Warszawa, dnia 28 listopada 2024 r.

Poz. 274

ZARZĄDZENIE
MINISTRA SPRAWIEDLIWOŚCI

z dnia 28 listopada 2024 r.

w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji Ministerstwa Sprawiedliwości

Na podstawie art. 34 ust. 1 ustawy z dnia 8 sierpnia 1996 r. o Radzie Ministrów (Dz. U. z 2024 r. poz. 1050 i 1473) zarządza się, co następuje:

§ 1. W Ministerstwie Sprawiedliwości wprowadza się Politykę Bezpieczeństwa Informacji Ministerstwa Sprawiedliwości, stanowiącą załącznik do zarządzenia.

§ 2. Właściciele obszarowi zobowiązani są do przeprowadzenia aktualizacji przypisanych im dokumentów obszarowych, w terminie 6 miesięcy od dnia wejścia w życie zarządzenia.

§ 3. Traci moc zarządzenie Ministra Sprawiedliwości z dnia 27 marca 2019 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji Ministerstwa Sprawiedliwości (Dz. Urz. Min. Sprawiedl. poz. 118 oraz z 2021 r. poz. 115).

§ 4. Zarządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

MINISTER SPRAWIEDLIWOŚCI

Adam Bodnar

Załącznik do zarządzenia
Ministra Sprawiedliwości
z dnia 28 listopada 2024 r.
(Dz. Urz. Min. Sprawiedl.
poz. 274)

Ministerstwo Sprawiedliwości

Polityka Bezpieczeństwa Informacji Ministerstwa Sprawiedliwości

wersja 1.1

SPIS TREŚCI

Wstęp

Bezpieczeństwo informacji oraz systemów, w których informacje te są przetwarzane jest jednym z kluczowych elementów zapewniających realizację zadań Ministerstwa Sprawiedliwości.

Kierownictwo Ministerstwa Sprawiedliwości pozostając zobligowanym do: spełnienia wymagań prawnych w odniesieniu do ochrony informacji, tj. zapewnienia wymogów określonych w § 19 ust. 1 rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2024 r. poz. 773), która zobowiązuje podmiot wykonujący czynności publiczne do wdrażania, monitorowania, utrzymywania i doskonalenia systemu zarządzania bezpieczeństwem informacji; zapewnienia odpowiedniego poziomu bezpieczeństwa informacji tworzonych, przetwarzanych i przechowywanych w urzędzie, a także zapewnienia właściwej ochrony kluczowych zasobów Ministerstwa Sprawiedliwości, tj. bezpieczeństwa osób, mienia i informacji, ustanawia Politykę Bezpieczeństwa Informacji Ministerstwa Sprawiedliwości, zwanej dalej „PBI Ministerstwa Sprawiedliwości".

Kierownictwo Ministerstwa Sprawiedliwości 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.

Niniejszy dokument określa ramy Systemu Zarządzania Bezpieczeństwem Informacji, zwanego dalej „SZBI w Ministerstwie Sprawiedliwości". PBI Ministerstwa Sprawiedliwości jest aktem prawa wewnętrznego Ministra Sprawiedliwości.

Dokument opisuje zasady ochrony informacji obowiązujące w Ministerstwie Sprawiedliwości, zarządzania ryzykiem, role i zadania osób uczestniczących w procesie przetwarzania informacji oraz zarządzania bezpieczeństwem informacji, zgodne z przepisami obowiązującego prawa, przyjętymi uwarunkowaniami umownymi i normatywnymi oraz wypracowanymi własnymi standardami w zakresie funkcjonowania organizacji. PBI Ministerstwa Sprawiedliwości określa również warunki, jakie muszą spełniać systemy teleinformatyczne przetwarzające informacje w Ministerstwie Sprawiedliwości. Szczegóły zostały opisane w dokumentach obszarowych.

PBI Ministerstwa Sprawiedliwości nie obejmuje kwestii związanych z ochroną informacji niejawnych z uwagi na uregulowanie powyższego obszaru w przepisach o ochronie informacji niejawnych.

Wszystkie polityki, procedury, instrukcje oraz inne regulacje wewnętrzne Ministerstwa Sprawiedliwości dotyczące bezpieczeństwa informacji muszą być zgodne z zasadami zawartymi w niniejszym dokumencie.

Z dokumentem PBI Ministerstwa Sprawiedliwości powinny zapoznać się wszystkie osoby mające dostęp do informacji – pracownicy, osoby oddelegowane, funkcjonariusze, kadra kierownicza i inne osoby uprawnione, a także pracownicy firm zewnętrznych realizujący prace na rzecz Ministerstwa Sprawiedliwości.

PBI Ministerstwa Sprawiedliwości zamieszczona jest w Intranecie Ministerstwa Sprawiedliwości w zakładce Bezpieczeństwo Informacji.

Słownik pojęć, definicje i skróty

Na potrzeby PBI Ministerstwa Sprawiedliwości i dokumentów związanych, definiuje się następujące pojęcia:

Aktywa – wszystkie środki trwałe i nietrwałe (informacje, systemy komputerowe, dane, oprogramowanie, infrastruktura, reputacja itd.), mające wpływ na wartość organizacji oraz jej funkcjonowanie, podatne na wszelkiego rodzaju zagrożenia i wymagające bezpośredniej ochrony.

Aktywa informacyjne – wszelkie informacje przetwarzane w Ministerstwie Sprawiedliwości, niezależnie od ich nośnika danych.

Audyt Krajowych Ram Interoperacyjności – audyt realizowany zgodnie z rozporządzeniem Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, zwany dalej „Audyt KRI".

Autentyczność – właściwość polegająca na tym, że pochodzenie lub zawartość danych opisujących obiekt, są takie, jak deklarowane.

Bezpieczeństwo informacji – zachowanie poufności, integralności i dostępności informacji, z uwzględnieniem takich cech jak: rozliczalność, autentyczność, niezaprzeczalność i niezawodność.

Cyberprzestrzeń Ministerstwa Sprawiedliwości – przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2024 r. poz. 1557) – w Ministerstwie Sprawiedliwości.

DODO – dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz. Urz. UE L 119 z 04.05.2016, str. 89), która do polskiego systemu prawnego została implementowana ustawą z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2023 r. poz. 1206).

Dokument – każda utrwalona w różnej postaci treść stanowiąca dowód prawa, stosunku prawnego, okoliczności mającej znaczenie prawne lub zawierająca oświadczenie woli albo wiedzy podmiotu, od którego pochodzi, a w szczególności nośnik informacji umożliwiający zapoznanie się z tą treścią.

Dokumenty obszarowe – polityki określające szczegółowe zasady zarządzania bezpieczeństwem informacji w określonych obszarach (tzw. polityki obszarowe), do których przypisany jest właściciel odpowiedzialny za prawidłowe działanie opisanego procesu.

Dostępność – właściwość polegająca na możliwości wykorzystania zasobu w założonym czasie na żądanie upoważnionego podmiotu.

Funkcjonariusz – funkcjonariusz Służby Więziennej, któremu wyznaczono miejsce pełnienia służby w obiektach Ministerstwa Sprawiedliwości, lub funkcjonariusz innych służb oddelegowany do Ministerstwa Sprawiedliwości.

