktywów SILP

W procesie wycofywania aktywów SILP z eksploatacji, DGLP zobowiązuje się do zapewnienia pełnego bezpieczeństwa informacji przetwarzanych na tych zasobach. Przed likwidacją należy przeprowadzić archiwizację istotnych danych oraz skuteczne i trwałe usunięcie wszystkich informacji chronionych, zgodnie z obowiązującymi przepisami prawa oraz wewnętrznymi regulacjami.

4. Relacje z podmiotami zewnętrznymi

Polityka Bezpieczeństwa Informacji DGLP zapewnia, że każdy dostęp do zasobów SILP DGLP przez podmioty zewnętrzne jest ściśle kontrolowany, ograniczony do niezbędnego minimum, monitorowany i zgodny z najwyższymi standardami bezpieczeństwa informacji.

4.1. Formalizacja współpracy

1) Współpraca z podmiotami zewnętrznymi odbywa się wyłącznie na podstawie pisemnych umów lub porozumień, które precyzują zakres, czas trwania oraz warunki dostępu do zasobów SILP i systemów informatycznych DGLP.
2) Podmiot mający otrzymać dostęp do zasobów SILP DGLP zobowiązany jest do podpisania stosownego oświadczenia akceptującego zasady udzielenia dostępu.

4.2. Zakres i czas dostępu do systemów

1) Dostęp do SILP i innych zasobów informatycznych dla podmiotów zewnętrznych przyznawany jest wyłącznie na czas obowiązywania umowy lub porozumienia.
2) Dostęp jest udzielany wyłącznie do minimalnego, niezbędnego zakresu zasobów wymaganych do realizacji powierzonych zadań, zgodnie z zasadą najmniejszych uprawnień.
3) Po zakończeniu współpracy lub wygaśnięciu umowy dostęp do systemów i zasobów jest niezwłocznie wycofywany, a konta użytkowników podmiotów zewnętrznych są blokowane.
4) Zabrania się prób uzyskania dostępu do innych zasobów niż te, na które została wydana zgoda.

4.3. Uprawnienia i identyfikacja użytkowników

1) Dostęp otrzymują wyłącznie wskazani imiennie pracownicy podmiotu zewnętrznego, dla których tworzone są indywidualne konta użytkownika.
2) Wszystkie konta podmiotów zewnętrznych są rejestrowane i zarządzane w centralnym katalogu użytkowników.

4.4. Bezpieczeństwo połączeń serwisowych

1) Zdalny dostęp z sieci Internet może być realizowany jedynie za pośrednictwem szyfrowanych połączeń VPN.
2) Dostęp może być realizowany wyłącznie z urządzeń spełniających wymagania bezpieczeństwa.
3) Dostęp może być realizowany jedynie z obszaru Unii Europejskiej.
4) Maksymalne dopuszczalne pasmo połączenia VPN jest ograniczone zgodnie z polityką DGLP dla ruchu sieciowego.
5) Wszystkie połączenia VPN są rejestrowane i monitorowane zgodnie z obowiązującymi politykami bezpieczeństwa.

4.5. Krytyczność dostawców

1) W celu identyfikacji i klasyfikacji dostawców, DGLP prowadzi i aktualizuje rejestr podmiotów które dostarczają oprogramowanie, sprzęt lub usługi cyfrowe krytyczne dla ciągłości działania kluczowych procesów w organizacji.
2) Rejestr zawiera dane o dostawcach, zakresie dostaw i świadczonych usług, informacje o potencjalnym wpływie na organizacje oraz informacje o zawartych umowach.
3) Za prowadzenie rejestru odpowiada Zespół ds. Cyberbezpieczeństwa.

5. Zarządzanie incydentami bezpieczeństwa informacji

DGLP prowadzi zarządzanie zgłoszonymi lub wykrytymi incydentami i zagrożeniami bezpieczeństwa informacji. Proces ten ma na celu szybką analizę i mitygację negatywnych dla organizacji skutków incydentów i zagrożeń oraz poprawę skuteczności ochrony w zastosowanych zabezpieczeniach technicznych i organizacyjnych.

5.1. Zgłaszanie incydentów i zagrożeń bezpieczeństwa

1) Każdy użytkownik SILP ma obowiązek poinformować kierownika własnej komórki lub bezpośrednio pracowników Wydziału Informatyki DGLP o zidentyfikowanych incydentach, zagrożeniach dla bezpieczeństwa informacji oraz nieprawidłowościach w pracy systemów informatycznych.
2) Dla użytkowników SILP został utworzone dedykowane kanały elektroniczne do zgłaszania incydentów i zagrożeń bezpieczeństwa informacji.

5.2. Obsługa incydentów i zagrożeń bezpieczeństwa

1) Działania związane z obsługą zgłoszonych incydentów i zagrożeń bezpieczeństwa prowadzi Zespół ds. Cyberbezpieczeństw.
2) Utrzymywany jest rejestr zgłoszeń incydentów i zagrożeń informacji.

3) Incydenty bezpieczeństwa są obsługiwane zgodnie z ustaloną procedurą, która obejmują analizę, klasyfikację, reakcję i działania naprawcze.
4) Zagrożenia bezpieczeństwa są obsługiwane zgodnie z ustaloną procedurą, która obejmują analizę, klasyfikację oraz w wymaganych przypadkach reakcję i działania naprawcze.

5.3. Współpraca i komunikacja

1) W przypadku incydentów i zagrożeń bezpieczeństwa informacji dotyczących systemów SILP utrzymywanych przez DGLP, ZCI informuje i prowadzi współpracę z ich administratorami.
2) W ramach obsługi incydentów i zagrożeń bezpieczeństwa informacji o dużym znaczeniu dla organizacji, ZCI informuje i prowadzi współpracę operacyjną z krajowymi Zespołami Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT GOV, CSIRT NASK, CSIRT MON).
3) W ramach obsługi incydentów i zagrożeń bezpieczeństwa informacji o dużym znaczeniu dla organizacji i dotyczących systemów utrzymywanych przez podległą jednostkę LP, ZCI koordynuje działania wspólne prowadzone z jednostką LP oraz z krajowymi Zespołami Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT GOV, CSIRT NASK, CSIRT MON).
4) W przypadku naruszenia bezpieczeństwa informacji zawierających dane osobowe ZCI informuje i prowadzi współprace z Inspektorem ochrony danych osobowych w DGLP.
5) W przypadku incydentów mogących mieć wpływ na ciągłość działania organizacji ZCI informuje i prowadzi współpracę z Głównym Inspektorem Straży Leśnej.

5.4. Reakcja i działania naprawcze

W ramach reakcji na wykryte incydenty naruszenia bezpieczeństwa informacji Zespół ds. Cyberbezpieczeństwa może wykonać lub zlecić:

1) izolację zagrożonych systemów,
2) zmianę konfiguracji systemów,
3) zabezpieczenie dowodów tj. logi czy kopie zapasowe,
4) przywrócenie usług i danych z kopi bezpieczeństwa,
5) inne, adekwatne do wykrytych zagrożeń działania mitygujące.

W ramach działań naprawczych dla wykrytych incydentów naruszenia bezpieczeństwa informacji Zespół ds. Cyberbezpieczeństwa może wykonać lub zlecić:

6) Identyfikacje podatności i słabych punktów w bezpieczeństwie systemów SILP w DGLP.
7) Przygotowanie rekomendacji i zlecenie działań naprawczych dla podatnych systemów.
8) Wprowadzenie zmian w dokumentacji bezpieczeństwa na podstawie wniosków z incydentów.
9) Przeprowadzenie dodatkowych szkoleń dla pracowników w zakresie wykrytych zagrożeń.

6. Bezpieczeństwo informacji w zarządzaniu ciągłością działania organizacji

6.1. Identyfikacja kluczowych procesów

DGLP prowadzi identyfikacje procesów kluczowych dla zachowania ciągłości działania organizacji. Prowadzona analiza funkcjonujących procesów biznesowych ma na celu wyłonienia tych, które są niezbędne dla funkcjonowania organizacji oraz mają kluczowe znaczenie dla ochrony informacji oraz minimalizacje skutków potencjalnych incydentów bezpieczeństwa. Identyfikacja kluczowych procesów umożliwia skuteczne planowanie i wdrażanie zabezpieczeń, a także zapewnia, że działania związane z bezpieczeństwem informacji są ukierunkowane na obszary o największym znaczeniu dla ciągłości działania organizacji.

6.2. Opracowanie planów ciągłości działania

Dla zidentyfikowanych procesów kluczowych opracowywane są plany ciągłości działania, które muszą uwzględniać co najmniej następujące aspekty:

1) Zabezpieczenie informacji, w tym regularne wykonywanie kopii zapasowych danych oraz zapewnienie ich bezpiecznego przechowywania i szybkiego odtworzenia.
2) Procedury odtwarzania systemów informatycznych, obejmujące szczegółowe instrukcje postępowania na wypadek awarii lub incydentu.
3) Działania minimalizujące czas przestoju oraz umożliwiające przywrócenie kluczowych procesów w możliwie najkrótszym czasie.
4) Określenie niezbędnych zasobów, zarówno technicznych, jak i personalnych, wymaganych do utrzymania ciągłości działania kluczowych operacji.
5) Podział ról i obowiązków w przypadku aktywacji planów ciągłości działania, zapewniający skuteczną koordynację i komunikację w sytuacjach kryzysowych.

6.3. Zarządzanie kopiami bezpieczeństwa danych SILP

Zarządzanie kopiami bezpieczeństwa danych SILP jest kluczowym elementem zapewniającym bezpieczeństwo informacji i jest realizowane w oparciu o dedykowaną politykę bezpieczeństwa dla kopii, przy szczególnym uwzględnieniu następujących aspektów:

1) Regularne wykonywanie kopii zapasowych wszystkich krytycznych danych i systemów SILP, prowadzone jest zgodnie z wymaganym harmonogramem.
2) Przechowywanie kopii bezpieczeństwa danych dla kluczowych systemów prowadzone jest w bezpiecznych lokalizacjach, które są geograficznie odseparowane od głównych systemów produkcyjnych, co minimalizuje ryzyko utraty danych w wyniku lokalnych incydentów obszarowych.
3) Prowadzone są okresowe testy odtwarzania kopii bezpieczeństwa danych w celu weryfikacji ich integralności, kompletności oraz możliwości skutecznego przywrócenia danych i systemów w przypadku awarii lub innych zdarzeń kryzysowych.

6.4. Przeglądy testowanie i aktualizacja planów ciągłości działania

Co najmniej raz na rok DGLP wykonuje okresowe testowanie, przeglądy i aktualizacje planów ciągłości działania, ponieważ jest to kluczowe dla zapewnienia ich skuteczności, spójności oraz dostosowania do bieżących potrzeb organizacji. Plany ciągłości są testowane, przy czym testy te powinny obejmować:

1) Symulacje różnych scenariuszy incydentów.
2) Odtwarzanie danych z kopii bezpieczeństwa.
3) Odtwarzania systemów informatycznych z uwzględnieniem czasu reakcji oraz minimalizacji czasu przestojów.
4) Kontrolowane wyłączenia centrów przetwarzania danych, które pozwalają zweryfikować rzeczywistą odporność infrastruktury oraz skuteczność przełączania na środowiska zapasowe.

