DZIENNIK URZĘDOWY
MINISTRA SPRAWIEDLIWOŚCI

Warszawa, dnia 1 kwietnia 2019 r.

Poz. 118

ZARZĄDZENIE MINISTRA SPRAWIEDLIWOŚCI

z dnia 27 marca 2019 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 2012 r. poz. 392, z 2015 r. poz. 1064 oraz z 2018 r. poz. 1669) zarządza się, co następuje:

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

§ 2. Traci moc zarządzenie Ministra Sprawiedliwości z dnia 27 czerwca 2012 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji Ministerstwa Sprawiedliwości i sądów powszechnych (Dz. Urz. Min. Sprawiedl. poz.93).

§ 3. Zarządzenie wchodzi w życie z dniem następującym po dniu ogłoszenia.

MINISTER SPRAWIEDLIWOŚCI

Zbigniew Ziobro

MINISTERSTWO SPRAWIEDLIWOŚCI
www.ms.gov.pl

Polityka Bezpieczeństwa Informacji Ministerstwa Sprawiedliwości

Spis treści

1. Wstęp

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

Niniejszy dokument Polityka Bezpieczeństwa Informacji Ministerstwa Sprawiedliwości, zwana dalej „PBI"- określa ramy Systemu Zarządzania Bezpieczeństwem Informacji, zwanego dalej „SZBI" w Ministerstwie Sprawiedliwości.

PBI jest aktem wewnętrznego stosowania. Dokument jest zgodny z aktami prawnymi oraz polskimi normami, o których mowa w rozdziale 18.

PBI opisuje ogólne zasady ochrony informacji obowiązujące w Ministerstwie Sprawiedliwości, zasady zarządzania ryzykiem, role i zadania osób uczestniczących w procesie przetwarzania informacji oraz zarządzania bezpieczeństwem informacji. PBI Ministerstwa Sprawiedliwości określa również warunki, jakie muszą spełniać systemy teleinformatyczne przetwarzające informacje w Ministerstwie Sprawiedliwości. Szczegóły zostaną opisane w dokumentach obszarowych.

Z dokumentem PBI powinny zapoznać się wszystkie osoby mające dostęp do informacji – pracownicy Ministerstwa Sprawiedliwości, osoby delegowane, kadra kierownicza oraz pracownicy firm zewnętrznych realizujący prace na rzecz Ministerstwa Sprawiedliwości. 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.

PBI jest publikowana w Intranecie Ministerstwa Sprawiedliwości.

2. Cel i zakres obowiązywania PBI Ministerstwa Sprawiedliwości

Celem PBI jest:

1. Określenie zasad właściwej ochrony aktywów Ministerstwa Sprawiedliwości.
2. Ustanowienie SZBI w Ministerstwie Sprawiedliwości.

Niniejszy dokument dotyczy wszystkich komórek organizacyjnych Ministerstwa Sprawiedliwości oraz wszystkich jego pracowników w rozumieniu w szczególności ustawy o służbie cywilnej oraz przepisów Kodeksu pracy, a także innych osób mających dostęp do informacji chronionych (np. pracowników firm zewnętrznych realizujących prace na rzecz Ministerstwa Sprawiedliwości lub zleceniobiorców).

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 oraz osoby wykonujące pracę na innej podstawie niż stosunek pracy. W przypadku ich utraty fakt ten pracownik zobowiązany jest niezwłocznie zgłosić bezpośredniemu przełożonemu.

3. Deklaracja Kierownictwa Ministerstwa Sprawiedliwości

Ministerstwo Sprawiedliwości przywiązuje dużą wagę do ochrony informacji tworzonych, przetwarzanych i przechowywanych w urzędzie. Szczególną wagę przywiązuje się do ochrony informacji prawnie chronionych. Zabezpieczenia funkcjonujące w Ministerstwie Sprawiedliwości mają na celu zapewnienie poufności, integralności i dostępności informacji oraz ciągłości działania Ministerstwa Sprawiedliwości.

Kierownictwo Ministerstwa Sprawiedliwości nadaje wysoką rangę bezpieczeństwu osób, mienia oraz informacji. Informacje są jednym z kluczowych zasobów Ministerstwa Sprawiedliwości i jako takie wymagają odpowiedniej ochrony.

Kierownictwo Ministerstwa Sprawiedliwości jest w pełni zaangażowane i wspiera procesy zmierzające do zapewnienia bezpieczeństwa informacji.

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

Kierownictwo Ministerstwa Sprawiedliwości wprowadzając PBI, deklaruje, że wdrożony SZBI, którego elementem jest niniejsza polityka, będzie podlegał ciągłemu doskonaleniu. Zakres SZBI obejmuje wszystkie kluczowe obszary działalności Ministerstwa Sprawiedliwości.

Bezpieczeństwo informacji w Ministerstwie Sprawiedliwości bazuje na trzech kluczowych 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).

Wdrożenie SZBI uwzględniając poziom organizacyjny i techniczny zapewni prawidłową realizację zadań Ministerstwa Sprawiedliwości, w szczególności:

1. Będzie gwarantem właściwej ochrony informacji oraz ciągłości procesu ich przetwarzania.
2. Zapewni zachowanie odpowiedniego poziomu poufności, integralności i dostępności poszczególnych klas informacji, bez względu na ich postać i nośnik.
3. Ograniczy podatności na zagrożenia dla bezpieczeństwa informacji, które wynikają z celowej bądź przypadkowej działalności człowieka oraz zminimalizuje ich ewentualny negatywny wpływ na Ministerstwo Sprawiedliwości.
4. Zapewni poprawne i bezpieczne funkcjonowanie wszystkich systemów teleinformatycznych przetwarzających informacje.
5. Zapewni gotowość do podjęcia działań w sytuacjach kryzysowych dla bezpieczeństwa Ministerstwa Sprawiedliwości, jego interesów oraz posiadanych i powierzonych Ministerstwu Sprawiedliwości informacji.

Powyższe cele realizowane są poprzez:

1. Ustalenie struktury organizacyjnej SZBI zapewniającej optymalny podział i koordynację zadań oraz odpowiedzialności związanych z zapewnieniem bezpieczeństwa informacji.
2. Wyznaczenie Właścicieli dla kluczowych aktywów przetwarzających informacje, którzy zobowiązani są do zapewnienia im możliwie jak najwyższego poziomu bezpieczeństwa.
3. Zobowiązanie do stosowania przez wszystkie osoby zatrudnione i wykonujące prace na innej podstawie niż stosunek pracy polityk i procedur, instrukcji oraz innych regulacji wewnętrznych Ministerstwa Sprawiedliwości dotyczących bezpieczeństwa informacji.
4. Wdrożenie i utrzymanie niezbędnych zabezpieczeń organizacyjnych i technicznych.
5. Przegląd i aktualizację polityk, procedur, instrukcji oraz innych regulacji wewnętrznych Ministerstwa Sprawiedliwości dotyczących bezpieczeństwa informacji dokonywane przez odpowiedzialne osoby w celu jak najlepszej reakcji na zagrożenia i incydenty.
6. Ciągłe podnoszenie świadomości i kwalifikacji pracowników w obszarze bezpieczeństwa informacji.
7. Ciągłe doskonalenie SZBI zgodnie z wymaganiami normy PN-EN ISO/IEC 27001 i zaleceniami wszystkich zainteresowanych stron.

4. Klasyfikacja informacji

4.1 Zasady ogólne

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 do spraw bezpieczeństwa informacji.

W Ministerstwie Sprawiedliwości poszczególne informacje są chronione na podstawie przepisów prawa. W oparciu o wymagania prawne, wszystkie przetwarzane w Ministerstwie Sprawiedliwości informacje podzielone zostały na następujące grupy:

Informacje niejawne

Ochrona informacji niejawnych odbywa się zgodnie z wymaganiami ustawy z dnia 5 sierpnia 2010r. o ochronie informacji niejawnych.

Informacje niejawne posiadają własny, niezależny od definiowanego przez niniejszą politykę system ochrony zgodnie z wymaganiami ustawy z dnia 5 sierpnia 2010r. o ochronie informacji niejawnych. Za organizację systemu ochrony informacji niejawnych w Ministerstwie Sprawiedliwości odpowiada pełnomocnik do spraw ochrony informacji niejawnych, który posiada uprawnienia oraz realizuje zadania określone w przepisach o ochronie informacji niejawnych i w sprawach merytorycznych podlega bezpośrednio Ministrowi Sprawiedliwości.

Informacje prawnie chronione

Informacje chronione na podstawie powszechnie obowiązujących aktów prawa.

Do kategorii informacji prawnie chronionych należą m.in.:

Dane osobowe, kadrowe, finansowo – księgowe, dokumentacja medyczna, informacje zawarte w aktach spraw uzyskane w trakcie i dla potrzeb postępowań, opinie biegłych, oferty przetargowe przed ich otwarciem, polityki bezpieczeństwa, wewnętrzne procedury dotyczące bezpieczeństwa, strategiczne projekty, informacje zastrzeżone do wyłącznej wiadomości Ministerstwa Sprawiedliwości oraz inne tajemnice ustawowo chronione (tajemnice powołane na mocy ustaw, których obowiązek ochrony wynika z tychże ustaw) – chronione ze względu na ich poufność, integralność i dostępność.