Incydent – pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działalności Ministerstwa Sprawiedliwości i zagrażają bezpieczeństwu informacji.

Informacja – aktywo, które ma wartość dla organizacji i wymaga odpowiedniej ochrony – może obejmować różnorodne dane, w tym dane osobowe, dokumenty, rekordy, bazy danych, polityki, umowy z dostawcami, plany ciągłości działania itd. Informacja podlega przechowywaniu, przetwarzaniu, przesyłaniu lub udostępnianiu zarówno w formie papierowej, elektronicznej i każdej innej, jest narażona na różnego rodzaju zagrożenia, tzn. nieuprawniony dostęp, zmianę, uszkodzenia, utratę lub ujawnienie.

Inne osoby uprawnione – m.in**.** praktykanci, stażyści, wolontariusze.

Integralność – właściwość polegająca na zapewnieniu dokładności i kompletności aktywów.

Jednostka organizacyjna (urząd) – Ministerstwo Sprawiedliwości.

Komórka organizacyjna – biuro, departament lub równorzędna komórka organizacyjna określona w statucie Ministerstwa Sprawiedliwości.

Niezaprzeczalność – zdolność do udowodnienia, że wystąpiły deklarowane zdarzenia lub działania.

Niezawodność – właściwość oznaczająca spójne, zamierzone zachowanie i skutki.

Nośnik danych – przedmiot, na którym możliwe jest zapisanie i odczytanie informacji, np. papier, dysk twardy, pamięć typu flash, smartphone, tablet, karta pamięci, nośnik optyczny.

Osoba oddelegowana – osoba oddelegowana na podstawie odrębnych przepisów do pełnienia czynności służbowych w Ministerstwie Sprawiedliwości.

PBI Ministerstwa Sprawiedliwości – Polityka Bezpieczeństwa Informacji Ministerstwa Sprawiedliwości.

Poufność – właściwość polegająca na tym, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom.

Pracownik – osoba zatrudniona w Ministerstwie Sprawiedliwości w ramach stosunku pracy zawartego na podstawie umowy o pracę, mianowania, powołania.

RODO – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.[1)]).

Rozliczalność – właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi (ISO 7498-2:1989).

Ryzyko – kombinacja prawdopodobieństwa wystąpienia zdarzenia i jego konsekwencji.

System teleinformatyczny – zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2024 r. poz. 34, 731 i 834).

SZBI – System Zarządzania Bezpieczeństwem Informacji.

Testy – proces analizy systemów informatycznych lub innych zasobów cyfrowych, mający na celu identyfikację i ocenę ich potencjalnych słabych punktów, zagrożeń i podatności dla bezpieczeństwa informacji, a także ocenę efektywności procedur zabezpieczających, których skutkiem jest dostarczenie rekomendacji dotyczących eliminacji takich zagrożeń.

Testy penetracyjne – rodzaj testu obejmujący tworzenie symulacji ataku na system informatyczny lub inny zasób cyfrowy, którego celem jest zidentyfikowanie jego słabych punktów, luk i podatności, a następnie stworzenie rekomendacji dotyczących eliminacji tych nieprawidłowości.

Właściciel aktywów – osoba odpowiedzialna za posiadane aktywa np. główny księgowy, dyrektor komórki organizacyjnej.

Właściciel obszarowy – osoba odpowiedzialna za opracowanie i nadzorowanie stosowania wewnętrznych regulacji w ramach posiadanych kompetencji wynikających z regulaminu organizacyjnego Ministerstwa Sprawiedliwości i innych aktów wewnętrznych.

Zagrożenie – potencjalna przyczyna niepożądanego incydentu, który może spowodować szkodę dla systemu lub instytucji.

Zapewnienie ciągłości działania – ciąg planowanych działań zmierzających do zapobieżenia zakłóceniom lub usuwania przyczyn i skutków zaistnienia zakłócenia lub wprowadzenia zastępczych warunków działania kluczowych procesów do czasu usunięcia zakłócenia.

[1)] Zmiana wymienionego rozporządzenia została ogłoszona w Dz. Urz. UE L 127 z 23.05.2018, str. 2.

Zasoby – ludzkie, rzeczowe, finansowe i informacyjne.

1. CEL I ZAKRES OBOWIĄZYWANIA POLITYKI BEZPIECZEŃSTWA INFORMACJI MINISERTSWA SPRAWIEDLIWOŚCI

Celem PBI Ministerstwa Sprawiedliwości jest:

1. Zapewnienie prawidłowej ochrony zasobów Ministerstwa Sprawiedliwości.
2. Zapewnienie poprawnego funkcjonowania wszystkich systemów teleinformatycznych przetwarzających informacje.
3. Ograniczenie występowania zagrożeń związanych z naruszeniem informacji.
4. Ustanowienie SZBI w Ministerstwie Sprawiedliwości.

Niniejszy dokument dotyczy wszystkich komórek organizacyjnych Ministerstwa Sprawiedliwości oraz wszystkich jego pracowników w szczególności w rozumieniu: ustawy z dnia 21 listopada 2008 r. o służbie cywilnej (Dz. U. z 2024 r. poz. 409), ustawy o pracownikach urzędów państwowych (Dz. U. z 2023 r. poz. 1917) oraz ustawy z dnia 26 czerwca 1974 – Kodeks pracy (Dz. U. z 2023 r. poz. 1465 oraz z 2024 r. poz. 878 i 1222), a także innych osób mających dostęp do informacji chronionych (np. osób oddelegowanych, funkcjonariuszy, pracowników firm zewnętrznych realizujących prace na rzecz Ministerstwa Sprawiedliwości lub zleceniobiorców oraz innych osób uprawnionych).

Dokument ma zastosowanie do wszystkich informacji chronionych niezależnie od postaci, w jakiej są przechowywane (papierowej, elektronicznej i innej).

Za aktywa wynoszone poza siedzibę urzędu odpowiada pracownik, osoba oddelegowana, osoby wykonujące zadania na innej podstawie niż stosunek pracy, a także inne osoby uprawnione. W przypadku ich utraty fakt należy niezwłocznie zgłosić bezpośredniemu przełożonemu.

Z dokumentem PBI Ministerstwa Sprawiedliwości zapoznają się wszystkie nowozatrudnione osoby oraz osoby mające dostęp do informacji – pracownicy, osoby oddelegowane, kadra kierownicza, funkcjonariusze, pracownicy firm zewnętrznych realizujący prace na rzecz Ministerstwa Sprawiedliwości oraz inne osoby uprawnione. Oświadczenie o zapoznaniu powinno być przechowywane w aktach osobowych każdego pracownika, natomiast oświadczenia innych osób niż pracownik Ministerstwa Sprawiedliwości, powinny być przechowywane w komórce merytorycznej w dokumentacji dotyczącej realizacji postanowień umowy.