Na podstawie wyników wykonanych testów organizacja prowadzi konieczne aktualizacje planów ciągłości działania

7. Monitorowanie SILP, przeglądy SZBI i PBI

7.1. Monitorowanie systemów

Systemy informatycznych SILP w organizacji są stale monitorowane w celu szybkiego wykrywania nieautoryzowanych działań, prób naruszenia bezpieczeństwa oraz potencjalnych zagrożeń dla informacji. Monitoring obejmuje zarówno infrastrukturę techniczną, jak i kluczowe aplikacje oraz systemy przetwarzające informacje. Takie działania umożliwiają wczesne reagowanie na incydenty oraz minimalizację ryzyka naruszeń bezpieczeństwa informacji. Wyniki monitoringu są rejestrowane, analizowane i raportowane do ZCI.

7.2. Przeglądy i ich zakres

Polityka bezpieczeństwa informacji i SZBI podlegają okresowym przeglądom i aktualizacjom, w celu zapewnienia ich zgodność z aktualnymi wymaganiami prawnymi, regulacyjnymi, zmianami technologii oraz nowymi rodzajami zagrożeń. Przeglądy powinny być przeprowadzane co najmniej raz w roku, a także po każdej istotnej zmianie w infrastrukturze, procesach biznesowych lub po wystąpieniu poważnego incydentu bezpieczeństwa.

Zakres przeglądów obejmuje kompleksową ocenę wyników audytów wewnętrznych i zewnętrznych, analizę incydentów bezpieczeństwa, realizację wyznaczonych celów w zakresie bezpieczeństwa informacji, a także uwzględnia zmiany w kontekście wewnętrznym tj. struktura organizacyjna, zmiany w procesach biznesowych i zewnętrznym tj. nowe regulacje, zmiany technologiczne, rodzaje zagrożeń. Przeglądy powinny również obejmować ocenę skuteczności wdrożonych środków zaradczych oraz identyfikację nowych ryzyk.

7.3. Dokumentacja przeglądów systemu zarządzania bezpieczeństwem

Wnioski z przeglądów oraz rekomendacje dotyczące zmian powinny być dokumentowane i wdrażane w celu ciągłego doskonalenia. Taka dokumentacja stanowi podstawę do podejmowania decyzji dotyczących wdrażania działań korygujących i zapobiegawczych, a także pozwala na monitorowanie postępów w realizacji celów bezpieczeństwa oraz utrzymanie zgodności z obowiązującymi standardami i wymaganiami.

8. Realizacja procesu analizy i oceny ryzyka

Proces analizy i oceny ryzyka jest podstawą zarządzania bezpieczeństwem informacji w DGLP. Prowadzenie tego procesu jest kluczowe dla prowadzenia działań ochrony zasobów informatycznych SILP w organizacji. Regularna identyfikacja, analiza oraz zarządzanie ryzykiem pozwalają na podejmowanie świadomych decyzji dotyczących wdrażania odpowiednich zabezpieczeń i minimalizowania potencjalnych zagrożeń.

8.1. Identyfikacja ryzyka

Podatności SILP oraz zagrożenia, które mogą wpłynąć na bezpieczeństwo danych, są okresowo identyfikowane. Proces ten obejmuje zarówno analizę środowiska wewnętrznego, jak i zewnętrznego, a także uwzględnia zmiany technologiczne, organizacyjne oraz regulacyjne.

8.2. Analiza ryzyka

Każde zidentyfikowane ryzyko poddawane jest szczegółowej analizie, obejmującej ocenę prawdopodobieństwa jego wystąpienia oraz potencjalnego wpływu na działalność organizacji. Analiza ta pozwala określić krytyczność ryzyka i ustalić priorytety działań wskazując podatne obszary, które są najbardziej istotne dla organizacji.

8.3. Zarządzanie ryzykiem

W oparciu o wyniki prowadzonych analiz ryzyka, wdrażane są adekwatne środki zaradcze i kontrolne, mające na celu ograniczenie ryzyka do poziomu akceptowalnego przez organizację. Proces zarządzania ryzykiem jest cyklicznie powtarzany, a skuteczność zastosowanych działań podlega regularnej ocenie i aktualizacji, co stanowi element procesu ciągłego doskonalenia SZBI.

9. Zarządzanie projektami teleinformatycznymi

DGLP zarządza projektami teleinformatycznymi w sposób zorganizowany, uwzględniając aspekty związane z zapewnieniem bezpieczeństwa informacji na każdym etapie realizowanych przedsięwzięć.

Na etapie planowania każdy projekt musi brać pod szczególną uwagę elementy zapewnienia bezpieczeństwa danych, w ramach których prowadzona jest analiza ryzyka w celu identyfikacji potencjalnych zagrożeń oraz określenie koniecznych do wdrożenia odpowiednich środków zaradczych.

W procesie projektowym uczestniczy Zespół ds. cyberbezpieczeństwa, który powinien być zaangażowany na wszystkich etapach zarządzania projektem tj. planowanie, realizację, wdrożenie, monitorując zgodność działań z polityką bezpieczeństwa informacji.

10. Kryptografia i szyfrowanie danych SILP

10.1. Stosowanie technik kryptograficznych

Ochrona informacji wrażliwych w systemach SILP realizowana jest poprzez stosowanie technik kryptograficznych zgodnych z aktualnymi standardami i wytycznymi branżowymi.

Zabrania się stosowania uznanych za niebezpieczne algorytmów i protokołów kryptograficznych tj. SHA-1, MD5, DES, RSA, SSLv3.

Techniki kryptograficzne stosuje się do:

1) szyfrowania danych w spoczynku,
2) szyfrowania danych w transmisji,
3) podpisu cyfrowego do weryfikacji autentyczności i integralności danych,
4) podpisu cyfrowego do weryfikacji tożsamości.

10.2. Ochrona danych SILP w spoczynku

Dane SILP stanowiące tajemnicę przedsiębiorstwa i inne dane, które mogą mieć wpływ na działanie i bezpieczeństwo organizacji, zapisane na nośnikach elektronicznych wynoszonych poza siedzibę jednostki LP, muszą być zaszyfrowane.

10.3. Ochrona danych SILP w transmisji

1) Dane przesyłane w sieciach wewnętrznych i zewnętrznych muszą być chronione przy użyciu odpowiednich technik kryptograficznych, aby zapewnić ich poufność i integralność, za wyjątkiem dedykowanych sieci połączeniowych.
2) Proces uwierzytelniania użytkowników w systemach SILP za pośrednictwem sieci należy realizować z użyciem połączeń szyfrowanych zapewniających poufność i integralność przesyłanych danych.
3) Dostęp administracyjny do systemów SILP za pośrednictwem sieci należy realizować z użyciem połączeń szyfrowanych zapewniających poufność i integralność przesyłanych danych.
4) Dostęp do wewnętrznej sieci DGLP z sieci Internet jest możliwy jedynie za pomocą dedykowanych systemów VPN LP autoryzowanych przez Wydział Informatyki DGLP.

10.4. Infrastruktura klucza publicznego

1) Do zarządzania wewnętrznymi certyfikatami kryptograficznymi DGLP korzysta z infrastruktura klucza publicznego Lasów Państwowych (systemu PKI LP), który jest utrzymywany w ramach wewnętrznych zasobów SILP.
2) Uwierzytelnianie usług sieciowych jest realizowane na podstawie certyfikatów wystawionych przez PKI LP lub certyfikaty kwalifikowane wystawione przez zewnętrznych dostawców.

3) Uwierzytelnianie użytkowników w dostępie do stacji roboczych SILP obywa się za pomocą kart kryptograficznych i certyfikatów PKI LP.
4) Cykl funkcjonowania certyfikatów SILP i ich nośników są określone przez szczegółowe wytyczne Wydziału Informatyki DGLP.

11. Bezpieczeństwo Operacyjne

11.1. Procedury operacyjne

Operacje utrzymania systemów SILP przetwarzających dane DGLP muszą być realizowane zgodnie z procedurą, która uwzględnia co najmniej:

1) Kopie bezpieczeństwa danych, wykonywane zgodnie z obwiązującą polityką dla kopii bezpieczeństwa danych SILP.
2) Aktualizacje oprogramowania, instalowane na bieżąco, udostępniane przez producentów, poprawki krytyczne i bezpieczeństwa dla oprogramowania sprzętowego, sterowników urządzeń w systemach operacyjnych, systemów operacyjnych, aplikacji.
3) Monitoring systemów, prowadzony w sposób ciągły monitoring dostępności usług i parametrów systemów oraz monitoring zagregowanych dzienników zdarzeń w systemie klasy SIEM.
4) Monitoring i raportowanie nieudanych prób logowań do systemów.
5) Monitoring i raportowanie zdarzeń systemów ochrony przed złośliwym oprogramowaniem.

11.2. Zarządzanie zmianami

1) Krytyczne zmiany w konfiguracji systemów SILP są prowadzone zgodnie z ustalonym procesem zarządzania zmianami, w celu minimalizacji ryzyka zagrożeń bezpieczeństwa informacji.
2) Proces wprowadzania zmian krytycznych w systemach SILP musi uwzględniać szczegółową analizę możliwych skutków oraz odpowiednie przygotowanie do wdrożenia każdej zmiany. Przed przystąpieniem do realizacji zmiany należy przeprowadzić ocenę wpływu planowanej modyfikacji na funkcjonowanie systemów, bezpieczeństwo informacji, zgodność z obowiązującymi regulacjami oraz potencjalny wpływ na użytkowników i procesy biznesowe.
3) Wdrażanie zmian w systemach SILP musi uwzględniać mechanizmy przywracania poprzedniej konfiguracji (rollback) w przypadku wystąpienia awarii, niezgodności z wymaganiami lub zagrożeń bezpieczeństwa.
4) Wprowadzanie zmian krytycznych w systemach SILP musi obejmować etap testowania po modyfikacji, aby zapewnić stabilność, bezpieczeństwo i zgodność z wymaganiami.
5) W sytuacjach awaryjnych lub wymagających natychmiastowego przeciwdziałania zagrożeniu bezpieczeństwa informacji tj. aktywne ataki, krytyczne luki, dopuszcza się wprowadzenie zmian poza standardowym procesem zarządzania zmianami, pod warunkiem późniejszego udokumentowania wprowadzonych modyfikacji i weryfikacji skutków zmian pod kątem zgodności z polityką bezpieczeństwa i standardami technicznymi.

12. Ochrona sieci transmisji danych

Sieć transmisji danych DGLP podlega szczególnym wymogom ochronnym, mającym na celu zabezpieczenie przed nieautoryzowanym dostępem oraz zagrożeniami wewnętrznymi i zewnętrznymi. Wdrożone mechanizmy ochrony obejmują:

12.1. Firewalle nowej generacji

Prowadzą filtrowanie ruchu na podstawie polityk bezpieczeństwa, inspekcję głęboką pakietów, inspekcję ruchu szyfrowanego, blokowanie podejrzanych protokołów. Szczególnej ochronie podlega punkt styku sieci organizacji z siecią Internet oraz punk styku sieci lokalnych DGLP z siecią rozległą.

12.2. Systemy wykrywania i zapobiegania włamaniom

Prowadzą monitoring i analizę ruchu sieciowego w czasie rzeczywistym. Analiza prowadzona jest pod kątem wykrywania anomalii i nietypowych zachowań tj. skanowanie portów, podejrzane wzorce ruchu, próby wykorzystania luk w usługach sieciowych. W przypadku wykrycia takich zdarzeń wykonywane jest automatyczne blokowanie źródła ruchu.

12.3. Segmentacja sieci

Sieci lokalne DGLP są podzielone na segmenty funkcjonalne i strefy bezpieczeństwa w celu zwiększenia ochrony zasobów podłączonych do sieci oraz ograniczenia ryzyka nieautoryzowanego dostępu. Segmentacja sieci polega na wydzieleniu odrębnych obszarów sieciowych tj. VLAN, strefy DMZ, sieci monitoringu, sieci administracyjne, sieci użytkowników, sieci systemów krytycznych, co umożliwia zarządzanie dostępem oraz kontrolę przepływu danych pomiędzy segmentami. Każdy segment posiada przypisane poziomy uprawnień i zabezpieczeń, a ruch pomiędzy nimi jest monitorowany i filtrowany przy użyciu dedykowanych urządzeń sieciowych, takich jak firewalle oraz systemy wykrywania i zapobiegania włamaniom.