Pozostałe informacje przetwarzane w urzędzie

W szczególności informacje, których zakres i tryb udostępniania określa**,** ustawia z dnia 6 września 2001 roku o dostępie do informacji publicznej.

Należą do nich między innymi publikacje na stronie www, każda informacja o sprawach publicznych udostępniana na wniosek lub zamieszczona w BIP, dane teleadresowe instytucji i innych jednostek państwowych, ulotki, plakaty, oferty reklamowe.

4.2 Sposób postępowania z informacjami

Ochrona informacji w Ministerstwie Sprawiedliwości funkcjonuje na trzech poziomach:
1. Informacje o poziomie ochrony Niski to informacje, których ujawnienie, uszkodzenie lub utrata powoduje znikome skutki dla Ministerstwa Sprawiedliwości.
2. Informacje o poziomie ochrony Średni to informacje, których ujawnienie, uszkodzenie lub utrata może wpłynąć na działalność Ministerstwa Sprawiedliwości i spowodować skutki (np. straty wizerunkowe).

3. Informacje o poziomie ochrony Wysoki to informacje o najwyższym stopniu ochrony, których ujawnienie, uszkodzenie lub utrata powoduje naruszenie przepisów prawa i skutki prawne dla Ministerstwa Sprawiedliwości.
W ramach każdego z poziomów ochrony, zdefiniowane zostały zasady postępowania z przypisanymi do nich grupami informacji.
Szczegóły postępowania z informacjami określone zostaną w procedurze w obszarze nadzoru nad dokumentacją, której właścicielem jest Pełnomocnik do spraw bezpieczeństwa informacji.

4.3 Zmiana klasyfikacji informacji

Klasyfikacja odzwierciedla aktualne potrzeby ochrony informacji. Wraz z upływem czasu potrzeby ochrony danej informacji mogą ulegać zmianom. Uwzględniając cykl życia informacji, należy dokonywać okresowych przeglądów i w uzasadnionych przypadkach zmieniać przypisaną klasyfikację, odzwierciedlając aktualne wymagania w zakresie dostępności, poufności i integralności informacji.

Zmiany klasyfikacji informacji może dokonać, na pisemny wniosek skierowany do Pełnomocnika do spraw bezpieczeństwa informacji Właściciel obszaru lub osoba przez niego wyznaczona. Przy czym ostateczna decyzja należy do Pełnomocnika do spraw bezpieczeństwa informacji.

Zmiany może również dokonać Pełnomocnik do spraw bezpieczeństwa informacji w porozumieniu z właścicielem obszaru lub osobą do tego wyznaczoną.

5. Zarządzanie dokumentacją SZBI

5.1 Struktura dokumentacji SZBI

PBI Ministerstwa Sprawiedliwości określa wymagania i zasady bezpieczeństwa informacji obowiązujące w Ministerstwie Sprawiedliwości oraz ramy SZBI ustanowionego w Ministerstwie Sprawiedliwości.

PBI nie reguluje wprost zasad zarządzania bezpieczeństwem informacji w innych jednostkach podległych lub nadzorowanych przez Ministra Sprawiedliwości, ale może być przez nie zaadaptowana z uwzględnieniem ich specyfiki organizacyjnej.

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

Kolejny poziom dokumentacji SZBI stanowią Polityki określające zasady zarządzania bezpieczeństwem informacji w poszczególnych obszarach, które muszą powstać i zostać wprowadzone w życie w terminie do 12 miesięcy od dnia wejścia w życie zarządzenia w sprawie Polityki Bezpieczeństwa Informacji Ministerstwa Sprawiedliwości. Każda z Polityk, uzgodniona z Pełnomocnikiem do spraw bezpieczeństwa informacji, może zawierać odwołania do dokumentów niższego poziomu, takich jak: procedury, instrukcje oraz inne regulacje wewnętrze Ministerstwa Sprawiedliwości dotyczące bezpieczeństwa informacji, może również zawierać regulacje dotyczące zakresu dokumentacji poszczególnych systemów IT.

Za opracowanie i wdrożenie niezbędnych wyżej wymienionych dokumentów odpowiedzialni są Właściciele obszarów, wymienieni w rozdziale 6.

Procedury, instrukcje i inne dokumenty SZBI tworzone są w celu uszczegółowienia zasad opisanych w politykach.

Oprócz wymienionych powyżej klas dokumentów, stanowiących regulacje wewnętrzne, elementem dokumentacji są również zapisy potwierdzające wystąpienie zdarzeń lub realizację działań określonych w dokumentach regulacyjnych. Zapisy (lub innymi słowy dokumentacja dowodowa) mogą powstawać w systemach teleinformatycznych w postaci elektronicznej lub na nośnikach papierowych, które często mają formę zatwierdzonych formularzy.

5.2 Nadzór nad dokumentacją SZBI

Nadzór nad dokumentami SZBI jest procesem ciągłym. Każdy dokument ma przypisanego Właściciela, który odpowiada za prawidłowe działanie procesu opisanego w danym dokumencie. Nie rzadziej niż raz na rok, do końca stycznia za rok poprzedni, Właściciel odpowiedzialny za dany dokument przeprowadza jego przegląd, w celu potwierdzenia aktualności i adekwatności danego dokumentu. O wynikach przeglądu Właściciel dokumentu pisemnie informuje Pełnomocnika do spraw bezpieczeństwa informacji.

W przypadku zidentyfikowania rozbieżności lub potrzeby doskonalenia, Właściciel dokumentu ma obowiązek przedstawić projekt zaktualizowanego dokumentu Pełnomocnikowi do spraw bezpieczeństwa informacji do uzgodnienia.

Dokumenty są opracowywane przez ich właścicieli, uzgadniane z Pełnomocnikiem do spraw bezpieczeństwa informacji, który ostatecznie je zatwierdza. Następnie wdrażane, przechowywane jak również archiwizowane zgodnie z Instrukcją w sprawie organizacji i zakresu działania archiwum zakładowego w Ministerstwie Sprawiedliwości.

Nadzór nad aktualnością dokumentacji SZBI obejmuje:

- Opracowywanie i zatwierdzanie dokumentów;
- Zasady oznaczania informacji;
- Rozpowszechnianie dokumentów;
- Identyfikację potrzeb aktualizacji dokumentu;
- Wprowadzanie zmian do dokumentów (w tym zwiększaniu numerów wersji);
- Archiwizację dokumentacji SZBI;
- Przechowywanie i ochronę dokumentów;
- Wycofywanie nieaktualnych wersji dokumentów.

Powyższe działania prowadzone będą według zasad określonych w procedurze obszaru nadzoru nad dokumentacją, którego Właścicielem jest Pełnomocnik do spraw bezpieczeństwa informacji.

6. Organizacja SZBI

Zarządzanie bezpieczeństwem informacji w Ministerstwie Sprawiedliwości odbywa się na poziomach:

Strategicznym – prowadzone jest zarządzanie strategią rozwoju i doskonalenia SZBI w odniesieniu do zmieniającego się otoczenia prawnego i technologicznego jak również w oparciu o wyniki analizy ryzyka. W procesy decyzyjne tego poziomu zaangażowane jest Kierownictwo Ministerstwa Sprawiedliwości.

Taktycznym – tworzone są standardy bezpieczeństwa informacji oraz zasady kontroli ich wypełniania w stosowanych rozwiązaniach i systemach teleinformatycznych oraz przestrzegania w praktyce używania tych rozwiązań i systemów. W te procesy decyzyjne zaangażowane są osoby związane z zarządzaniem bezpieczeństwem w poszczególnych obszarach, regulowanych przez polityki obszarowe.

Operacyjnym – prowadzona jest administracja procesami bezpieczeństwa informacji zgodnie z przyjętymi standardami oraz rozwiązywanie sytuacji kryzysowych wynikających z naruszenia zabezpieczeń.

6.1. Działania operacyjne

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

1. Zarządzanie ryzykiem.
2. Postępowanie z ryzykiem.
3. Monitorowanie podjętych działań.
4. Audyty.
5. Utrzymanie i doskonalenie SZBI.
6. Zarządzanie dostępem do zasobów.
7. Monitorowanie skuteczności i efektywności zabezpieczeń.
8. Zarządzanie incydentami.

.

6.2 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.

Podstawowym kryterium oceny ryzyk jest zidentyfikowanie ryzyk o maksymalnej wartości w obszarach o największym ryzyku oraz zidentyfikowanie ryzyk związanych z niezgodnością z regulacjami prawnymi. Na podstawie wyników analizy ryzyka opracowywane są plany postępowania z ryzykiem dla zagrożeń o ryzyku większym niż ustalony poziom ryzyka akceptowalnego oraz dla zagrożeń związanych z niezgodnością z przepisami prawa. Analiza ryzyka jest przeprowadzana regularnie, nie rzadziej niż raz do roku, ryzyka są regularnie raportowane do Kierownictwa oraz do zainteresowanych stron. Analiza ryzyka przeprowadzana jest również po wprowadzeniu zmian mających wpływ na system zarządzania bezpieczeństwa informacji.