Biuro Dyrektora Generalnego oraz Dyrektor Departamentu Kadr i Organizacji Sądów Powszechnych i Wojskowych, w zakresie swojej właściwości, zapoznają pracowników, osoby oddelegowane, a także inne osoby uprawnione z PBI Ministerstwa Sprawiedliwości oraz przechowują oświadczenia o zapoznaniu z ww. dokumentem. Po wprowadzeniu aktualizacji PBI Ministerstwa Sprawiedliwości, Pełnomocnik do spraw bezpieczeństwa informacji w Ministerstwie Sprawiedliwości, zwany dalej: „Pełnomocnikiem” obliguje dyrektorów komórek organizacyjnych do zapoznania podległych pracowników z nowym dokumentem.

Komórki organizacyjne powinny zebrać od pracowników oświadczenia o zapoznaniu się z PBI Ministerstwa Sprawiedliwości, a następnie w postaci zbiorczej przekazać je do właściwych komórek kadrowych.

Komórki organizacyjne zawierające umowy powierzające wykonanie określonych czynności związanych z dostępem do informacji chronionych (poza komórką kadrową), zobligowane są do przechowywania oświadczenia o zapoznaniu się z PBI Ministerstwa Sprawiedliwości w aktach dotyczących takich umów.

2. ODPOWIEDZIALNOŚĆ ZA BEZPIECZEŃSTWO INFORMACJI

2.1 Ogólny podział odpowiedzialności

Zarządzanie bezpieczeństwem informacji w Ministerstwie Sprawiedliwości opiera się na następującym podziale:

2.1.1 Minister Sprawiedliwości lub upoważniony Członek Kierownictwa Ministerstwa Sprawiedliwości odpowiedzialny za bezpieczeństwo informacji

1. Nadzoruje realizację zadań określonych w PBI Ministerstwa Sprawiedliwości.
2. Wyznacza i odwołuje Pełnomocnika, któremu powierza koordynowanie zadań określonych w PBI Ministerstwa Sprawiedliwości dotyczących funkcjonowania SZBI.
3. Jest właścicielem polityki w obszarze bezpieczeństwa danych osobowych, której opracowywanie i aktualizację powierza Zespołowi Inspektora Ochrony Danych.

2.1.2 Pełnomocnik do spraw bezpieczeństwa informacji w Ministerstwie Sprawiedliwości

Pełnomocnik do spraw bezpieczeństwa informacji, zwany dalej „Pełnomocnikiem", jest odpowiedzialny za koordynację realizacji zadań związanych z zarządzaniem SZBI oraz koordynuje działania w zakresie zadań wynikających z PBI Ministerstwa Sprawiedliwości poprzez dokonywanie przeglądów SZBI, tzn.:

1. Organizuje okresowe przeglądy SZBI.
2. Monitoruje postępowanie z ryzykiem w obszarze bezpieczeństwa informacji.
3. Koordynuje działania związane z wykonaniem corocznego audytu KRI.

Ponadto, Pełnomocnik jest właścicielem niniejszej PBI Ministerstwa Sprawiedliwości, Procedury nadzoru nad dokumentacją Systemu Zarządzania Bezpieczeństwem Informacji, Procedury zarządzania incydentami bezpieczeństwa informacji oraz Procedury zarządzania ryzykiem bezpieczeństwa informacji Ministerstwa Sprawiedliwości.

Pełnomocnik zatwierdza Polityki Bezpieczeństwa dla poszczególnych obszarów z zastrzeżeniem, że Politykę bezpieczeństwa danych osobowych, zgodnie z obowiązującymi przepisami, ostatecznie zatwierdza administrator danych Ministerstwa Sprawiedliwości.

Pełnomocnik może, w uzasadnkionych przypadkach, wyznaczyć właścicieli polityk obszarowych innych niż wskazani w dokumencie.

W zakresie wykonywanych zadań Pełnomocnik może wydawać wytyczne, występować z wnioskami oraz żądać udzielenia informacji i opinii dotyczących bezpieczeństwa informacji od komórek organizacyjnych Ministerstwa Sprawiedliwości w zakresie ich właściwości.

Obsługę Pełnomocnika w zakresie realizacji jego obowiązków zapewnia komórka organizacyjna odpowiadająca za koordynowanie działań w zakresie zadań wynikających z Polityki Bezpieczeństwa Informacji Ministerstwa Sprawiedliwości.

2.1.3 Dyrektorzy komórek organizacyjnych

Dyrektorzy Departamentów i Biur odpowiadają za:

1. Identyfikację aktywów informacyjnych (w tym w szczególności za identyfikację zbiorów danych osobowych oraz informacji prawnie chronionych) w ramach właściwości departamentu/biura.
2. Zapewnienie merytorycznego/legislacyjnego wsparcia Departamentowi Informatyzacji i Rejestrów Sądowych jako komórce nadzorującej/obsługującej dany system teleinformatyczny w celu jego należytego utrzymania i rozwoju.

3. Prowadzenie dokumentacji systemów teleinformatycznych, nad którymi sprawują nadzór.
4. Przestrzeganie zasad ochrony informacji przez podległych im pracowników, osób oddelegowanych i innych osób uprawnionych realizujących zadania w danej komórce organizacyjnej.
5. Przeprowadzanie cyklicznej analizy ryzyka bezpieczeństwa informacji, związanej z realizowanymi w komórce organizacyjnej zadaniami i wykorzystywanymi przez nią aktywami, zgodnie z Procedurą zarządzania ryzykiem bezpieczeństwa informacji Ministerstwa Sprawiedliwości.
6. Definiowanie oraz realizację działań zapobiegających zagrożeniom lub minimalizujących ich skutki.
7. Zapoznanie pracowników, osób oddelegowanych oraz innych osób uprawnionych z obowiązkami związanymi z ochroną informacji na stanowiskach pracy.
8. Zapoznanie pracowników, osób delegowanych oraz innych osób uprawnionych z wewnętrznymi zasadami dotyczącymi ochrony informacji.
9. Informowanie Biura Cyberbezpieczeństwa o zdarzeniach mogących wpływać na bezpieczeństwo cyberprzestrzeni Ministerstwa Sprawiedliwości.

Ponadto, dyrektorzy komórek organizacyjnych mogą tworzyć na potrzeby funkcjonowania komórek organizacyjnych, którymi kierują, wewnętrzne instrukcje w obszarze bezpieczeństwa informacji – instrukcje te nie mogą być sprzeczne z PBI Ministerstwa Sprawiedliwości i muszą zostać skonsultowane z właścicielami obszarowymi oraz Pełnomocnikiem. Dokument po ostatecznym zatwierdzeniu przez dyrektora komórki organizacyjnej należy przekazać do wiadomości Pełnomocnikowi.

2.1.4 Pracownicy

Odpowiedzialność za bezpieczeństwo informacji w Ministerstwie Sprawiedliwości zgodnie z posiadanymi zakresami obowiązków ponoszą wszyscy pracownicy, osoby oddelegowane, osoby wykonujące pracę na innej podstawie niż stosunek pracy, pracownicy firm zewnętrznych realizujących prace na rzecz Ministerstwa Sprawiedliwości oraz inne osoby uprawnione. Każdy z wyżej wymienionych zobowiązany jest dbać o bezpieczeństwo powierzonych mu do przetwarzania, przechowywania lub archiwizowania informacji, zgodnie z przepisami prawa powszechnie obowiązującego oraz obowiązującymi w Ministerstwie Sprawiedliwości przepisami wewnętrznymi.

