Warszawa, dnia 29 kwietnia 2025 r.

Poz. 12

ZARZĄDZENIE

MINISTRA FUNDUSZY I POLITYKI REGIONALNEJ[1)]

z dnia 28 kwietnia 2025 r.

w sprawie Polityki bezpieczeństwa informacji w Ministerstwie Funduszy i Polityki Regionalnej

Na podstawie art. 34 ust. 1 ustawy z dnia 8 sierpnia 1996 r. o Radzie Ministrów (Dz. U. z 2024 r. poz. 1050 i 1473) w związku z § 19 rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. poz. 773) zarządza się, co następuje:

§ 1. W Ministerstwie Funduszy i Polityki Regionalnej wprowadza się Politykę bezpieczeństwa informacji, zwaną dalej „Polityką", stanowiącą załącznik do zarządzenia.

§ 2. 1. W terminie miesiąca od dnia wejścia w życie niniejszego zarządzenia wszystkie osoby posiadające dostęp do aktywów, w rozumieniu § 2 pkt 1 Polityki, mają obowiązek zapoznania się z jej treścią i złożenia oświadczenia, o którym mowa w § 16 ust. 3 lub 4 Polityki.

2. W terminie 6 miesięcy od dnia wejścia w życie niniejszego zarządzenia właściwe komórki organizacyjne Ministerstwa Funduszy i Polityki Regionalnej dostosują do Polityki pozostałą dokumentację Systemu Zarządzania Bezpieczeństwem Informacji w Ministerstwie Funduszy i Polityki Regionalnej.

§ 3. Traci moc zarządzenie Ministra Funduszy i Polityki Regionalnej z dnia 2 lutego 2022 r. w sprawie Polityki Bezpieczeństwa Informacji w Ministerstwie Funduszy i Polityki Regionalnej.

[1)] Minister Funduszy i Polityki Regionalnej kieruje działem administracji rządowej – rozwój regionalny, na podstawie § 1 ust. 2 rozporządzenia Prezesa Rady Ministrów z dnia 18 grudnia 2023 r. w sprawie szczegółowego zakresu działania Ministra Funduszy i Polityki Regionalnej (Dz. U. poz. 2711).

§ 4. Zarządzenie wchodzi w życie z dniem podpisania.

MINISTER FUNDUSZY

I POLITYKI REGIONALNEJ

Załącznik do zarządzenia Ministra Funduszy i Polityki Regionalnej z dnia 28 kwietnia 2025 r. (poz. 12)

POLITYKA BEZPIECZEŃSTWA INFORMACJI

Rozdział 1

Postanowienia ogólne

§ 1. 1. Polityka bezpieczeństwa informacji, zwana dalej „Polityką”, określa:

1) podstawowe zasady zarządzania bezpieczeństwem informacji;
2) podmioty odpowiedzialne za ochronę informacji w Ministerstwie Funduszy i Polityki Regionalnej, zwanym dalej „Ministerstwem”, zakres ich odpowiedzialności oraz uprawnień;
3) mechanizmy realizacji Polityki;
4) klasyfikację informacji i zasady postępowania z nimi;
5) podstawowe kwestie związane z szacowaniem ryzyka bezpieczeństwa informacji.

2. Zasady zarządzania bezpieczeństwem informacji, o których mowa w ust. 1 pkt 1, zostały opracowane:

1) zgodnie z obowiązującymi przepisami, w tym w szczególności z:
   a) rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.[1)]), zwanym dalej „RODO”,
   b) ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781),
   c) ustawą z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2022 r. poz. 902),

---

[1)] Zmiany wymienionego rozporządzenia zostały ogłoszone w Dz. Urz. UE L 127 z 23.05.2018, str. 2 oraz Dz. Urz. UE L 74 z 04.03.2021, str. 35.

d) ustawą z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego (Dz. U. z 2023 r. poz. 1524),

e) ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2024 r. poz. 632 i 1222),

f) ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222),

g) ustawą z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2025 r. poz. 24),

h) ustawą z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2024 r. poz. 1557 i 1717),

i) rozporządzeniem Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. poz. 948),

j) rozporządzeniem Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. poz. 773),

k) rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 18 stycznia 2007 r. w sprawie Biuletynu Informacji Publicznej (Dz. U. poz. 68);

2) w oparciu o wymagania norm i standardów w obszarze bezpieczeństwa informacji, w tym w szczególności Polskich Norm:

a) PN-EN ISO/IEC 27001,

b) PN-EN ISO/IEC 27002:2023-01,

c) ISO/IEC 27005:2018,

d) PN-ISO/IEC 24762,

e) PN-EN ISO 22301.