Poszczególne grupy zabezpieczeń dobierane są przez Właścicieli obszarów adekwatnie do wymagań prawnych i wyników analizy ryzyka dla bezpieczeństwa informacji.

Zabezpieczenia fizyczne, techniczne i organizacyjne dobierane są tak, aby uzupełniać się wzajemnie, zapewniając wspólnie wymagany poziom bezpieczeństwa informacji.

Szczegółowe zasady zarządzania ryzykiem w bezpieczeństwie informacji zostaną uregulowane w procedurze obszaru zarządzania ryzykiem w bezpieczeństwie informacji.

6.3 Odpowiedzialność za bezpieczeństwo informacji

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

1. Członek Kierownictwa Ministerstwa Sprawiedliwości odpowiedzialny za Bezpieczeństwo Informacji zapewnienia zasoby niezbędne dla opracowania, wdrożenia, funkcjonowania, utrzymania i doskonalenia SZBI oraz poszczególnych zabezpieczeń.
2. Pełnomocnik do spraw bezpieczeństwa informacji jest odpowiedzialny za proces ustanawiania i należytego funkcjonowania SZBI.
3. Dyrektorzy Departamentów i Biur odpowiadają za:
   a. identyfikację aktywów informacyjnych (w tym w szczególności za identyfikację zbiorów danych osobowych, informacji niejawnych oraz innych informacji prawnie chronionych) w ramach właściwości departamentu/biura,
   b. prowadzenie dokumentacji systemów teleinformatycznych i aplikacji, nad którymi sprawują nadzór,
   c. przestrzeganie zasad ochrony informacji przez podległych im pracowników,
   d. przeprowadzanie cyklicznej analizy ryzyka bezpieczeństwa informacji, związanej z realizowanymi w komórce organizacyjnej zadaniami i wykorzystywanymi przez

nią aktywami, zgodnie z procedurą w obszarze zarządzania ryzykiem w bezpieczeństwie informacji

e. definiowanie oraz realizację działań zapobiegających zagrożeniom lub minimalizujących ich skutki,

f. zapoznanie pracowników z obowiązkami związanymi z ochroną informacji na stanowiskach pracy,

g. zapoznanie pracowników z przepisami prawa oraz wewnętrznymi zasadami dotyczącymi ochrony informacji.

4. Odpowiedzialność za bezpieczeństwo informacji w Ministerstwie Sprawiedliwości ponoszą wszyscy pracownicy oraz osoby wykonujące pracę na innej podstawie niż stosunek pracy zgodnie z posiadanymi zakresami obowiązków. Każdy z wyżej wymienionych obowiązany jest dbać o bezpieczeństwo powierzonych mu do przetwarzania, archiwizowania lub przechowywania informacji zgodnie z przepisami prawa oraz obowiązującymi w Ministerstwie Sprawiedliwości przepisami wewnętrznymi, w tym m.in:

   a. stosować zasady opisane w Polityce oraz innych dokumentach wewnętrznych,

   b. zabezpieczać informacje/dane podlegające ochronie przed dostępem do nich osób nieuprawnionych, zniszczeniem, utratą lub nieautoryzowaną modyfikacją,

   c. chronić urządzenia służące uwierzytelnieniu w systemach teleinformatycznych oraz powierzone identyfikatory służące uwierzytelnianiu w systemach kontroli dostępu przed przypadkowym lub umyślnym zniszczeniem, utratą lub modyfikacją,

   d. zabezpieczać sprzęt, wydruki komputerowe i nośniki zawierające informacje chronione,

   e. utrzymywać w bezwzględnej tajemnicy hasła oraz szczegóły technologiczne systemów także po ustaniu zatrudnienia w Ministerstwie Sprawiedliwości,

   f. stosować się do szczegółowych zaleceń w zakresie ochrony antywirusowej i innych zasad SZBI,

   g. zgłosić incydent bezpieczeństwa, zgodnie z regulacjami zawartymi w rozdziale 16.1, w sytuacji wskazującej na:

      - ujawnienie lub możliwość ujawnienia informacji chronionych osobom nieupoważnionym,
      - nieautoryzowaną zmianę informacji chronionych lub możliwość wprowadzenia nieautoryzowanych zmian,
      - zniszczenie lub możliwość zniszczenia informacji chronionych,
      - zablokowanie lub możliwość zablokowania pracy systemu teleinformatycznego przetwarzającego informacje chronione lub uniemożliwienia innego dostępu do informacji chronionych.

Właściciel obszaru może w ramach SZBI mieć szczególne zadania, spójne z zakresem jego obowiązków wynikających z regulaminu organizacyjnego Ministerstwa Sprawiedliwości.

Szczegółowy podział odpowiedzialności jest następujący:

Członek Kierownictwa Ministerstwa Sprawiedliwości odpowiedzialny za bezpieczeństwo informacji

1. Nadzoruje realizację zadań określonych w PBI Ministerstwa Sprawiedliwości.
2. Powierza realizację zadań określonych w PBI Ministerstwa Sprawiedliwości Pełnomocnikowi do spraw bezpieczeństwa informacji.

Pełnomocnik do spraw bezpieczeństwa informacji

1. Realizuje swoje zadania we współpracy z właścicielami obszarów.
2. Jest odpowiedzialny za proces ustanawiania, wdrożenia i należytego funkcjonowania SZBI w Ministerstwie Sprawiedliwości.
3. Sprawuje nadzór nad realizacją regulacji w PBI Ministerstwa Sprawiedliwości.
4. Zatwierdza Polityki Bezpieczeństwa dla poszczególnych obszarów.
5. Inicjuje działania związane z aktualizacją PBI Ministerstwa Sprawiedliwości.
6. Organizuje okresowe przeglądy SZBI, w wyniku, których powstaje raport o stanie bezpieczeństwa informacji w Ministerstwie Sprawiedliwości. Następnie przedstawia go Ministrowi Sprawiedliwości, za pośrednictwem członka Kierownictwa Ministerstwa Sprawiedliwości odpowiedzialnego za bezpieczeństwo informacji.
7. Jest Właścicielem dokumentu w obszarze audytów systemu zarządzania bezpieczeństwem informacji.
8. Jest Właścicielem procedury w obszarze nadzoru nad dokumentacją.
9. Jest Właścicielem procedury w obszarze zarządzania ryzykiem w bezpieczeństwie informacji.
10. Może, w uzasadnionych przypadkach, wyznaczyć Właścicieli polityk obszarowych innych niż wskazani w dokumencie.
11. Koordynuje działania związane z wykonaniem corocznego audytu, o którym mowa w § 20 ust. 2 pkt 14 w rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych oraz innych audytów SZBI za pomocą wyznaczonej komórki organizacyjnej.
12. Nadzoruje obsługę niezgodności oraz realizację zaleceń poaudytowych korygująco-naprawczych i doskonalących oraz dokumentowanie realizacji zaleceń poaudytowych.
13. Monitoruje postępowanie z ryzykiem w obszarze bezpieczeństwa informacji.
14. Analizuje wnioski z przeglądów SZBI oraz wnioski z analizy naruszeń bezpieczeństwa informacji w poszczególnych obszarach.
15. Inicjuje 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 z poszczególnych obszarów.
16. Zapewnia przeszkolenie pracowników z zakresu bezpieczeństwa informacji.

Dyrektor Biura Ochrony, pełnomocnik do spraw ochrony informacji niejawnych

1. Jest Właścicielem polityki w obszarze bezpieczeństwa fizycznego.
2. Zarządza ryzykiem w obszarze bezpieczeństwa fizycznego.
3. Zapewnia zabezpieczenia techniczno-organizacyjne służące do kontroli dostępu oraz wykrycia nieautoryzowanych działań związanych z kontrolą wejść i wyjść do pomieszczeń i budynków Ministerstwa Sprawiedliwości.
4. Rejestruje i obsługuje incydenty związane z naruszeniem ochrony fizycznej.
5. Jest odpowiedzialny za treść i nadzór nad umowami z dostawcami w zakresie zabezpieczeń fizycznych.
6. Jest odpowiedzialny za ciągłość działania urzędu w zakresie dostępności biur i działania w sytuacjach kryzysowych.
7. Jest Właścicielem polityki w obszarze bezpieczeństwa informacji niejawnych.

8. Odpowiada za zgodne z przepisami przetwarzanie w urzędzie informacji niejawnych.
9. Prowadzi ewidencje osób upoważnionych do przetwarzania danych osobowych.

