Warszawa, dnia 15 marca 2022 r.

Poz. 19

Z A R Z Ą D Z E N I E

M I N I S T R A F I N A N S Ó W [1)]

z dnia 10 marca 2022 r.

w sprawie Systemu Zarządzania Bezpieczeństwem Informacji i Polityki Bezpieczeństwa Informacji Resortu Finansów

Na podstawie art. 34 ust. 1 ustawy z dnia 8 sierpnia 1996 r. o Radzie Ministrów (Dz. U. z 2021 r. poz. 178, 1192, 1535 i 2105) zarządza się, co następuje:

§ 1. 1. Tworzy się System Zarządzania Bezpieczeństwem Informacji, zwany dalej „SZBI”, zgodny z wymogami normy PN – ISO/IEC 27001 w:

1) Ministerstwie Finansów;
2) izbach administracji skarbowej;
3) urzędach skarbowych;
4) urzędach celno-skarbowych wraz z podległymi oddziałami celnymi;
5) Krajowej Informacji Skarbowej;
6) Krajowej Szkole Skarbowości;
7) Centrum Informatyki Resortu Finansów;
8) delegaturach jednostek organizacyjnych Krajowej Administracji Skarbowej utworzonych przez ministra właściwego do spraw finansów publicznych na podstawie art. 36 ust. 2 ustawy z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej (Dz. U. z 2021 r. poz. 422, z późn. zm.[2]).

2. W jednostkach, o których mowa w ust. 1, wprowadza się Politykę Bezpieczeństwa Informacji Resortu Finansów, zwaną dalej „Polityką”, stanowiącą załącznik do zarządzenia.

---

1) Minister Finansów kieruje działem administracji rządowej – finanse publiczne, na podstawie § 1 ust. 2 pkt 2 rozporządzenia Prezesa Rady Ministrów z dnia 27 października 2021 r. w sprawie szczegółowego zakresu działania Ministra Finansów (Dz. U. poz. 1947).

2) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2021 r. poz. 464, 694, 802, 815, 954, 1005, 1718, 2076 i 2105.

3. Do stosowania Polityki są obowiązane komisje, rady, zespoły i inne podmioty, w tym centra kompetencyjne, działające w Ministerstwie Finansów oraz jednostkach, o których mowa w § 1 ust. 1 pkt 2-8.

§ 2. 1. Kierujący komórkami organizacyjnymi w Ministerstwie Finansów oraz w jednostkach, o których mowa w § 1 ust. 1 pkt 2-8, zapoznają podległych pracowników i funkcjonariuszy pełniących służbę w Ministerstwie Finansów oraz w tych jednostkach z treścią Polityki w terminie 3 miesięcy od dnia wejścia w życie zarządzenia.

2. Fakt zapoznania się z treścią Polityki potwierdza się przez złożenie oświadczenia, o którym mowa w § 5 ust. 11 Polityki.

3. W terminie 6 miesięcy od dnia wejścia w życie zarządzenia jednostki, o których mowa w § 1 ust. 1 pkt 2-8, posiadające w dniu jego wejścia w życie odrębne polityki bezpieczeństwa informacji, dokonają ich przeglądu i aktualizacji, w celu zachowania spójności z Polityką oraz opracują dokumentację SZBI w zakresie określonym § 6 ust. 3 Polityki.

§ 3. Traci moc zarządzenie nr 54 Ministra Finansów z dnia 24 grudnia 2013 r. w sprawie zatwierdzenia do stosowania „Księgi Bezpieczeństwa Informacji Ministerstwa Finansów” i „Deklaracji Stosowania Zabezpieczeń w Ministerstwie Finansów”.

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

Minister Finansów: wz. A. Soboń

Załącznik do zarządzenia
Ministra Finansów
z dnia ……2022 r.
(poz. ……)

POLITYKA BEZPIECZEŃSTWA INFORMACJI RESORTU FINANSÓW

SPIS TREŚCI

Rozdział 1

Postanowienia ogólne

§ 1. 1. Polityka określa zasady zarządzania bezpieczeństwem informacji we wszystkich obszarach wskazanych w załączniku A do normy ISO 27001 oraz wypracowania szczegółowych polityk dla Ministerstwa oraz Jednostek, o których mowa w § 6 ust. 2.

2. Określone w Polityce zasady zarządzania bezpieczeństwem informacji w Resorcie Finansów zostały opracowane zgodnie z obowiązującymi przepisami prawa oraz w oparciu o wymagania Polskich i Międzynarodowych Norm i standardów w obszarze bezpieczeństwa informacji, a także wewnętrzne akty normatywne w szczególności:

1) rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 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/RODO);
2) ustawę z dnia 16 kwietnia 1993 r o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2020 r. poz. 1913, z późn. zm.);
3) ustawę z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2021 r. poz. 1062);
4) ustawę z dnia 21 sierpnia 1997 r. o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne (Dz. U. z 2019 r. poz. 2399, z późn. zm.);
5) ustawę z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125);
6) ustawę z dnia 29 sierpnia 1997 r. - Ordynacja podatkowa (Dz. U. z 2021 r. poz. 1540, z późn. zm.);
7) ustawę z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2020 r. poz. 2176, z późn. zm.);
8) ustawę z dnia 19 marca 2004 r. - Prawo celne (Dz. U. z 2021 r. poz. 1856);
9) ustawę z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2021 r. poz. 2070, z późn. zm.);
10) ustawę o Krajowej Administracji Skarbowej z dnia 16 listopada 2016 r.;
11) ustawę z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. 2021 r. poz. 1132, z późn. zm.);
12) ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781);
13) ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369, z późn. zm.);
14) ustawę z dnia 22 listopada 2018 r. o dokumentach publicznych (Dz. U. z 2021 r. poz. 1660, z późn. zm.);

15) ustawę z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego (Dz. U. poz. 1641);
16) rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 stycznia 2007 r. w sprawie Biuletynu Informacji Publicznej (Dz. U. poz. 68);
17) 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 (Dz. U. z 2017 r. poz. 2247);
18) rozporządzenie Rady Ministrów z dnia 12 marca 2014 r. w sprawie Centralnego Repozytorium Informacji Publicznej (Dz. U. poz. 361, z późn. zm.);
19) rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 2 lipca 2019 r. w sprawie wymagań w zakresie bezpieczeństwa wytwarzania blankietów dokumentów publicznych (Dz. U. poz. 1266);
20) rozporządzenie Rady Ministrów z dnia 11 lipca 2019 r. w sprawie wykazu dokumentów publicznych (Dz. U. poz. 1289, z późn. zm.);
21) zarządzenie Ministra Finansów z dnia 31 stycznia 2022 r. w sprawie ustalenia regulaminu organizacyjnego Ministerstwa Finansów (Dz. Urz. Min. Fin. poz. 8), zwane dalej „Regulaminem organizacyjnym Ministerstwa”;
22) Polskimi i Międzynarodowymi Normami:
    a) PN-ISO/IEC 27001 - Technika informatyczna – Techniki bezpieczeństwa – Systemy Zarządzania bezpieczeństwem informacji – Wymagania,
    b) PN-ISO/IEC 27002 - Technika informatyczna - Techniki bezpieczeństwa - Praktyczne zasady zabezpieczania informacji,
    c) PN-ISO/IEC 27005 - Technika informatyczna - Techniki bezpieczeństwa - Zarządzanie ryzykiem w bezpieczeństwie informacji.

Słownik pojęć

§ 2. Użyte w Polityce pojęcia oznaczają:

1) Administrator - Ministra, Szefa Krajowej Administracji Skarbowej, Generalnego Inspektora Informacji Finansowej – każdy w zakresie danych osobowych, dla których jest administratorem w rozumieniu art. 4 pkt 7 RODO;
2) ASI - Administratora Systemu Teleinformatycznego;
3) AZU – Administratora Zarządzającego Uprawnieniami;
4) aktywa – wszystko, co posiada wartość dla organizacji; ludzie, umiejętności, informacje, dane, technologie, urządzenia, obiekty, które są niezbędne do prowadzenia działania i osiągania celów organizacji;

5) aktywa informacyjne - wszelkie informacje będące własnością, administrowane lub wykorzystywane przez Ministerstwo i Jednostki, niezależnie od postaci (papierowej, cyfrowej, jak i niematerialnej w postaci wiedzy posiadanej przez pracowników) i sposobu ich przetwarzania, mające zasadnicze znaczenie dla osiągnięcia celów Ministerstwa i Jednostek, a tym samym odpowiednio chronione, w szczególności przed utratą dostępności, poufności i integralności;
6) analiza ryzyka - proces dążący do poznania charakteru ryzyka oraz określenia poziomu ryzyka (wielkości ryzyka);
7) BAD – komórka organizacyjna Ministerstwa właściwa do spraw gospodarowania mieniem Ministerstwa;
8) BDG – komórka organizacyjna Ministerstwa właściwa do prowadzenia spraw wynikających ze stosunku pracy osób zatrudnionych w Ministerstwie;
9) bezpieczeństwo informacji - zachowanie integralności, dostępności, poufności rozliczalności, autentyczności przetwarzanych informacji;
10) BKA – komórka organizacyjna Ministerstwa właściwa w sprawach prowadzenia audytu wewnętrznego;
11) ciągłość działania - zdolność organizacji do realizacji zadań organizacji i świadczenia usług na akceptowanym, wcześniej zdefiniowanym, poziomie po wystąpieniu incydentu zakłócającego działanie;
12) CSIRT GOV - Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego;
13) dane osobowe – wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
14) DB – komórka organizacyjna Ministerstwa właściwa w sprawach zarządzania bezpieczeństwem informacji;
15) DIP – komórka organizacyjna Ministerstwa właściwa w sprawach koordynowania i monitorowania w Ministerstwie działań w obszarze IT, w tym priorytetyzację usług na rzecz Ministerstwa;
16) dostępność – właściwość polegająca na zapewnieniu, że osoby upoważnione mają dostęp do informacji wtedy, gdy jest to potrzebne;

17) incydent bezpieczeństwa informacji - pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań organizacji i zagrażają bezpieczeństwu informacji;
18) informatyczny nośnik danych - materiał lub urządzenie służące do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej;
19) IOD – Inspektor Ochrony Danych, powołany przez każdego z Administratorów;
20) integralność - właściwość polegająca na zapewnieniu dokładności i kompletności informacji;
21) Jednostki – następujące jednostki organizacyjne:
    a) izby administracji skarbowej;
    b) urzędy skarbowe;
    c) urzędy celno-skarbowych wraz z podległymi oddziałami celnymi;
    d) Krajową Informację Skarbową;
    e) Krajowa Szkołę Skarbowości;
    f) Centrum Informatyki Resortu Finansów;
    g) delegatury jednostek organizacyjnych Krajowej Administracji Skarbowej utworzone przez ministra właściwego do spraw finansów publicznych na podstawie art. 36 ust. 2 ustawy z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej;
22) Kierownictwo Ministerstwa – Ministra, Sekretarzy Stanu, Podsekretarzy Stanu oraz Dyrektora Generalnego Ministerstwa;
23) kierujący Jednostką - kierujący jednostką organizacyjną, o której mowa w pkt 21;
24) komórka organizacyjna - departament albo biuro w Ministerstwie lub równorzędna komórka organizacyjna w Jednostce;
25) Minister - ministra właściwego do spraw budżetu państwa, finansów publicznych oraz instytucji finansowych;
26) Ministerstwo - Ministerstwo Finansów;
27) monitorowanie - bieżąca weryfikacja poprawności działania systemu teleinformatycznego lub realizacji procesu, prowadzona niezależnie od okresowych działań audytowych;
28) obsługa incydentu - czynności umożliwiające rejestrowanie, analizowanie, klasyfikowanie, priorytetyzację, podejmowanie działań naprawczych i ograniczenie skutków incydentu;
29) ocena ryzyka - proces porównywania wyników analizy ryzyka z kryteriami ryzyka w celu stwierdzenia, czy ryzyko lub jego wielkość są akceptowalne lub tolerowane; ocena ryzyka wspomaga podejmowanie decyzji w zakresie postępowania z ryzykiem;
30) podatność - słabość, luka, brak odpowiednich zabezpieczeń informacji przed występującymi zagrożeniami;
31) Polityka - Polityka Bezpieczeństwa Informacji Resortu Finansów;