§ 2. Użyte w Polityce określenia i skróty oznaczają:

1) aktywa – wszystko, co stanowi wartość dla Ministerstwa i w związku z tym wymaga ochrony, w szczególności:

a) aktywa informacyjne rozumiane jako wiedza, dane oraz wszelkie informacje wpływające na wartość Ministerstwa, w tym informacje udokumentowane,

b) zasoby ludzkie rozumiane jako pracownicy oraz ich wiedza, umiejętności, doświadczenie i kwalifikacje,

c) usługi i licencje,

d) wartości niematerialne, w tym wizerunek, kultura organizacyjna i wartości etyczne,
e) systemy teleinformatyczne i cyberprzestrzeń Ministerstwa,
f) urządzenia dostępowe i oprogramowanie,
g) zabezpieczenia organizacyjne, techniczne oraz fizyczne i środowiskowe,
h) siedziba i nieruchomości oraz poszczególne pomieszczenia użytkowane przez Ministerstwo;

2) bezpieczeństwo informacji – zabezpieczenie i zachowanie informacji w zakresie integralności, dostępności i poufności przed nieuprawnionym dostępem lub nieuprawnioną zmianą; dodatkowo mogą być brane pod uwagę takie atrybuty jak rozliczalność, autentyczność, niezaprzeczalność oraz niezawodność;
3) dostępność – właściwość polegającą na tym, że informacja jest dostępna i użyteczna na żądanie uprawnionego podmiotu;
3) dyrektor generalny – dyrektora generalnego Ministerstwa lub osobę przez niego upoważnioną lub osobę zastępującą;
4) dyrektor komórki organizacyjnej – dyrektora departamentu lub biura w Ministerstwie albo kierującego takim departamentem lub biurem;
5) gestor systemu teleinformatycznego – dyrektora komórki organizacyjnej, który decyduje o funkcjonalnościach systemu teleinformatycznego przetwarzającego dane z obszaru właściwego dla kierowanej przez niego komórki organizacyjnej;
6) incydent związany z bezpieczeństwem informacji – pojedyncze niepożądane lub niespodziewane zdarzenie związane z bezpieczeństwem informacji lub serię takich zdarzeń, które zagrażają bezpieczeństwu informacji oraz stwarzają znaczne prawdopodobieństwo utraty aktywów lub zakłócenia realizacji zadań;
7) informatyczny nośnik danych – materiał lub urządzenie służące do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej, w szczególności dysk magnetyczny, dysk SSD, dysk hybrydowy, pamięć typu flash, CD, DVD, BluRay, karta pamięci;
8) integralność – właściwość polegającą na zapewnieniu dokładności i kompletności informacji;
9) komórka organizacyjna – departament lub biuro wymienione w zarządzeniu Nr 226 Prezesa Rady Ministrów z dnia 29 lipca 2022 r. w sprawie nadania statutu Ministerstwu Funduszy i Polityki Regionalnej (M.P. z 2024 r. poz. 500, 555 i 923);
10) Minister – ministra właściwego do spraw rozwoju regionalnego;

11) pełnomocnik – Pełnomocnika do spraw Bezpieczeństwa Informacji w Ministerstwie;
12) podatność – słabość lub wrażliwość aktywa lub grupy aktywów w zakresie funkcjonowania Ministerstwa, która może wpłynąć na wystąpienie zagrożenia i jego ewentualne skutki; podatność może dotyczyć w szczególności sposobu zarządzania lub postępowania, personelu, zależności, relacji, kontaktów wewnętrznych i zewnętrznych, czynnika technologicznego lub niedoskonałości zabezpieczeń;
13) poufność – właściwość polegającą na tym, że informacja nie jest udostępniana ani ujawniana nieuprawnionym osobom, podmiotom lub procesom;
14) przegląd – element Systemu Zarządzania Bezpieczeństwem Informacji obejmujący weryfikację i analizę procesów, procedur, planów i innych dokumentów związanych z wdrożeniem, funkcjonowaniem i kontrolą tego Systemu w rozumieniu przepisów rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych;
15) ryzyko – potencjalną sytuację, w której określone zagrożenie wykorzysta podatność aktywa lub grupy aktywów, powodując w ten sposób naruszenie poufności, integralności, dostępności lub innych atrybutów bezpieczeństwa informacji;
16) 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 12 lipca 2024 r. – Prawo komunikacji elektronicznej (Dz. U. poz. 1221);
17) sytuacja awaryjna – zdarzenie powodujące zakłócenie procesów w jednej albo kilku komórkach organizacyjnych, którego skutki powodują utratę ciągłości działania Ministerstwa;
18) sytuacja kryzysowa – niespodziewane i niepożądane zdarzenie związane z bezpieczeństwem przetwarzania informacji, w szczególności w systemach teleinformatycznych, lub serię takich zdarzeń, które mogą zakłócić lub zakłócają proces realizacji zadań Ministerstwa; może dotyczyć w szczególności bezpieczeństwa ludzi, mienia w znacznych rozmiarach lub środowiska, wywołując znaczne ograniczenia w funkcjonowaniu Ministerstwa;