Dyrektor Biura Cyberbezpieczeństwa

1. Jest Właścicielem polityki w obszarze bezpieczeństwa cyberprzestrzeni w Ministerstwie Sprawiedliwości.
2. Koordynuje funkcjonowanie systemu zarządzania bezpieczeństwem cyberprzestrzeni Ministerstwie Sprawiedliwości.
3. Analizuje ryzyko bezpieczeństwa systemów teleinformatycznych w cyberprzestrzeni Ministerstwa Sprawiedliwości.
4. Przekazuje informację o zidentyfikowanym ryzyku, określonym w p.3 Właścicielom aktywów Ministerstwa Sprawiedliwości.
5. Opiniuje polityki bezpieczeństwa dla poszczególnych systemów teleinformatycznych.
6. Prowadzi monitoring stanu oraz analizę podatności bezpieczeństwa systemów teleinformatycznych w obszarze cyberprzestrzeni Ministerstwa Sprawiedliwości.
7. Rejestruje przypadki naruszenia bezpieczeństwa informacji w cyberprzestrzeni Ministerstwa Sprawiedliwości.
8. Obsługuje incydenty związane z bezpieczeństwem informacji w cyberprzestrzeni Ministerstwa Sprawiedliwości.
9. Planuje audyty odporności systemów teleinformatycznych na cyberzagrożenia.
10. Prowadzi analizę podatności systemów informatycznych.
11. Realizuje czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji w cyberprzestrzeni Ministerstwa Sprawiedliwości.
12. Koordynuje działania związane z przeprowadzaniem doraźnych przeglądów i testów penetracyjnych systemów.
13. Sprawuje nadzór nad bezpieczeństwem systemów teleinformatycznych.
14. Koordynuje działania edukacyjno-informacyjne w zakresie cyberbezpieczeństwa w Ministerstwie Sprawiedliwości, a w szczególności dotyczące edukacji użytkownika końcowego, edukacji eksperckiej oraz polityki informacyjnej w zakresie zaistniałych incydentów IT, również we współpracy z instytucjami i podmiotami zewnętrznymi.
15. Współpracuje z ministrem właściwym do spraw informatyzacji, Narodowym Centrum Cyberbezpieczeństwa oraz Rządowym Zespołem do spraw Reagowania na Incydenty Komputerowe (RZRnIK) – CERT.GOV.PL w zakresie ochrony cyberprzestrzeni Rzeczypospolitej Polskiej.

Inspektor Ochrony Danych

1. Jest wyznaczany przez Administratora Danych Osobowych, realizuje zadania zgodnie z przepisami Ustawy oraz regulacjami unijnymi.
2. Jest Właścicielem polityki w obszarze bezpieczeństwa danych osobowych.
3. Inicjuje działania związane z aktualizacją polityki w obszarze bezpieczeństwa danych osobowych.
4. Opiniuje polityki bezpieczeństwa dla poszczególnych systemów teleinformatycznych przetwarzających dane osobowe oraz polityki bezpieczeństwa dla poszczególnych obszarów.
5. Zarządza ryzykiem w obszarze bezpieczeństwa danych osobowych.

6. Przygotowuje wzorce wymaganych dokumentów niezbędne do realizacji procesu przetwarzania danych osobowych.
7. Przygotowuje minimalne wymagania bezpieczeństwa dla systemów przetwarzających dane osobowe.
8. Rejestruje i obsługuje incydenty związane z bezpieczeństwem danych osobowych.
9. Opiniuje umowy powierzenia przetwarzania danych osobowych.
10. Zapewnia przeszkolenie pracowników Ministerstwa Sprawiedliwości z zakresu ochrony danych osobowych.
11. Reprezentuje Ministra Sprawiedliwości w sprawach prowadzonych przed Prezesem Urzędu Ochrony Danych Osobowych.

Dyrektor Departamentu Informatyzacji i Rejestrów Sądowych

1. Jest właścicielem polityki w obszarze bezpieczeństwa systemów teleinformatycznych Ministerstwa Sprawiedliwości.
2. Opiniuje polityki w obszarze bezpieczeństwa dla poszczególnych systemów teleinformatycznych przetwarzających dane osobowe.
3. Jest właścicielem dokumentu w obszarze korzystania z mobilnego sprzętu komputerowego Ministerstwa Sprawiedliwości.
4. Jest właścicielem regulaminu dotyczącego użytkownika systemów teleinformatycznych Ministerstwa Sprawiedliwości.
5. Zarządza ryzykiem w obszarze bezpieczeństwa podległych systemów teleinformatycznych.
6. Zapewnia zabezpieczenia techniczne dostępu do informacji w podległych systemach teleinformatycznych.
7. Zapewnia w niezbędnym zakresie rozliczalność z dostępu do informacji w podległych systemach teleinformatycznych.
8. Odpowiada za poufność, integralność i dostępność informacji przetwarzanych w podległych systemach teleinformatycznych.
9. Nadaje na wniosek właściciela merytorycznego uprawnienia do dostępu w podległych systemach teleinformatycznych.
10. Jest odpowiedzialny za treść i nadzór nad umowami z dostawcami w zakresie sprzętu teleinformatycznego, oprogramowania, okablowania i nośników danych oraz usług przetwarzania informacji.
11. Prowadzi rejestr zasobów w zakresie sprzętu teleinformatycznego, oprogramowania, okablowania i nośników danych oraz usług przetwarzania informacji.
12. Prowadzi dokumentację administracyjną systemów teleinformatycznych i aplikacji, nad którymi sprawuje nadzór.
13. Jest odpowiedzialny za techniczne aspekty zabezpieczeń ciągłości działania nadzorowanych systemów teleinformatycznych Ministerstwa Sprawiedliwości.
14. Autoryzuje informatyczne środki przetwarzania informacji dopuszczone w Ministerstwie Sprawiedliwości.
15. Zatwierdza standardy dotyczące systemów teleinformatycznych.
16. Wydaje zezwolenia na wynoszenie aktywów poza siedzibę w zakresie sprzętu teleinformatycznego, oprogramowania i nośników danych.
17. Analizuje raporty ze zdarzeń związanych z bezpieczeństwem podległych systemów teleinformatycznych.
18. Zapewnia bezpieczną pracę na odległość i mobilne przetwarzanie danych.

19. Zapewnia rozliczalność z dostępu do informacji w systemie Krajowego Rejestru Karnego w swoim zakresie.
20. Jest odpowiedzialny za treść i nadzór nad umowami z dostawcami w zakresie elementów systemu Krajowego Rejestru Karnego.

Dyrektor Biura Informacyjnego Krajowego Rejestru Karnego

1. Jest Właścicielem polityki w obszarze bezpieczeństwa Krajowego Rejestru Karnego.
2. Jest Właścicielem polityki w obszarze bezpieczeństwa danych osobowych rejestru sprawców przestępstw na tle seksualnym.
3. W porozumieniu z Dyrektorem Departamentu Informatyzacji i Rejestrów Sądowych opracowuje politykę w obszarze bezpieczeństwa Krajowego Rejestru Karnego i przekłada do zatwierdzenia Administratorowi Danych Osobowych.
4. W porozumieniu z Dyrektorem Departamentu Informatyzacji i Rejestrów Sądowych opracowuje polityki w obszarze bezpieczeństwa danych osobowych rejestru sprawców przestępstw na tle seksualnym i przekłada do zatwierdzenia Administratorowi Danych Osobowych.
5. Zarządza ryzykiem w obszarze bezpieczeństwa informacji Biura Informacyjnego Krajowego Rejestru Karnego.
6. Zapewnia zabezpieczenia organizacyjne dostępu do informacji w systemie Biura Informacyjnego Krajowego Rejestru Karnego w zakresie swoich kompetencji.
7. Wnioskuje o nadanie uprawnień do pracy w systemie Biura Informacyjnego Krajowego Rejestru Karnego oraz prowadzi ich ewidencję.
8. Prowadzi ewidencje osób upoważnionych do przetwarzania danych osobowych w Biurze Informacyjnym Krajowego Rejestru Karnego.
9. Jest odpowiedzialny za ciągłość działania Biura Informacyjnego Krajowego Rejestru Karnego w zakresie swoich kompetencji.

Dyrektor Biura Administracyjnego

1. Jest Właścicielem procedury w obszarze bezpieczeństwa dostaw i wyposażenia w zakresie właściwości Biura.
2. Jest Właścicielem regulaminu dotyczącego korzystania z telefonów służbowych w Ministerstwie Sprawiedliwości w zakresie właściwości Biura.
3. Zarządza ryzykiem w obszarze bezpieczeństwa dostaw i wyposażenia w zakresie właściwości Biura.
4. Jest odpowiedzialny za treść i nadzór nad umowami z dostawcami w zakresie wyposażenia biur oraz podstawowych usług technicznych we właściwości biura.
5. Tworzy, przekazuje, aktualizuje rejestr zasobów w zakresie biur i ich wyposażenia, podstawowych usług technicznych oraz ludzi (aktywa wspierające).
6. Wydaje zezwolenia na wynoszenie aktywów poza siedzibę w zakresie wyposażenia biur w zakresie właściwości Biura.
7. Współpracuje z Departamentem Informatyzacji i Rejestrów Sądowych w zakresie prowadzenia ewidencji sprzętu komputerowego i wartości niematerialnych i prawnych o charakterze informatycznym.