32) PBF - Polityka Bezpieczeństwa Fizycznego Ministerstwa Finansów;
33) PBSO - Polityka Bezpieczeństwa Spraw Osobowych Ministerstwa Finansów;
34) PBT - Polityka Bezpieczeństwa Teleinformatycznego Resortu Finansów;
35) PZCD - Polityka Zarządzania Ciągłością Działania;
36) PODO - Polityka Ochrony Danych Osobowych;
37) poufność - właściwość polegająca na tym, że informacja nie jest udostępniana nieupoważnionym osobom, podmiotom lub procesom;
38) postępowanie z ryzykiem - proces polegający na wyborze i wdrożeniu środków modyfikujących ryzyko lub wpływających na zmianę wielkości ryzyka;
39) pracownik - osoba fizyczna realizująca zadania na rzecz Ministerstwa lub Jednostki na podstawie umowy o pracę, powołania, mianowania albo umowy cywilnoprawnej lub pełniąca w nich służbę, w tym funkcjonariusz Służby Celno-Skarbowej, oraz praktykant, stażysta lub wolontariusz;
40) prawdopodobieństwo - możliwość wystąpienia zdarzenia;
41) przetwarzanie - wszelkie operacje wykonywane na danych i informacjach w sposób zautomatyzowany lub niezautomatyzowany, takie jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie przez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
42) PZIBI - Polityka Zarządzania Incydentami Bezpieczeństwa Informacji w Resorcie Finansów;
43) Resort Finansów – Ministerstwo Finansów oraz Jednostki;
44) rozliczalność – właściwość zapewniająca, że działania osoby albo podmiotu mogą być przypisane w sposób jednoznaczny tylko tej osobie albo temu podmiotowi oraz pozwalająca umiejscowić je w czasie;
45) rozporządzenie KRI – 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;
46) ryzyko – potencjalna sytuacja, w której określone zdarzenie może wykorzystać podatność aktywów lub grupy aktywów, powodując w ten sposób szkodę dla organizacji;
46) słabość systemu – podatność systemu, która może być wykorzystana przez zagrożenie do naruszenia poufności, integralności lub dostępności;
48) 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 2021 r. poz. 576, z późn. zm.);

49) SZBI – System Zarządzania Bezpieczeństwem Informacji, będący częścią systemu zarządzania, oparty na podejściu wynikającym z ryzyka biznesowego, odnoszący się do ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymania i doskonalenia bezpieczeństwa informacji w celu osiągnięcia celów biznesowych organizacji;
50) szacowanie ryzyka – całościowy proces identyfikacji, analizy i oceny ryzyka;
51) użytkownik – pracownik lub inna osoba, która uzyskała uprawnienie do dostępu i przetwarzania informacji w systemach teleinformatycznych;
52) właściciel biznesowy danych – komórka organizacyjna odpowiedzialna merytorycznie za przetwarzanie danych i informacji, w tym danych osobowych, w zakresie wynikającym z zadań określonych w Regulaminie organizacyjnym Ministerstwa lub Jednostki. Właściciel biznesowy danych może być jednocześnie właścicielem biznesowym systemu teleinformatycznego, w którym te dane są przetwarzane;
53) właściciel biznesowy systemu teleinformatycznego – komórka organizacyjna odpowiedzialna za wykonanie zadań właściciela biznesowego systemu teleinformatycznego, określonych w Regulaminie organizacyjnym Ministerstwa lub Jednostki;
54) zabezpieczenie – środek ochrony, który ma na celu minimalizację ryzyka;
55) zagrożenie – potencjalna przyczyna niepożądanego incydentu, który może wywołać szkodę w systemie lub organizacji;
56) zarządzanie ryzykiem – skoordynowane działania dotyczące kierowania i nadzorowania organizacji w odniesieniu do ryzyka mające na celu identyfikację zagrożeń i podatności, minimalizacji zagrożeń do poziomu ryzyka akceptowalnego przez zastosowanie zabezpieczenia lub zabezpieczeń;
57) zdarzenie związane z bezpieczeństwem informacji – stwierdzone wystąpienie stanu systemu, usługi lub sieci, który wskazuje na możliwe naruszenie polityki bezpieczeństwa informacji lub błąd zabezpieczenia, lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem informacji.

Deklaracja Kierownictwa

§ 3. 1. Informacje są jednym z najważniejszych aktywów Resortu Finansów niezbędnym do realizacji jego ustawowych zadań. W związku z tym rozumie konieczność zapewnienia odpowiedniego poziomu ochrony informacji przetwarzanych w Resorcie Finansów zarówno dla zachowania wysokiego poziomu bezpieczeństwa informacji, jak również w celu spełnienia wymagań prawnych dotyczących ochrony informacji, w szczególności informacji prawnie chronionych.

2. Mając na uwadze powyższe, Minister:

1) wspiera procesy zmierzające do zapewnienia bezpieczeństwa informacji w Resorcie Finansów;
2) wspiera DB w wypełnianiu zadań, przez zapewnienie zasobów niezbędnych do ich wykonania i utrzymania wiedzy fachowej;
3) zapewnia środki do wdrożenia w Ministerstwie, w obszarach objętych SZBI, zabezpieczeń organizacyjnych i technicznych mających na celu spełnienie wymogów określonych w przepisach prawa, adekwatnych i proporcjonalnych do kategorii przetwarzanych informacji oraz dopasowanych do poziomu występujących zagrożeń i wyników szacowania ryzyka;
4) wspiera utrzymywanie i ciągłe doskonalenie SZBI zgodnie z wymaganiami normy PN-ISO/IEC 27001.

Cel Polityki

§ 4. 1. Celem Polityki jest zapewnienie odpowiedniej ochrony informacji przetwarzanych w Resorcie Finansów, ze szczególnym uwzględnieniem zachowania ich poufności, dostępności i integralności oraz rozliczalności, a także zapewnienie ciągłości przetwarzania informacji.

2. Powyższy cel jest realizowany przez następujące działania:

1) określenie ogólnych zasad i wymagań w zakresie ochrony informacji, stanowiących podstawę do wdrożenia jednolitego dla Resortu Finansów SZBI;
2) określenie sposobu organizacji SZBI w Resorcie Finansów;
3) określenie zadań i odpowiedzialności osób uczestniczących w procesie przetwarzania informacji oraz zarządzania bezpieczeństwem informacji;
4) przeprowadzenie inwentaryzacji aktywów informacyjnych oraz wyznaczenie ich właścicieli odpowiedzialnych za zapewnienie właściwego poziomu ochrony aktywów;
5) kategoryzację informacji oraz wdrożenie zasad postępowania z poszczególnymi grupami informacji i ich ochrony;
6) wdrożenie i utrzymanie adekwatnych do zagrożeń i wyników szacowania ryzyka zabezpieczeń organizacyjnych i technicznych;
7) zapewnienie realizacji audytów bezpieczeństwa informacji oraz ocen skuteczności i efektywności SZBI;
8) dokonywanie przeglądów i utrzymanie aktualnych polityk i procedur oraz pozostałej dokumentacji SZBI;
9) budowanie świadomości pracowników w obszarze bezpieczeństwa informacji oraz kompetencji osób zaangażowanych w zarządzanie bezpieczeństwem informacji;
10) reagowanie na zagrożenia i incydenty w obszarze bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań zapobiegawczych i korygujących;
11) zapewnienie gotowości do reakcji na sytuacje awaryjne i możliwości sprawnego odtworzenia aktywów informacyjnych w przypadku ich zniszczenia;

12) ciągłe doskonalenie systemu zarządzania bezpieczeństwem informacji zgodnie z wymaganiami normy PN-ISO/IEC 27001.

Zakres stosowania

§ 5. 1. SZBI w Resorcie Finansów obejmuje następujące obszary:

1) dokumentację bezpieczeństwa, w tym polityki, procedury i instrukcje regulujące zasady bezpieczeństwa informacji;
2) organizację bezpieczeństwa informacji;
3) zarządzanie aktywami, w tym klasyfikację informacji;
4) bezpieczeństwo zasobów ludzkich;
5) bezpieczeństwo fizyczne i środowiskowe;
6) bezpieczeństwo teleinformatyczne;
7) relacje z podmiotami zewnętrznymi;
8) aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania;
9) zarządzania incydentami bezpieczeństwa informacji.

2. Polityką są objęte wszystkie informacje wykorzystywane przez Resort Finansów niezależnie od formy i sposobu ich przetwarzania, w tym utrwalone na informatycznych nośnikach danych, w systemach teleinformatycznych oraz wytworzone w postaci papierowej, będące własnością Resortu Finansów, administrowane lub powierzone Resortowi Finansów w ramach umów lub porozumień z kontrahentami lub wykonawcami.

3. Określone w Polityce zasady są zgodne z przepisami prawa regulującymi ochronę informacji prawnie chronionych.

4. Obowiązujące w Resorcie Finansów regulacje wewnętrzne należy procedować i wdrażać z uwzględnieniem zasad zapewniających ochronę aktywów informacyjnych, w szczególności określonych w Polityce.

5. Polityka ma zastosowanie do wszystkich komórek organizacyjnych Ministerstwa oraz Jednostek. Polityka ma również zastosowanie do podmiotu zewnętrznego, który na mocy zawartej umowy lub porozumienia, uzyskał dostęp i przetwarza informacje Resortu Finansów w celu i zakresie niezbędnym do realizacji zleconych mu zadań, o ile taki warunek został wskazany w zawartej umowie lub porozumieniu.

6. Polityka obejmuje zakresem:

1) budynki i znajdujące się w nich pomieszczenia użytkowane przez Ministerstwo i Jednostki, w których aktywa informacyjne są przetwarzane , w tym:
   a) miejsca, w których są wykonywane operacje na informacjach, realizowane w postaci papierowej lub elektronicznej, w tym w systemach teleinformatycznych,

b) miejsca, w których przechowuje się wszelkie nośniki informacji, w szczególności dokumentację papierową, przenośne informatyczne nośniki danych, urządzenia służące do przetwarzania informacji, w tym komputery, serwery, macierze dyskowe,

c) pomieszczenia, gdzie są składowane uszkodzone informatyczne nośniki danych zawierające informacje,

d) pomieszczenia i ciągi komunikacyjne, w których są eksploatowane urządzenia służące do wydruku, kopiowania, skanowania lub niszczenia dokumentów;

2) miejsca, w których aktywa informacyjne są przetwarzane poza siedzibą Ministerstwa lub Jednostki, w szczególności w przypadku zdalnego korzystania z sieci komputerowej Resortu Finansów i zdalnego dostępu do systemów Resortu Finansów, w tym w ramach telepracy i pracy zdalnej.