19) szacowanie ryzyka bezpieczeństwa informacji – kompleksowy proces identyfikowania, analizy i oceny ryzyka bezpieczeństwa informacji;
20) SZBI – System Zarządzania Bezpieczeństwem Informacji stanowiący część systemu zarządzania, odnoszący się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji, obejmujący strukturę organizacyjną, polityki, planowane działania, odpowiedzialności, zasady, procedury, procesy i aktywa;
21) użytkownik – pracownika, stażystę, wolontariusza, praktykanta lub inną osobę świadczącą usługi lub wykonującą inne zadania na rzecz Ministerstwa lub Ministra na podstawie umowy cywilnoprawnej;
22) zabezpieczenie – działanie lub rozwiązanie, które ogranicza prawdopodobieństwo wystąpienia ryzyka lub minimalizuje jego negatywne skutki oraz wpływa na osiągnięcie celów; wyróżnia się trzy rodzaje zabezpieczeń funkcjonujących w Ministerstwie:
    a) organizacyjne – w szczególności struktury organizacyjne, polityki, procedury postępowania, zarządzenia, regulaminy, klauzule bezpieczeństwa, w tym klauzule poufności, zakresy obowiązków pracowników, szkolenia, audyty wewnętrzne i zewnętrzne bezpieczeństwa informacji, kontrole,
    b) techniczne – w szczególności systemy bezpieczeństwa teleinformatycznego, systemy kontroli dostępu, depozytory kluczy, urządzenia alarmowe, sygnalizacyjne lub monitoringu, oprogramowanie antywirusowe,
    c) fizyczne i środowiskowe – w szczególności ogrodzenie, drzwi, pomieszczenia plombowane, zamykane szafy, sejfy i strefy ochronne, zabezpieczenia okablowania i klimatyzacji, a także urządzenia do pomiarów temperatury i wilgotności;
23) zagrożenie – zdarzenie, zjawisko, działanie lub zaniechanie, które może skutkować naruszeniem bezpieczeństwa informacji, w tym jej integralności, dostępności lub poufności, lub doprowadzić do szkody lub nieosiągnięcia celów Ministerstwa.

§ 3. 1. Polityka jest podstawowym elementem dokumentacji SZBI.

2. Polityką objęte są wszystkie informacje wykorzystywane przez Ministerstwo, niezależnie od formy i nośnika przetwarzania lub dystrybucji (ustne, pisemne, nagrania audio i video), w tym utrwalone na informatycznych nośnikach danych, w systemach teleinformatycznych oraz wytworzone w dokumentach papierowych i elektronicznych, będące własnością Ministerstwa lub powierzone w ramach umów lub porozumień z podmiotami zewnętrznymi, w tym z kontrahentami lub wykonawcami.

3. Postanowienia Polityki są uwzględniane przy opracowaniu pozostałej dokumentacji SZBI, w szczególności polityk, regulaminów, procedur, instrukcji i wytycznych obowiązujących w Ministerstwie.

4. Obowiązujące w Ministerstwie regulacje wewnętrzne należy procedować i wdrażać z uwzględnieniem konieczności zapewnienia ochrony aktywów, w szczególności aktywów informacyjnych.

5. Polityka nie ingeruje w treść dokumentów:

1) dedykowanych dla systemów zarządzania bezpieczeństwem informacji, certyfikowanych na zgodność z Polską Normą PN-EN ISO/IEC 27001 lub zarządzanych przez firmy zewnętrzne (outsourcing), które funkcjonują lub mogą funkcjonować w Ministerstwie;
2) wynikających z przepisów o ochronie informacji niejawnych.

6. Jeżeli odrębne przepisy odnoszące się do przetwarzania informacji przewidują dalej idącą ochronę niż wynika to z Polityki, stosuje się te przepisy.

§ 4. Polityka ma zastosowanie do wszystkich komórek organizacyjnych i obejmuje zakresem nie tylko obszar Ministerstwa, ale także miejsca i sytuacje, w których informacje związane z działalnością Ministerstwa są przetwarzane poza jego siedzibą, w szczególności w przypadku zdalnego korzystania z systemów teleinformatycznych Ministerstwa, w tym pracy zdalnej.

§ 5. Do przestrzegania Polityki są obowiązane wszystkie osoby posiadające dostęp do aktywów, w tym w szczególności użytkownicy.