13. Identyfikacja i analiza zagrożeń

13.1. Zbieranie informacji o zagrożeniach

DGLP regularnie monitoruje różnorodne źródła informacji o zagrożeniach, zarówno wewnętrzne, jak i zewnętrzne, w szczególności:

1) Raporty i bazy danych wskaźników IoC dostarczane przez dostawców stosowanych rozwiązań cyberbezpiczeńetwa.
2) Raporty i informacje oraz listy wskaźników IoC z krajowych zespołów CSIRT.
3) Informacje o anomaliach z ciągłego monitoring własnego ruchu sieciowego.
4) Informacje o zagrożeniach z ciągłego monitoringu dzienników zdarzeń systemów SILP.
5) Informacje o zagrożeniach z systemu korelacji zdarzeń w systemie SIEM.
6) Sieciowe skanery podatności.

13.2. Analiza zagrożeń

Zespół ds. Cyberbezpieczeństwa weryfikuje wiarygodność i skalę zagrożeń dla danych SILP, eliminuje fałszywe alarmy (false positives), a następnie nadaje priorytety ryzyka według ich potencjalnego wpływu na organizację. Dla każdego zagrożenia uruchamia się dedykowaną ścieżkę prowadzenia działań naprawczych.

13.3. Wdrażanie środków remediacji

Na podstawie przeprowadzonej analizy Zespół ds. cyberbezpieczeństwa wprowadza lub zleca administratorom systemów SILP wdrożenie odpowiednich środków zaradczych, w celu minimalizacji ryzyka i ochrony zasobów informatycznych. W szczególności są to:

1) Aktualizacje polityk bezpieczeństwa.
2) Wdrażanie poprawek i łatek bezpieczeństwa.
3) Zmiana konfiguracji systemów.
4) Analiza zawartości nośników danych pod katem złośliwego oprogramowania.
5) Wymiana haseł kont użytkowników SILP.
6) Wdrożenie dodatkowych narzędzi monitorujących i detekcyjnych.

Działania są monitorowane i weryfikowane pod kątem ich realizacji i skuteczności, a proces analizy zagrożeń jest procesem ciągłym.

14. Instalacja Oprogramowania

Proces instalacji oprogramowania jest prowadzony zgodnie z zasadami bezpieczeństwa informacji, aby zapobiec wprowadzeniu do systemu SILP nieautoryzowanego lub złośliwego oprogramowania.

14.1. Polityka instalacji oprogramowania

1) Weryfikacja oprogramowania
   Przed instalacją każde nowe oprogramowanie podlega weryfikacji pod kątem bezpieczeństwa oraz zgodności z wymaganiami organizacji. Instalowane mogą być wyłącznie aplikacje zatwierdzone przez Zespół ds. cyberbezpieczeństwa lub administratorów SILP.
2) Zarządzanie licencjami
   Oprogramowanie musi być objęte ważną licencją, zgodną z warunkami umowy licencyjnej. Licencje są ewidencjonowane, monitorowane i okresowo weryfikowane w celu zapewnienia legalności użytkowania.
3) Aktualizacje:
   Oprogramowanie musi być regularnie aktualizowane. Wszystkie dostępne poprawki krytyczne i bezpieczeństwa muszą być niezwłocznie wdrażane, aby zminimalizować ryzyko podatności i zapewnić ciągłość ochrony oraz działania systemów SILP.

VII. Lista dokumentów wspierających politykę bezpieczeństwa informacji

Dokumenty wprowadzone do stosowania zarządzeniami Dyrektora Generalnego Lasów Państwowych:

1. „Zasady funkcjonowania zintegrowanego systemu informatycznego w Lasach Państwowych",
2. „Zasady bezpiecznej eksploatacji zasobów informatycznych Lasów Państwowych",
3. „Zasady dostępu do danych w Systemach Informatycznych Lasów Państwowych",
4. „Zasady funkcjonowania systemu telefonii IP i wideokonferencji",
5. „Wzór oświadczenia pracownika"

- wprowadzone do stosowania Zrządzeniem nr 31 Dyrektora Generalnego Lasów Państwowych z dnia 18 września 2017 r. w sprawie zasad funkcjonowania i zasad bezpieczeństwa systemu informatycznego w Państwowym Gospodarstwie Leśnym Lasy Państwowe, wraz z późniejszymi zmianami;

6. „Regulamin organizacyjny Dyrekcji Generalnej Lasów Państwowych" – wprowadzony do stosowania Zarządzeniem nr 19 Dyrektora Generalnego Lasów Państwowych z dnia 14 marca 2024 r., wraz z późniejszymi zmianami;
7. „Zasady klasyfikacji, ochrony i udostępniania informacji stanowiących tajemnicę przedsiębiorstwa w Państwowym Gospodarstwie Leśnym Lasy Państwowe",
8. „Wykaz informacji stanowiących tajemnicę przedsiębiorstwa",
9. „Wzór oświadczenia pracownika lub innej osoby mającej dostęp do informacji stanowiącej tajemnicę przedsiębiorstwa w PGL Lasy Państwowe"

- wprowadzone do stosowania Zarządzeniem nr 48 Dyrektora Generalnego Lasów Państwowych z dnia 6 października 2010 r. w sprawie ustalenia zasad klasyfikacji, ochrony i udostępniania informacji stanowiącej tajemnicę przedsiębiorstwa w Państwowym Gospodarstwie Leśnym Lasy Państwowe, wraz z późniejszymi zmianami.

Regulaminy i projekty techniczne ustanawiane i aktualizowane przez Naczelnika Wydziału Informatyki DGLP

1. Projekt usług katalogowych PGL LP
2. Polityka kopii zapasowych SILP
3. Zasady adresacji IP w sieci LP
4. Regulamin użytkowania systemu poczty elektronicznej LP
5. Polityka dla ruchu w sieci WAN LP
6. Polityka dla ruchu na styku sieci WAN LP i Internet
7. Zasady inspekcji ruchu szyfrowanego
8. Zasady budowy lokalnych sieci bezprzewodowych w jednostkach PGL LP
9. Polityka bezpieczeństwa urządzeń mobilnych
10. Polityka przetwarzania danych LP w publicznej chmurze obliczeniowej

Procedury, rejestry i inne dokumenty ustanawiane i aktualizowane przez Kierownika Zespołu ds. Cyberbezpieczeństwa WI DGLP

1. Procedura nadania dostępu VPN dla podmiotów zewnętrznych

2. Dokumentacja analizy ryzyk prowadzonej w oparciu o szablon MITRE ATT&CK
3. Rejestr wspomagających aktywów IT prowadzony w oparciu o adresację IP
4. Rejestr zgłoszeń zagrożeń i incydentów bezpieczeństwa danych SILP prowadzony w oparciu o dedykowane oprogramowanie
5. Rejestr krytycznych dostawców sprzętu i usług cyfrowych
6. Procedura nadania dostępu do SILP
7. Plan ciągłości działania SILP
8. Procedura odtworzenia SILP po katastrofie
9. Procedura zarządzania zagrożeniami bezpieczeństwa
10. Procedura zarządzania incydentem bezpieczeństwa
11. Procedura utrzymania systemów SILP
12. Procedura zarządzania krytycznymi zmianami SILP
13. Procedura funkcjonowania karty kryptograficznych systemu PKI LP
14. Zestaw procedur odtworzenia systemów SILP z kopii zapasowych
15. Zestaw procedury awaryjnego dostępu administracyjnego do systemów SILP

Decyzja nr 126
Dyrektora Generalnego Lasów Państwowych
z dnia 6 sierpnia 2025 r.

w sprawie wprowadzania Polityki Bezpieczeństwa Informacji Dyrekcji Generalnej Lasów Państwowych

(znak: EI.0413.16.2025)

Na podstawie art. 33 ust. 1 ustawy z dnia 28 września 1991 r. o lasach (t.j. Dz. U. z 2025 r. poz. 567) oraz § 6 Statutu Państwowego Gospodarstwa Leśnego Lasy Państwowe, wprowadzonego zarządzeniem nr 50 Ministra Ochrony Środowiska, Zasobów Naturalnych i Leśnictwa z dnia 18 maja 1994 r. – w wykonaniu zadań Dyrektora Generalnego Lasów Państwowych, wynikających z realizacji jego uprawnienia określonego w § 8 ust. 1 pkt 6 ww. statutu, zarządzam, co następuje:

§ 1

Wprowadzam do stosowania Politykę Bezpieczeństwa Informacji Dyrekcji Generalnej Lasów Państwowych, stanowiącą załącznik do niniejszej decyzji.

§ 2

Decyzja wchodzi w życie z dniem podpisania

Dyrektor Generalny
Lasów Państwowych

Adam Wasiak

Polityka Bezpieczeństwa Informacji Dyrekcji Generalnej Lasów Państwowych

Spis treści

I. Wprowadzenie

Bezpieczeństwo informacji oraz systemów, w których informacje są przetwarzane jest jednym z kluczowych elementów zapewniających realizację zadań Dyrekcji Generalnej Lasów Państwowych. Dyrekcja Generalna Lasów Państwowych zobowiązuje się do zapewnienia najwyższych standardów ochrony bezpieczeństwa informacji, w szczególności w zakresie zachowania jej poufności, integralności oraz dostępności.

Polityka Bezpieczeństwa Informacji (PBI) określa ramy dla funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji w Dyrekcji Generalnej Lasów Państwowych. PBI opisuje zasady ochrony informacji obowiązujące w DGLP, proces zarządzania ryzykiem, role i zadania osób uczestniczących w procesie przetwarzania informacji oraz zarządzania jej bezpieczeństwem, zgodne z przepisami obowiązującego prawa, regulacjami branżowymi oraz wypracowanymi własnymi standardami w zakresie funkcjonowania organizacji.

Kierownictwo DGLP jest w pełni zaangażowane i deklaruje pełne wsparcie dla podejmowanych działań zmierzających do zapewnienia bezpieczeństwa informacji, a także zapewnia niezbędne zasoby i czas na ich realizację.

Kwestie które dotyczą bezpieczeństwa informacji i wykraczają poza ramy niniejszej polityki, zostały szczegółowo uregulowane w odrębnych decyzjach i zarządzeniach Dyrektora Generalnego Lasów Państwowych.

II. Definicje

- **Audyt bezpieczeństwa** - proces systematycznego przeglądu i oceny skuteczności systemu zarządzania bezpieczeństwem informacji zgodnie z określonymi kryteriami.
- **Bezpieczeństwo informacji** - działania mające na celu ochronę informacji przetwarzanej w systemach teleinformatycznych przed nieuprawnionym dostępem, wykorzystaniem, ujawnieniem, zakłóceniem działania, modyfikacją lub zniszczeniem.
- **Incydent bezpieczeństwa** - każde zdarzenie, które narusza polityki bezpieczeństwa lub stwarza ryzyko dla poufności, integralności lub dostępności informacji.
- **Zagrożenie bezpieczeństwa danych** - potencjalna sytuacja lub zdarzenie, które może zagrozić bezpieczeństwu informacji przetwarzanych w systemach informatycznych.
- **Poufność** - cecha informacji która zapewnienia, że informacja jest udostępniana jedynie osobom upoważnionym.
- **Integralność** - cecha, która zapewnia, że dane i systemy jej przetwarzające są dokładne, spójne i niezmienione przez osoby nieupoważnione, w sposób przypadkowy lub celowy.
- **Dostępność** - cecha, która zapewnia, terminowy i niezawodny dostęp do informacji i ich wykorzystania w przypadku wystąpienia potrzeby takiego dostępu.
- **Ciągłość działania** - Zdolność organizacji do utrzymania kluczowych funkcji i usług na akceptowalnym poziomie w przypadku zakłóceń.
- **DGLP, Organizacja** - Dyrekcja Generalna Lasów Państwowych.
- **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, zgodnie z definicją zawartą w Rozporządzeniu Parlamentu

Europejskiego i Rady (UE) 2016/679 oraz obowiązującą ustawą o ochronie danych osobowych.