Dyrektor Biura Dyrektora Generalnego oraz Dyrektor Departamentu Kadr i Organizacji Sądów Powszechnych i Wojskowych

1. Jest Właścicielem polityki w obszarze bezpieczeństwa zasobów ludzkich w zakresie swojej właściwości.
2. Zarządza ryzykiem w obszarze bezpieczeństwa zasobów ludzkich.
3. Tworzy, przekazuje, aktualizuje rejestr zasobów informacyjnych według swojej właściwości.
4. Rejestruje i obsługuje incydenty związane z personelem.
5. Biuro Dyrektora Generalnego przechowuje oświadczenia o zapoznaniu się pracownika z PBI Ministerstwa Sprawiedliwości
6. Dyrektor Departamentu Kadr i Organizacji Sądów Powszechnych i Wojskowych przechowuje oświadczenia o zapoznaniu się osób delegowanych z PBI Ministerstwa Sprawiedliwości z wyłączeniem osób delegowanych na podstawie § 28 ust 1 pkt 2 lit. e regulaminu organizacyjnego Ministerstwa Sprawiedliwości.
7. Biuro Dyrektora Generalnego jest Właścicielem dokumentu w obszarze zasad i trybu wykonywania czynności kancelaryjnych w Ministerstwie Sprawiedliwości.

Dyrektor właściwy merytorycznie dla danego systemu teleinformatycznego

1. Jest Właścicielem polityki w obszarze bezpieczeństwa systemu teleinformatycznego będącego w jego właściwości merytorycznej.
2. Zarządza ryzykiem w obszarze bezpieczeństwa informacji będącej w jego właściwości merytorycznej.
3. Zapewnia zabezpieczenia organizacyjne dostępu do informacji w systemie teleinformatycznym będącym w jego właściwości merytorycznej.
4. Zarządza uprawnieniami do pracy w systemie teleinformatycznym będącym w jego właściwości merytorycznej oraz prowadzi ewidencję nadanych uprawnień do niego.
5. Prowadzi dokumentację systemu teleinformatycznego będącego w jego właściwości merytorycznej.
6. Jest odpowiedzialny za ciągłość działania systemu teleinformatycznego będącego w jego właściwości merytorycznej w zakresie swoich kompetencji.

7. Zarządzanie zasobami ludzkimi

Ministerstwo Sprawiedliwości dba o zapewnienie kompetentnych i świadomych pracowników do realizacji wyznaczonych w procesach zadań. Celem jest ograniczenie ryzyka błędu ludzkiego, kradzieży, nadużycia lub niewłaściwego użytkowania zasobów.

Skuteczna realizacja postawionego celu możliwa jest dzięki ustanowionym procedurom i podziałowi odpowiedzialności związanemu z weryfikacją kandydatów do pracy podczas naboru, zasadom zatrudniania pracowników oraz ustalonym procedurom rozwiązywania umów o pracę.

Zasoby ludzkie są ważnym czynnikiem analizowanym podczas przeprowadzania okresowej analizy ryzyka.

Zasoby ludzkie są jednym z najważniejszych źródeł zagrożeń dla organizacji. W celu zapewnienia odpowiedniej ochrony zasobów ludzkich zabezpieczenie tego obszaru zostało podzielone na następujące sekcje czasowe:

1. Przed zatrudnieniem.
2. W trakcie zatrudnienia.
3. Zakończenie zatrudnienia.

7.1 Przed zatrudnieniem

W trakcie procesu zatrudniania należy postępować zgodnie z obowiązującymi przepisami prawa. Kandydat wybrany w procesie rekrutacji, przed przystąpieniem do pracy powinien zapoznać się z obowiązującymi regulacjami wewnętrznymi, a w szczególności z PBI. Fakt zapoznania się z dokumentem powinien zostać potwierdzony podpisem pracownika na stosownym oświadczeniu, za przechowywanie, których odpowiedzialne jest Biuro Dyrektora Generalnego w przypadku osób będących w stosunku pracy z Ministerstwem Sprawiedliwości, Departament Kadr i Organizacji Sądów Powszechnych i Wojskowych w przypadku osób delegowanych z wyłączeniem osób delegowanych na podstawie § 28 ust 1 pkt 2 lit e regulaminu organizacyjnego Ministerstwa Sprawiedliwości. W zakresie Biura Informacyjnego Krajowego Rejestru Karnego oświadczenia o zapoznaniu się z dokumentacją PBI przechowywane są zgodnie z polityką w obszarze bezpieczeństwa Krajowego Rejestru Karnego. Oświadczenia pracowników firm zewnętrznych i zleceniobiorców, którzy realizują swoje zadania w siedzibie Ministerstwa Sprawiedliwości przechowywane są w komórce merytorycznej w dokumentacji dotyczącej realizacji postanowień umowy.

7.2 W trakcie zatrudnienia

Każdy pracownik w zakresie bezpieczeństwa informacji musi zostać przeszkolony. Szkolenie dla pracowników z zakresu bezpieczeństwa informacji należy przeprowadzić każdorazowo:

1. Po zmianie przepisów dotyczących bezpieczeństwa informacji.
2. Po wprowadzeniu istotnych zmian w PBI Ministerstwa Sprawiedliwości
3. Na wniosek dyrektora komórki organizacyjnej.

Szkolenie może zostać przeprowadzone w dowolnej formie, w tym przez zapoznanie pracowników ze zmianami, potwierdzone podpisem własnoręcznym lub elektronicznym.

7.3 Zakończenie zatrudnienia

Kończenie pracy przez pracownika może być związane z ryzykiem: kradzieży, przejęcia i wykorzystania informacji chronionej. W związku z wymienionymi zagrożeniami należy minimalizować ryzyko z nimi związane. W uzasadnionych przypadkach odebranie uprawnień do informacji chronionych powinno nastąpić jak najszybciej po podjęciu decyzji o zakończeniu zatrudnienia.

Proces odbierania uprawnień do systemów teleinformatycznych powinien przebiegać zgodnie z odpowiednimi procedurami, określonymi w polityce obszaru bezpieczeństwa systemów teleinformatycznych Ministerstwa Sprawiedliwości, bądź w dokumentacji polityk bezpieczeństwa poszczególnych systemów teleinformatycznych. Szczegóły procesu nadawania, modyfikacji lub odbierania uprawnień do systemów IT uregulowane zostaną poprzez odpowiednie procedury określone w polityce obszaru bezpieczeństwa systemów teleinformatycznych Ministerstwa Sprawiedliwości.

Szczegóły procesu nadawania i odbierania uprawnień do wejścia do budynku określone zostaną w polityce obszaru bezpieczeństwa fizycznego.

8. Zarządzanie zasobami

8.1 Klasyfikacja zasobów w Ministerstwie Sprawiedliwości

Ministerstwo Sprawiedliwości zarządza swoimi aktywami (zasobami) 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.

Wszystkim zasobom z wyjątkiem zasobów ludzkich przypisuje się poziom ważności:

a) ważność wysoka przyznawana jest, gdy utrata lub naruszenie bezpieczeństwa zasobów powoduje przerwanie procesu. Należą do nich m.in.:
   - informacje nadzorowane, wrażliwe pod względem poufności w szczególności: informacje niejawne dodatkowo podlegające ochronie w stopniu zgodnym z postanowieniami, ustawy o ochronie informacji niejawnych, dane osobowe dodatkowo podlegające ochronie w stopniu zgodnym z postanowieniami Rozporządzenia Parlamentu Europejskiego i Rady UE, ustawy o ochronie danych osobowych, dane finansowo - księgowe, inne informacje, których poufność określają ustawy lub zarządzenia wewnętrzne (RODO),
   - zasoby materialne kluczowe niezbędne do realizowania statutowych celów Ministerstwa Sprawiedliwości,
b) ważność średnia przyznawana jest, gdy utrata lub naruszenie bezpieczeństwa zasobów może mieć wpływ na prawidłową realizację procesu. Należą do nich m.in.:
   - pozostałe informacje nadzorowane, niewrażliwe (np. korespondencja wewnętrzna Ministerstwa Sprawiedliwości),
   - zasoby fizyczne wartościowe, które są drogie lub trudno zastępowalne, ale od których nie zależy bezpośrednio funkcjonowanie Ministerstwa Sprawiedliwości,
c) ważność niska przyznawana jest, gdy utrata lub naruszenie bezpieczeństwa zasobu ma znikomy wpływ na funkcjonowanie procesu. Należą do nich m.in.:
   - informacje nienadzorowane i inne informacje publiczne,
   - zasoby fizyczne zwykłe, które są łatwo odtwarzalne lub zastępowalne i od których nie zależy bezpośrednio funkcjonowanie Ministerstwa Sprawiedliwości.

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.

Właściciele obszarów tworzą, przekazują Pełnomocnikowi do spraw bezpieczeństwa informacji oraz aktualizują rejestr zasobów informacyjnych zgodnie z właściwością wynikającą z regulaminu organizacyjnego Ministerstwa Sprawiedliwości.
Rejestr zawiera, co najmniej następujące informacje:

1. Nazwę zasobu;
2. Typ zasobu;
3. Opis zasobu (zagrożenia dla poufności, integralności i dostępności zasobu);
4. Właściciela zasobu.

8.2 Autoryzacja nowych środków przetwarzania informacji

Każde nowe lub zmienione urządzenie służące do przetwarzania informacji lub mogące w jakikolwiek inny sposób wpływać na bezpieczeństwo informacji musi zostać zweryfikowane na zgodność z wymaganiami SZBI i zautoryzowane przez osobę, w której kompetencjach leży dany zasób. Wprowadzany nowy lub modyfikowany istniejący zasób musi umożliwiać spełnienie wymogów PBI oraz dokumentów zależnych.