Rozdział 2

Realizacja Polityki i zasady zarządzania bezpieczeństwem informacji

§ 6. 1. Polityka jest realizowana w Ministerstwie przez:

1) zapewnienie odpowiedniej jakości procesów przetwarzania informacji, w szczególności odpowiednich warunków do ich realizacji przez sprawne i efektywne narzędzia;
2) szkolenie pracowników w zakresie bezpieczeństwa informacji adekwatne do wykonywanych zadań oraz posiadanej wiedzy, umiejętności i doświadczenia;
3) zapewnienie ochrony organizacyjnej, technicznej oraz fizycznej i środowiskowej aktywów przed dostępem osób nieuprawnionych, w szczególności przed nieuprawnionym wykorzystaniem, kradzieżą, uszkodzeniem, nieuprawnioną zmianą lub zniszczeniem;
4) zabezpieczenie aktywów, w tym systemów teleinformatycznych eksploatowanych w Ministerstwie, przed skutkami zagrożeń;

5) zabezpieczenie fizyczne i środowiskowe aktywów przed ich uszkodzeniem lub zniszczeniem w wyniku pożaru, zalania, ataku terrorystycznego, zjawisk naturalnych lub innych zagrożeń;
6) zapewnienie ciągłości przetwarzania informacji w Ministerstwie;
7) zapewnienie możliwości sprawnego odtworzenia aktywów w przypadku ich zniszczenia;
8) zapewnienie gotowości do reakcji na sytuację awaryjną lub kryzysową;
9) zapewnienie rozwiązań organizacyjnych i systemowych regulujących zasady i sposób zarządzania bezpieczeństwem informacji;
10) zapewnienie spójnej polityki informacyjnej Ministerstwa;
11) zapewnienie właściwych zapisów w zakresie bezpieczeństwa informacji w umowach cywilnoprawnych z podmiotami zewnętrznymi, w tym z kontrahentami lub wykonawcami, w szczególności stosowanie klauzul poufności;
12) przestrzeganie podstawowych zasad zarządzania bezpieczeństwem informacji, o których mowa w § 8;
13) zapewnienie działań kontrolnych w zakresie przestrzegania Polityki.

2. Stosowanie zabezpieczeń lub ich grup powinno uwzględniać następujące warunki:

1) zabezpieczenia powinny być adekwatne do wymogów prawnych oraz wyników audytów wewnętrznych i zewnętrznych bezpieczeństwa informacji i szacowania ryzyka bezpieczeństwa informacji;
2) zabezpieczenia organizacyjne, techniczne oraz fizyczne i środowiskowe powinny uzupełniać się wzajemnie (grupy zabezpieczeń), zapewniając wymagany poziom bezpieczeństwa informacji;
3) w doborze zabezpieczeń należy kierować się w szczególności:
   a) adekwatnością,
   b) zaleceniami Polskiej Normy PN-EN ISO/IEC 27002:2023-01,
   c) wynikami szacowania ryzyka bezpieczeństwa informacji;
4) świadomość użytkowników w zakresie bezpieczeństwa informacji powinna być rozwijana, w szczególności przez różne formy podnoszenia kwalifikacji;
5) należy unikać niepotrzebnego dublowania zabezpieczeń, uwzględniając racjonalne gospodarowanie środkami publicznymi, optymalizację potrzeb oraz ograniczenia i uwarunkowania prawno-organizacyjne Ministerstwa;
6) należy podejmować działania na rzecz utrzymania standardów współpracy Ministerstwa z podmiotami zewnętrznymi, w tym z kontrahentami lub wykonawcami, przez stosowanie

klauzul poufności w ramach realizacji umów, porozumień, listów intencyjnych i innych form relacji, obowiązujących te podmioty również po ustaniu współpracy.

3. Szczegółowe metody i sposoby implementacji mechanizmów, o których mowa w ust. 1, mogą być określone w innych niż Polityka dokumentach stanowiących dokumentację SZBI.

§ 7. 1. Skuteczność SZBI zachowuje się przy jednoczesnym zastosowaniu uzupełniających się elementów regulujących obszary bezpieczeństwa organizacyjnego, technicznego oraz fizycznego i środowiskowego.

2. Poziom bezpieczeństwa informacji jest odpowiedni wówczas, gdy spełnione są następujące warunki:

1) dokonano szacowania ryzyka bezpieczeństwa informacji;
2) wdrożono skuteczne zabezpieczenia wymagane przepisami prawa i postanowieniami Polityki.