- **Hasło** - sekretne słowo lub fraza używana do uwierzytelnienia użytkownika w systemie informatycznym.
- **Kontrola dostępu** - mechanizmy i procedury używane do zapewnienia, że dostęp do zasobów informatycznych jest udzielany tylko upoważnionym użytkownikom.
- **MFA (Multi-Factor Authentication), uwierzytelnianie wieloskładnikowe** - metoda uwierzytelniania użytkowników, która wymaga podania dwóch lub więcej niezależnych form weryfikacji tożsamości.
- **Polityka bezpieczeństwa informacji, PBI** - niniejszy dokument definiujący podejście organizacji do zarządzania bezpieczeństwem informacji, w tym cele, zasady i obowiązki.
- **Zasady ochrony informacji** - wszystkie ustanowione w LP zasady dotyczące bezpieczeństwa informacji.
- **Reagowanie na incydenty** - proces zarządzania i odpowiedzi na zdarzenia związane z bezpieczeństwem informacji w celu minimalizacji skutków.
- **System Informatyczny Lasów Państwowych, SILP** - zbiór elementów, którego funkcją jest przetwarzanie, przechowywanie i przesyłanie danych w PGL LP przy użyciu techniki komputerowej.
- **Użytkownik SILP** - pracownik DGLP, w okresie pozostawania w stosunku zatrudnienia lub inna osoba fizyczna wykonująca prace na podstawie umowy o dzieło, umowy zlecenia lub innej umowy cywilnoprawnej w okresie obowiązywania umowy.
- **Administrator SILP** - pracownicy Wydziału Informatyki DGLP którzy są odpowiedzialni za zasoby SILP.
- **Dane SILP stanowiące tajemnice przedsiębiorstwa** - dane stanowiące tajemnicę przedsiębiorstwa zgodnie z klasyfikacją danych określoną przez stosowne zarządzenie Dyrektora Generalnego Lasów Państwowych.
- **Przetwarzanie danych, przetwarzanie informacji** - operacja lub zestaw operacji wykonywanych na danych lub zestawach danych w sposób zautomatyzowany lub niezautomatyzowany, taką jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
- **System Zarządzania Bezpieczeństwem Informacji, SZBI** - zestaw zasad, procesów, procedur, struktur organizacyjnych i zasobów wykorzystywanych do ochrony informacji w organizacji.
- **VPN (Virtual Private Network**) - technologia umożliwiająca bezpieczne połączenie z siecią LP za pośrednictwem sieci publicznych przez zaszyfrowany tunel, co zapewnia poufność i integralność przesyłanych danych.
- **Zarządzanie ryzykiem** - proces identyfikacji, oceny i klasyfikacji ryzyk oraz wdrażania środków zaradczych w celu ich minimalizacji.
- **Zarządzanie tożsamością i dostępem** - procedury i technologie służące do zarządzania dostępem do zasobów informatycznych, w tym identyfikacja i uwierzytelnianie użytkowników.

- **ZCI, Zespół ds. Cyberbezpieczeństwa -** komórka organizacyjna w Wydziale Informatyki DGLP dedykowana do sprawa związanych z bezpieczeństwem informacji.
- **ZILP, Zakład Informatyki Lasów Państwowych –** jednostka w strukturze PGL LP, która utrzymuje składniki SILP służące do przetwarzania oraz prowadzi przetwarzanie danych na rzecz innych jednostek w tym DGLP.

III. Cel

Celem PBI jest zdefiniowanie i ustanowienie zasad właściwej ochrony i utrzymania bezpieczeństwa informacji przetwarzanych przez DGLP oraz zasad funkcjonowania SZBI w organizacji. Realizowane jest to poprzez wdrożenie odpowiednich działań i środków zarządzania, które minimalizują ryzyko związane z zagrożeniami wewnętrznymi i zewnętrznymi dla bezpieczeństwa informacji przetwarzanych przez DGLP. Dla osiągnięcia zamierzonego celu podjęte zostały następujące działania:

1. Zabezpieczenie informacji przed zagrożeniami wewnętrznymi i zewnętrznymi poprzez wdrożenie odpowiednich procedur organizacyjnych oraz systemów zabezpieczeń technicznych.
2. Dążenie do zapewnienia poufności (dostępność informacji jedynie dla uprawnionych osób), integralności (zapewnienie kompletności i dokładności danych) oraz dostępności informacji (zapewnienie ich dostępności w wymaganym czasie).
3. Wszystkie działania w zakresie zarządzania bezpieczeństwem informacji będą prowadzone zgodnie z obowiązującymi przepisami prawa oraz regulacjami wewnętrznymi organizacji.
4. Ustanowienie odpowiednich procedur organizacyjnych i utrzymanie środków technicznych, które tworzą sprawny System Zarządzania Bezpieczeństwem Informacji.
5. Wyznaczenie zadań i odpowiedzialności osób zaangażowanych w przetwarzanie informacji. Określenie ich zadań i odpowiedzialności związanych z ochroną informacji.
6. Identyfikacja właścicieli aktywów i zasobów informatycznych poprzez wyznaczenie właścicieli aktywów i zasobów informatycznych, którzy będą odpowiedzialni za zapewnienie zgodnego z PBI poziomu bezpieczeństwa przetwarzanych informacji.
7. Prowadzenie współpracy z podmiotami zewnętrznymi w sposób gwarantujący realizację zleconych przez DGLP zadań w zgodności z obowiązującą PBI.
8. Prowadzenie regularnego przeglądu i dostosowanie polityk, procedur oraz dokumentacji związanej z bezpieczeństwem informacji, mające na celu weryfikację i zapewnienie zgodności z bieżącymi wymogami.
9. Wdrażanie procedur reakcji na zagrożenia i incydenty związane z bezpieczeństwem informacji. Prowadzenie działań korygujących i minimalizujących skutki incydentu.
10. Prowadzenie regularnych działań podnoszących świadomość pracowników w zakresie bezpieczeństwa informacji, poprzez szkolenia i działania edukacyjne.
11. Stałe doskonalenie System Zarządzania Bezpieczeństwem Informacji zgodnie z wymaganiami prawnymi oraz uwagami wszystkich uczestniczących w procesie ochrony informacji stron, w celu optymalizacji poziomu ochrony danych.

IV. Role i odpowiedzialności uczestników procesu

Dyrektor Generalny Lasów Państwowych ustanawia i realizuje strategiczne cele Polityki Bezpieczeństwa Informacji, a właścicielem procesu zarządzania bezpieczeństwem informacji jest Kierownik Zespołu ds. Cyberbezpieczeństwa w Wydziale Informatyki DGLP.

Odpowiedzialności

Określenie odpowiedzialności związanych z bezpieczeństwem informacji to kluczowy element skutecznego zarządzania ochroną danych i zasobów informatycznych. Zostały zdefiniowane i określone podstawowe role i odpowiedzialności związane z procesem utrzymania bezpieczeństwem informacji w DGLP:

Dyrektor Generalny Lasów Państwowych:

1) Ustanawia Polityki Bezpieczeństwa Informacji, określa strategiczne cele dla bezpieczeństwa informacji.
2) Zapewnienia odpowiednie środki finansowe, osobowe i technologiczne dla działań związanych z bezpieczeństwem informacji.
3) Zatwierdza okresowe raporty dotyczące realizacji celów i skuteczności ustanowionych polityk bezpieczeństwa informacji.
4) Zarządza okresowe audyty oceniające skuteczności stosowanych w DGLP środków ochrony bezpieczeństwa informacji SILP.
5) Ustanawia wymagania odnośnie bezpieczeństwa SILP dla wszystkich jednostek PGL LP, w tym dla Dyrekcji Generalnej Lasów Państwowych oraz kontroluje ich realizację.

Zespół ds. Cyberbezpieczeństwa w Wydziale Informatyki DGLP:

1) Nadzoruje i monitoruje realizację Polityki Bezpieczeństwa Informacji.
2) Zapewnienia, że procesy wymagane w zarządzaniu bezpieczeństwem są ustanowione, wdrożone i utrzymywane.
3) Prowadzi nadzór nad dokumentacją dotyczącą bezpieczeństwa informacji w systemach informatycznych organizacji na etapach jej opracowywania, weryfikacji, aktualizacji, udostępniania i przechowywania.
4) Prowadzi analizy ryzyka dla bezpieczeństwa informacji w systemach teleinformatycznych organizacji.
5) Utrzymuje lub nadzoruje utrzymanie aktywa teleinformatyczne uczestniczące w przetwarzaniu informacji.
6) Implementuje lub nadzoruje implementacje polityk bezpieczeństwa informacji.
7) Opracowuje szczegółowe polityki bezpieczeństwa dla systemów teleinformatycznych Informatycznych.
8) Prowadzi nadzór nad bezpieczeństwem informacji systemów teleinformatycznych. Monitoruje i nadzoruje przestrzeganie ustanowionych zasad polityki bezpieczeństwa informacji.
9) Utrzymuje System Zarządzania Bezpieczeństwem Informacji. Prowadzi okresową ocenę skuteczności oraz działania korygujące i usprawniające jego działanie.

10) Koordynuje realizacje audytów w zakresie bezpieczeństwa informacji w systemach informatycznych.
11) Prowadzi audyt w jednostkach LP w zakresie bezpieczeństwa informacji w systemach teleinformatycznych.
12) Koordynuje lub organizuje przeglądy bezpieczeństwa systemów teleinformatycznych DGLP.
13) Prowadzi nadzór nad realizacją zaleceń wynikających z audytów i przeglądów.
14) Raportuje Dyrektorowi Generalnemu Lasów Państwowych o funkcjonowaniu procesu zarządzania bezpieczeństwem informacji oraz o informuje o realizacji jego celów i skuteczności.
15) Prowadzi i koordynuje organizacje szkoleń dotyczących bezpieczeństwa informacji w systemach informatycznych dla użytkowników SILP.
16) Analizuje raporty dotyczące zdarzeń i incydentów związanych z bezpieczeństwem systemów teleinformatycznych.
17) Informuje i ostrzega administratorów oraz użytkowników SILP o znanych zagrożeniach dla bezpieczeństwa informacji przetwarzanych w systemach teleinformatycznych.
18) Opracowuje, wprowadza i okresowo testuje plany ciągłości działania i planów awaryjnych dla systemów teleinformatycznych DGLP.
19) Prowadzi współpracę operacyjną z krajowymi Zespołami Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT GOV, CSIRT NASK, CSIRT MON).
20) Prowadzi okresową analizę podatności systemów teleinformatycznych na zagrożenia.
21) Prowadzi obsługę i reaguje na zgłoszenia dotyczące zagrożeń bezpieczeństwa informacji przetwarzanych w systemach teleinformatycznych.
22) Prowadzi wsparcie merytoryczne komórek organizacyjnych DGLP w działaniach, które mogą mieć wpływ na bezpieczeństwo informacji w systemach teleinformatycznych.
23) Prowadzi i aktualizuje rejestr podmiotów które dostarczają oprogramowanie, sprzęt lub usługi cyfrowe krytyczne dla ciągłości działania kluczowych procesów w organizacji.