7. W Ministerstwie stosuje się adekwatne do szacowania ryzyka zabezpieczenia we wszystkich obszarach wskazanych w załączniku A do normy ISO 27001.

8. Jednostki dokonują analizy celów i stosowanych zabezpieczeń w odniesieniu do załącznika A normy ISO 27001 i przygotowują deklarację stosowania zabezpieczeń przez Jednostkę, zawierającą informacje o ewentualnych wyłączeniach wraz z uzasadnieniem. Deklaracja wymaga formalnego zatwierdzenia przez kierującego Jednostką.

9. Do przestrzegania Polityki są obowiązane wszystkie osoby korzystające z aktywów informacyjnych Resortu Finansów, w szczególności:

1) pracownicy Resortu Finansów;

2) osoby realizujące usługi na rzecz Resortu Finansów na podstawie zawartych umów cywilnoprawnych;

3) pracownicy podmiotów zewnętrznych, realizujący usługi na rzecz Resortu Finansów na podstawie zawartych umów lub porozumień – w zakresie określonym w umowie lub porozumieniu.

10. Za zapoznanie się z Polityką osób, o których mowa w ust. 9, odpowiada:

1) kierujący komórką organizacyjną, w której pracownik będzie zatrudniony lub wskazana przez niego osoba, w przypadku osób, o których mowa w ust. 9 pkt 1;

2) kierujący komórką organizacyjną odpowiedzialny za realizację umowy lub porozumienia lub wskazana przez niego osoba, w przypadku osób, o których mowa w ust. 9 pkt 2 i 3.

11. Osoby, o których mowa w ust. 9, są obowiązane do złożenia własnoręcznie podpisanego oświadczenia o zapoznaniu z treścią Polityki przed rozpoczęciem wykonywania przez nie zadań służbowych lub świadczenia usług. Wzór oświadczenia określa i udostępnia w Intranecie dyrektor DB. Wzór oświadczenia stanowi załącznik do zawartej umowy lub porozumienia.

12. Oświadczenie, o którym mowa w ust. 11, jest przechowywane:

1) w aktach osobowych, w przypadku osób pozostających w stosunku pracy albo służby w Resorcie Finansów;
2) z dokumentami, na podstawie których odbywa się praktyka, staż lub wolontariat, w przypadku praktykantów, stażystów i wolontariuszy;
3) z umową lub porozumieniem przez komórkę organizacyjną odpowiedzialną za realizację danej umowy lub porozumienia, w przypadku osób, o których mowa w ust. 9 pkt 2 i 3.

Rozdział 2

Dokumentacja SZBI

§ 6. 1. Polityka jest dokumentem podstawowym w zakresie zasad bezpieczeństwa informacji w Resorcie Finansów w poszczególnych obszarach, o których mowa w § 5 ust. 1. Przepisy Polityki należy uwzględniać w procesie opracowania dokumentacji SZBI, o której mowa w ust. 2 pkt 1-8.

2. Dokumentacja SZBI Resortu Finansów obejmuje Politykę oraz:

1) polityki szczegółowe, w tym:
   a)PBT,
   b)PBF oraz polityki bezpieczeństwa fizycznego Jednostek,
   c)PZIBI,
   d)PZCD,
   e)PODO,
   f)PBSO oraz polityki bezpieczeństwa spraw osobowych Jednostek;
2) deklaracje stosowania zabezpieczeń;
3) metodyki:
   a) analizy ryzyka w bezpieczeństwie informacji (RA),
   b) analizy wpływu na działalność (BIA);
4) procedury i instrukcje bezpieczeństwa informacji, określające zasady postępowania i mechanizmy kontroli w obszarach, o których mowa w § 5 ust. 1;
5) wytyczne wydawane przez DB;
6) roczne plany szkoleń z zakresu bezpieczeństwa informacji;
7) roczne plany audytów wewnętrznych w zakresie bezpieczeństwa informacji;
8) przygotowywaną w ramach Ministerstwa i Jednostek dokumentację:
   a) z cyklicznych przeglądów SZBI,
   b) z szacowania ryzyka w bezpieczeństwie informacji, akceptacji ryzyka i postępowania z ryzykiem,
   c) audytów bezpieczeństwa informacji, w tym zalecenia i sposób ich realizacji,
   d) incydentów bezpieczeństwa informacji,
   e) zarządzania uprawnieniami do pracy w systemach teleinformatycznych,

f) zarządzania aktywami informacyjnymi,

g) szkoleń osób zaangażowanych w proces przetwarzania informacji i zarządzania bezpieczeństwem informacji,

h) upoważnienia do przetwarzania określonych grup informacji, związane z nimi oświadczenia i ewidencje.

3. Jednostki opracowują dokumentację SZBI obejmującą:

1) deklarację stosowania zabezpieczeń;
2) zależnie od specyfiki zadań Jednostki - polityki szczegółowe w zakresie nie objętym politykami Resortu Finansów wskazanymi w ust. 2 pkt 1;
3) procedury, o których mowa w ust. 2 pkt 4, w zakresie nie objętym procedurami Resortu Finansów.

4. Ministerstwo i Jednostki opracowują corocznie, plan szkoleń i plan audytów, o których mowa w ust. 2 pkt 6 i 7.

Zasady rozpowszechniania dokumentacji SZBI

§ 7. 1. Dokumentacja SZBI, o której mowa w § 6 ust. 1 i ust. 2 pkt 1-4, podlega rejestracji, akceptacji i zatwierdzeniu przez upoważnione osoby.

2. Udostępnianie dokumentacji SZBI podlega ograniczeniu zgodnie z zasadą wiedzy koniecznej.

3. Dokumentacja SZBI może być udostępniana w całości lub części, osobom albo podmiotom zewnętrznym, realizującym na podstawie zwartych umów lub porozumień na rzecz Resortu Finansów lub we współpracy z Ministerstwem lub Jednostkami określone zadania, zgodnie z zasadą wiedzy koniecznej i po uzyskaniu oświadczenia o zachowaniu w poufności uzyskanych informacji.

4. Dokumentacja SZBI jest udostępniania w wersji obowiązującej.

5. Właściciel biznesowy dokumentacji SZBI odpowiada za:

1) opracowanie dokumentu;
2) uzgodnienie treści z właściwymi komórkami organizacyjnymi Ministerstwa lub Jednostkami, w tym uzyskanie akceptacji dyrektora DB;
3) przegląd i aktualizację;
4) prowadzenie rejestru dokumentacji;
5) przechowywanie i archiwizację dokumentacji zgodnie z wymogami Instrukcji kancelaryjnej i JRWA;
6) udostępnienie dokumentacji w Intranecie lub udostępnienie określonym pracownikom i osobom albo podmiotom zewnętrznym zgodnie z zasadami określonymi w ust. 3 i 4.

6. Wzór rejestru, o którym mowa w ust. 6 pkt 4, określa i udostępnia w Intranecie dyrektor DB.

7. Właścicielem biznesowym Polityki jest DB.

8. Na wniosek dyrektora DB, w tym w związku z prowadzonym przeglądem zarządzania bezpieczeństwem informacji, właściciele biznesowi dokumentacji SZBI są obowiązani do przekazania aktualnych rejestrów dokumentacji i dokumentów w nich wskazanych.

Rozdział 3

Obszary SZBI

Bezpieczeństwo spraw osobowych

§ 8. 1. Obszar bezpieczeństwa zasobów ludzkich obejmuje zasady w zakresie ochrony informacji na wszystkich etapach zarządzania personelem, począwszy od procesu naboru, przez zatrudnienie, zmiany stanowiska lub zakresu obowiązków, po zakończenie zatrudnienia.

2. Zarządzania bezpieczeństwem zasobów ludzkich ma na celu:

1) zapewnienie, że pracownicy rozumieją swoją odpowiedzialność i posiadają odpowiednią wiedzę i kwalifikacje, umożliwiające im należyte zabezpieczenie informacji, przetwarzanych w ramach realizowanych przez nich zadań;
2) zapewnienie, że pracownicy są świadomi swoich obowiązków dotyczących bezpieczeństwa informacji i je wypełniają;
3) zabezpieczenie interesów Resortu Finansów, w tym ochronę aktywów informacyjnych, w trakcie procesu zmiany stanowiska pracy lub zakończenia zatrudnienia.

3. Szczegółowe zasady dotyczące zarządzania bezpieczeństwem informacji w ramach procesów kadrowych w Ministerstwie są zawarte w PBSO.

4. Właścicielem biznesowym PBSO są zgodnie z właściwością komórki organizacyjne Ministerstwa właściwe w sprawach zarządzania zasobami ludzkimi.

6. Jednostki opracowują polityki i procedury w obszarze bezpieczeństwa zasobów ludzkich, przy uwzględnieniu wymogów określonych w ust. 1 i 2.

Ochrona danych osobowych

§ 9. 1. Obszar ochrony danych osobowych obejmuje zasady związane z przetwarzaniem, zarządzaniem i ochroną danych osobowych.

2. Szczegółowe zasady określające sposób postępowania gwarantujący bezpieczeństwo przetwarzanych w Resorcie Finansów danych osobowych, określone są w PODO.

3. Właścicielem biznesowym PODO jest DB.

Bezpieczeństwo fizyczne

§ 10. 1. Obszar bezpieczeństwa fizycznego i środowiskowego obejmuje zasady związane z zapewnieniem ochrony informacji przed dostępem osób nieuprawnionych, uszkodzeniem lub

zniszczeniem aktywów służących do przetwarzania informacji lub innymi zakłóceniami w siedzibie Ministerstwa lub Jednostki, przez:

1) stosowanie środków bezpieczeństwa fizycznego, obejmujących w szczególności:
   a) rozmieszczenie i granice stref bezpieczeństwa,
   b) zabezpieczenia wejść do obiektu oraz do stref bezpieczeństwa,
   c) system sygnalizacji włamania i napadu,
   d) system monitoringu wizyjnego,
   e) system elektronicznej kontroli dostępu,
   f) mechaniczne zabezpieczenia obiektów i pomieszczeń;
2) stosowanie środków bezpieczeństwa środowiskowego, obejmujących w szczególności:
   a) systemy przeciwpożarowe i gaśnicze,
   b) zabezpieczenie przed zalaniem,
   c) systemy klimatyzacji i wentylacji,
   d) systemy monitorowania warunków temperatury i wilgotności powietrza,
   e) środki ochrony odgromowej na liniach telekomunikacyjnych,
   f) zabezpieczenia przeciwprzepięciowe i przeciwprzeciążeniowe,
   g) systemy awaryjnego zasilania;
3) zapewnienie, że kluczowe systemy techniczne i teleinformatyczne są wyposażone w zabezpieczenia utrzymujące optymalne warunki środowiskowe i podtrzymujące zasilanie;
4) zapewnienie bezpieczeństwa okablowania teletechnicznego;
5) stosowanie zabezpieczeń organizacyjnych, w szczególności dotyczących:
   a) zasad dostępu do obszarów i pomieszczeń,
   b) zasad organizacji ruchu osób, materiałów i pojazdów,
   c) stosowania bezpośredniej ochrony fizycznej.