§ 8. 1. W Ministerstwie stosuje się następujące podstawowe zasady zarządzania bezpieczeństwem informacji:

1) wiedzy koniecznej (ograniczonego dostępu do informacji) – użytkownik posiada dostęp tylko do tych informacji, które są konieczne do realizacji powierzonych mu zadań; zasada ta dotyczy głównie informacji wrażliwych i ma ograniczone znaczenie dla określonych grup informacji, w szczególności informacji dostępnych publicznie;
2) 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 w szczególności wydruków z systemu centralnego wydruku;
3) niewygody uzasadnionej – bezpieczeństwo informacji opiera się na ograniczeniach oraz jest niewygodne; środki ochrony nie mogą nadmiernie utrudniać realizacji celów i zadań Ministerstwa;
4) separacji obowiązków – pojedyncze osoby nie mogą wykonywać krytycznych zadań w całości;
5) dyskrecji (ograniczonego zaufania i odpowiedzialnej konwersacji) – wszelkie informacje służbowe mogą być przekazywane wyłącznie osobom uprawnionym do ich pozyskania w celu wykonywania zadań i w zakresie do tego niezbędnym; zasada ta ma ograniczone

znaczenie dla określonych grup informacji, w szczególności informacji dostępnych publicznie;

6) obecności koniecznej – prawo przebywania w określonych miejscach, istotnych dla bezpieczeństwa informacji, powinny mieć tylko osoby uprawnione;
7) zamykania pomieszczeń – niedopuszczalne jest pozostawienie pod nieobecność użytkownika niezabezpieczonego pomieszczenia służbowego, zarówno w godzinach pracy, jak i po jej zakończeniu; na zakończenie dnia pracy ostatnia wychodząca z pomieszczenia osoba powinna zamknąć wszystkie okna i drzwi oraz zabezpieczyć klucz do pomieszczenia;
8) nadzorowania dokumentów – po godzinach pracy wszystkie dokumenty zawierające informacje podlegające ochronie powinny być przechowywane w miejscach zabezpieczonych przed dostępem osób nieuprawnionych;
9) stałej gotowości – niedopuszczalne jest tymczasowe wyłączanie mechanizmów zabezpieczających systemy teleinformatyczne funkcjonujące w Ministerstwie bez zastosowania alternatywnych mechanizmów; systemy powinny być sprawne i przygotowane na zidentyfikowane zagrożenia;
10) zachowania prywatności kont w systemach teleinformatycznych – użytkownik jest obowiązany do pracy w systemach teleinformatycznych na przypisanych lub udostępnionych mu kontach; zabronione jest udostępnianie własnych kont osobom trzecim;
11) poufności haseł – użytkownik jest obowiązany do zachowania poufności udostępnionych mu haseł i kodów dostępu, w szczególności do systemów teleinformatycznych;
12) legalnego oprogramowania – w Ministerstwie wykorzystywane jest oprogramowanie zakupione z odpowiednią licencją i gwarantujące pełne wsparcie ze strony producenta tego oprogramowania;
13) zgłaszania incydentów związanych z bezpieczeństwem informacji – użytkownik ma obowiązek niezwłocznie zgłosić wystąpienie lub podejrzenie wystąpienia incydentu związanego z bezpieczeństwem informacji;
14) automatyzacji backupu – procesy tworzenia kopii zapasowych powinny być zautomatyzowane oraz niemożliwe do przerwania przez użytkownika;
15) ochrony informatycznych nośników danych – dane kopiowane na nośniki i wynoszone poza Ministerstwo powinny być odpowiednio zabezpieczone w czasie transportu i przechowywania, co najmniej przez szyfrowanie;

16) ochrony informacji zwartych w dokumentach w formie papierowej wynoszonych poza Ministerstwo – dokumenty powinny być umieszczane w kopertach lub teczkach, na których jest zamieszczona instrukcja dotycząca postępowania w przypadku znalezienia koperty lub teczki przez osobę nieuprawnioną, zawierająca informację o zakazie jej otwierania i adresie, na który powinna zostać zwrócona; w przypadku odbioru takich materiałów należy je przekazać do odpowiedniej komórki organizacyjnej lub do komórki organizacyjnej właściwej do spraw bezpieczeństwa informacji;
17) adekwatności zabezpieczeń – używane zabezpieczenia powinny być adekwatne do zagrożeń, podatności, wartości aktywów oraz innych istotnych okoliczności wpływających na środowisko wewnętrzne i zewnętrzne Ministerstwa, takich jak zagrożenie przestępczością pospolitą, niepokoje społeczne, poziom ochrony fizycznej na terenie Ministerstwa oraz świadomość i dyscyplina użytkowników;
18) kompleksowości ochrony (asekuracji zabezpieczeń) – ochrona aktywów, w tym systemów teleinformatycznych tworzących system przetwarzania informacji, powinna opierać się na stosowaniu różnych zabezpieczeń organizacyjnych, technicznych oraz fizycznych i środowiskowych, a także ich ochronie prawnej;
19) ochrony niezbędnej – minimalny wymagany poziom bezpieczeństwa informacji wynika z obowiązujących przepisów prawa; zastosowanie wyższych poziomów bezpieczeństwa informacji uzasadniają szczególne potrzeby Ministerstwa i wyniki szacowania ryzyka bezpieczeństwa informacji;
20) bezpiecznej współpracy z podmiotami zewnętrznymi – dokumenty regulujące współpracę powinny zawierać stosowne klauzule bezpieczeństwa, w tym klauzule: poufności, o zasadach postępowania z pozyskaną informacją, niszczenia lub zwrotu dokumentacji po jej wykorzystaniu;
21) ewolucji – SZBI jest stale monitorowany i dostosowywany do zmieniających się warunków wewnętrznych i zewnętrznych;
22) podwyższonego poziomu ochrony zbiorów informacji – w szczególnie uzasadnionych przypadkach zbiór informacji powinien być bardziej chroniony niż poszczególne informacje, które się na niego składają;
23) czystego biurka – podczas nieobecności użytkownika na stanowisku pracy dokumenty i informatyczne nośniki danych należy odpowiednio zabezpieczyć przed dostępem osób nieuprawnionych, w szczególności przez umieszczenie i zamknięcie w szafie lub sejfie;