Administratorzy SILP w Wydziale Informatyki DGLP:

1) Implementują w zarządzanych systemach polityki i procedury bezpieczeństwa informacji.
2) Zarządzają dostępem do systemów zapewniając, że dostępy są przyznawane jedynie uprawnionym użytkownikom z zachowaniem zasady najmniejszych uprawnień.
3) Monitorują aktywności utrzymywanych systemów, identyfikują anomalie, reagują i niezwłocznie raportują do Zespołu ds. Cyberbezpieczeństwa o wykrytych incydentach.
4) Współpracują w zakresie realizacji zadań związanych z bezpieczeństwem informacji oraz realizuje wytyczne Zespołu ds. Cyberbezpieczeństwa.
5) Na bieżąco instalują aktualizacje krytyczne i bezpieczeństwa w utrzymywanych systemach w celu eliminacji ich podatności.
6) Zabezpieczają dowody i tworzy dokumentacje dla wykrytych incydentów.
7) Tworzą lub gwarantują tworzenie kopii zapasowych dla utrzymywanych systemów teleinformatycznych.
8) Regularnie weryfikują poprawność tworzonych kopii zapasowych.
9) Tworzą procedury odzyskiwania zarządzanych systemów teleinformatycznych z kopii zapasowych.

10) Tworzą procedury awaryjnego dostępu administracyjnego do zarządzanych systemów dla pozostałych administratorów.
11) Zapewniają, że wszystkie prowadzone działania administracyjne są zgodne z polityką bezpieczeństwa informacji oraz regulacjami wewnętrznymi organizacji.
12) Identyfikują ryzyka dla systemów i uczestniczą w prowadzonym procesie analizy ryzyka.

Kierownicy komórek organizacyjnych DGLP:

1) Wnioskują do kierownictwa DGLP o nadanie, zmianę lub odebranie uprawnień do danych SILP dla podległych pracowników w zakresie działań podległej komórki organizacyjnej.
2) Informują pracowników o obowiązkach związanych z ochroną informacji na stanowiskach pracy.
3) Egzekwują przestrzeganie zasad ochrony informacji przetwarzanych w systemach teleinformatycznych przez podległych pracowników.
4) Informują Zespół ds. Cyberbezpieczeństwa w Wydziale Informatyki DGLP o prowadzonych działaniach, które mogą mieć wpływ na bezpieczeństwo informacji w systemach teleinformatycznych.
5) Informują Zespół ds. Cyberbezpieczeństwa o zidentyfikowanych zagrożeniach dla bezpieczeństwa informacji w obszarze działania nadzorowanej komórki organizacyjnej.

Użytkownicy SILP w DGLP

1) Przestrzegają zasad ochrony informacji przetwarzanych w SILP.
2) Informują kierownika własnej komórki lub bezpośrednio pracowników Wydziału Informatyki DGLP o zidentyfikowanych incydentach, zagrożeniach dla bezpieczeństwa informacji oraz nieprawidłowościach w pracy systemów informatycznych.
3) Współpracują z pracownikami Wydziału Informatyki DGLP w celu identyfikacji i dokumentowania zagrożeń dla bezpieczeństwa informacji SILP.
4) Dbają o poprawności merytoryczną wprowadzanych za pomocą systemów informatycznych danych.
5) Stosują złożone i unikalne hasła dostępu, zgodnie z zasadami bezpieczeństwa.
6) Dbają o bezpieczeństwo fizyczne powierzonych środków przetwarzania danych, w szczególności w przypadku ich wynoszenia poza siedzibę organizacji.

Komórka organizacyjna właściwa ds. administracji;

1) Opracowuje i wdraża zasady kontroli dostępu do biura DGLP.
2) Zapewnienia, że dostęp do wydzielonych stref w biurze mają wyłącznie osoby upoważnione.
3) Prowadzi wewnętrzny i zewnętrzny monitoring wizyjny budynku DGLP.
4) Organizuje ochronę fizyczną biura DGLP poprzez personel ochrony fizycznej i monitoring wizyjny.
5) Prowadzi monitoring wejść i wyjść oraz ważnych obszarów za pomocą kamer i innych systemów bezpieczeństwa.
6) Prowadzi rejestr zdarzeń związanych z naruszeniem lub próbami naruszeń fizycznego bezpieczeństwa.
7) Utrzymuje systemy doprowadzenia zasilania podstawowego i awaryjnego do serwerowni w biurze DGLP.

Komórka organizacyjna właściwa ds. ochrony danych osobowych, w której skład wchodzi Inspektor Ochrony Danych;

1) Opracowuje, wdraża i nadzoruje realizację polityki bezpieczeństwa danych osobowych w DGLP, zapewniając zgodność z przepisami Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 oraz przepisami krajowymi.
2) Wspiera Inspektora Ochrony Danych (IOD) w wykonywaniu jego zadań oraz zapewnia mu niezbędne zasoby i warunki pracy.
3) Informuje Administratora danych oraz pracowników i współpracowników o ich obowiązkach wynikających z RODO oraz innych przepisów dotyczących ochrony danych osobowych, a także udziela im doradztwa w tych sprawach.
4) Monitoruje przestrzeganie przepisów RODO i wewnętrznych regulacji dotyczących ochrony danych osobowych przez osoby upoważnione do ich przetwarzania.
5) Prowadzi działania podnoszące świadomość oraz organizuje szkolenia dla osób uczestniczących w operacjach przetwarzania danych osobowych w DGLP.
6) Współpracuje z organem nadzorczym do spraw ochrony danych osobowych — Prezesem Urzędu Ochrony Danych Osobowych i pełni funkcję punktu kontaktowego dla organu nadzorczego w kwestiach związanych z ochroną danych osobowych.
7) Pełni funkcję punktu kontaktowego dla osób, których dane są przetwarzane, w zakresie realizacji ich praw określonych w RODO.
8) Koordynuje oraz współuczestniczy w opracowywaniu, aktualizowaniu i opiniowaniu wewnętrznych aktów prawnych oraz procedur, odnoszących się do ochrony danych osobowych.
9) Zapewnia obsługę dedykowanego adresu e-mail: dane.osobowe@lasy.gov.pl.
10) Identyfikuje zagrożenia oraz przeprowadza analizę ryzyka związanego z przetwarzaniem danych osobowych, w tym – w przypadkach wymaganych przepisami prawa – dokonuje oceny skutków dla ochrony danych (DPIA).Analizuje sytuacje i przyczyny naruszeń bezpieczeństwa danych oraz zarządza procesem reagowania na naruszenia, w tym ich zgłaszaniem organowi nadzorczemu oraz informowaniem osób, których dane dotyczą. Wnioskuje do Dyrektora Generalnego o wdrożenie adekwatnych zabezpieczeń dostosowanych do poziomu ryzyka.
11) Zapewnia bieżące wsparcie merytoryczne dla wszystkich komórek organizacyjnych DGLP w zakresie ochrony danych osobowych.
12) Nadzoruje oraz koordynuje sprawy dotyczące ochrony danych osobowych w LP.
13) Prowadzi audyty mające na celu ocenę skuteczności stosowanych środków ochrony danych osobowych oraz aktualności dokumentacji związanej z przetwarzaniem danych.
14) Inicjuje oraz realizuje działania doskonalące system ochrony danych osobowych w DGLP.

Komórka organizacyjna właściwa ds. informacji niejawnych;

1) Prowadzi nadzór nad ochroną informacji niejawnych w DGLP
2) Prowadzi kancelarię tajną DGLP oraz zapewnia ochronę informacji niejawnych.

V. Zakres i sposób postępowania

Zakres

Polityka reguluje wszystkie aspekty bezpieczeństwa informacji w Dyrekcji Generalnej Lasów Państwowych, w szczególności dotyczące informacji przetwarzanych w systemach teleinformatycznych z wykluczeniem danych osobowych i niejawnych, które są uregulowane w osobnych dokumentach.

Zaangażowanie kierownictwa

Kierownictwo DGLP przywiązuje szczególną wagę do ochrony informacji przetwarzanych przez organizację. Inicjuje i nadzoruje działania zmierzające do zapewnienia odpowiedniego poziomu bezpieczeństwa oraz aktywnie wspiera realizację procesów ochrony. Zapewnia niezbędne zasoby i czas na realizacje działań zmierzających do uzyskania odpowiedniego poziomu bezpieczeństwa informacji ze szczególnym uwzględnieniem wymagań wobec ich poufności, dostępności oraz integralności.

Kierownictwo DGLP ustanawia SZBI i wprowadza zasady jego funkcjonowania oraz deklaruje, że wdrożony SZBI, którego elementem jest niniejsza PBI, będzie podlegał regularnym przeglądom i doskonaleniu.

VI. System Zarządzania Bezpieczeństwem Informacji

System Zarządzania Bezpieczeństwem Informacji w DGLP stanowi zintegrowany zbiór polityk, procedur, procesów i środków technologicznych, których celem jest zapewnienie odpowiedniego poziomu ochrony przetwarzanych danych. SZBI opiera się na podejściu systemowym, które pozwala na identyfikowanie, ocenę i minimalizowanie ryzyka związanego z zagrożeniami bezpieczeństwa informacji, jednocześnie uwzględniając realizację strategicznych celów organizacji. Kluczowym celem SZBI jest dążenie do utrzymania poufności, integralności i dostępności danych, co przekłada się na ochronę interesów organizacji, jej klientów oraz partnerów biznesowych.

SZBI definiuje ramy operacyjne, w których działa DGLP, określając jakie środki techniczne i organizacyjne należy zastosować, aby spełnić wymagania prawne, regulacyjne i branżowe. Umożliwia wdrażanie i egzekwowanie zasad bezpieczeństwa w sposób spójny i efektywny. SZBI wspiera również budowanie świadomości pracowników w zakresie ochrony informacji poprzez szkolenia, audyty oraz monitorowanie zgodności z polityką.

Dzięki SZBI DGLP chroni swoje zasoby i może sprawnie reagować na incydenty bezpieczeństwa, stale doskonalić swoje procedury i zwiększać odporność na potencjalne zagrożenia.

1. Zarządzanie aktywami

1.1. Identyfikacja aktywów

Wszystkie aktywa służące do przetwarzania informacji muszę być zidentyfikowane i zinwentaryzowane w zakresie obejmującym co najmniej:

1) Opis urządzenia/systemu
2) Przypisanie do zasobu jego użytkownika lub odpowiedzialnego administratora.
3) Informacje o klasyfikacji przetwarzanych danych

1.2. Klasyfikacja informacji

Informacje przetwarzane w SILP są sklasyfikowane zgodnie z ich wartością, krytycznością oraz wrażliwością. Informacje klasyfikowane są do grup:

1) Dane SILP stanowiące tajemnicę przedsiębiorstwa i inne dane, które mogą mieć wpływ na działanie i bezpieczeństwo PGL LP
2) Pozostałe dane SILP
3) Dane osobowe
4) Informacje niejawne

2. Kontrola dostępu

2.1. Zasada najmniejszych uprawnień

Dostęp do informacji i systemów informatycznych jest przyznawany wyłącznie na podstawie zasadzie najmniejszych uprawnień, co oznacza, że użytkownicy mają dostęp tylko do tych zasobów, które są niezbędne do wykonywania ich obowiązków.

Podstawową metodą uwierzytelnienia użytkownika i administratorów w systemach wewnętrznych jest uwierzytelnienie przy pomocy kraty kryptograficznej i certyfikatu korporacyjnego PKI LP lub haseł jednorazowych do sieci SILP.