8.3 Wynoszenie i bezpieczeństwo zasobów poza siedzibę

Sprzęt, informacje lub oprogramowanie nie powinny być wynoszone poza siedzibę Ministerstwa Sprawiedliwości bez uprzedniego zezwolenia. Należy wskazać pracowników, osoby delegowane oraz osoby realizujące zadania na zasadach umów cywilnoprawnych lub o dzieło którzy mają prawo do wynoszenia aktywów i jeśli będzie taka potrzeba, rejestrować, kiedy sprzęt jest wynoszony i kiedy jest zwracany. Aktywów nie wolno w żadnym wypadku pozostawiać w miejscach publicznych bez nadzoru, a użytkownik zobowiązany jest zapewnić im adekwatną ochronę, m. in. zgodnie z regulacjami zawartymi w rozdziale 10.

Zezwolenia na wynoszenie aktywów poza siedzibę wydają Właściciele zasobów.

9. Kontrola dostępu do informacji

Zarządzanie dostępem do informacji odbywa się w ramach procesu opartego na systemie obiegu wniosków. Procedury przyznawania uprawnień do informacji w ramach poszczególnych obszarów regulują polityki obszarowe.

10. Kryptografia

Narzędzi kryptograficznych używa się w następujących sytuacjach:

1. Hasła użytkowników w systemie teleinformatycznym przechowywane są w postaci zaszyfrowanej lub innej postaci, uniemożliwiającej odczytanie ich właściwej treści;
2. Do pracy zdalnej można wykorzystywać jedynie łącza zapewniające szyfrowanie transmisji;
3. Mobilne nośniki informacji przetwarzające informacje inne niż publicznie dostępne, podczas przenoszenia poza siedzibą powinny być zaszyfrowane;
4. Przesyłanie informacji prawnie chronionych (np. danych osobowych) za pośrednictwem publicznej sieci teleinformatycznej jest możliwe przy zapewnieniu ich zaszyfrowania.

Szczegóły zarządzania zabezpieczeniami kryptograficznymi określone zostaną w politykach obszarowych.

11. Bezpieczeństwo fizyczne i środowiskowe

Ministerstwo Sprawiedliwości dba o zapewnienie wysokiego poziomu bezpieczeństwa fizycznego i środowiskowego. Celem jest również zapewnienie bezpieczeństwa informacji przed dostępem osób niepowołanych, uszkodzeniem aktywów służących do przetwarzania informacji lub innymi zakłóceniami 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 środowiskowe i podtrzymujące zasilanie.

Szczegóły zarządzania bezpieczeństwem fizycznym i środowiskowym określone zostaną w polityce obszaru bezpieczeństwa fizycznego, polityce obszaru danych osobowych Ministerstwa Sprawiedliwości, polityce obszaru bezpieczeństwa systemów teleinformatycznych Ministerstwa Sprawiedliwości.

12. Bezpieczna eksploatacja

Ministerstwo Sprawiedliwości dba o przestrzeganie zasad bezpieczeństwa związanych z utrzymywaniem i użytkowaniem systemów teleinformatycznych. Celem jest zapewnienie poufności, integralności i dostępności przetwarzanych przy ich użyciu informacji.

Skuteczna realizacja postawionego celu możliwa jest dzięki:

1. Kompetencjom i świadomości pracowników oraz podpisanym umowom ze specjalistycznymi firmami wspomagającymi Ministerstwo Sprawiedliwości.
2. Zasadzie, że wszystkie systemy Ministerstwa Sprawiedliwości przed dopuszczeniem do eksploatacji muszą spełniać minimalne wymagania bezpieczeństwa i być zgodne z obowiązującymi standardami.
3. Obowiązującym zasadom konserwacji urządzeń w celu zapewnienia ich nieprzerwanej pracy.
4. Kontrolowaniu wprowadzania zmian do infrastruktury technicznej.
5. Zapewnieniu bezpieczeństwa systemów produkcyjnych, poprzez prowadzenie prac rozwojowych i testowych na oddzielnych urządzeniach lub środowiskach.
6. Nadzorowaniu usług dostarczanych przez strony trzecie, a w szczególności wszelkim wprowadzanym do nich zmianom. Po zakupie, lub wprowadzeniu zmiany do systemu jest on odbierany i akceptowany w sposób świadomy, uwzględniający jego wpływ na istniejący system bezpieczeństwa.
7. Wdrożonym zabezpieczeniom, chroniącym przed złośliwym oprogramowaniem i złośliwym kodem.
8. Usystematyzowanemu tworzeniu, przechowywaniu i testowaniu kopii bezpieczeństwa.
9. Przestrzeganiu opracowanych zasad postępowania z nośnikami.
10. Bieżącemu monitorowaniu aktywów informacyjnych, w tym informatycznych, pod kątem wcześniejszego wykrycia wszelkich niebezpieczeństw mogących zagrozić bezpieczeństwu systemów.
11. Wykrywaniu incydentów w systemach teleinformatycznych i mechanizmom reagowania w przypadkach ich wystąpienia.
12. Ograniczonemu dostępowi do niektórych usług internetowych, w tym w szczególności portali społecznościowych (m.in. Facebook, Twitter, Instagram) Dostęp do ww. usług może być dostępny dla niektórych osób, jeżeli wynika to z zakresu obowiązków i wymaga odrębnego wniosku.

Szczegółowe zasady zarządzania systemami teleinformatycznymi opisane zostaną w polityce obszaru bezpieczeństwa systemów teleinformatycznych Ministerstwa Sprawiedliwości.

13. Bezpieczeństwo komunikacji

Ministerstwo Sprawiedliwości dba o przestrzeganie zasad bezpieczeństwa związanych z komunikacją. Celem jest zapewnienie poufności, integralności i dostępności przesyłanej informacji.

Skuteczna realizacja postawionego celu możliwa jest dzięki:

1. Kompetencjom i świadomości pracowników oraz podpisanym umowom ze specjalistycznymi firmami wspomagającymi Ministerstwo Sprawiedliwości.
2. Zasadzie, że wszystkie systemy komunikacji Ministerstwa Sprawiedliwości przed dopuszczeniem do eksploatacji muszą spełniać minimalne wymagania bezpieczeństwa i być zgodne z obowiązującymi standardami.
3. Obowiązującym zasadom konserwacji i redundancji urządzeń sieciowych w celu zapobieżenia przerwom w łączności.
4. Kontrolowaniu wprowadzania zmian do infrastruktury sieciowej.
5. Wdrożonym zabezpieczeniom chroniącym przed próbami włamań z sieci publicznej.
6. Systematycznym testom penetracyjnym.
7. Przestrzeganiu opracowanych zasad zarządzanie bezpieczeństwem usług sieciowych.
8. Przestrzeganiu opracowanych zasad korzystania z urządzeń i narzędzi komunikacyjnych.
9. Ministerstwo Sprawiedliwości monitoruje poziom bezpieczeństwa informacji i posiada mechanizmy reagowania w przypadkach wystąpienia incydentów.

Szczegółowe zasady dotyczące bezpieczeństwa komunikacji opisane zostaną w politykach dotyczących poszczególnych obszarów.

14. Pozyskiwanie, rozwój i utrzymanie systemów IT

Ministerstwo Sprawiedliwości zapewnia, że wszystkie procesy związane z pozyskaniem, rozwojem bądź utrzymaniem systemów informacyjnych, w tym systemów i aplikacji teleinformatycznych, realizowanych zarówno we własnym zakresie, jak i przy wsparciu podwykonawców, wykorzystywanych wewnętrznie lub oferowanych obywatelom, realizowane są w sposób nadzorowany, gwarantujący utrzymanie odpowiedniego poziomu bezpieczeństwa.

Pozyskiwanie, rozwój i utrzymanie systemów teleinformatycznych obejmuje:

1. Uwzględnianie wymogów bezpieczeństwa podczas zakupu lub budowy nowych systemów teleinformatycznych;
2. Dopuszczenie nowego systemu do eksploatacji poprzedzone jest zawsze fazą testów funkcjonalnych, wydajnościowych i testów bezpieczeństwa na środowisku testowym;
3. Nadzorowanie dostępu do kodów źródłowych oprogramowania;
4. Wdrożenie mechanizmów aktualizacji oprogramowania;
5. Wdrożenie procedur kontroli zmian oprogramowania.

Za zapewnienie właściwego przebiegu procesu pozyskiwania, rozwoju i utrzymania systemów teleinformatycznych odpowiedzialny jest dyrektor Departamentu Informatyzacji i Rejestrów Sądowych.

Szczegółowe zasady bezpieczeństwa przy projektowaniu systemów i pracach rozwojowych opisane zostaną w polityce obszaru bezpieczeństwa systemów teleinformatycznych Ministerstwa Sprawiedliwości.

15. 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 (z ang. NDA);

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

16. Zgłaszanie incydentów związanych z bezpieczeństwem informacji

Incydenty powinny być bezzwłocznie zgłaszane do wyznaczonego punktu kontaktowego.