24) czystej drukarki – materiały wydrukowane nie mogą być pozostawiane na drukarce; należy je zabrać z drukarki od razu po wydrukowaniu i odpowiednio zabezpieczyć;
25) czystego ekranu – na czas nieobecności użytkownika na stanowisku pracy dostęp do komputera jest blokowany, a po zakończeniu pracy komputer jest wyłączany, chyba że dany komputer musi pracować w trybie ciągłym; w czasie obecności użytkownika monitor powinien być tak ustawiony, aby nie pozwalał na zapoznanie się z wyświetlanymi treściami przez osoby nieuprawnione;
26) czystego kosza – dokumenty papierowe, z wyjątkiem materiałów promocyjnych, marketingowych i innych publicznie dostępnych, powinny być niszczone w sposób uniemożliwiający ich odczytanie;
27) czystej tablicy – po zakończonym spotkaniu należy zabrać wszystkie materiały oraz wyczyścić tablice, jeśli były wykorzystywane.

2. Katalog zasad, o których mowa w ust. 1, może być rozszerzony lub uszczegółowiony w innych niż Polityka dokumentach stanowiących dokumentację SZBI.

Rozdział 3

Odpowiedzialność i uprawnienia w zakresie bezpieczeństwa informacji

§ 9. 1. Właściwe zarządzanie bezpieczeństwem informacji w Ministerstwie zapewnia ustalona odpowiednio na potrzeby tego zarządzania wewnętrzna struktura organizacyjna, w której skład wchodzą w szczególności:

1) Minister;
2) sekretarze stanu, podsekretarze stanu i dyrektor generalny;
3) Zespół do spraw SZBI;
4) pełnomocnik;
5) Inspektor Ochrony Danych;
6) pełnomocnicy do spraw ochrony danych osobowych w komórkach organizacyjnych;
7) Pełnomocnik do spraw ochrony informacji niejawnych;
8) Pełnomocnik do spraw otwartości danych;
9) dyrektorzy komórek organizacyjnych.

2. Dane osób pełniących funkcje, o których mowa w ust. 1 pkt 5–8, są opublikowane w intranecie lub na stronie internetowej Ministerstwa.

§ 10. 1. Odpowiedzialność za bezpieczeństwo informacji w Ministerstwie ponoszą wszystkie osoby posiadające dostęp do aktywów, w tym w szczególności osoby, o których mowa w § 9 ust. 1.

2. Niezależnie od odpowiedzialności, o której mowa w ust. 1, pracownicy są dodatkowo obowiązani do zachowania tajemnicy pracodawcy zgodnie z przepisami prawa pracy.

3. Odpowiedzialność i uprawnienia w zakresie bezpieczeństwa informacji w systemach teleinformatycznych, dla których ustanowiono SZBI certyfikowany za zgodność z Polską Normą PN-EN ISO/IEC 27001, określa dokumentacja tego systemu.

§ 11. 1. Minister:

1) decyduje o celach i środkach przetwarzania informacji, w tym danych osobowych, jako ich administrator;
2) ustanawia SZBI oraz Politykę;
3) wyznacza lub powołuje:
   a) Inspektora Ochrony Danych,
   b) Pełnomocnika do spraw ochrony informacji niejawnych,
   c) Pełnomocnika do spraw otwartości danych.

2. Sekretarze stanu, podsekretarze stanu oraz dyrektor generalny odpowiadają, w zakresie swojej właściwości, za nadzorowanie bezpieczeństwa informacji w Ministerstwie.

3. Dyrektor generalny:

1) zatwierdza raport z przeglądu, o którym mowa w § 12 ust. 6;
2) wydaje wewnętrzne akty regulujące zasady funkcjonowania i zarządzania bezpieczeństwem informacji;
3) w przypadku wystąpienia takiej potrzeby określa zadania dyrektorów komórek organizacyjnych mające na celu zapewnienie bezpieczeństwa informacji;
4) egzekwuje odpowiedzialność pracowników oraz stażystów, wolontariuszy i praktykantów w Ministerstwie za naruszenia bezpieczeństwa informacji, w zakresie adekwatnym do nałożonych na nich obowiązków i posiadanych uprawnień.