2.2. Uwierzytelnianie wieloskładnikowe (MFA)

W celu podniesienie poziomu bezpieczeństwa, dostęp użytkowników do zasobów SILP w standardowym trybie realizowany jest z wykorzystaniem uwierzytelniania wieloskładnikowego (MFA). Każdy użytkownik łączący się z SILP, musi przejść proces autoryzacji z użyciem co najmniej dwóch niezależnych składników uwierzytelniających.

2.3. Ochrona przed nieautoryzowanym dostępem

Wszystkie systemy o ile to technicznie możliwe muszą posiadać blokady konta po kilku nieudanych próbach logowania oraz regularne monitorowanie logowań i wykrywanie podejrzanej aktywności.

2.4. Monitorowanie dostępu

Wszystkie próby dostępu do systemów informatycznych LP muszą być logowane i regularnie monitorowane w celu wykrywania i reagowania na nieautoryzowane próby dostępu.

2.5. Przeglądy dostępu

Wykonywane są regularne przeglądy uprawnień dostępu do systemów informatycznych w celu zapewnienia, że dostęp jest zgodny z aktualnymi potrzebami użytkowników.

2.6. Złożoność haseł i numerów PIN

Hasła i numery PIN uwierzytelniające dostępy do SILP musza mieć określone i weryfikowane minimalne wymagania dla złożoności.

2.7. Dostępy administratorów do systemów

Zabroniony jest dostęp administracyjny do systemów w celach innych niż prace związane z administracją, utrzymaniem lub diagnostyką działania systemów.

2.8. Zapamiętywanie haseł w przeglądarkach

Zabronione jest używanie przeglądarek internetowych z włączoną funkcją zapamiętywania identyfikatorów i haseł.

3. Cykl funkcjonowania systemów informatycznych w DGLP

3.1. Bezpieczeństwo w cyklu życia systemu

W celu zapewnienia skutecznej ochrony informacji oraz zgodności z obowiązującymi regulacjami, organizacja zobowiązuje się do uwzględniania aspektów bezpieczeństwa informacji na każdym etapie projektowania, wdrażania, testowania, utrzymania i wycofania z eksploatacji systemów IT.

3.2. Bezpieczeństwo na etapie projektowania

Każdy wdrażany system informatyczny oraz każda znacząca modernizacja istniejących rozwiązań muszą być poprzedzone analizą ryzyka, mającą na celu identyfikację potencjalnych zagrożeń, podatności oraz ocenę wpływu na poufność, integralność i dostępność przetwarzanych danych. Wymagane jest uwzględnienie odpowiednich środków technicznych i organizacyjnych, takich jak kontrola dostępu, szyfrowanie, monitorowanie oraz mechanizmy reagowania na incydenty, już na etapie projektowania systemów - zasada „security by design and default”.

3.3. Testowanie bezpieczeństwa

Wdrażane systemy informatyczne, a także istotne modyfikacje w istniejących systemach, które mogą mieć wpływ na bezpieczeństwo informacji, muszą być poddane testom bezpieczeństwa przed ich dopuszczeniem do eksploatacji. Testy te powinny obejmować zarówno analizę potencjalnych podatności, jak i ocenę skuteczności zastosowanych mechanizmów ochronnych.

W przypadku wykrycia jakichkolwiek nieprawidłowości dotyczących funkcjonowania systemu po wprowadzeniu zmian, należy niezwłocznie wycofać wprowadzone modyfikacje oraz podjąć działania mające na celu usunięcie wszystkich stwierdzonych nieprawidłowości. Dodatkowo, przed ponownym wdrożeniem zmian, konieczne jest przeprowadzenie powtórnych testów bezpieczeństwa w celu potwierdzenia, że wszystkie

problemy zostały skutecznie wyeliminowane i system spełnia wymagane standardy bezpieczeństwa informacji.

3.4. Likwidacja aktywów SILP

W procesie wycofywania aktywów SILP z eksploatacji, DGLP zobowiązuje się do zapewnienia pełnego bezpieczeństwa informacji przetwarzanych na tych zasobach. Przed likwidacją należy przeprowadzić archiwizację istotnych danych oraz skuteczne i trwałe usunięcie wszystkich informacji chronionych, zgodnie z obowiązującymi przepisami prawa oraz wewnętrznymi regulacjami.

4. Relacje z podmiotami zewnętrznymi

Polityka Bezpieczeństwa Informacji DGLP zapewnia, że każdy dostęp do zasobów SILP DGLP przez podmioty zewnętrzne jest ściśle kontrolowany, ograniczony do niezbędnego minimum, monitorowany i zgodny z najwyższymi standardami bezpieczeństwa informacji.

4.1. Formalizacja współpracy

1) Współpraca z podmiotami zewnętrznymi odbywa się wyłącznie na podstawie pisemnych umów lub porozumień, które precyzują zakres, czas trwania oraz warunki dostępu do zasobów SILP i systemów informatycznych DGLP.
2) Podmiot mający otrzymać dostęp do zasobów SILP DGLP zobowiązany jest do podpisania stosownego oświadczenia akceptującego zasady udzielenia dostępu.

4.2. Zakres i czas dostępu do systemów

1) Dostęp do SILP i innych zasobów informatycznych dla podmiotów zewnętrznych przyznawany jest wyłącznie na czas obowiązywania umowy lub porozumienia.
2) Dostęp jest udzielany wyłącznie do minimalnego, niezbędnego zakresu zasobów wymaganych do realizacji powierzonych zadań, zgodnie z zasadą najmniejszych uprawnień.
3) Po zakończeniu współpracy lub wygaśnięciu umowy dostęp do systemów i zasobów jest niezwłocznie wycofywany, a konta użytkowników podmiotów zewnętrznych są blokowane.
4) Zabrania się prób uzyskania dostępu do innych zasobów niż te, na które została wydana zgoda.

4.3. Uprawnienia i identyfikacja użytkowników

1) Dostęp otrzymują wyłącznie wskazani imiennie pracownicy podmiotu zewnętrznego, dla których tworzone są indywidualne konta użytkownika.
2) Wszystkie konta podmiotów zewnętrznych są rejestrowane i zarządzane w centralnym katalogu użytkowników.

4.4. Bezpieczeństwo połączeń serwisowych

1) Zdalny dostęp z sieci Internet może być realizowany jedynie za pośrednictwem szyfrowanych połączeń VPN.
2) Dostęp może być realizowany wyłącznie z urządzeń spełniających wymagania bezpieczeństwa.
3) Dostęp może być realizowany jedynie z obszaru Unii Europejskiej.
4) Maksymalne dopuszczalne pasmo połączenia VPN jest ograniczone zgodnie z polityką DGLP dla ruchu sieciowego.
5) Wszystkie połączenia VPN są rejestrowane i monitorowane zgodnie z obowiązującymi politykami bezpieczeństwa.

4.5. Krytyczność dostawców

1) W celu identyfikacji i klasyfikacji dostawców, DGLP prowadzi i aktualizuje rejestr podmiotów które dostarczają oprogramowanie, sprzęt lub usługi cyfrowe krytyczne dla ciągłości działania kluczowych procesów w organizacji.
2) Rejestr zawiera dane o dostawcach, zakresie dostaw i świadczonych usług, informacje o potencjalnym wpływie na organizacje oraz informacje o zawartych umowach.
3) Za prowadzenie rejestru odpowiada Zespół ds. Cyberbezpieczeństwa.

5. Zarządzanie incydentami bezpieczeństwa informacji

DGLP prowadzi zarządzanie zgłoszonymi lub wykrytymi incydentami i zagrożeniami bezpieczeństwa informacji. Proces ten ma na celu szybką analizę i mitygację negatywnych dla organizacji skutków incydentów i zagrożeń oraz poprawę skuteczności ochrony w zastosowanych zabezpieczeniach technicznych i organizacyjnych.

5.1. Zgłaszanie incydentów i zagrożeń bezpieczeństwa

1) Każdy użytkownik SILP ma obowiązek poinformować kierownika własnej komórki lub bezpośrednio pracowników Wydziału Informatyki DGLP o zidentyfikowanych incydentach, zagrożeniach dla bezpieczeństwa informacji oraz nieprawidłowościach w pracy systemów informatycznych.
2) Dla użytkowników SILP został utworzone dedykowane kanały elektroniczne do zgłaszania incydentów i zagrożeń bezpieczeństwa informacji.

5.2. Obsługa incydentów i zagrożeń bezpieczeństwa

1) Działania związane z obsługą zgłoszonych incydentów i zagrożeń bezpieczeństwa prowadzi Zespół ds. Cyberbezpieczeństw.
2) Utrzymywany jest rejestr zgłoszeń incydentów i zagrożeń informacji.

3) Incydenty bezpieczeństwa są obsługiwane zgodnie z ustaloną procedurą, która obejmują analizę, klasyfikację, reakcję i działania naprawcze.
4) Zagrożenia bezpieczeństwa są obsługiwane zgodnie z ustaloną procedurą, która obejmują analizę, klasyfikację oraz w wymaganych przypadkach reakcję i działania naprawcze.

5.3. Współpraca i komunikacja

1) W przypadku incydentów i zagrożeń bezpieczeństwa informacji dotyczących systemów SILP utrzymywanych przez DGLP, ZCI informuje i prowadzi współpracę z ich administratorami.
2) W ramach obsługi incydentów i zagrożeń bezpieczeństwa informacji o dużym znaczeniu dla organizacji, ZCI informuje i prowadzi współpracę operacyjną z krajowymi Zespołami Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT GOV, CSIRT NASK, CSIRT MON).
3) W ramach obsługi incydentów i zagrożeń bezpieczeństwa informacji o dużym znaczeniu dla organizacji i dotyczących systemów utrzymywanych przez podległą jednostkę LP, ZCI koordynuje działania wspólne prowadzone z jednostką LP oraz z krajowymi Zespołami Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT GOV, CSIRT NASK, CSIRT MON).
4) W przypadku naruszenia bezpieczeństwa informacji zawierających dane osobowe ZCI informuje i prowadzi współprace z Inspektorem ochrony danych osobowych w DGLP.
5) W przypadku incydentów mogących mieć wpływ na ciągłość działania organizacji ZCI informuje i prowadzi współpracę z Głównym Inspektorem Straży Leśnej.

5.4. Reakcja i działania naprawcze

W ramach reakcji na wykryte incydenty naruszenia bezpieczeństwa informacji Zespół ds. Cyberbezpieczeństwa może wykonać lub zlecić:

1) izolację zagrożonych systemów,
2) zmianę konfiguracji systemów,
3) zabezpieczenie dowodów tj. logi czy kopie zapasowe,
4) przywrócenie usług i danych z kopi bezpieczeństwa,
5) inne, adekwatne do wykrytych zagrożeń działania mitygujące.

W ramach działań naprawczych dla wykrytych incydentów naruszenia bezpieczeństwa informacji Zespół ds. Cyberbezpieczeństwa może wykonać lub zlecić:

6) Identyfikacje podatności i słabych punktów w bezpieczeństwie systemów SILP w DGLP.
7) Przygotowanie rekomendacji i zlecenie działań naprawczych dla podatnych systemów.
8) Wprowadzenie zmian w dokumentacji bezpieczeństwa na podstawie wniosków z incydentów.
9) Przeprowadzenie dodatkowych szkoleń dla pracowników w zakresie wykrytych zagrożeń.