Pracownikom nie wolno używać swoich uprawnień oraz dostępów nie związanych z wykonywaniem zadań służbowych i używać ich do własnych celów.

2.2 Podział odpowiedzialności w poszczególnych obszarach

W celu zapewnienia wymaganego poziomu bezpieczeństwa informacji, wyodrębniono kluczowe obszary zarządzania bezpieczeństwem informacji, które zostały podzielone ze względu na kompetencje ich właścicieli, a ich zadania wynikają wprost z regulaminu organizacyjnego Ministerstwa Sprawiedliwości oraz wewnętrznych regulaminów organizacyjnych właścicieli, są to:

2.2.1 Ochrona fizyczna obiektów Ministerstwa Sprawiedliwości

Obszar znajduje się we właściwości Dyrektora Biura Bezpieczeństwa, który:

1. Jest właścicielem polityki w obszarze bezpieczeństwa fizycznego.
2. Zapewnia zabezpieczenia techniczno-organizacyjne służące do kontroli dostępu oraz wykrycia nieautoryzowanych działań związanych z kontrolą wejść i wyjść do pomieszczeń i budynków Ministerstwa Sprawiedliwości.
3. Zarządza ryzykiem w obszarze bezpieczeństwa fizycznego.
4. Rejestruje i obsługuje incydenty związane z naruszeniem ochrony fizycznej.

2.2.2 Bezpieczeństwo cyberprzestrzeni w Ministerstwie Sprawiedliwości

Obszar znajduje się we właściwości Dyrektora Biura Cyberbezpieczeństwa, który:

1. Jest właścicielem polityki w obszarze cyberbezpieczeństwa resortu sprawiedliwości.
2. Opiniuje polityki bezpieczeństwa systemów teleinformatycznych.
3. Koordynuje funkcjonowanie systemu zarządzania bezpieczeństwem cyberprzestrzeni w Ministerstwie Sprawiedliwości.
4. Zarządza ryzykiem w obszarze cyberprzestrzeni w Ministerstwie Sprawiedliwości.
5. Rejestruje i obsługuje incydenty związane z bezpieczeństwem informacji w cyberprzestrzeni Ministerstwa Sprawiedliwości.
6. Współpracuje m.in. z Zespołem Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV prowadzonym przez Szefa Agencji Bezpieczeństwa Wewnętrznego w zakresie ochrony cyberprzestrzeni Rzeczypospolitej Polskiej.

2.2.3 Ochrona danych osobowych

Obszar znajduje się we właściwości Inspektora Ochrony Danych, który:

1. Opiniuje polityki bezpieczeństwa systemów teleinformatycznych oraz wymagania bezpieczeństwa dla systemów przetwarzających dane osobowe.
2. Opiniuje umowy powierzenia przetwarzania danych osobowych.
3. Zarządza ryzykiem w obszarze bezpieczeństwa danych osobowych.
4. Rejestruje i obsługuje incydenty związane z bezpieczeństwem danych osobowych.

2.2.4 Bezpieczeństwo systemów teleinformatycznych

Obszar (z wyłączeniem systemów pozostających we właściwości poszczególnych dyrektorów) znajduje się we właściwości Dyrektora Departamentu Informatyzacji i Rejestrów Sądowych, który:

1. Jest właścicielem polityki w obszarze bezpieczeństwa systemów teleinformatycznych Ministerstwa Sprawiedliwości.
2. Jest właścicielem regulaminu użytkownika systemów teleinformatycznych Ministerstwa Sprawiedliwości, zawierającego w szczególności zasady korzystania z mobilnego sprzętu komputerowego Ministerstwa Sprawiedliwości.
3. Opiniuje polityki bezpieczeństwa systemów teleinformatycznych Ministerstwa Sprawiedliwości.
4. Odpowiada za poufność, integralność i dostępność informacji przetwarzanych w podległych systemach teleinformatycznych.
5. Odpowiada za techniczne aspekty zabezpieczeń dla zapewnienia ciągłości działania nadzorowanych systemów teleinformatycznych Ministerstwa Sprawiedliwości.
6. Zarządza ryzykiem w obszarze bezpieczeństwa podległych systemów teleinformatycznych oraz infrastruktury teleinformatycznej.
7. Rejestruje i obsługuje incydenty związane z bezpieczeństwem systemów teleinformatycznych.

2.2.5 Bezpieczeństwo dostaw i wyposażenia

Obszar znajduje się we właściwości Dyrektora Biura Administracyjnego (z wyłączeniem obszarów będących w kompetencjach innych komórek organizacyjnych), który:

1. Jest właścicielem procedury w obszarze bezpieczeństwa dostaw i wyposażenia.
2. Jest właścicielem regulaminu dotyczącego korzystania z telefonów służbowych w Ministerstwie Sprawiedliwości.
3. Jest właścicielem rejestru zasobów w zakresie biur i ich wyposażenia, a także podstawowych usług technicznych.

4. Jest odpowiedzialny za treść i nadzór nad umowami z dostawcami w zakresie wyposażenia biur oraz podstawowych usług technicznych, do których zapewnienia jest zobowiązany.
5. Zarządza ryzykiem w obszarze bezpieczeństwa dostaw i wyposażenia.

2.2.6 Bezpieczeństwo zasobów ludzkich

Obszar znajduje się we właściwości Dyrektorów Biura Dyrektora Generalnego oraz Dyrektora Departamentu Kadr i Organizacji Sądów Powszechnych i Wojskowych, którzy:

1. Są właścicielami polityk w obszarze bezpieczeństwa zasobów ludzkich w zakresie swojej właściwości.
2. Zarządzają ryzykiem w obszarze bezpieczeństwa zasobów ludzkich w zakresie swojej właściwości.
3. Rejestrują i obsługują incydenty związane z personelem w zakresie swojej właściwości.

2.2.7 Bezpieczeństwo Krajowego Rejestru Karnego

Obszar znajduje się we właściwości Dyrektora Biura Informacyjnego Krajowego Rejestru Karnego, który:

1. Jest właścicielem polityki w obszarze bezpieczeństwa Krajowego Rejestru Karnego.
2. Jest właścicielem polityki w obszarze bezpieczeństwa Rejestru Sprawców Przestępstw na Tle Seksualnym.
3. Zarządza ryzykiem w obszarze bezpieczeństwa informacji Biura Informacyjnego Krajowego Rejestru Karnego.
4. Zapewnia zabezpieczenia organizacyjne dostępu do informacji w systemie oraz ciągłość działania Biura Informacyjnego Krajowego Rejestru Karnego w zakresie swoich kompetencji.

3. KLASYFIKACJA INFORMACJI

Wszelkie informacje tworzone, przekazywane i przetwarzane w Ministerstwie Sprawiedliwości nieoznaczone, jako należące do osób trzecich, stanowią własność Ministerstwa Sprawiedliwości i podlegają ochronie.