4. Zadania Zespołu do spraw SZBI określają odrębne przepisy.

5. Pełnomocnik:

1) zapewnia koordynację spraw z zakresu bezpieczeństwa informacji;
2) nadzoruje opracowanie dokumentacji SZBI;
3) współpracuje z dyrektorem komórki organizacyjnej właściwej do spraw szkoleń przy realizacji szkoleń, o których mowa w ust. 10;

4) inicjuje oraz nadzoruje działania wdrożeniowe, korygujące i zapobiegawcze w zakresie bezpieczeństwa informacji;
5) nadzoruje działania naprawcze podjęte w związku z wykrytymi incydentami związanymi z bezpieczeństwem informacji;
6) organizuje przeglądy oraz nadzoruje realizację wynikających z nich ustaleń;
7) jest obowiązany do:
   a) wydawania zaleceń w zakresie funkcjonowania SZBI,
   b) uzyskania wyjaśnień od użytkowników, w szczególności w przypadku wystąpienia incydentów związanych z bezpieczeństwem informacji i nieprawidłowości w zakresie funkcjonowania SZBI,
   c) podejmowania działań dotyczących bezpieczeństwa informacji w zakresie niezastrzeżonym do kompetencji innych osób,
   d) rekomendowania rozwiązań organizacyjno-technicznych zwiększających skuteczność zarządzania w obszarze SZBI,
   e) opracowania i prowadzenia wykazu dokumentacji SZBI, jego aktualizacji oraz udostępnienia w wewnętrznym systemie informatycznym Ministerstwa.

6. Zadania Inspektora Ochrony Danych określa art. 39 RODO oraz akty wewnętrzne Ministra lub wewnętrzne akty dyrektora generalnego.

7. Uprawnienia i obowiązki:

1) pełnomocników do spraw ochrony danych osobowych w komórkach organizacyjnych,
2) Pełnomocnika do spraw ochrony informacji niejawnych,
3) Pełnomocnika do spraw otwartości danych,

– określają odrębne przepisy lub udzielone upoważnienia.

8. Dyrektorzy komórek organizacyjnych, w zakresie swojej właściwości, odpowiadają za:

1) wdrożenie i przestrzeganie Polityki;
2) ochronę aktywów;
3) szacowanie ryzyka bezpieczeństwa informacji;
4) realizację procedur zapewniających ciągłość funkcjonowania kierowanej komórki organizacyjnej w sytuacjach awaryjnych i kryzysowych;
5) umożliwienie pracownikom udziału w szkoleniach, o których mowa w ust. 10;
6) właściwy tryb zgłaszania, postępowania i dokumentowania incydentów związanych z bezpieczeństwem informacji, zgodnie z wewnętrznymi regulacjami w tym zakresie.

9. Dyrektor komórki właściwej do spraw audytu wewnętrznego zapewnia przeprowadzanie co najmniej raz w roku audytu SZBI.

10. Dyrektor komórki organizacyjnej właściwej do spraw szkoleń zapewnia pracownikom, w szczególności członkom Zespołu do spraw SZBI i audytorom wewnętrznym, szkolenia w zakresie bezpieczeństwa informacji.

11. Udział pracowników w szkoleniach, o których mowa w ust. 10, jest obowiązkowy.

12. Szkolenia, o których mowa w ust. 10:

1) organizuje komórka organizacyjna właściwa do spraw szkoleń;
2) przeprowadza komórka organizacyjna właściwa do spraw bezpieczeństwa informacji.

13. Dyrektor komórki organizacyjnej właściwej do spraw komunikacji bierze udział w zarządzaniu dostępem do informacji zgodnie z przepisami prawa i polityką informacyjną Ministerstwa.

14. Dyrektor komórki organizacyjnej właściwej do spraw ochrony fizycznej zapewnia zabezpieczenia organizacyjne, techniczne oraz fizyczne i środowiskowe aktywów, biorąc pod uwagę udokumentowane wytyczne przekazane przez właścicieli aktywów, opracowane na podstawie szacowania ryzyka bezpieczeństwa informacji.