16.1 Zgłaszanie incydentów naruszenia bezpieczeństwa informacji

1. Każdy zauważony incydent powinien zostać zgłoszony, zarejestrowany oraz obsłużony.
2. Incydenty są zgłaszane do punktu kontaktowego poprzez:
    a. pocztę elektroniczną na adres właściciela obszaru odpowiedzialnego za obsługę incydentów będących w jego właściwości;
    b. osobiste zgłoszenie do właściciela obszaru odpowiedzialnego za obsługę incydentów będących w jego właściwości.

16.2 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 Ochrony.
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:
    a. Incydenty naruszenia ochrony fizycznej do obszaru ochrony fizycznej, szczegóły zostaną opisane w polityce obszaru bezpieczeństwa fizycznego;
    b. Incydenty związane z naruszeniem bezpieczeństwa danych osobowych do obszaru bezpieczeństwa danych osobowych, szczegóły zostaną opisane w polityce obszaru bezpieczeństwa danych osobowych;
    c. Incydenty związane z bezpieczeństwem informacji w cyberprzestrzeni Ministerstwa Sprawiedliwości do obszaru bezpieczeństwa informacji w cyberprzestrzeni Ministerstwa

Sprawiedliwości, szczegóły zostaną opisane w polityce obszaru bezpieczeństwa cyberprzestrzeni Ministerstwa Sprawiedliwości;

d. Incydenty związane z bezpieczeństwem informacji dotyczące personelu, szczegóły zostaną opisane w polityce obszaru bezpieczeństwa zasobów ludzkich.

4. W przypadku sporu pomiędzy właścicielami obszarów co do merytorycznego rozpatrzenia zgłoszonego incydentu, ostateczną decyzję w tej kwestii podejmuje Pełnomocnik do spraw bezpieczeństwa informacji.
5. Właściciele obszarów odpowiedzialni za obsługę incydentów zobowiązani są do prowadzenia rejestru zgłoszonych incydentów. Rejestr powinien zawierać:
   a. datę i godzinę zgłoszenia incydentu;
   b. dane zgłaszającego;
   c. opis przedmiotu incydentu;
   d. podjęte działania;
   e. datę zakończenia czynności.

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

17. Zarządzanie ciągłością działania

Ministerstwo Sprawiedliwości dba o zapewnienie ciągłości funkcjonowania usług związanych z przetwarzaniem informacji i generalnie ciągłości działalności urzędu. Dla poszczególnych obszarów i systemów krytycznych tworzone są plany postępowania w sytuacjach awaryjnych i kryzysowych. Celem jest przeciwdziałanie przerwom w działalności Ministerstwa Sprawiedliwości oraz ochrona krytycznych procesów przed rozległymi awariami lub katastrofami.

O konieczności tworzenia planu ciągłości działania dla konkretnego systemu decyduje jego Właściciel na podstawie analizy ryzyka. Jest on odpowiedzialny również za jego cykliczne testowanie.

Zarządzanie ciągłością działania realizowane jest w trzech obszarach, zgodnie z zakresem kompetencji określonym w regulaminie organizacyjnym Ministerstwa Sprawiedliwości:

1. Dyrektor Departamentu Informatyzacji i Rejestrów Sądowych jest odpowiedzialny za techniczne aspekty zabezpieczeń ciągłości działania nadzorowanych systemów teleinformatycznych Ministerstwa Sprawiedliwości – szczegóły zarządzania ciągłością działania systemów określone zostaną w polityce obszaru bezpieczeństwa systemów teleinformatycznych Ministerstwa Sprawiedliwości
2. Dyrektor Biura Informacyjnego Krajowego Rejestru Karnego jest odpowiedzialny za ciągłość działania Biura Informacyjnego Krajowego Rejestru Karnego w zakresie jego kompetencji.
3. Dyrektor Biura Ochrony, Pełnomocnik do spraw ochrony informacji niejawnych jest odpowiedzialny za ciągłość działania urzędu w zakresie dostępności biur i działania w sytuacjach kryzysowych – szczegóły zarządzania ciągłością działalności Ministerstwa Sprawiedliwości określone zostaną w polityce obszaru bezpieczeństwa fizycznego.

18. Zgodność z przepisami prawa i dokumentami związanymi

Ministerstwo Sprawiedliwości dba o zapewnienie zgodności zasad postępowania z przepisami obowiązującego prawa, przyjętych uwarunkowań umownych i normatywnych oraz wypracowanych własnych standardów.

Kierownictwo Ministerstwa Sprawiedliwości identyfikuje wszystkie przepisy prawa właściwe dla funkcjonowania organizacji.

18.1 Przepisy prawa

W Ministerstwie Sprawiedliwości zarządzanie informacją i jej ochrona podlegają następującym przepisom prawa:

1. Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny;
2. Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny;
3. Ustawa z dnia 26 czerwca 1974 r. – Kodeks pracy;
4. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych;
5. Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych;
6. Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji;
7. Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia;
8. Ustawa z dnia 29 września 1994 r. o rachunkowości;
9. Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych;
10. Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej;
11. Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej;
12. Ustawa z dnia 5 lipca 2002 r. o ochronie niektórych usług świadczonych drogą elektroniczną opartych lub polegających na dostępie warunkowym;
13. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne;
14. Ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe;
15. Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych;
16. Ustawa z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym;
17. Ustawa z dnia 13 maja 2016 r. o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym;
18. Ustawa z dnia 6 lipca 1982 r. o księgach wieczystych i hipotece;
19. Rozporządzenie Ministra Finansów z dnia 4 września 2015 r. w sprawie audytu wewnętrznego oraz informacji o pracy i wynikach tego audytu;
20. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy teleinformatyczne służące do przetwarzania danych osobowych;
21. Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie określenia podstawowych wymagań bezpieczeństwa teleinformatycznego;
22. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych;
23. Rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 1 grudnia 1998 r. w sprawie bezpieczeństwa i higieny pracy na stanowiskach wyposażonych w monitory ekranowe;

24. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. Ustawy o ochronie danych osobowych z dnia 10 maja 2018 r.

18.2 Polskie normy

Podstawą normalizacyjną dokumentacji SZBI są niżej wymienione polskie normy:

1. PN-EN ISO/IEC 27001 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania;
2. PN-EN ISO/IEC 27002 Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zabezpieczania informacji;
3. PN-ISO/IEC 27005 Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji;
4. PN-I-13335-1:1999 Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych – Pojęcia i modele bezpieczeństwa systemów informatycznych;

18.3 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 z renomowanych źródeł dla zapewnienia, 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 jest wyłącznie autoryzowane oprogramowanie i licencjonowane produkty.

18.4 Odstępstwa od reguł ochrony

Dopuszcza się incydentalne odstąpienia od przyjętej PBI. 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. Odstępując od przyjętych zasad, starać się zachować możliwie jak najwięcej z obowiązujących przepisów PBI 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 członkowie Kierownictwa Ministerstwa Sprawiedliwości lub Pełnomocnik do spraw bezpieczeństwa informacji.

19. Monitorowanie, pomiary, analiza i ocena

19.1 Monitorowanie SZBI

Skuteczność SZBI jest poddawana stałemu monitorowaniu. Nadzór nad procesem monitorowania sprawuje Pełnomocnik do spraw bezpieczeństwa informacji.

Monitorowanie SZBI odbywa się na podstawie analizy wyników przeprowadzonych audytów i kontroli, analizie incydentów w obszarze bezpieczeństwa informacji, cyklicznej ocenie

przeprowadzanej analizy ryzyka, a także innych zdarzeń mających wpływ na bezpieczeństwo informacji.

19.2 Niezależne przeglądy i testy systemów

Poza stałym monitorowaniem stanu bezpieczeństwa informacji, część kierowników komórek organizacyjnych posiada uprawnienia do przeprowadzania doraźnych przeglądów i testów systemów.

Z uwagi na realizowane zadania, takie uprawnienia posiadają:

1. Dyrektor Departamentu Informatyzacji i Rejestrów Sądowych – w zakresie wszystkich systemów teleinformatycznych Ministerstwa Sprawiedliwości – szczegóły dotyczące realizacji niezależnych przeglądów i testów systemów w ww. zakresie określone zostaną w polityce obszaru bezpieczeństwa systemów teleinformatycznych Ministerstwa Sprawiedliwości;
2. Dyrektor Biura Cyberbezpieczeństwa – w zakresie cyberprzestrzeni Ministerstwa Sprawiedliwości – szczegóły dotyczące realizacji niezależnych audytów, przeglądów i testów systemów w ww. zakresie określone zostaną w polityce obszaru bezpieczeństwa cyberprzestrzeni Ministerstwa Sprawiedliwości.

Z uwagi na pokrywanie się obszaru cyberprzestrzeni Ministerstwa Sprawiedliwości z poszczególnymi jego systemami, realizacja testów, a zwłaszcza testów penetracyjnych, musi być uzgadniana pomiędzy ww. Dyrektorami. W razie braku porozumienia, ostateczną decyzję podejmuje Pełnomocnik do spraw bezpieczeństwa informacji.