Wszystkie aktywa informacyjne powstające w Ministerstwie Sprawiedliwości oraz do niego dostarczane muszą mieć swojego właściciela.

Rejestr zasobów informacyjnych tworzony przy wsparciu właścicieli obszaru jest utrzymywany przez Pełnomocnika. W Ministerstwie Sprawiedliwości wprowadza się następującą klasyfikację informacji:

1. **Klasyfikacja oparta na poufności:**
   a) Informacje publiczne: Informacje dostępne publicznie, które nie wymagają zabezpieczeń. W odniesieniu do informacji publicznych należy zachować ich integralność i dostępność,
   b) Informacje wewnętrzne: Informacje przeznaczone dla wewnętrznego użytku organizacji, które mogą być udostępniane właściwym pracownikom, podmiotom itp.,
   c) Informacje poufne: Informacje o wrażliwym charakterze, udostępniane konkretnym pracownikom, podmiotom, wymagające szczególnych zabezpieczeń.

W odniesieniu do informacji niepodlegających udostepnieniu, należy zachować ich integralność, dostępność oraz poufność.

2. **Klasyfikacja oparta na znaczeniu:**
   a) Informacje standardowe: Informacje, które mają znaczenie dla działalności organizacji, ale których utrata lub naruszenie nie niesie za sobą poważnych konsekwencji,

b) Informacje ważne: Informacje istotne dla organizacji, których utrata lub naruszenie może mieć negatywne skutki i konsekwencje,
c) Informacje krytyczne: Informacje kluczowe dla działalności organizacji, których utrata lub naruszenie może mieć poważne konsekwencje operacyjne, finansowe lub reputacyjne.

Wprowadzenie klasyfikacji informacji nie powoduje konieczności oznaczania dokumentów w żaden szczególny sposób, nakłada natomiast na dyrektorów komórek organizacyjnych Ministerstwa Sprawiedliwości obowiązek budowania świadomości podległych sobie pracowników w odniesieniu do zakresu ochrony poszczególnych rodzajów informacji.

Klasyfikacja ta ma za zadanie wspomóc w stosowaniu odpowiednich zabezpieczeń i mechanizmów kontrolnych, w celu prawidłowej ochrony informacji o właściwym poziomie poufności i znaczeniu.

4. ZARZĄDZANIE DOKUMENTACJĄ SYSTEMU ZARZĄDZANIA BEZPIEŃSTWEM INFORMACJI

Dokumentacja SZBI ma strukturę hierarchiczną. Nadrzędnym dokumentem jest niniejsza PBI Ministerstwa Sprawiedliwości.

Kolejny poziom dokumentacji SZBI stanowią Polityki określające zasady zarządzania bezpieczeństwem informacji w poszczególnych obszarach. W celu uszczegółowienia zasad opisanych w politykach, dozwolone jest tworzenie dokumentów niższego rzędu takich jak: procedury, instrukcje oraz inne regulacje wewnętrze Ministerstwa Sprawiedliwości dotyczące bezpieczeństwa informacji oraz z zakresu dokumentacji poszczególnych systemów IT.

Za opracowanie i wdrożenie dokumentów w wymienionych obszarach odpowiedzialni są wskazani w rozdziale 2 właściciele obszarowi.

Dokumenty opracowywane są przez właścicieli, zgodnie z Procedurą nadzoru nad dokumentacją Systemu Zarządzania Bezpieczeństwem Informacji. Do końca lutego każdego roku właściciel odpowiedzialny za dany dokument przeprowadza jego przegląd, w celu potwierdzenia jego aktualności.

5. ORGANIZACJA I NADZÓR SYSTEMU ZARZĄDZANIA BEZPIEŃSTWEM INFORMACJI

Wdrożony SZBI podlega ciągłemu doskonaleniu. Zakres SZBI obejmuje wszystkie kluczowe obszary działalności Ministerstwa Sprawiedliwości, bazując na trzech zasadach:

1. Zapewnienia, że informacja jest udostępniana jedynie osobom upoważnionym (zasada poufności informacji).
2. Zapewnienia dokładności i kompletności informacji oraz metod jej przetwarzania (zasada integralności informacji).
3. Zapewnienia, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów zawsze wtedy, gdy istnieje taka potrzeba (zasada dostępności informacji).

Pełnomocnik odpowiada za zaproponowanie struktury organizacyjnej SZBI zapewniającej optymalny podział i koordynację zadań oraz odpowiedzialności związanych z zapewnieniem bezpieczeństwa informacji w Ministerstwie Sprawiedliwości.

Pełnomocnik uprawniony jest do:

1. Rozstrzygania sporów dotyczących stosowania wymagań zawartych w dokumentacji SZBI w Ministerstwie Sprawiedliwości oraz wydawania wiążących decyzji w tym zakresie.
2. Dostępu do dokumentów występujących w Ministerstwie Sprawiedliwości, których treść i sposób przechowywania mogą być istotne z punktu widzenia funkcjonowania SZBI w Ministerstwie Sprawiedliwości.

3. Uzyskania informacji i wyjaśnień od pracowników w zakresie realizowanych działań w ramach SZBI w Ministerstwie Sprawiedliwości.
4. Podejmowania decyzji w kwestiach bezpieczeństwa informacji w Ministerstwie Sprawiedliwości .

Zarządzanie bezpieczeństwem informacji w Ministerstwie Sprawiedliwości opiera się na następujących podstawowych procesach:

1. Zarządzanie ryzykiem.
2. Monitorowanie i doskonalenie.
3. Audyt KRI.
4. Zarządzanie zasobami.
5. Zarządzanie incydentami.

5.1 Zarządzanie ryzykiem

Strategicznym elementem zarządzania aktywami związanymi z przetwarzaniem informacji i bezpieczeństwem informacji w Ministerstwie Sprawiedliwości jest przeprowadzanie okresowej analizy ryzyka i opracowanie planu postępowania z ryzykiem. Analiza ryzyka stanowi podstawę podejmowania wszelkich działań w zakresie utrzymania i doskonalenia SZBI. Szczegółowe zasady zarządzania ryzykiem w bezpieczeństwie informacji zostały uregulowane w Procedurze zarządzania ryzykiem bezpieczeństwa informacji Ministerstwa Sprawiedliwości.

5.2 Monitorowanie i doskonalenie

5.2.1 System Zarządzania Bezpieczeństwem Informacji

Skuteczność SZBI jest poddawana stałemu monitorowaniu. Nadzór nad procesem monitorowania sprawuje Pełnomocnik.

Monitorowanie SZBI odbywa się na podstawie analizy wyników przeprowadzonych audytów i kontroli, analizy incydentów w obszarze bezpieczeństwa informacji, cyklicznej oceny przeprowadzanej analizy ryzyka, zmian wynikających z przepisów prawa, a także innych zdarzeń mających wpływ na bezpieczeństwo informacji.

Pełnomocnik może zainicjować działania związane z aktualizacją regulacji wewnętrznych w zakresie zmieniającego się otoczenia, będące konsekwencją wyników monitorowania ryzyka, wniosków z przeglądów SZBI, wniosków z analizy incydentów naruszenia bezpieczeństwa informacji w poszczególnych obszarach.