2. Szczegółowe wymagania dotyczące stosowania w Resorcie Finansów fizycznych i środowiskowych środków ochrony informacji, a także odpowiedzialność w tym zakresie, są określone w politykach szczegółowych:

1) PBF i politykach bezpieczeństwa fizycznego Jednostek;
2) PBT;
3) PZCD.

3. Zakres stosowania środków bezpieczeństwa fizycznego i środowiskowego wynika z przeprowadzonego i udokumentowanego szacowania ryzyka.

4. Właścicielem biznesowym PBF jest DB.

5. Za opracowanie polityki i procedur związanych z zapewnieniem bezpieczeństwa fizycznego serwerowni i infrastruktury teleinformatycznej odpowiada Centrum Informatyki Resortu Finansów, zwane dalej „CIRF”.

6. Jednostki opracowują własne polityki i procedury w zakresie bezpieczeństwa fizycznego przy uwzględnieniu wymogów określonych w ust. 1, oraz uwarunkowań związanych w szczególności z położeniem siedziby Jednostki, typem obiektu oraz występującymi zagrożeniami lokalnymi.

Bezpieczeństwo teleinformatyczne

§ 11. 1. Obszar bezpieczeństwa teleinformatycznego obejmuje zasady związane z zapewnieniem niezawodności systemów teleinformatycznych, a także ochrony aktywów informacyjnych przetwarzanych w systemach teleinformatycznych, w tym zachowania poufności, integralności i dostępności danych w nich przetwarzanych oraz zapewnienia rozliczalności działań użytkowników w systemach, w szczególności dotyczące:

1) utrzymania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji;
2) aktualizacji oprogramowania;
3) usystematyzowanego tworzenia i testowania kopii zapasowych;
4) zarządzania uprawnieniami użytkowników, w tym administratorów;
5) uwierzytelniania użytkowników w systemach;
6) bezpiecznego pozyskiwania, rozwoju i utrzymania systemów teleinformatycznych, w tym kontroli systemów, przed dopuszczeniem do użytkowania, pod kątem spełniania standardów bezpieczeństwa;
7) zabezpieczenia sieci;
8) eksploatacji, wycofywania i niszczenia informatycznych nośników informacji;
9) konserwacji urządzeń w celu zapewnienia ich ciągłej pracy;
10) stosowania mechanizmów kryptograficznych w sposób adekwatny do zagrożeń i wymogów przepisów prawa;
11) zapewnienia bezpieczeństwa plików systemowych;
12) zarządzania podatnościami technicznymi systemów teleinformatycznych, w tym niezwłoczne podejmowanie działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa;
13) nadzorowania usług informatycznych dostarczanych przez strony trzecie;
14) bieżącego monitorowania aktywów informacyjnych, w tym informatycznych, pod kątem wcześniejszego wykrycia wszelkich niebezpieczeństw mogących zagrozić bezpieczeństwu systemów;
15) bezpiecznej pracy przy przetwarzaniu mobilnym i pracy na odległość.

2. Szczegółowe zasady zarządzania systemami i sieciami oraz odpowiedzialność w tym zakresie, opisane są w PBT oraz procedurach z nią związanych.

3. Właścicielem biznesowym PBT jest DIP.

4. CIRF opracowuje i aktualizuje PBT oraz uzgadnia z DB oraz komórką organizacyjną, o której mowa w ust. 3.

Ciągłość działania

§ 12. 1. Obszar ciągłości działania obejmuje zasady mające na celu przeciwdziałanie przerwom w działalności Resortu Finansów oraz ochrony krytycznych procesów przed rozległymi awariami lub katastrofami, w szczególności przez:

1) identyfikację procesów krytycznych i określenie aktywów kluczowych dla ich realizacji;
2) opracowanie i wdrożenie planów ciągłości działania i planów odtwarzania po katastrofie oraz procedur wykonawczych;
3) określenie odpowiedzialności związanej z zarządzaniem ciągłością działania;
4) wyznaczenie osób odpowiedzialnych za realizację zadań w ramach utrzymania ciągłości działania, w tym ciągłości działania systemów teleinformatycznych.

2. Szczegółowe zasady dotyczące ciągłości działania Resortu Finansów zostały uregulowane w PZCD oraz, w odniesieniu do technicznych aspektów zabezpieczenia ciągłości działania systemów teleinformatycznych, w PBT.

3. Właścicielem biznesowym PZCD jest DB.

4. Jednostki opracowują własne plany ciągłości działania i procedury wykonawcze, uwzględniające warunki organizacyjne oraz związane z lokalizacją siedziby Jednostki, a także specyficzne warunki techniczne i organizacyjne, mających znaczenie dla realizacji procesów krytycznych.

Zarządzanie incydentami bezpieczeństwa informacji

§ 13. 1. Zarządzanie incydentami bezpieczeństwa informacji ma na celu ograniczenie wpływu przypadków naruszeń bezpieczeństwa zasobów informacyjnych oraz zapewnienie ciągłości działania Resortu Finansów.

2. Obszar zarządzania incydentami bezpieczeństwa informacji, obejmuje w szczególności:

1) zasady zgłaszania informacji o zdarzeniach i incydentach bezpieczeństwa informacji oraz słabości systemów teleinformatycznych;
2) zasady kategoryzacji i klasyfikacji incydentów;
3) sposób obsługi;
4) sposób dokumentowania zdarzeń i incydentów;
5) odpowiedzialności i podział ról w zakresie zarządzania i obsługi incydentów;

6) procedurę współpracy z CSIRT GOV, w tym odpowiedzialność i tryb zgłaszania oraz kategorie incydentów podlegających zgłoszeniu.

3. Szczegółowe zasady w zakresie zarządzania incydentami określa PZIBI.

4. Właścicielem biznesowym PZIBI jest DIP.

5. CIRF opracowuje i aktualizuje PZIBI oraz uzgadnia z DB oraz komórką organizacyjną, o której mowa w ust. 4.

Rozdział 4

Organizacja bezpieczeństwa informacji

§ 14. 1. Zarządzanie bezpieczeństwem informacji w Ministerstwie i Jednostkach odbywa się na następujących poziomach:

1) strategicznym;
2) taktycznym;
3) operacyjnym.

2. Na poziomie strategicznym:

1) jest wprowadzany SZBI oraz są określane poszczególne role, zasady i organizacja;
2) są dokonywane zmiany w zakresie doskonalenia SZBI w odniesieniu do zmieniającego się otoczenia prawnego i technologicznego, zmian organizacyjnych, jak również będące wynikiem przeprowadzonej analizy ryzyka;
3) jest wprowadzana dokumentacja SZBI, o której mowa w § 6 ust. 2;
4) kierownictwo Ministerstwa, kierujący właściwymi merytorycznie komórkami organizacyjnymi Ministerstwa i kierujący Jednostkami podejmują decyzje w zakresie bezpieczeństwa informacji zgodnie ze swoimi kompetencjami.

3. Na poziomie taktycznym:

1) są tworzone procedury bezpieczeństwa informacji w konkretnych obszarach, określające zasady postępowania i mechanizmy kontroli;
2) są tworzone metodyki: analizy ryzyka, analizy BIA, przeprowadzania audytów bezpieczeństwa informacji oraz ocen skuteczności i efektywności SZBI;
3) jest opracowywany i zatwierdzany:
   a) plan szkoleń,
   b) plan audytów bezpieczeństwa informacji;
4) jest opracowywana i zatwierdzana dokumentacja z przeglądów SZBI;
5) jest zatwierdzana:
   a) dokumentacja z szacowania ryzyka bezpieczeństwa informacji oraz akceptacji ryzyk i dokumentacja postępowania z ryzykiem,

b) dokumentacja incydentów bezpieczeństwa informacji i naruszeń ochrony danych osobowych;

6) na poziomie Ministerstwa - kierownictwo Ministerstwa oraz kierujący właściwymi merytorycznie komórkami organizacyjnymi Ministerstwa, właściciele biznesowi danych, właściciele biznesowi systemów teleinformatycznych, IOD MF, a na poziomie Jednostki – kierujący Jednostką i kierujący właściwymi komórkami organizacyjnymi Jednostki, podejmują decyzje w zakresie bezpieczeństwa informacji zgodnie ze swoimi kompetencjami.

4. Na poziomie operacyjnym:

1) zarządza się bezpieczeństwem informacji w zakresie pełnego stosowania standardów bezpieczeństwa oraz rozwiązywania problemów wynikających z naruszenia tych standardów;
2) jest prowadzony nadzór nad realizacją zadań określonych w politykach i procedurach;
3) jest prowadzony nadzór nad realizacją działań korekcyjnych i zapobiegawczych, działań określonych w planach postępowania z ryzykiem i zaleceniach audytowych;
4) są prowadzone analizy ryzyka i BIA;
5) są gromadzone i przekazywane na poziom taktyczny informacje o stopniu realizacji zadań oraz skuteczności podejmowanych działań i wdrażanych rozwiązań;
6) kierujący poszczególnymi komórkami organizacyjnymi Ministerstwa i Jednostek podejmują decyzje w zakresie bezpieczeństwa informacji zgodnie ze swoimi kompetencjami.

Role i odpowiedzialności w SZBI

§ 15. 1. Organizacja struktur zarządzania bezpieczeństwem informacji w Ministerstwie i Jednostkach jest zgodna z poniższymi zasadami:

1) rozdzielenie funkcji zarządzających i kontrolnych od funkcji wykonawczych;
2) rozdzielenie, w ramach procesów związanych z bezpieczeństwem informacji, obowiązków i odpowiedzialności pozostających w konflikcie ze sobą, w celu ograniczenia nadużyć i błędów;
3) zapewnienie obiektywizmu i bezstronności procesu audytu bezpieczeństwa informacji.

2. Wszyscy pracownicy są odpowiedzialni za zapewnienie bezpieczeństwa informacji do których mają dostęp, w związku z realizacją obowiązków służbowych, zgodnie z zasadami określonymi w Polityce i politykach szczegółowych.

3. Minister:

1) decyduje o celach i środkach przetwarzania informacji, w tym danych osobowych, jako ich właściciel lub administrator;
2) ustanawia SZBI.

4. Dyrektor Generalny Ministerstwa:

1) sprawuje nadzór nad doskonaleniem SZBI w Ministerstwie;

2) akceptuje wyniki przeglądów zarządzania bezpieczeństwem informacji oraz raporty z incydentów bezpieczeństwa informacji;
3) zatwierdza roczny plan audytów wewnętrznych w zakresie bezpieczeństwa informacji Ministerstwa.