6. Bezpieczeństwo informacji w zarządzaniu ciągłością działania organizacji

6.1. Identyfikacja kluczowych procesów

DGLP prowadzi identyfikacje procesów kluczowych dla zachowania ciągłości działania organizacji. Prowadzona analiza funkcjonujących procesów biznesowych ma na celu wyłonienia tych, które są niezbędne dla funkcjonowania organizacji oraz mają kluczowe znaczenie dla ochrony informacji oraz minimalizacje skutków potencjalnych incydentów bezpieczeństwa. Identyfikacja kluczowych procesów umożliwia skuteczne planowanie i wdrażanie zabezpieczeń, a także zapewnia, że działania związane z bezpieczeństwem informacji są ukierunkowane na obszary o największym znaczeniu dla ciągłości działania organizacji.

6.2. Opracowanie planów ciągłości działania

Dla zidentyfikowanych procesów kluczowych opracowywane są plany ciągłości działania, które muszą uwzględniać co najmniej następujące aspekty:

1) Zabezpieczenie informacji, w tym regularne wykonywanie kopii zapasowych danych oraz zapewnienie ich bezpiecznego przechowywania i szybkiego odtworzenia.
2) Procedury odtwarzania systemów informatycznych, obejmujące szczegółowe instrukcje postępowania na wypadek awarii lub incydentu.
3) Działania minimalizujące czas przestoju oraz umożliwiające przywrócenie kluczowych procesów w możliwie najkrótszym czasie.
4) Określenie niezbędnych zasobów, zarówno technicznych, jak i personalnych, wymaganych do utrzymania ciągłości działania kluczowych operacji.
5) Podział ról i obowiązków w przypadku aktywacji planów ciągłości działania, zapewniający skuteczną koordynację i komunikację w sytuacjach kryzysowych.

6.3. Zarządzanie kopiami bezpieczeństwa danych SILP

Zarządzanie kopiami bezpieczeństwa danych SILP jest kluczowym elementem zapewniającym bezpieczeństwo informacji i jest realizowane w oparciu o dedykowaną politykę bezpieczeństwa dla kopii, przy szczególnym uwzględnieniu następujących aspektów:

1) Regularne wykonywanie kopii zapasowych wszystkich krytycznych danych i systemów SILP, prowadzone jest zgodnie z wymaganym harmonogramem.
2) Przechowywanie kopii bezpieczeństwa danych dla kluczowych systemów prowadzone jest w bezpiecznych lokalizacjach, które są geograficznie odseparowane od głównych systemów produkcyjnych, co minimalizuje ryzyko utraty danych w wyniku lokalnych incydentów obszarowych.
3) Prowadzone są okresowe testy odtwarzania kopii bezpieczeństwa danych w celu weryfikacji ich integralności, kompletności oraz możliwości skutecznego przywrócenia danych i systemów w przypadku awarii lub innych zdarzeń kryzysowych.

6.4. Przeglądy testowanie i aktualizacja planów ciągłości działania

Co najmniej raz na rok DGLP wykonuje okresowe testowanie, przeglądy i aktualizacje planów ciągłości działania, ponieważ jest to kluczowe dla zapewnienia ich skuteczności, spójności oraz dostosowania do bieżących potrzeb organizacji. Plany ciągłości są testowane, przy czym testy te powinny obejmować:

1) Symulacje różnych scenariuszy incydentów.
2) Odtwarzanie danych z kopii bezpieczeństwa.
3) Odtwarzania systemów informatycznych z uwzględnieniem czasu reakcji oraz minimalizacji czasu przestojów.
4) Kontrolowane wyłączenia centrów przetwarzania danych, które pozwalają zweryfikować rzeczywistą odporność infrastruktury oraz skuteczność przełączania na środowiska zapasowe.

Na podstawie wyników wykonanych testów organizacja prowadzi konieczne aktualizacje planów ciągłości działania

7. Monitorowanie SILP, przeglądy SZBI i PBI

7.1. Monitorowanie systemów

Systemy informatycznych SILP w organizacji są stale monitorowane w celu szybkiego wykrywania nieautoryzowanych działań, prób naruszenia bezpieczeństwa oraz potencjalnych zagrożeń dla informacji. Monitoring obejmuje zarówno infrastrukturę techniczną, jak i kluczowe aplikacje oraz systemy przetwarzające informacje. Takie działania umożliwiają wczesne reagowanie na incydenty oraz minimalizację ryzyka naruszeń bezpieczeństwa informacji. Wyniki monitoringu są rejestrowane, analizowane i raportowane do ZCI.

7.2. Przeglądy i ich zakres

Polityka bezpieczeństwa informacji i SZBI podlegają okresowym przeglądom i aktualizacjom, w celu zapewnienia ich zgodność z aktualnymi wymaganiami prawnymi, regulacyjnymi, zmianami technologii oraz nowymi rodzajami zagrożeń. Przeglądy powinny być przeprowadzane co najmniej raz w roku, a także po każdej istotnej zmianie w infrastrukturze, procesach biznesowych lub po wystąpieniu poważnego incydentu bezpieczeństwa.

Zakres przeglądów obejmuje kompleksową ocenę wyników audytów wewnętrznych i zewnętrznych, analizę incydentów bezpieczeństwa, realizację wyznaczonych celów w zakresie bezpieczeństwa informacji, a także uwzględnia zmiany w kontekście wewnętrznym tj. struktura organizacyjna, zmiany w procesach biznesowych i zewnętrznym tj. nowe regulacje, zmiany technologiczne, rodzaje zagrożeń. Przeglądy powinny również obejmować ocenę skuteczności wdrożonych środków zaradczych oraz identyfikację nowych ryzyk.

7.3. Dokumentacja przeglądów systemu zarządzania bezpieczeństwem

Wnioski z przeglądów oraz rekomendacje dotyczące zmian powinny być dokumentowane i wdrażane w celu ciągłego doskonalenia. Taka dokumentacja stanowi podstawę do podejmowania decyzji dotyczących wdrażania działań korygujących i zapobiegawczych, a także pozwala na monitorowanie postępów w realizacji celów bezpieczeństwa oraz utrzymanie zgodności z obowiązującymi standardami i wymaganiami.

8. Realizacja procesu analizy i oceny ryzyka

Proces analizy i oceny ryzyka jest podstawą zarządzania bezpieczeństwem informacji w DGLP. Prowadzenie tego procesu jest kluczowe dla prowadzenia działań ochrony zasobów informatycznych SILP w organizacji. Regularna identyfikacja, analiza oraz zarządzanie ryzykiem pozwalają na podejmowanie świadomych decyzji dotyczących wdrażania odpowiednich zabezpieczeń i minimalizowania potencjalnych zagrożeń.

8.1. Identyfikacja ryzyka

Podatności SILP oraz zagrożenia, które mogą wpłynąć na bezpieczeństwo danych, są okresowo identyfikowane. Proces ten obejmuje zarówno analizę środowiska wewnętrznego, jak i zewnętrznego, a także uwzględnia zmiany technologiczne, organizacyjne oraz regulacyjne.

8.2. Analiza ryzyka

Każde zidentyfikowane ryzyko poddawane jest szczegółowej analizie, obejmującej ocenę prawdopodobieństwa jego wystąpienia oraz potencjalnego wpływu na działalność organizacji. Analiza ta pozwala określić krytyczność ryzyka i ustalić priorytety działań wskazując podatne obszary, które są najbardziej istotne dla organizacji.

8.3. Zarządzanie ryzykiem

W oparciu o wyniki prowadzonych analiz ryzyka, wdrażane są adekwatne środki zaradcze i kontrolne, mające na celu ograniczenie ryzyka do poziomu akceptowalnego przez organizację. Proces zarządzania ryzykiem jest cyklicznie powtarzany, a skuteczność zastosowanych działań podlega regularnej ocenie i aktualizacji, co stanowi element procesu ciągłego doskonalenia SZBI.

9. Zarządzanie projektami teleinformatycznymi

DGLP zarządza projektami teleinformatycznymi w sposób zorganizowany, uwzględniając aspekty związane z zapewnieniem bezpieczeństwa informacji na każdym etapie realizowanych przedsięwzięć.

Na etapie planowania każdy projekt musi brać pod szczególną uwagę elementy zapewnienia bezpieczeństwa danych, w ramach których prowadzona jest analiza ryzyka w celu identyfikacji potencjalnych zagrożeń oraz określenie koniecznych do wdrożenia odpowiednich środków zaradczych.

W procesie projektowym uczestniczy Zespół ds. cyberbezpieczeństwa, który powinien być zaangażowany na wszystkich etapach zarządzania projektem tj. planowanie, realizację, wdrożenie, monitorując zgodność działań z polityką bezpieczeństwa informacji.

10. Kryptografia i szyfrowanie danych SILP

10.1. Stosowanie technik kryptograficznych

Ochrona informacji wrażliwych w systemach SILP realizowana jest poprzez stosowanie technik kryptograficznych zgodnych z aktualnymi standardami i wytycznymi branżowymi.

Zabrania się stosowania uznanych za niebezpieczne algorytmów i protokołów kryptograficznych tj. SHA-1, MD5, DES, RSA, SSLv3.

Techniki kryptograficzne stosuje się do:

1) szyfrowania danych w spoczynku,
2) szyfrowania danych w transmisji,
3) podpisu cyfrowego do weryfikacji autentyczności i integralności danych,
4) podpisu cyfrowego do weryfikacji tożsamości.

10.2. Ochrona danych SILP w spoczynku

Dane SILP stanowiące tajemnicę przedsiębiorstwa i inne dane, które mogą mieć wpływ na działanie i bezpieczeństwo organizacji, zapisane na nośnikach elektronicznych wynoszonych poza siedzibę jednostki LP, muszą być zaszyfrowane.

10.3. Ochrona danych SILP w transmisji

1) Dane przesyłane w sieciach wewnętrznych i zewnętrznych muszą być chronione przy użyciu odpowiednich technik kryptograficznych, aby zapewnić ich poufność i integralność, za wyjątkiem dedykowanych sieci połączeniowych.
2) Proces uwierzytelniania użytkowników w systemach SILP za pośrednictwem sieci należy realizować z użyciem połączeń szyfrowanych zapewniających poufność i integralność przesyłanych danych.
3) Dostęp administracyjny do systemów SILP za pośrednictwem sieci należy realizować z użyciem połączeń szyfrowanych zapewniających poufność i integralność przesyłanych danych.
4) Dostęp do wewnętrznej sieci DGLP z sieci Internet jest możliwy jedynie za pomocą dedykowanych systemów VPN LP autoryzowanych przez Wydział Informatyki DGLP.

10.4. Infrastruktura klucza publicznego

1) Do zarządzania wewnętrznymi certyfikatami kryptograficznymi DGLP korzysta z infrastruktura klucza publicznego Lasów Państwowych (systemu PKI LP), który jest utrzymywany w ramach wewnętrznych zasobów SILP.
2) Uwierzytelnianie usług sieciowych jest realizowane na podstawie certyfikatów wystawionych przez PKI LP lub certyfikaty kwalifikowane wystawione przez zewnętrznych dostawców.

3) Uwierzytelnianie użytkowników w dostępie do stacji roboczych SILP obywa się za pomocą kart kryptograficznych i certyfikatów PKI LP.
4) Cykl funkcjonowania certyfikatów SILP i ich nośników są określone przez szczegółowe wytyczne Wydziału Informatyki DGLP.