5.2.2 Przeglądy i testy systemów

Poza stałym monitorowaniem stanu bezpieczeństwa informacji, kierownicy komórek organizacyjnych, do których należą systemy teleinformatyczne, posiadają uprawnienia do przeprowadzania doraźnych przeglądów i testów systemów.

Z uwagi na realizowane zadania, takie uprawnienia w szczególności posiadają:

1. Dyrektor Departamentu Informatyzacji i Rejestrów Sądowych – w zakresie wszystkich systemów teleinformatycznych Ministerstwa Sprawiedliwości.
2. Dyrektor Biura Cyberbezpieczeństwa – w zakresie cyberprzestrzeni Ministerstwa Sprawiedliwości.

Mając na uwadze pokrywanie się obszaru cyberprzestrzeni w Ministerstwie Sprawiedliwości z poszczególnymi jego systemami, realizacja testów, a zwłaszcza testów penetracyjnych musi być

uzgadniana pomiędzy ww. Dyrektorami. W przypadku braku porozumienia, ostateczną decyzję podejmuje Pełnomocnik.

5.3 Audyt Krajowych Ram Interoperacyjności

Audyt KRI realizowany jest zgodnie z rozporządzeniem Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

Pełnomocnik koordynuje działania związane z wykonaniem corocznego audytu KRI, w szczególności poprzez wyznaczanie komórek organizacyjnych Ministerstwa Sprawiedliwości do przeprowadzenia audytu, a także nadzoruje realizację zaleceń poaudytowych, korygująco-naprawczych i doskonalących oraz dokumentuje realizację zaleceń poaudytowych.

Audyt KRI może być wykonany przez komórkę organizacyjną Samodzielne Stanowisko do spraw Audytu Wewnętrznego.

5.4 Zarządzanie zasobami

5.4.1 Klasyfikacja zasobów w Ministerstwie Sprawiedliwości

Ministerstwo Sprawiedliwości zarządza swoimi aktywami w celu zapewnienia im wymaganego poziomu bezpieczeństwa.

Do chronionych aktywów zalicza się:

1. Informacje – dane osobowe i inne informacje prawnie chronione, bazy danych i pliki z danymi, polityki, regulaminy, instrukcje, umowy z dostawcami, dokumentacje systemów, plany ciągłości działania, plany odzyskiwania po awarii, logi systemowe i aplikacyjne, materiały szkoleniowe oraz informacje przechowywane w kopiach zapasowych.
2. Oprogramowanie – aplikacje, systemy operacyjne, narzędzia rozwojowe i inne.
3. Aktywa fizyczne – biura i ich wyposażenie, sprzęt teleinformatyczny, w tym okablowanie i nośniki danych.
4. Usługi – usługi przetwarzania informacji oraz podstawowe usługi techniczne.
5. Ludzi – kapitał wiedzy, jaki reprezentują oraz czas ich pracy.
6. Wartości niematerialne – dobre imię jednostki organizacyjnej, reputacja.

Aktywa chronione są ze względu na przepisy prawa oraz wartość materialną i intelektualną. Aktywa mogą być chronione na mocy:

1. Przepisów prawa (np. dane osobowe, informacje niejawne, prawo autorskie, tajemnica pracodawcy).
2. Warunków licencji.
3. Zapisów umów pomiędzy jednostką organizacyjną, a firmami zewnętrznymi.

Zarządzanie zasobami Ministerstwa Sprawiedliwości realizowane jest w poszczególnych obszarach, w zależności od kompetencji komórek organizacyjnych.

5.4.2 Wynoszenie zasobów poza siedzibę i ich bezpieczeństwo

Sprzęt, informacje lub oprogramowanie nie powinny być wynoszone poza siedzibę Ministerstwa Sprawiedliwości bez uprzedniego zezwolenia. Należy wskazać pracowników, osoby oddelegowane, inne osoby uprawnione oraz osoby realizujące zadania na zasadach umów cywilnoprawnych lub o dzieło, którzy mają prawo do wynoszenia aktywów i jeśli będzie taka potrzeba, rejestrować, kiedy są one wynoszone i kiedy są zwracane. Aktywów nie wolno w żadnym wypadku pozostawiać w miejscach publicznych bez nadzoru, a użytkownik zobowiązany jest zapewnić im adekwatną ochronę.

Zezwolenia na wynoszenie aktywów poza siedzibę wydają właściciele zasobów.

5.5 Zarządzanie incydentami

Incydenty muszą być bezzwłocznie zgłaszane do wyznaczonego punktu kontaktowego.

5.5.1 Zgłaszanie incydentów naruszenia bezpieczeństwa informacji

1. Każdy zauważony incydent jest zgłaszany, rejestrowany oraz obsłużony.
2. Incydenty są zgłaszane do punktu kontaktowego poprzez:
   a. pocztę elektroniczną na adres wyznaczony przez właściciela obszaru odpowiedzialnego za obsługę incydentów będących w jego właściwości,
   b. osobiste zgłoszenie do właściciela obszaru odpowiedzialnego za obsługę incydentów będących w jego właściwości.

5.5.2 Obsługa zgłoszonego incydentu

1. W przypadku wystąpienia klęski żywiołowej lub aktu terroru w pierwszej kolejności powiadamiane są właściwe służby, a następnie ochrona budynku oraz Dyrektor Biura Bezpieczeństwa.
2. W przypadku wystąpienia próby włamania, kradzieży dokumentów, sprzętu oraz wszelkich innych prób niszczenia mienia powiadamiana jest ochrona budynku jak również bezpośredni przełożony lub osoba go zastępująca.
3. Incydenty związane z bezpieczeństwem informacji obsługiwane są przez właścicieli obszarów zgodnie z Procedurą zarządzania incydentami bezpieczeństwa informacji.

Pełnomocnik jest informowany przez Właścicieli obszarów odpowiedzialnych za obsługę incydentów o wszystkich incydentach bezpieczeństwa zbiorczo, w formie raportów sporządzonych za każde półrocze, w terminie do 31 dnia miesiąca występującego po zakończeniu danego półrocza lub na żądanie Pełnomocnika – w innym terminie.

6. BEZPIECZEŃSTWO FIZYCZNE I ŚRODOWISKOWE

Ministerstwo Sprawiedliwości dba o zapewnienie wysokiego poziomu bezpieczeństwa fizycznego i środowiskowego, poprzez ochronę infrastruktury technicznej oraz środowiska pracy. Są one nieodłącznymi elementami dla zapewnienia ciągłości działania systemów informatycznych, ochrony danych, a także uniknięcia potencjalnych zagrożeń i incydentów, które mogą wyniknąć z braku odpowiednich zabezpieczeń w tych obszarach. Celem tych obszarów jest zapewnienie bezpieczeństwa informacji poprzez eliminację dostępu osób niepowołanych, możliwości uszkodzenia aktywów służących do przetwarzania informacji lub innych zakłóceń mogących powstać w siedzibie Ministerstwa Sprawiedliwości.