19.3 Audyt SZBI

Audyty są najważniejszym, obok zarządzania ryzyka narzędziem SZBI.

Do realizacji audytów SZBI, sprawdzeń i kontroli, zgodnie z zakresem zadań, uprawnienia posiadają:

1. Pełnomocnik do spraw bezpieczeństwa informacji – szczegóły dotyczące realizacji audytów SZBI określone zostaną w dokumencie obszaru audytów systemu zarządzania bezpieczeństwem informacji;
2. Dyrektor Biura Cyberbezpieczeństwa – dotyczące realizacji audytów w zakresie cyberbezpieczeństwa określone zostaną w polityce obszaru bezpieczeństwa cyberprzestrzeni Ministerstwa Sprawiedliwości.

Audyty SZBI są uzgadniane z Audytorem Wewnętrznym Ministerstwa Sprawiedliwości oraz Inspektorem Ochrony Danych jak również dyrektorem właściwej komórki organizacyjnej.

19.4 Doskonalenie SZBI

SZBI jest doskonalony poprzez podejmowanie następujących działań:

1. Przeprowadzanie działań korygujących oraz ocena ich skuteczności;
2. Przeprowadzanie działań zapobiegawczych oraz ocena ich skuteczności;
3. Informowanie zainteresowanych stron o działaniach i udoskonaleniach.

Szczegółowe zasady dotyczące realizacji działań doskonalących opisane zostaną w dokumencie obszaru audytu systemu zarządzania bezpieczeństwem informacji.

20. Przeglądy Zarządzania SZBI

20.1 Planowanie i przebieg Przeglądu Zarządzania

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

Pełnomocnik do spraw bezpieczeństwa informacji sporządza raport, w którym uwzględnia otrzymane informacje oraz uzupełnia je o informacje dotyczące przeprowadzonych audytów i wydanych zaleceń ich realizacji, incydentów, które wystąpiły, wyników analiz ryzyka i reakcji na nie, wdrożonych zabezpieczeniach, nowych politykach i procedurach.

20.2 Dokumentowanie Przeglądu Zarządzania

Na podstawie informacji przekazanych przez Właścicieli obszarów, Pełnomocnik do spraw bezpieczeństwa informacji sporządza zbiorczy raport o funkcjonowaniu SZBI, który przedstawia członkowi Kierownictwa Ministerstwa Sprawiedliwości odpowiedzialnemu za bezpieczeństwo informacji.

W przypadku stwierdzonych niezgodności Pełnomocnik do spraw bezpieczeństwa informacji występuje do Właścicieli obszarów z propozycjami podjęcia działań korygujących, zgodnie z zasadami określonymi w dokumencie obszaru audytów systemu zarządzania bezpieczeństwem informacji.

Dokumentację z Przeglądu Zarządzania przechowuje Pełnomocnik do spraw bezpieczeństwa informacji.

21. Nadzór nad SZBI

21.1 Uprawnienia i obowiązki Pełnomocnika do spraw bezpieczeństwa informacji

Pełnomocnik do spraw bezpieczeństwa informacji odpowiada za zaproponowanie struktury organizacyjnej SZBI zapewniającej optymalny podział i koordynację zadań oraz odpowiedzialności związanych z zapewnieniem bezpieczeństwa informacji, wyznaczenie Właścicieli kluczowych aktywów przetwarzających informacje, którzy zobowiązani są do zapewnienia im możliwie jak najwyższego poziomu bezpieczeństwa.

Odpowiedzialny jest za wdrażanie i koordynację zapewnienia bezpieczeństwa informacji w Ministerstwie Sprawiedliwości.

Pełnomocnik do spraw bezpieczeństwa informacji uprawniony jest do:

a. rozstrzygania sporów dotyczących stosowania wymagań zawartych w dokumentacji SZBI w Ministerstwie Sprawiedliwości oraz wydawania wiążących decyzji w tym zakresie;
b. dostępu do wszystkich dokumentów występujących w Ministerstwie Sprawiedliwości, których treść może być istotna z punktu widzenia funkcjonowania SZBI w Ministerstwie Sprawiedliwości;
c. uzyskania informacji i wyjaśnień od pracowników oraz osób wykonujących pracę na innej podstawie niż stosunek pracy w zakresie realizowanych działań w ramach SZBI w Ministerstwie Sprawiedliwości;
d. podejmowania decyzji w kwestiach bezpieczeństwa informacji w Ministerstwie Sprawiedliwości.

21.2 Sankcje za naruszenie zasad bezpieczeństwa informacji

Nieprzestrzeganie zasad zawartych w dokumentach polityk bezpieczeństwa jest naruszeniem obowiązków pracowniczych wynikających w szczególności z ustaw: o służbie cywilnej, o pracownikach sądów i prokuratury, Kodeksu Pracy, RODO oraz ustawy o ochronie danych osobowych i może pociągnąć za sobą skutki dyscyplinarne oraz spowodować pociągnięcie sprawcy do odpowiedzialności wynikającej z przepisów prawa i regulaminu pracy w Ministerstwie Sprawiedliwości.

22. Słownik pojęć

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

ADO – Administrator Danych Osobowych – (Administrator) zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO) oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania,

Aktywa – wszystko, co ma wartość dla organizacji,

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

Aktywa wspierające – wyposażenie oraz podstawowe usługi techniczne,

Autoryzacja – potwierdzenie czy uwierzytelniony podmiot jest uprawniony do korzystania z danego zasobu,

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 – w Ministerstwie Sprawiedliwości,

Dokument – każdą utrwaloną, w różnej postaci, treść stanowiącą dowód prawa, stosunku prawnego, okoliczności mającej znaczenie prawne lub zawierającą oświadczenie woli lub wiedzy podmiotu, od którego pochodzi,

Dokumentacja administracyjna - dokumentacja techniczna systemu informatycznego - zbiór dokumentów opisujących techniczne aspekty w tym: architektura danych, architektura techniczna, infrastruktura techniczna i licencyjna, itp.

Dostępność – właściwość bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu,
Grupy zabezpieczeń – grupy czynności zabezpieczających (na podstawie PN-ISO/IEC 27001)

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 – 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,

Integralność – właściwość polegająca na zapewnieniu dokładności i kompletności aktywów,

Jednostka organizacyjna (urząd) – Ministerstwo Sprawiedliwości,

Klauzula klasyfikacyjna – ważność zasobów (dopuszczalne wartości: wysoka, średnia, niska),

Komórka organizacyjna – departament lub równorzędną komórkę organizacyjną określoną w statucie Ministerstwa Sprawiedliwości,

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

Obszar bezpieczny – wydzielone i chronione pomieszczenie lub jego część, część budynku lub cały budynek (np. serwerownia, punkt dystrybucyjny, biuro obsługi klienta),

PBI – Polityka Bezpieczeństwa Informacji,

Podatność na zagrożenia – problem dotyczący bezpieczeństwa, który może zostać wykorzystany przez zagrożenie i skutkować naruszeniem bezpieczeństwa informacji w postaci uzyskania nieautoryzowanego dostępu, odmowy usługi przez system itp.,

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

Pracownik – osoba będąca w stosunku pracy z Ministerstwem Sprawiedliwości,

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)

Ryzyko – kombinacja prawdopodobieństwa zdarzenia i jego konsekwencji,

Sieć telekomunikacyjna – urządzenia telekomunikacyjne i linie telekomunikacyjne, zestawione i połączone w sposób umożliwiający przekaz sygnałów pomiędzy określonymi zakończeniami sieci, za pomocą przewodów, fal radiowych bądź optycznych lub innych środków wykorzystujących energię elektromagnetyczną,

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,

SZBI – System Zarządzania Bezpieczeństwem Informacji,

Umowa o zachowanie poufności – legalnie zawarta umowa, pomiędzy co najmniej dwiema stronami, które obowiązują się do wymiany poufnych materiałów lub wiedzy z zastrzeżeniem ich dalszego nierozpowszechniania,

Ustawa - ustawa z dnia 10 maja 2018 roku o ochronie danych osobowych,

Uwierzytelnianie – proces polegający na zweryfikowaniu zadeklarowanej tożsamości osoby, urządzenia bądź usługi biorącej udział w wymianie danych,

Użytkownik – osoba, która posiada konto w systemie Ministerstwa Sprawiedliwości,

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

Właściciel informacji- osoba/organ, z którym wiąże się odpowiedzialność za wytwarzanie, przetwarzanie i wykorzystanie informacji, w tym podejmowanie decyzji o udzielaniu pracownikom prawa dostępu do tych informacji,

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

Zapewnienie ciągłości działania – postępowanie w celu przeciwdziałania przerwom w działalności Ministerstwa Sprawiedliwości oraz ochrona krytycznych procesów przed rozległymi awariami lub katastrofami,

Zasoby – patrz aktywa,

Zasoby informacyjne – patrz aktywa informacyjne,

Złośliwy kod – kod, który poprzez luki w oprogramowaniu jest w stanie samodzielnie się rozprzestrzeniać wbrew woli użytkowników oraz nieść zagrożenie dla systemów teleinformatycznych.