5. Dyrektor DB odpowiada za zarządzanie bezpieczeństwem informacji w Ministerstwie i koordynowanie tego procesu w Jednostkach, w szczególności zapewnia:

1) opracowywanie, aktualizację i wdrażanie Polityki oraz, zgodnie z właściwością, określonych polityk szczegółowych oraz związanych z nimi procedur, instrukcji i innych dokumentów z zakresu bezpieczeństwa informacji;
2) opiniowanie polityk i procedur dotyczących bezpieczeństwa informacji będących we właściwości innych komórek organizacyjnych Ministerstwa;
3) koordynowanie i wspieranie działań komórek organizacyjnych Ministerstwa w zakresie bezpieczeństwa informacji, w tym ochrony danych osobowych;
4) nadzorowanie realizacji działań korygujących i zapobiegawczych w zakresie bezpieczeństwa informacji mających na celu doskonalenie SZBI;
5) koordynowanie procesu zarządzania ryzykiem w obszarze bezpieczeństwa informacji;
6) realizację spraw związanych z bezpieczeństwem systemów teleinformatycznych, w zakresie właściwości komórki organizacyjnej określonej w Regulaminie organizacyjnym Ministerstwa;
7) zarządzanie naruszeniami ochrony danych osobowych;
8) organizację okresowych przeglądów dokumentacji SZBI oraz nadzór nad realizacją zaleceń wynikających z ustaleń dokonanych w trakcie przeglądów;
9) planowania i prowadzenia audytów bezpieczeństwa informacji zgodnie z normą ISO 27001 w Ministerstwie, w tym we współpracy z BKA;
10) monitorowanie realizacji zaleceń poaudytowych;
11) przygotowywanie, w uzgodnieniu z BKA, dokumentacji i niezbędnych wyjaśnień na potrzeby kontroli zewnętrznych dotyczących bezpieczeństwa informacji;
12) realizację zadań z zakresu zabezpieczenia technicznego Ministerstwa określonych w PBF;
13) realizowanie i koordynowanie działań w Ministerstwie i Jednostkach w zakresie ciągłości działania, określonych w PZCD;
14) prowadzenie działań informacyjnych dotyczących ochrony informacji, a także planowanie i organizację we współpracy z BDG i Krajową Szkołą Skarbowości, szkoleń w tym zakresie.

6. Dyrektor DB jest uprawniony do:

1) wydawania zaleceń w zakresie związanym z funkcjonowaniem SZBI;
2) uzyskania wyjaśnień od pracowników Ministerstwa, w szczególności w przypadku wystąpienia incydentów bezpieczeństwa informacji i nieprawidłowości w zakresie funkcjonowania SZBI;

3) podejmowania działań w kwestiach bezpieczeństwa informacji, w zakresie niezastrzeżonym do kompetencji innych osób;
4) rekomendowania rozwiązań organizacyjno-technicznych zwiększających skuteczność zarządzania w obszarze SZBI.

7. Dyrektor DIP odpowiada za monitorowanie realizacji zadań związanych z rozwojem i utrzymaniem usług informatycznych w Resorcie Finansów, nadzór nad realizacją zadań w obszarze zapewnienia cyberbezpieczeństwa systemów teleinformatycznych oraz cyberprzestrzeni Resortu Finansów.

8. Dyrektor CIRF realizuje zadania związane z zapewnieniem bezpieczeństwa infrastruktury teleinformatycznej, systemów teleinformatycznych oraz cyberprzestrzeni Resortu Finansów.

9. Dyrektor BKA:
1) współpracuje z DB w zakresie realizacji audytów bezpieczeństwa informacji w Ministerstwie;
2) współpracuje z audytorami wewnętrznymi w Jednostkach w zakresie realizacji audytów bezpieczeństwa informacji w Jednostkach;
3) monitoruje realizację zaleceń poaudytowych;
4) zapewnia obsługę kontroli zewnętrznych dotyczących bezpieczeństwa informacji.

10. Dyrektor BDG zapewnia:
1) ujęcie w planie szkoleń Ministerstwa oraz organizację we współpracy z DB szkoleń z zakresu bezpieczeństwa informacji dedykowanych pracownikom Ministerstwa;
2) zapewnia osobom wykonującym zadania w zakresie zarządzania SZBI specjalistyczne szkolenia w zakresie bezpieczeństwa informacji;
3) realizację zadań, związanych z bezpieczeństwem informacji w ramach zarządzania personelem Ministerstwa, określonych w PBSO.

11. Dyrektor BAD odpowiada za realizację zadań związanych z zapewnieniem bezpieczeństwa okablowania teletechnicznego oraz systemów wspomagających, określonych w PBF i PZCD.

12. Kierujący komórkami organizacyjnymi Ministerstwa, w zakresie swojej właściwości, odpowiadają za:
1) wdrożenie Polityki w podległych komórkach organizacyjnych;
2) nadzór nad bezpieczeństwem przetwarzanych informacji w podległych komórkach organizacyjnych;
3) klasyfikację informacji;
4) realizację obowiązków właściciela biznesowego systemu określonych w § 30 ust. 1 pkt 10 Regulaminu organizacyjnego Ministerstwa i politykach szczegółowych;
5) ochronę aktywów informacyjnych w podległych komórkach organizacyjnych;

6) szacowanie ryzyka bezpieczeństwa informacji w odniesieniu do informacji, których jest właścicielem biznesowym;
7) podejmowanie decyzji w zakresie udostępniania danych i informacji, których są właścicielem biznesowym;
8) realizację procedur zapewniających ciągłość funkcjonowania komórki organizacyjnej w sytuacjach awaryjnych i kryzysowych;
9) umożliwienie pracownikom udziału w organizowanych szkoleniach z zakresu bezpieczeństwa informacji;
10) właściwy tryb zgłaszania i postępowania w związku z incydentami bezpieczeństwa informacji i naruszeniami ochrony danych osobowych, zgodnie z zasadami określonymi w PZIBI;
11) realizację wymogów bezpieczeństwa informacji w zakresie współpracy z podmiotami trzecimi;
12) realizację innych zadań określonych w politykach szczegółowych.

13. Kierujący Jednostkami, w zakresie swojej właściwości, odpowiadają za:

1) wdrożenie Polityki w podległych Jednostkach i komórkach organizacyjnych;
2) nadzór nad bezpieczeństwem przetwarzanych informacji w podległych jednostkach i komórkach organizacyjnych;
3) klasyfikację informacji;
4) ochronę aktywów informacyjnych w podległych Jednostkach i komórkach organizacyjnych;
5) szacowanie ryzyka bezpieczeństwa informacji w odniesieniu do informacji, których są właścicielem biznesowym;
6) zatwierdzanie rocznego planu audytów wewnętrznych w zakresie bezpieczeństwa informacji Jednostki;
7) podejmowanie decyzji w zakresie udostępniania danych i informacji, których są właścicielem biznesowym;
8) realizację procedur zapewniających ciągłość funkcjonowania podległych jednostek w sytuacjach awaryjnych i kryzysowych;
9) umożliwienie pracownikom udziału w organizowanych szkoleniach z zakresu bezpieczeństwa informacji;
10) właściwy tryb zgłaszania i postępowania w związku z incydentami bezpieczeństwa informacji i naruszeniami ochrony danych osobowych, zgodnie z zasadami określonymi w PZIBI;
11) realizację wymogów bezpieczeństwa informacji w zakresie współpracy z podmiotami trzecimi;
12) przygotowanie rocznych planów szkolenia;
13) realizację innych zadań określonych w politykach szczegółowych.

14. Pracownicy odpowiadają w szczególności za:

1) przestrzeganie zasad ochrony informacji określonych w przepisach prawa i Polityce oraz politykach szczegółowych;
2) przetwarzanie informacji wyłącznie w ramach posiadanych upoważnień i przyznanych uprawnień oraz zgodnie z celami przetwarzania i zasadami określonymi w Polityce;
3) przestrzeganie zasad bezpieczeństwa dotyczących eksploatacji systemów teleinformatycznych, określonych w PBT, w tym korzystania z systemów teleinformatycznych służących do przetwarzania informacji prawnie chronionych, wyłącznie zgodnie z ich przeznaczeniem i w zakresie swoich zadań, a także ochrona przed nieupoważnionym dostępem do tych systemów;
4) ochronę aktywów informacyjnych, w tym w trakcie transportu i korzystania z nich poza siedzibą Ministerstwa lub Jednostki;
5) należytego zabezpieczania stanowiska pracy, w tym użytkowanych urządzeń komputerowych, i pomieszczenia pracy, przy uwzględnieniu przepisów dotyczących tajemnic prawnie chronionych;
6) informowanie przełożonego o wszelkich zauważonych nieprawidłowościach i zdarzeniach skutkujących lub mogących skutkować obniżeniem poziomu ochrony informacji;
7) zgłaszanie zdarzeń mogących stanowić incydent bezpieczeństwa informacji, zgodnie z procedurą zarządzania incydentami i aktywnego uczestniczenia w czynnościach wyjaśniających;
8) zapewnienie poufności przetwarzanych informacji oraz poufności sposobów ich zabezpieczenia, w trakcie wykonywania powierzonych zadań i po ich zakończeniu, w tym zabezpieczeniem informacji prawnie chronionych przed nieuprawnionym dostępem, w tym fizycznym, nieuzasadnioną modyfikacją, zniszczeniem, ujawnieniem lub pozyskaniem informacji.

Rozdział 5

Zasady bezpieczeństwa informacji

§ 16. 1. W Resorcie Finansów stosuje się następujące zasady dotyczące bezpieczeństwa informacji:

1) zasada wiedzy koniecznej (ograniczonego dostępu do informacji) – pracownicy posiadają dostęp tylko do tych informacji, które są konieczne do realizacji powierzonych im zadań (różne zadania oznaczają różną wiedzę konieczną do ich wykonania, a tym samym inny profil dostępu);
2) zasada potrzeby koniecznej - pracownicy mają zapewniony dostęp tylko do środków przetwarzania informacji (urządzeń teleinformatycznych, systemów, aplikacji, pomieszczeń), które są im konieczne do wykonania powierzonych im zadań;
3) zasada uprawnionego dostępu – pracownicy są dopuszczeni do przetwarzania informacji prawnie chronionych i wrażliwych po uzyskaniu wiedzy z zakresu postępowania, w tym ochrony, określonych grup informacji, a także obowiązani do odbycia szkolenia z zasad ochrony informacji (w celu spełnienia kryteria dopuszczenia do przetwarzania określonych informacji i danych);