Skuteczna realizacja postawionego celu możliwa jest dzięki wyznaczeniu stref bezpieczeństwa oraz zdefiniowaniu i egzekwowaniu stosownych zasad dostępu i pracy w każdej z nich.

Kluczowe systemy techniczne i teleinformatyczne wyposażone są w systemy utrzymujące optymalne warunki fizyczne, środowiskowe i podtrzymujące zasilanie.

Szczegóły zarządzania bezpieczeństwem fizycznym i środowiskowym określone zostały w Polityce bezpieczeństwa fizycznego, Polityce bezpieczeństwa danych osobowych Ministerstwa Sprawiedliwości, Polityce bezpieczeństwa systemów teleinformatycznych Ministerstwa Sprawiedliwości.

7. BEZPIECZNA EKSPLOATACJA

Ministerstwo Sprawiedliwości dba o przestrzeganie zasad bezpieczeństwa związanych z utrzymywaniem i użytkowaniem systemów teleinformatycznych. Celem jest zapewnienie poufności, integralności i dostępności informacji z uwzględnieniem takich atrybutów jak: autentyczność, rozliczalność, niezaprzeczalność i niezawodność, a także poprawne i bezpieczne eksploatowanie systemów przetwarzających te informacje.

Kluczowymi aspektami bezpiecznej eksploatacji systemów teleinformatycznych, dzięki którym możliwa jest skuteczna realizacja postawionego celu to:

1. Spełnienie minimalnych wymagań bezpieczeństwa eksploatacji systemów teleinformatycznych oraz ich zgodność z obowiązującymi standardami.
2. Wdrożenie zabezpieczeń chroniących przed złośliwym oprogramowaniem lub kodem.
3. Zapewnienie bezpieczeństwa systemów produkcyjnych poprzez prowadzenie prac rozwojowych i testowych na oddzielnych urządzeniach lub środowiskach.
4. Systematyczne tworzenie, przechowywanie i testowanie kopii bezpieczeństwa.
5. Zapewnienie odporności oraz ciągłości działania systemów teleinformatycznych Ministerstwa Sprawiedliwości.
6. Wykrywanie incydentów w systemach teleinformatycznych i wdrażanie odpowiednich mechanizmów reagowania w przypadkach ich wystąpienia.
7. Obowiązywanie mechanizmów uwierzytelniania, autoryzacji i kontroli dostępu do systemów teleinformatycznych.
8. Bieżące monitorowanie aktywów informacyjnych i informatycznych.
9. Bieżące kontrolowanie wprowadzania zmian do infrastruktury technicznej.
10. Nadzorowanie usług dostarczanych przez strony trzecie, a w szczególności wprowadzanie do nich zmian.

Szczegółowe zasady zarządzania tymi systemami określi Polityka bezpieczeństwa systemów teleinformatycznych Ministerstwa Sprawiedliwości.

8. BEZPIECZEŃSTWO KOMUNIKACJI

Ministerstwo Sprawiedliwości dba o przestrzeganie zasad bezpieczeństwa związanych z komunikacją. Celem jest zapewnienie poufności, integralności i dostępności transmitowanej informacji. Kluczowymi aspektami bezpiecznej komunikacji, dzięki którym możliwa jest skuteczna realizacja postawionego celu to:

1. Przestrzeganie zasad zarządzania bezpieczeństwem usług sieciowych.
2. Przestrzeganie zasad korzystania z urządzeń i narzędzi komunikacyjnych.
3. Systematyczna realizacja testów penetracyjnych.
4. Obowiązywanie zasady konserwacji i redundancji urządzeń sieciowych w celu zapobieżenia przerwom w łączności.
5. Kontrolowanie wprowadzania zmian do infrastruktury sieciowej.
6. Wdrożenie zabezpieczeń chroniących przed próbami włamań z sieci publicznej.
7. Monitorowanie poziomu bezpieczeństwa informacji oraz posiadanie mechanizmów reagowania w przypadku wystąpienia incydentu.

Szczegółowe zasady dotyczące bezpieczeństwa komunikacji określone zostały w obszarowych politykach.

9. POZYSKIWANIE, ROZWÓJ I UTRZYMANIE SYSTEMÓW IT

Ministerstwo Sprawiedliwości zapewnia, że wszelkie procesy związane z pozyskaniem, rozwojem i utrzymaniem systemów informacyjnych, w tym systemów i aplikacji teleinformatycznych, wprowadzanych we własnym zakresie lub przy wsparciu podwykonawców, realizowane są w sposób gwarantujący utrzymanie odpowiedniego poziomu bezpieczeństwa.

Pozyskiwanie, rozwój i utrzymanie systemów IT obejmuje:

1. Uwzględnienie wymogów bezpieczeństwa podczas zakupu lub budowy nowych systemów teleinformatycznych.
2. Dopuszczenie systemu do eksploatacji realizowane jest po fazie testów funkcjonalnych, wydajnościowych i bezpieczeństwa – na środowisku testowym.
3. Zapewnianie regularnego skanowania systemów w celu identyfikacji potencjalnych podatności i ich bezzwłocznej naprawy.
4. Nadzorowanie dostępu do kodów źródłowych oprogramowania.
5. Wdrożenie procedur kontroli zmian oprogramowania.

Za zapewnienie właściwego przebiegu procesu pozyskiwania, rozwoju i utrzymywania systemów IT odpowiedzialny jest Dyrektor Departamentu Informatyzacji i Rejestrów Sądowych oraz kierownik komórki organizacyjnej sprawujący nadzór nad systemem IT. Szczegółowe zasady bezpieczeństwa systemów IT opisane zostaną w Polityce bezpieczeństwa systemów teleinformatycznych Ministerstwa Sprawiedliwości.

10. RELACJE Z DOSTAWCAMI

Z uwagi na realizowane zadania, kompetencje w obszarze kontaktów z dostawcami leżą w gestii właściciela obszaru.

Precyzując zasady kontaktów z dostawcami w ramach poszczególnych rodzajów dostaw, powinny zostać uwzględnione w miarę możliwości następujące aspekty:

1. Umowy o zachowaniu poufności.
2. Zasady uświadamiania i szkolenia pracowników dostawców oraz podpisywanie stosownych oświadczeń i upoważnień (dane osobowe).
3. Procedury przesyłania informacji, w tym przekazywania informacji innym podmiotom.
4. Umowy powierzenia przetwarzania danych osobowych.
5. Wymagania bezpieczeństwa informacji, w tym dotyczące klasyfikacji informacji.
6. Zarządzanie usługami i zmianami w usługach, w tym:
    a) precyzyjne zdefiniowanie zakresu usługi,
    b) zakres odpowiedzialności poszczególnych stron umowy,
    c) wykaz poddostawców,
    d) wymagania i uprawnienia dotyczące monitorowania realizacji usług,
    e) parametry zapewnienia jakości usług, takie jak zgodność z przepisami, czas reakcji, wydajność, monitoring i raportowanie czy czas naprawy,
    f) umowy powinny zapewniać atrybuty bezpieczeństwa, w których:
        – określa się czas reakcji na nieprawidłowość,
        – określa się czas przywrócenia pierwotnego stanu,
    g) zarządzanie ryzykiem związanym ze zgłoszoną zmianą.
7. Wykaz zawartych umów z dostawcami wraz z ich statusem.
8. Tryb zakończenia realizacji umowy, z uwzględnieniem zwrócenia powierzonych wzajemnie aktywów.