11. Bezpieczeństwo Operacyjne

11.1. Procedury operacyjne

Operacje utrzymania systemów SILP przetwarzających dane DGLP muszą być realizowane zgodnie z procedurą, która uwzględnia co najmniej:

1) Kopie bezpieczeństwa danych, wykonywane zgodnie z obwiązującą polityką dla kopii bezpieczeństwa danych SILP.
2) Aktualizacje oprogramowania, instalowane na bieżąco, udostępniane przez producentów, poprawki krytyczne i bezpieczeństwa dla oprogramowania sprzętowego, sterowników urządzeń w systemach operacyjnych, systemów operacyjnych, aplikacji.
3) Monitoring systemów, prowadzony w sposób ciągły monitoring dostępności usług i parametrów systemów oraz monitoring zagregowanych dzienników zdarzeń w systemie klasy SIEM.
4) Monitoring i raportowanie nieudanych prób logowań do systemów.
5) Monitoring i raportowanie zdarzeń systemów ochrony przed złośliwym oprogramowaniem.

11.2. Zarządzanie zmianami

1) Krytyczne zmiany w konfiguracji systemów SILP są prowadzone zgodnie z ustalonym procesem zarządzania zmianami, w celu minimalizacji ryzyka zagrożeń bezpieczeństwa informacji.
2) Proces wprowadzania zmian krytycznych w systemach SILP musi uwzględniać szczegółową analizę możliwych skutków oraz odpowiednie przygotowanie do wdrożenia każdej zmiany. Przed przystąpieniem do realizacji zmiany należy przeprowadzić ocenę wpływu planowanej modyfikacji na funkcjonowanie systemów, bezpieczeństwo informacji, zgodność z obowiązującymi regulacjami oraz potencjalny wpływ na użytkowników i procesy biznesowe.
3) Wdrażanie zmian w systemach SILP musi uwzględniać mechanizmy przywracania poprzedniej konfiguracji (rollback) w przypadku wystąpienia awarii, niezgodności z wymaganiami lub zagrożeń bezpieczeństwa.
4) Wprowadzanie zmian krytycznych w systemach SILP musi obejmować etap testowania po modyfikacji, aby zapewnić stabilność, bezpieczeństwo i zgodność z wymaganiami.
5) W sytuacjach awaryjnych lub wymagających natychmiastowego przeciwdziałania zagrożeniu bezpieczeństwa informacji tj. aktywne ataki, krytyczne luki, dopuszcza się wprowadzenie zmian poza standardowym procesem zarządzania zmianami, pod warunkiem późniejszego udokumentowania wprowadzonych modyfikacji i weryfikacji skutków zmian pod kątem zgodności z polityką bezpieczeństwa i standardami technicznymi.

12. Ochrona sieci transmisji danych

Sieć transmisji danych DGLP podlega szczególnym wymogom ochronnym, mającym na celu zabezpieczenie przed nieautoryzowanym dostępem oraz zagrożeniami wewnętrznymi i zewnętrznymi. Wdrożone mechanizmy ochrony obejmują:

12.1. Firewalle nowej generacji

Prowadzą filtrowanie ruchu na podstawie polityk bezpieczeństwa, inspekcję głęboką pakietów, inspekcję ruchu szyfrowanego, blokowanie podejrzanych protokołów. Szczególnej ochronie podlega punkt styku sieci organizacji z siecią Internet oraz punk styku sieci lokalnych DGLP z siecią rozległą.

12.2. Systemy wykrywania i zapobiegania włamaniom

Prowadzą monitoring i analizę ruchu sieciowego w czasie rzeczywistym. Analiza prowadzona jest pod kątem wykrywania anomalii i nietypowych zachowań tj. skanowanie portów, podejrzane wzorce ruchu, próby wykorzystania luk w usługach sieciowych. W przypadku wykrycia takich zdarzeń wykonywane jest automatyczne blokowanie źródła ruchu.

12.3. Segmentacja sieci

Sieci lokalne DGLP są podzielone na segmenty funkcjonalne i strefy bezpieczeństwa w celu zwiększenia ochrony zasobów podłączonych do sieci oraz ograniczenia ryzyka nieautoryzowanego dostępu. Segmentacja sieci polega na wydzieleniu odrębnych obszarów sieciowych tj. VLAN, strefy DMZ, sieci monitoringu, sieci administracyjne, sieci użytkowników, sieci systemów krytycznych, co umożliwia zarządzanie dostępem oraz kontrolę przepływu danych pomiędzy segmentami. Każdy segment posiada przypisane poziomy uprawnień i zabezpieczeń, a ruch pomiędzy nimi jest monitorowany i filtrowany przy użyciu dedykowanych urządzeń sieciowych, takich jak firewalle oraz systemy wykrywania i zapobiegania włamaniom.

13. Identyfikacja i analiza zagrożeń

13.1. Zbieranie informacji o zagrożeniach

DGLP regularnie monitoruje różnorodne źródła informacji o zagrożeniach, zarówno wewnętrzne, jak i zewnętrzne, w szczególności:

1) Raporty i bazy danych wskaźników IoC dostarczane przez dostawców stosowanych rozwiązań cyberbezpiczeńetwa.
2) Raporty i informacje oraz listy wskaźników IoC z krajowych zespołów CSIRT.
3) Informacje o anomaliach z ciągłego monitoring własnego ruchu sieciowego.
4) Informacje o zagrożeniach z ciągłego monitoringu dzienników zdarzeń systemów SILP.
5) Informacje o zagrożeniach z systemu korelacji zdarzeń w systemie SIEM.
6) Sieciowe skanery podatności.

13.2. Analiza zagrożeń

Zespół ds. Cyberbezpieczeństwa weryfikuje wiarygodność i skalę zagrożeń dla danych SILP, eliminuje fałszywe alarmy (false positives), a następnie nadaje priorytety ryzyka według ich potencjalnego wpływu na organizację. Dla każdego zagrożenia uruchamia się dedykowaną ścieżkę prowadzenia działań naprawczych.

13.3. Wdrażanie środków remediacji

Na podstawie przeprowadzonej analizy Zespół ds. cyberbezpieczeństwa wprowadza lub zleca administratorom systemów SILP wdrożenie odpowiednich środków zaradczych, w celu minimalizacji ryzyka i ochrony zasobów informatycznych. W szczególności są to:

1) Aktualizacje polityk bezpieczeństwa.
2) Wdrażanie poprawek i łatek bezpieczeństwa.
3) Zmiana konfiguracji systemów.
4) Analiza zawartości nośników danych pod katem złośliwego oprogramowania.
5) Wymiana haseł kont użytkowników SILP.
6) Wdrożenie dodatkowych narzędzi monitorujących i detekcyjnych.

Działania są monitorowane i weryfikowane pod kątem ich realizacji i skuteczności, a proces analizy zagrożeń jest procesem ciągłym.

14. Instalacja Oprogramowania

Proces instalacji oprogramowania jest prowadzony zgodnie z zasadami bezpieczeństwa informacji, aby zapobiec wprowadzeniu do systemu SILP nieautoryzowanego lub złośliwego oprogramowania.

14.1. Polityka instalacji oprogramowania

1) Weryfikacja oprogramowania
   Przed instalacją każde nowe oprogramowanie podlega weryfikacji pod kątem bezpieczeństwa oraz zgodności z wymaganiami organizacji. Instalowane mogą być wyłącznie aplikacje zatwierdzone przez Zespół ds. cyberbezpieczeństwa lub administratorów SILP.
2) Zarządzanie licencjami
   Oprogramowanie musi być objęte ważną licencją, zgodną z warunkami umowy licencyjnej. Licencje są ewidencjonowane, monitorowane i okresowo weryfikowane w celu zapewnienia legalności użytkowania.
3) Aktualizacje:
   Oprogramowanie musi być regularnie aktualizowane. Wszystkie dostępne poprawki krytyczne i bezpieczeństwa muszą być niezwłocznie wdrażane, aby zminimalizować ryzyko podatności i zapewnić ciągłość ochrony oraz działania systemów SILP.

VII. Lista dokumentów wspierających politykę bezpieczeństwa informacji

Dokumenty wprowadzone do stosowania zarządzeniami Dyrektora Generalnego Lasów Państwowych:

1. „Zasady funkcjonowania zintegrowanego systemu informatycznego w Lasach Państwowych”,
2. „Zasady bezpiecznej eksploatacji zasobów informatycznych Lasów Państwowych”,
3. „Zasady dostępu do danych w Systemach Informatycznych Lasów Państwowych”,
4. „Zasady funkcjonowania systemu telefonii IP i wideokonferencji”,
5. „Wzór oświadczenia pracownika”

- wprowadzone do stosowania Zrządzeniem nr 31 Dyrektora Generalnego Lasów Państwowych z dnia 18 września 2017 r. w sprawie zasad funkcjonowania i zasad bezpieczeństwa systemu informatycznego w Państwowym Gospodarstwie Leśnym Lasy Państwowe, wraz z późniejszymi zmianami;

6. „Regulamin organizacyjny Dyrekcji Generalnej Lasów Państwowych” – wprowadzony do stosowania Zarządzeniem nr 19 Dyrektora Generalnego Lasów Państwowych z dnia 14 marca 2024 r., wraz z późniejszymi zmianami;
7. „Zasady klasyfikacji, ochrony i udostępniania informacji stanowiących tajemnicę przedsiębiorstwa w Państwowym Gospodarstwie Leśnym Lasy Państwowe”,
8. „Wykaz informacji stanowiących tajemnicę przedsiębiorstwa”,
9. „Wzór oświadczenia pracownika lub innej osoby mającej dostęp do informacji stanowiącej tajemnicę przedsiębiorstwa w PGL Lasy Państwowe”

- wprowadzone do stosowania Zarządzeniem nr 48 Dyrektora Generalnego Lasów Państwowych z dnia 6 października 2010 r. w sprawie ustalenia zasad klasyfikacji, ochrony i udostępniania informacji stanowiącej tajemnicę przedsiębiorstwa w Państwowym Gospodarstwie Leśnym Lasy Państwowe, wraz z późniejszymi zmianami.

Regulaminy i projekty techniczne ustanawiane i aktualizowane przez Naczelnika Wydziału Informatyki DGLP

1. Projekt usług katalogowych PGL LP
2. Polityka kopii zapasowych SILP
3. Zasady adresacji IP w sieci LP
4. Regulamin użytkowania systemu poczty elektronicznej LP
5. Polityka dla ruchu w sieci WAN LP
6. Polityka dla ruchu na styku sieci WAN LP i Internet
7. Zasady inspekcji ruchu szyfrowanego
8. Zasady budowy lokalnych sieci bezprzewodowych w jednostkach PGL LP
9. Polityka bezpieczeństwa urządzeń mobilnych
10. Polityka przetwarzania danych LP w publicznej chmurze obliczeniowej

Procedury, rejestry i inne dokumenty ustanawiane i aktualizowane przez Kierownika Zespołu ds. Cyberbezpieczeństwa WI DGLP

1. Procedura nadania dostępu VPN dla podmiotów zewnętrznych

2. Dokumentacja analizy ryzyk prowadzonej w oparciu o szablon MITRE ATT&CK
3. Rejestr wspomagających aktywów IT prowadzony w oparciu o adresację IP
4. Rejestr zgłoszeń zagrożeń i incydentów bezpieczeństwa danych SILP prowadzony w oparciu o dedykowane oprogramowanie
5. Rejestr krytycznych dostawców sprzętu i usług cyfrowych
6. Procedura nadania dostępu do SILP
7. Plan ciągłości działania SILP
8. Procedura odtworzenia SILP po katastrofie
9. Procedura zarządzania zagrożeniami bezpieczeństwa
10. Procedura zarządzania incydentem bezpieczeństwa
11. Procedura utrzymania systemów SILP
12. Procedura zarządzania krytycznymi zmianami SILP
13. Procedura funkcjonowania karty kryptograficznych systemu PKI LP
14. Zestaw procedur odtworzenia systemów SILP z kopii zapasowych
15. Zestaw procedury awaryjnego dostępu administracyjnego do systemów SILP