4) zasada obecności koniecznej – prawo przebywania w obszarze przetwarzania, w tym przechowywania informacji i danych prawnie chronionych i wrażliwych, mogą mieć tylko osoby upoważnione; przebywanie osób nieupoważnionych w tym obszarze jest możliwe wyłącznie w obecności upoważnionych pracowników;
5) zasada świadomości zbiorowej - wszyscy pracownicy mają świadomość konieczności ochrony aktywów informacyjnych i aktywnie uczestniczą w tym procesie; świadomość pracowników w zakresie istniejących zagrożeń i zasad ochrony informacji jest doskonalona, w szczególności przez szkolenia i działania informacyjne;
6) indywidualnej odpowiedzialności – za utrzymanie odpowiedniego poziomu bezpieczeństwa poszczególnych aktywów lub ich elementów odpowiadają konkretne osoby, w zakresie nałożonych obowiązków i nadanych uprawnień. Zasada ta dotyczy np. powierzonego sprzętu - każdy pracownik odpowiada za powierzony mu do użytkowania sprzęt komputerowy, wydruków z systemu centralnego wydruku - każdy pracownik odpowiada za sporządzony przez siebie wydruk;
7) rozdzielenia obowiązków - zadania krytyczne z punktu widzenia bezpieczeństwa systemu nie mogą być realizowane przez jedną osobę. Obowiązki i odpowiedzialności pozostające w konflikcie ze sobą należy rozdzielić w celu ograniczenia okazji do nieuprawnionej lub nieumyślnej modyfikacji lub nadużycia aktywów organizacji, w szczególności należy rozdzielić realizację funkcji operacyjnych od nadzorczych i kontrolnych;
8) czystego biurka - podczas nieobecności pracownika na stanowisku pracy, także w przypadku krótkotrwałego opuszczenia pomieszczenia, dokumenty i informatyczne nośniki danych zawierające informacje prawnie chronione lub przeznaczone do użytku wewnętrznego należy zabezpieczyć przed dostępem osób postronnych i nieupoważnionych. Po zakończeniu pracy wszystkie dokumenty i informatyczne nośniki przechowuje się w miarę możliwości organizacyjno-technicznych w nieprzeszklonych, zamykanych na klucz meblach biurowych, zamykanych na klucz lub kod szafach metalowych, przeznaczonych do tego pomieszczeniach zamykanych na klucz lub wyposażonych w system kontroli dostępu;
9) czystego ekranu - na czas nieobecności pracownika dostęp do komputera jest blokowany, a po zakończeniu pracy komputer jest wyłączany, chyba że dany komputer musi pracować w trybie ciągłym – w szczególności dotyczy to serwera obsługującego systemy alarmowe, komputerów administratorów, serwerów do monitoringu. W czasie obecności pracownika monitor jest ustawiony tak, aby nie pozwalał na zapoznawanie się z wyświetlanymi treściami przez osoby postronne, nieupoważnione;
10) czystego kosza – dokumenty papierowe, z wyjątkiem materiałów zawierających informacje publicznie dostępne, w tym promocyjno-informacyjne, muszą być niszczone w sposób

uniemożliwiający ich odczytanie lub odtworzenie. W celu zniszczenia dokumentów papierowych zawierających informacje wrażliwe i prawnie chronione należy korzystać z udostępnionych niszczarek o odpowiedniej klasie niszczenia, adekwatnej do informacji oraz danych utrwalonych na niszczonych dokumentach. Niszczenie elektronicznych nośników danych należy przeprowadzić zgodnie z zasadami określonymi w PBT;

11) czystej tablicy - po zakończonym spotkaniu należy uprzątnąć wszystkie materiały oraz wyczyścić tablice oraz flipchart;

12) czystych drukarek – w przypadku drukowania dokumentów z użyciem ogólnodostępnej drukarki drukowane informacje są zabierane z drukarek niezwłocznie po wydrukowaniu. W przypadku nieudanej próby wydrukowania użytkownik ma obowiązek skontaktować się z osobą odpowiedzialną za eksploatację urządzenia, jeżeli zachodzi podejrzenie, iż wydruk zostanie wydrukowany bez nadzoru;

13) poufności informacji uwierzytelniających – każdy pracownik jest obowiązany do zachowania poufności udostępnionych mu haseł, kodów dostępu, kodów PIN, w szczególności do systemów informatycznych i teleinformatycznych;

14) prywatności kont w systemach – każdy użytkownik jest obowiązany do pracy w systemach informatycznych wyłącznie na przypisanych lub udostępnionych mu kontach, które jednoznacznie go identyfikują. Zabronione jest udostępnianie własnych kont osobom trzecim. Zasada ta ma również zastosowanie do kart wykorzystywanych w systemach kontroli dostępu funkcjonujących w Resorcie Finansów. Stosowanie się do tej reguły pozwala zachować rozliczalność działań użytkowników;

15) dyskrecji – wszelkie informacje służbowe mogą być przekazywane innym osobom uprawnionym do pozyskania tych informacji zgodnie z obowiązującymi przepisami prawa i przyjętymi w Resorcie Finansów zasadami;

16) zamkniętego pomieszczenia – niedopuszczalne jest pozostawienie pod nieobecność pracownika niezabezpieczonego pomieszczenia służbowego, zarówno w godzinach pracy, jak i po jej zakończeniu. Na zakończenie dnia pracy ostatnia wychodząca z pomieszczenia osoba jest obowiązana zamknąć wszystkie okna i drzwi oraz zabezpieczyć klucze do pomieszczenia;

17) zgłaszania incydentów bezpieczeństwa informacji i naruszeń ochrony danych osobowych – każdy użytkownik ma obowiązek niezwłocznie zgłosić wystąpienie lub podejrzenie wystąpienia incydentu lub naruszenia mającego lub mogącego mieć wpływ na bezpieczeństwo informacji, w tym danych osobowych w Resorcie Finansów;

18) bezpiecznej współpracy z podmiotami zewnętrznymi – dokumenty regulujące współpracę, w tym umowy, porozumienia, zawierają stosowne klauzule bezpieczeństwa, w tym o zachowaniu

poufności, zasadach postępowania z pozyskaną informacją, niszczenia lub zwrotu aktywów informacyjnych po zakończeniu współpracy;

19) automatyzacji backupu - procesy tworzenia kopii zapasowych są odpowiednio zaplanowane z uwzględnieniem wymogów prawnych i potrzeb Resortu Finansów, jak również są zautomatyzowane oraz niemożliwe do przerwania przez pracownika;

20) legalnego oprogramowania – na serwerach i stacjach roboczych jest zainstalowane wyłącznie legalne oprogramowanie;

21) ochrony zewnętrznych (wymiennych) nośników danych – dane i informacje utrwalone na zewnętrznych nośnikach danych i wynoszone poza pomieszczenia użytkowane przez Resort Finansów są odpowiednio zabezpieczone przed nieuprawnionym dostępem, zniszczeniem oraz utratą integralności w czasie transportu i przechowywania. W szczególności dotyczy to informacji prawnie chronionych takich jak tajemnica skarbowa, dane osobowe oraz innych informacji wrażliwych. Szczegółowo zasady zarządzania wymiennymi nośnikami danych, w tym ich ochrony, reguluje PBT.

2. Stosowanie zabezpieczeń lub ich grup uwzględnia następujące zasady:

1) minimalny stosowany poziom zabezpieczeń odpowiada wymogom obowiązujących przepisów prawa;

2) zabezpieczenia są wdrażane we wszystkich obszarach określonych w deklaracji stosowania zabezpieczeń, zgodnie z wymogami normy PN-ISO/IEC 27001 i zasadami określonymi w normie PN-ISO/IEC 27002;

3) używane mechanizmy zabezpieczeń są adekwatne (odpowiednie) do zagrożeń, podatności, wartości aktywów oraz wyników szacowania ryzyka w bezpieczeństwa informacji;

4) w doborze zabezpieczeń należy uwzględnić zalecenia i rekomendacje sformułowanymi w wyniku przeprowadzonych audytów i kontroli;

5) zabezpieczenia fizyczne, techniczne, prawne i organizacyjne uzupełniają się wzajemnie (grupy zabezpieczeń), zapewniając wymagany poziom bezpieczeństwa informacji;

6) należy unikać niepotrzebnego dublowania zabezpieczeń, przy uwzględnieniu racjonalnego gospodarowania środkami publicznymi, optymalizacji potrzeb oraz ograniczeń i uwarunkowań prawno-organizacyjnych Resortu Finansów;

7) niedopuszczalne jest tymczasowe wyłączanie mechanizmów zabezpieczających systemy teleinformatyczne funkcjonujące w Resorcie Finansów bez zastosowania alternatywnych mechanizmów; systemy są sprawne i przygotowane na wystąpienie zidentyfikowanych zagrożeń;

8) domniemanej odmowy - przyjęcia jako standardowych najbardziej restrykcyjnych ustawień, które można zwolnić jedynie w określonych sytuacjach („to, co nie jest dozwolone, jest zabronione”);

9) ciągłego doskonalenia – SZBI jest stale monitorowany, stosowane zabezpieczenia są dostosowywane do zmieniających się warunków wewnętrznych i zewnętrznych, w celu zapewnienia ich przydatności, adekwatności i skuteczności.

3. Katalog zasad, o których mowa w ust. 1, oraz szczegółowe metody i sposoby implementacji zabezpieczeń, o których mowa w ust. 2, mogą być rozszerzone i uszczegółowione w innych dokumentach stanowiących dokumentację SZBI.

Rozdział 6

Zasady zarządzania aktywami

§ 17. 1. Ministerstwo i Jednostki zarządzają aktywami w celu zapewnienia im wymaganego poziomu bezpieczeństwa.

2. Aktywa chronione obejmują:

1) aktywa główne - przetwarzane przez Ministerstwo lub Jednostkę informacje oraz procesy i działania związane z realizacją zadań ustawowych Ministerstwa lub Jednostki;
2) aktywa wspierające – wszystkie elementy wspierające realizację procesów i działań oraz służące do przetwarzania informacji, o których mowa w pkt 1, w szczególności:
   a) sprzęt - urządzenia komputerowe stacjonarne i przenośne, serwery, urządzenia peryferyjne (drukarki, skanery), nośniki danych,
   b) oprogramowanie, w tym aplikacje i systemy operacyjne,
   c) sieć, w tym urządzenia telekomunikacyjne,
   d) personel – Kierownictwo Ministerstwa, pracownicy i inne osoby realizujące zadania na rzecz Ministerstwa lub Jednostki,
   e) siedziba, nieruchomości, strefy oraz poszczególne pomieszczenia użytkowane przez Ministerstwo lub Jednostkę,
   f) struktura organizacyjna – jednostki, komórki organizacyjne, dostawcy, wykonawcy.

3. Aktywa są chronione ze względu na:

1) wymagania wynikające z przepisów prawa;
2) warunki licencji;
3) wymagania wynikające z postanowień umów lub porozumień między Ministerstwem lub Jednostką a podmiotami zewnętrznymi;
4) wartość biznesową aktywów odpowiadającą ich wadze dla prowadzonej działalności, realizacji zadań ustawowych Ministerstwa lub Jednostki;
5) regulacje wewnętrzne, z których wynika ochrona właściwych aktywów.

4. Zarządzanie aktywami w Resorcie Finansów odbywa się zgodnie z zasadami:

1) identyfikacji aktywów – wszystkie aktywa są zidentyfikowane oraz jest sporządzony i utrzymywany spis aktywów związany z informacjami i środkami przetwarzania informacji.

Przedmiotowy spis może być elementem dokumentacji systemów, rejestru procesów, usług i czynności lub być prowadzony oddzielnie;

2) odpowiedzialności za aktywa – właściciele wszystkich aktywów są określeni oraz jest im przydzielona odpowiedzialność w zakresie zarządzania aktywami, w tym:
   a) sporządzenia i utrzymywania spisu, o którym mowa w pkt 1,
   b) zapewnienia właściwej klasyfikacji aktywów oraz utrzymania odpowiednich zabezpieczeń dla aktywów,
   c) monitorowania stanu zabezpieczeń aktywów,
   d) zapewnienia usuwania i niszczenia aktywów zgodnie z przyjętymi zasadami,
   e) przeglądów w zakresie dostępu do aktywów;
3) akceptowalnego użycia aktywów i ich zwrotu – określone i stosowane są zasady dopuszczalnego korzystania z aktywów przez pracowników, jak również przez podmioty zewnętrzne uzyskujące dostęp do aktywów na podstawie podpisanych umów lub porozumień oraz ich zwrotu w związku z zakończeniem zatrudnienia, umowy lub porozumienia;
4) klasyfikacji informacji – jest wdrożona i stosowana metodyka klasyfikacji informacji, są określone zasady postępowania z informacją, jej przetwarzania, przechowywania i przekazywania oraz oznaczania zgodnie z przyjętym schematem klasyfikacji informacji, a także ochrony informacji zgodnie z wymaganiami określonymi w odniesieniu do danej grupy informacji;
5) zarządzanie nośnikami wymiennymi – są określone i wdrożone zasady zarządzania nośnikami wymiennymi i ich ochrony, w tym poza siedzibą Ministerstwa lub Jednostki i w trakcie transportu, a także zasady wycofywania nośników z użycia i ich niszczenia.