Zaleca się korzystanie ze wspólnych wzorów umów, zawierających między innymi zapisy dotyczące zachowania poufności lub powierzenia przetwarzania danych osobowych, dla ułatwienia procesu ich zawierania.

11. ZARZĄDZANIE CIĄGŁOŚCIĄ DZIAŁANIA

Ministerstwo Sprawiedliwości dba o zapewnienie ciągłości funkcjonowania usług związanych z przetwarzaniem informacji i ciągłości działania urzędu jako całości. Dla poszczególnych obszarów i systemów krytycznych tworzone są plany postępowania w sytuacjach awaryjnych i kryzysowych. Ich celem jest przeciwdziałanie przerwom w działalności Ministerstwa Sprawiedliwości, ochrona krytycznych procesów przed rozległymi awariami lub katastrofami oraz zapewnienie w niekorzystnej sytuacji wymaganego poziomu bezpieczeństwa informacji.

O konieczności tworzenia planu ciągłości działania dla konkretnego systemu decyduje jego właściciel na podstawie przeprowadzonej analizy ryzyka. Jest on odpowiedzialny również za ciągłe monitorowanie zagrożeń i ryzyk, cykliczne testowanie systemu oraz aktualizację planu ciągłości działania.

12. PRZEGLĄDY ZARZĄDZANIA SYSTEMU ZARZĄDZANIA BEZPIEŃSTWEM INFORMACJI

Przegląd Zarządzania musi się odbyć przynajmniej raz w roku. Do końca marca właściciele obszarów składają Pełnomocnikowi pisemny raport, w którym informują o realizacji zadań za rok poprzedni, zgodnie z zakresem właściwości.

Pełnomocnik sporządza raport o funkcjonowaniu SZBI, w którym uwzględnia otrzymane informacje oraz uzupełnia je o informacje dotyczące przeprowadzonych audytów, incydentów, które wystąpiły i reakcji na nie, wyników analiz ryzyka, a także wdrożonych nowych politykach i procedurach.

Raport o funkcjonowaniu SZBI Pełnomocnik przedstawia Ministrowi Sprawiedliwości lub upoważnionemu przez niego Członkowi Kierownictwa Ministerstwa Sprawiedliwości/Dyrektorowi Generalnemu odpowiedzialnemu za bezpieczeństwo informacji. W przypadku stwierdzonych niezgodności Pełnomocnik występuje do właścicieli obszarów z propozycjami podjęcia działań korygujących. Raport Pełnomocnika obejmuje okres od 1 stycznia do 31 grudnia ubiegłego roku. Pełnomocnik może w raporcie uwzględnić informacje z okresu bieżącego, jeśli uważa je za istotne.

13. PRAWA WŁASNOŚCI INTELEKTUALNEJ

Ministerstwo Sprawiedliwości dba o ochronę wszelkich materiałów, które mogą być uznane za własność intelektualną i stosuje poniższe zabezpieczenia:

1. Oprogramowanie pozyskiwane jest jedynie ze źródeł zapewniających, że prawa autorskie nie są naruszane.
2. Kierownictwo Ministerstwa Sprawiedliwości podnosi świadomość w zakresie ochrony własności intelektualnej, gdyż jej naruszenie może prowadzić do działań prawnych, w tym mandatów i postępowań karnych.
3. Przechowywane są dowody własności licencji, oryginalne dyski, podręczniki itp.
4. Instalowane są wyłącznie autoryzowane oprogramowania i licencjonowane produkty.

14. ODSTĘPSTWA OD REGUŁ OCHRONY

Odstępstwo należy rozumieć jako czasowe odstąpienie od ustanowionych i wdrożonych PBI Ministerstwa Sprawiedliwości zasad bezpieczeństwa informacji, które możliwie w najkrótszym terminie powinno być wycofane. Nadzorowanie odstępstw służy zapewnieniu bezpieczeństwa

informacji poprzez formalne uregulowanie czasowych odstąpień od realizacji zdefiniowanych w PBI zasad bezpieczeństwa informacji.

Każde odstępstwo podlega ścisłemu nadzorowi, udokumentowaniu, uprzedniemu szacowaniu ryzyka, jak również późniejszej ocenie skutków jego dopuszczenia.

Dopuszcza się incydentalne odstąpienia od przyjętej PBI Ministerstwa Sprawiedliwości, aby móc postąpić inaczej niż określono w dokumencie, należy:

1. Ustalić osobistą odpowiedzialność osoby niestosującej się do przyjętych zasad bezpieczeństwa.
2. Uzasadnić pisemnie powód odstąpienia od przyjętych zasad bezpieczeństwa.
3. Oszacować ryzyko zastosowania odstąpienia od przewidywanych reguł bezpieczeństwa.
4. Odstępując od przyjętych zasad, starać się zachować możliwie jak najwięcej z obowiązujących przepisów PBI Ministerstwa Sprawiedliwości, przy jednoczesnym zapewnieniu postępowania zgodnie z wymogami obowiązującego prawa.

Zabrania się stosowania precedensu w celu zmiany przyjętych reguł. O odstąpieniu od przewidzianych reguł bezpieczeństwa decydować mogą Minister Sprawiedliwości lub upoważniony przez niego Członek Kierownictwa Ministerstwa Sprawiedliwości/Dyrektor Generalny lub Pełnomocnik.

Dyrektor komórki organizacyjnej, który uzyskał zgodę Ministra Sprawiedliwości lub upoważnionego przez niego Członka Kierownictwa Ministerstwa Sprawiedliwości/Dyrektora Generalnego w sprawie odstąpienia od przyjętej PBI Ministerstwa Sprawiedliwości, zobligowany jest do bezzwłocznego powiadomienia Pełnomocnika o udzielonej zgodzie i zakresie uzyskanego odstępstwa.

Pełnomocnik nadzoruje proces zarządzania odstępstwami, m.in. weryfikuje kompletność wymaganej dokumentacji, przedstawia rekomendacje dotyczące zgłoszonych odstępstw i ocenia skutki ich zastosowania.

Sposób postępowania z odstępstwami w poszczególnych systemach teleinformatycznych jest doprecyzowany w dokumentacji tych systemów.

15. SANKCJE ZA NARUSZENIE ZASAD BEZPIECZEŃSTWA INFORMACJI

Nieprzestrzeganie zasad zawartych w dokumentach polityk bezpieczeństwa jest naruszeniem obowiązków pracowniczych wynikających w szczególności: ustawy z dnia 21 listopada 2008 r. o służbie cywilnej, ustawy z dnia 26 czerwca 1974 – Kodeks pracy, rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW, która do polskiego systemu prawnego została implementowana ustawą z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, może pociągnąć za sobą skutki dyscyplinarne i spowodować pociągnięcie do odpowiedzialności wynikającej z przepisów prawa i regulaminu pracy w Ministerstwie Sprawiedliwości.