5. Szczegółowy wykaz kategorii aktywów teleinformatycznych oraz sposób zarządzania nimi jest określony w PBT.

6. Zasady identyfikacji aktywów kluczowych dla realizacji procesów krytycznych oraz wymagania w zakresie utrzymywania spisów tych aktywów i szczególne wymogi dotyczące zarządzania aktywami kluczowymi zostały określone w PZCD.

Rozdział 7

Klasyfikacja informacji

§ 18. 1. W Resorcie Finansów przyjmuje się następującą klasyfikację informacji:

1) Grupa I - informacje niejawne;
2) Grupa IA - inne informacje podlegające ochronie przewidzianej dla informacji niejawnych;
3) Grupa II - informacje międzynarodowe, do których dostęp podlega ograniczeniu;
4) Grupa III - inne informacje prawnie chronione;
5) Grupa IV - informacje przeznaczone wyłącznie do użytku wewnętrznego - niestanowiące informacji publicznej;

6) Grupa V - informacje publiczne i informacje sektora publicznego, w tym publicznie dostępne dokumenty Parlamentu Europejskiego, Rady Unii Europejskiej i Komisji Europejskiej.

2. Szczegółowy opis poszczególnych grup informacji ujęty jest w katalogu klasyfikacji informacji.

3. Zasady oznaczania i sposób postępowania ze sklasyfikowanymi informacjami są określone w Zasadach oznaczania i postępowania ze sklasyfikowanymi informacjami oraz ich ochrony.

4. Katalog klasyfikacji informacji i Zasady oznaczania i postępowania ze sklasyfikowanymi informacjami oraz ich ochrony są zatwierdzane przez dyrektora DB.

Rozdział 8

Bezpieczeństwo informacji w zakresie współpracy z podmiotami zewnętrznymi

§ 19. 1. Umowa albo porozumienie z podmiotem zewnętrznym, która wiąże się z możliwością dostępu do informacji będących własnością, administrowanych lub wykorzystywanych przez Ministerstwo lub Jednostkę, zawiera postanowienia regulujące zagadnienia dostępu i ochrony tych informacji oraz innych aktywów Ministerstwa lub Jednostki, przez ten podmiot oraz jego pracowników i podwykonawców uczestniczących w realizacji umowy albo porozumienia.

2. Umowa albo porozumienie z podmiotem zewnętrznym reguluje w szczególności następujące zagadnienia:

1) wymagania prawne w zakresie świadczenia usługi w związku z ochroną informacji; w przypadku dostępu podmiotu zewnętrznego do informacji niejawnych, danych osobowych lub innych informacji prawnie chronionych jest wymagane potwierdzenie przez ten podmiot zdolności do ochrony określonych informacji, zgodnie z wymaganiami określonymi w przepisach prawa oraz przepisach wewnętrznych regulujących kwestie dostępu i ochrony określonych grup informacji;
2) określenie sposobu dostępu do informacji i dopuszczalnej formy ich przetwarzania;
3) określenie sposobu bezpiecznej wymiany informacji;
4) określenie zakresu dostępu do informacji i dopuszczalnego celu przetwarzania przekazanych informacji;
5) określenie zasad dostępu do infrastruktury informatycznej Resortu Finansów oraz bezpiecznego korzystania z niej, jeżeli wynika to ze specyfiki świadczenia usługi;
6) ochronę poufności uzyskanych w związku z realizacją umowy albo porozumienia informacji, w szczególności wszelkich informacji technicznych, technologicznych i organizacyjnych, mających szczególne znaczenie dla Ministerstwa lub Jednostki w trakcie trwania umowy albo porozumienia oraz po zakończeniu jej realizacji. Z obowiązku zachowania poufności są zwolnione informacje publicznie dostępne oraz informacje, których ujawnienie jest wymagane przepisami prawa. Wzór klauzuli poufności określa i udostępnia w Intranecie dyrektor DB;
7) odpowiedzialność za naruszenie bezpieczeństwa informacji;

8) tryb postępowania w przypadku wystąpienia zdarzenia lub incydentu bezpieczeństwa informacji lub naruszenia ochrony danych osobowych. Tryb ten musi uwzględniać co najmniej niezwłoczne powiadomienie Ministerstwa lub Jednostki o wystąpieniu incydentu albo naruszenia z uwzględnieniem wymogów określonych w PZIBI;
9) w związku z zakończeniem obowiązywania umowy albo porozumienia - obowiązek zwrotu otrzymanych nośników informacji, zwrotu lub usunięcia otrzymanych informacji, w tym w postaci elektronicznej, i ich kopii niezależnie od sposobu i formy ich utrwalenia oraz danych wytworzonych w związku z realizacją umowy albo porozumienia, chyba że obowiązek ich dalszego przechowywania wynika wprost z przepisów prawa, oraz obowiązek protokolarnego udokumentowania zwrotu lub usunięcia danych;
10) obowiązek informowania o wszelkich zmianach po stronie podmiotu zewnętrznego, mogących wpłynąć na realizację umowy albo porozumienia;
11) obowiązek przekazania na żądanie Ministerstwa lub Jednostki wszelkich informacji niezbędnych do wykazania spełnienia obowiązków określonych w przepisach prawa o ochronie danych osobowych i innych informacji prawnie chronionych;
12) specyfikację warunków świadczenia usługi;
13) prawo do przeprowadzenia audytów i inspekcji.

3. Zagadnienia, o których mowa w ust. 2, nie stanową katalogu zamkniętego i są każdorazowo stosowane z uwzględnieniem specyfiki i przedmiotu zawieranej umowy albo porozumienia.

4. Umowa albo porozumienie, której przedmiot obejmuje budowę, modyfikacje lub prace rozwojowe w zakresie oprogramowania i systemów teleinformatycznych służących do przetwarzania informacji, zawiera klauzule umożliwiające egzekwowanie wymagań określonych w PBT, a w przypadku systemów służących do przetwarzania danych osobowych również wymagania określone w PODO.

5. Wymiana informacji wrażliwych i prawnie chronionych między podmiotem zewnętrznym a Ministerstwem lub Jednostką wymaga ich zabezpieczenia zgodnie z wymogami prawa.

6. Wymiana informacji przez sieć informatyczną niebędącą pod kontrolą Ministerstwa lub Jednostki wymaga w szczególności:

1) w przypadku wymiany informacji wymagających ochrony z wykorzystaniem poczty elektronicznej – zapewnienia szyfrowania przesyłanych informacji. Dopuszcza się szyfrowanie wyłącznie załączników, o ile treść wiadomości nie zawiera informacji wymagających ochrony;
2) w przypadku połączenia między systemami teleinformatycznymi Resortu Finansów, Ministerstwa lub Jednostki a systemem teleinformatycznym podmiotu zewnętrznego – zapewnienia przesyłania danych w postaci zaszyfrowanej, w szczególności z wykorzystaniem protokołów zapewniających transfer danych zaszyfrowanych lub przez przesyłanie zaszyfrowanych plików;

3) transfer lub udostępnianie plików zawierających informacje będących własnością Ministerstwa lub Jednostki może się odbywać wyłącznie za pośrednictwem narzędzi udostępnionych przez CIRF. Niedopuszczalne jest korzystanie z ogólnodostępnych zewnętrznych usług oraz serwisów transferu plików.

7. Wymiana informacji przy użyciu dokumentów w postaci papierowej odbywa się zgodnie z zasadami określonymi w instrukcji kancelaryjnej Ministerstwa lub Jednostki.

8. Kierujący komórkami organizacyjnymi Ministerstwa lub Jednostki korzystający z usług podmiotów zewnętrznych są obowiązani do monitorowania jakości usług świadczonych przez te podmioty z uwzględnieniem wymagań prawnych oraz zdefiniowanych parametrów świadczenia tych usług.

9. Częstotliwość monitorowania jakości usług i monitorowane parametry są określane indywidualnie, w zależności od charakteru usługi.

10. W przypadku stwierdzenia, iż jakość usługi nie spełnia wymagań określonych w umowie albo porozumieniu, kierujący komórką organizacyjną Ministerstw lub Jednostki odpowiedzialną za nadzór nad ich realizacją, podejmuje działania w celu wyegzekwowania warunków świadczenia usługi z nich wynikających. W przypadku, gdy egzekwowanie warunków świadczenia usługi nie przynosi oczekiwanych rezultatów, podejmuje się, zgodnie z postanowieniami zawartych umowy albo porozumienia i możliwości prawnych, działania w celu zakończenia współpracy z podmiotem zewnętrznym.

Rozdział 9

Zarządzanie ryzykiem w bezpieczeństwie informacji

§ 20. 1. Zarządzanie ryzykiem wspiera i wpływa na większą efektywność zarządzania bezpieczeństwem informacji, przez:

1) identyfikację potencjalnych zagrożeń i podatności oraz określenie ich wpływu na realizację celów bezpieczeństwa informacji;
2) zapobieganie wystąpieniu niepożądanych skutków lub ich zredukowanie przez zastosowanie zabezpieczeń obniżających ryzyka do poziomu ryzyka akceptowalnego.

2. Zarządzanie ryzykiem jest procesem ciągłym obejmującym następujące działania:

1) szacowanie ryzyka (identyfikację, analizę i ocenę ryzyka),
2) postępowanie z ryzykiem,
3) akceptowanie ryzyka,
4) informowanie o ryzyku,
5) monitorowanie i przegląd ryzyka

– w ramach ustalonego kontekstu.

3. Szacowanie ryzyka jest obligatoryjne i przeprowadza się je cykliczne, nie rzadziej niż raz w roku.

4. Szacowanie ryzyka jest dodatkowo realizowane zgodnie z potrzebami, w szczególności przed opracowaniem dokumentacji bezpieczeństwa dla danego obszaru, procesu, czynności lub systemu teleinformatycznego oraz po wystąpieniu w nich istotnych zmian.

5. Za przeprowadzenie szacowania ryzyka są odpowiedzialni właściwi kierownicy komórek organizacyjnych, będący właścicielami biznesowymi danych i systemów. W przypadku gdy informacje są przetwarzane w systemie teleinformatycznym, a właściciel biznesowy informacji nie jest jednocześnie właścicielem biznesowym systemu teleinformatycznego, właściciel biznesowy informacji prowadzi ocenę ryzyka z uwzględnieniem opinii właściciela biznesowego systemu teleinformatycznego.

6. Szacowanie ryzyka przeprowadza się w oparciu o przyjętą metodykę, zatwierdzaną przez dyrektora DB.

7. Szacowanie ryzyka, plan postepowania z ryzykiem i akceptowanie ryzyka są dokumentowane.

8. Ocenę skutków ochrony danych osobowych jest prowadzona zgodnie z zasadami określonymi w PODO.

9. Wyniki szacowania ryzyka i plan postępowania z ryzykiem są zatwierdzane przez właściciela biznesowego danych i systemu.

Rozdział 10

Audyty bezpieczeństwa informacji oraz oceny skuteczności i efektywności funkcjonowania SZBI

§ 21. 1. W celu oceny skuteczności i efektywności funkcjonowania SZBI w Ministerstwie i Jednostkach są realizowane audyty bezpieczeństwa informacji.

2. Audyty bezpieczeństwa informacji obejmują audyty prowadzone zgodnie z normą PN-ISO/IEC 27001 oraz audyty wewnętrzne w zakresie bezpieczeństwa informacji przeprowadzane nie rzadziej niż raz na rok, zgodnie z § 20 ust. 2 pkt 14 rozporządzenia KRI.

3. Audyty bezpieczeństwa informacji uwzględnia się w rocznym planie audytów Ministerstwa i Jednostki.

4. Poza planowymi audytami bezpieczeństwa informacji mogą zostać przeprowadzone również oceny skuteczności i efektywności funkcjonowania SZBI, w szczególności w przypadku wystąpienia incydentu bezpieczeństwa informacji.

5. Realizacja audytu bezpieczeństwa informacji lub oceny skuteczności i efektywności funkcjonowania SZBI wymaga:

1) przygotowania programu lub założeń określających cel, szczegółowy zakres i harmonogram jego realizacji;
2) przygotowania dokumentów roboczych, w tym list kontrolnych;

3) prezentowania, uzgadniania i komunikowania wyników w formie raportu lub sprawozdania.

6. Ocenę skuteczności i efektywności funkcjonowania SZBI realizują:

1) w Ministerstwie:
   a) DB,
   b) BKA;
2) w Jednostkach:
   a) komórka do spraw audytu wewnętrznego Jednostki,
   b) inna komórka albo osoba wyznaczona przez kierownika Jednostki,
   c) DB,
   d) BKA.

7. Audytorzy przeprowadzający audyt bezpieczeństwa informacji lub osoby przeprowadzające ocenę skuteczności i efektywności funkcjonowania SZBI posiadają odpowiednie kwalifikacje, doświadczenie oraz znajomość metodyki prowadzenia audytu bezpieczeństwa informacji.

8. Audyty bezpieczeństwa informacji lub oceny skuteczności i efektywności funkcjonowania SZBI są prowadzone z zachowaniem obiektywności i bezstronności procesu audytu, w szczególności niezbędne jest zapewnienie, aby audytorzy i osoby przeprowadzające ocenę nie byli odpowiedzialni za przegląd tej części systemu, w której realizacji biorą udział w ramach obowiązków służbowych.

9. Zadania związane z prowadzeniem audytu bezpieczeństwa informacji lub oceny skuteczności i efektywności funkcjonowania SZBI mogą zostać powierzone podmiotowi zewnętrznemu zapewniającemu:

1) realizację zgodnie ze standardami audytowania systemów zarządzania bezpieczeństwem informacji określonymi w polskich i międzynarodowych normach, w tym ISO 19011;
2) wykwalifikowanych audytorów, w tym audytora wiodącego, posiadających certyfikaty potwierdzające wiedzę w zakresie audytowania na zgodność z normą ISO 27001;
3) odpowiednie doświadczenie potwierdzone referencjami.

10. Wyniki audytów bezpieczeństwa informacji lub ocen skuteczności i efektywności funkcjonowania SZBI realizowanych w Jednostkach są przekazywane do DB.

Rozdział 11

Przegląd zarządzania bezpieczeństwem informacji i aktualizacja polityk bezpieczeństwa

§ 22. 1. Dokumentacja SZBI, o której mowa w § 6 ust. 1 i ust. 2 pkt 1-4, podlega okresowym przeglądom pod kątem przydatności, adekwatności i skuteczności określonych w nich zabezpieczeń nie rzadziej niż raz do roku.

2. W ramach przeglądu uwzględnia się:

1) zmiany przepisów prawa oraz zmiany związane z organizacją i funkcjonowaniem Ministerstwa i Jednostek, istotne dla systemu zarządzania bezpieczeństwem informacji;
2) stan działań podjętych w następstwie wcześniejszych przeglądów zarządzania;
3) raporty z działań kontrolnych oraz wyniki audytów w zakresie bezpieczeństwa informacji;
4) raporty z realizacji przez komórki organizacyjne Ministerstwa i Jednostek działań korygujących;
5) raporty z analizy zdarzeń i incydentów związanych z naruszeniem bezpieczeństwa informacji;
6) opinie na temat dokumentacji SZBI i określonych w nich zabezpieczeń przygotowywane przez kierujących komórkami organizacyjnymi Ministerstwa i kierujących Jednostkami;
7) wyniki szacowania ryzyka i stan realizacji planów postępowania z ryzykiem.

3. Przegląd jest przeprowadzany niezwłocznie w przypadku:

1) gdy zmianie ulegają przepisy prawa określające minimalne zabezpieczenia aktywów informacyjnych i będące źródłem wskazanych w Dokumentacji SZBI obowiązków;
2) zaistnieją istotne zmiany organizacyjne;
3) na skutek zaleceń i rekomendacji wynikających z kontroli, audytów, sprawdzeń oraz z wykrytych naruszeń.

4. Na podstawie wyników przeglądu przygotowywany jest plan działań wdrażających wnioski z przeprowadzonego przeglądu, w tym uwzględniających aktualizację Polityki i pozostałej dokumentacji SZBI, który podlega zatwierdzeniu przez Dyrektora Generalnego Ministerstwa.

5. Przegląd jest realizowany przy współudziale właściwych komórek organizacyjnych Ministerstwa i Jednostek, których kompetencje zostały określone w dokumentacji SZBI.

6. W Ministerstwie przegląd oraz plan działań wdrażających wnioski z przeprowadzonego przeglądu przygotowuje DB we współpracy z właściwymi komórkami organizacyjnymi Ministerstwa.

7. Za wdrożenie planu, o którym mowa w ust. 6, są odpowiedzialne wskazane w nim komórki organizacyjne Ministerstwa.

8. Za organizację przeglądów SZBI w ramach Jednostek odpowiada kierownik Jednostki.

Rozdział 12

Szkolenia z zakresu bezpieczeństwa informacji

§ 23. 1. Szkolenia z zakresu bezpieczeństwa informacji w Ministerstwie są organizowane przez DB w formie szkoleń bezpośrednich, z wykorzystaniem technologii informatycznych lub w innych formach adekwatnych do celów szkolenia. Dopuszczalne jest również samokształcenie pod warunkiem zapewnienia możliwości konsultacji niejasnych zagadnień.

2. Roczny plan szkoleń z zakresu bezpieczeństwa informacji oraz zakres, formę i tematykę szkoleń ustala DB.

3. Szkolenia są przeprowadzane dla nowo przyjętych pracowników, a także według potrzeb – okresowo oraz w związku z powrotem pracownika do pracy po dłuższej nieobecności. W ramach

szkolenia nowo przyjęty pracownik jest obowiązany do zapoznania się z zasadami ochrony informacji określonymi w Polityce i politykach szczegółowych oraz przepisami prawa w zakresie ochrony informacji prawnie chronionych, do których będzie miał dostęp zgodnie z określonym zakresem obowiązków.

4. Szkolenia mogą być również przeprowadzone dla innych osób przetwarzających informacje, w szczególności wskazane w § 5 ust. 1 pkt 2-4.

5. Podczas realizacji szkoleń w obszarze bezpieczeństwa informacji konieczne jest zapewnienie dowodu audytowego odbycia szkolenia. W tym celu mogą być prowadzone listy obecności zawierające datę szkolenia, tytuł szkolenia oraz listę uczestników wraz z podpisami lub inne dowody audytowe adekwatne do wybranej formy szkolenia.

6. Specjalistyczne szkolenia dotyczące ochrony poszczególnych grup informacji prawnie chronionych są realizowane zgodnie z wymogami określonymi w przepisach prawa i odrębnymi regulacjami wewnętrznymi.

Rozdział 13

Odpowiedzialność (sankcje)

§ 24. 1. Naruszenie bezpieczeństwa informacji może być uznane za ciężkie naruszenie obowiązków pracowniczych.

2. Niezastosowanie się do przepisów o ochronie informacji prawnie chronionych, a także do Polityki, polityk szczegółowych i procedur dotyczących ochrony informacji, może powodować odpowiedzialność karną, dyscyplinarną lub służbową.

Rozdział 14

Odstępstwa

§ 25. 1. Odstąpienie od zasad opisanych w dokumentacji SZBI jest możliwe wyłącznie po spełnieniu następujących warunków:

1) musi być zasadne - wniosek o odstępstwo zawiera uzasadnienie odstąpienia od przyjętych zasad;
2) wymaga wskazania rozwiązań zamiennych niwelujących ewentualne skutki zastosowania odstępstwa;
3) wymaga uzyskania zgody dyrektora:
   a) DIP - w przypadku wnioskowania o odstępstwo od zasad bezpieczeństwa dotyczących przetwarzania informacji w systemach teleinformatycznych, po uzyskaniu pozytywnej opinii dyrektorów CIRF i DB,
   b) DB – w przypadku wnioskowania o odstępstwo od zasad bezpieczeństwa dotyczących przetwarzania informacji prawnie chronionych, w przypadku danych osobowych wymagane jest uzyskanie opinii IOD,

c) DB - w przypadku wnioskowania o odstępstwo od stosowania środków bezpieczeństwa fizycznego,

d) kierującego Jednostką – w przypadku wnioskowania o odstępstwo od zasad bezpieczeństwa dotyczących opracowywanych polityk wymienionych w § 6 ust. 2;

4) nie może wpływać negatywnie na realizację podstawowego celu Polityki, o którym mowa w § 4 ust. 1.

2. Wnioski o odstępstwo są składane za pośrednictwem kierującego komórką organizacyjną Ministerstwa albo Jednostką.

3. Dyrektorzy komórek organizacyjnych albo kierujący Jednostką wskazani w ust. 1 pkt 3 mogą wyrazić zgodę na odstępstwo zgodnie z wnioskiem, odrzucić wniosek lub zmienić zakres odstępstwa lub proponowane rozwiązania zamienne.

4. Dyrektorzy komórek organizacyjnych albo kierujący Jednostką wskazani w ust. 1 pkt 3 prowadzą rejestr odstępstw.

5. Wzór wniosku o odstępstwo, o którym mowa w ust. 2, oraz rejestru, o którym mowa w ust. 4, określa i udostępnia w Intranecie dyrektor DB.

Rozdział 15

Postanowienia końcowe

§ 26. 1. Kierujący komórkami organizacyjnymi Ministerstwa oraz w Jednostkach zapoznają nowo zatrudnionych pracowników i funkcjonariuszy podejmujących służbę w Ministerstwie oraz w tych Jednostkach z treścią Polityki.

2. Fakt zapoznania się z treścią Polityki potwierdza się przez złożenie oświadczenia, o którym mowa w § 5 ust. 11 Polityki.

Załącznik do Polityki Bezpieczeństwa Informacji

Wykaz dokumentacji powiązanej z PBI

L.P.	WSKAZANIE DOKUMENTU	WŁAŚCICIEL BIZNESOWY
1	Katalog klasyfikacji informacji	DB
2	Zasady oznaczania i postępowania ze sklasyfikowanymi informacjami oraz ich ochrony	DB
3	Metodyka analizy ryzyka w bezpieczeństwie informacji	DB
4	PODO	DB
5	PZCD	DB
6	PBF	DB
7	PZIBI	DIP
8	PBT	DIP
9	PBSO	BDG/DBM