15. Dyrektor komórki organizacyjnej właściwej do spraw informatyki:

1) zapewnia:
   a) bezpieczeństwo systemów teleinformatycznych i łączności telefonicznej w Ministerstwie,
   b) budowę, rozwój i utrzymanie systemów, o których mowa w lit. a,
   c) środki techniczne i organizacyjne umożliwiające ochronę informacji przetwarzanych w systemach, o których mowa w lit. a;
2) odpowiada za koordynację zadań Ministerstwa jako podmiotu krajowego systemu cyberbezpieczeństwa w rozumieniu ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

16. Użytkownicy odpowiadają w szczególności za:

1) przestrzeganie Polityki;
2) ochronę aktywów w zakresie adekwatnym do nałożonych na nich obowiązków i posiadanych uprawnień;
3) niezwłoczne reagowanie w przypadku wystąpienia lub podejrzenia wystąpienia incydentu związanego z bezpieczeństwem informacji oraz postępowanie zgodnie z wewnętrznymi regulacjami w tym zakresie;

4) zabezpieczenie informacji przed ich udostępnieniem osobom nieuprawnionym, zabraniem przez osoby nieuprawnione, przetwarzaniem z naruszeniem przepisów prawa oraz nieuprawnioną zmianą, utratą, uszkodzeniem lub zniszczeniem;
5) zachowanie w tajemnicy informacji pozyskanych w ramach wykonywania obowiązków służbowych w Ministerstwie oraz przestrzeganie zasad bezpiecznego ich przetwarzania, w tym w systemach teleinformatycznych.

17. Gestorzy systemów teleinformatycznych, w zakresie swojej właściwości, zapewniają bezpieczeństwo systemów teleinformatycznych funkcjonujących w Ministerstwie.

18. Osoby reprezentujące Ministra lub Ministerstwo w zakresie umów cywilnoprawnych odpowiadają za prawidłowość ich zawierania i realizacji.

§ 12. 1. W Ministerstwie, co najmniej raz w roku, jest przeprowadzany przegląd.

2. W przypadku istotnych zmian organizacyjnych lub działań związanych z przeprowadzonym audytem wewnętrznym lub zewnętrznym bezpieczeństwa informacji, może być przeprowadzony dodatkowy przegląd.

3. Przegląd jest przeprowadzany w formule pełnej, obejmującej wszystkie aspekty SZBI, albo w formule częściowej.

4. Dyrektor generalny zleca pełnomocnikowi realizację przeglądu ustalając termin, zakres oraz szczegółowe zasady jego przeprowadzenia.

5. Dyrektorzy komórek organizacyjnych uczestniczących w przeglądzie współpracują z pełnomocnikiem w zakresie jego realizacji.

6. Pełnomocnik sporządza raport z przeglądu, który uzgadnia z dyrektorami komórek organizacyjnych uczestniczących w przeglądzie.

7. Raport, o którym mowa w ust. 6, podlega zaopiniowaniu przez Zespół do spraw SZBI przed jego przekazaniem do zatwierdzenia przez dyrektora generalnego.

8. Komórka organizacyjna właściwa do spraw bezpieczeństwa informacji zapewnia obsługę organizacyjno-techniczną przeglądu oraz przechowuje dokumentację wytworzoną w ramach przeglądów.

9. Pełnomocnik może określić szczegółową procedurę przeglądu.

Rozdział 4

Klasyfikacja informacji i zasady postępowania z informacjami

§ 13. 1. W Ministerstwie przyjmuje się następującą klasyfikację informacji oraz ich oznaczenie:

KLASYFIKACJA INFORMACJI	OPIS
Informacja nie stanowiąca informacji prawnie chronionej lub wrażliwej	Informacje, których obowiązek udostępniania wynika z przepisów prawa, w szczególności informacje publiczne w rozumieniu ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej. Są to – co do zasady – informacje ogólnie dostępne. Informacje te udostępniane są w szczególności w intranecie lub na stronie internetowej Ministerstwa.
Informacja prawnie chroniona	Informacje stanowiące dane osobowe podlegające ochronie na mocy przepisów o ochronie danych osobowych. Informacje przekazane Ministerstwu przez przedsiębiorcę, co do których podjął on działania w celu zachowania ich w poufności, w szczególności nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą (tajemnica przedsiębiorstwa). Informacje chronione na mocy ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (uregulowane odrębnymi przepisami). Inne informacje chronione z mocy prawa.
Informacja wrażliwa	Informacje wewnętrzne Ministerstwa, wytworzone w Ministerstwie lub na jego rzecz, niewchodzące w zakres informacji zaklasyfikowanych do pozostałych grup. Są to informacje o ograniczonym dostępie zarówno wewnątrz Ministerstwa, jak i poza nim – udostępniane na zasadzie wiedzy koniecznej, a zatem w szczególności nie mogą być opublikowane w intranecie lub na stronie internetowej Ministerstwa.
Informacja wymagająca klasyfikacji	Informacje, których nie zaklasyfikowano do żadnej z grup, i które powinny zostać sklasyfikowane obecnie lub w przyszłości.

2. Wprowadzenie klasyfikacji informacji, o której mowa w ust. 1, nie powoduje konieczności fizycznego oznaczania informacji udokumentowanych. Dokonuje się w nich jedynie odwzorowania cyfrowego zgodnie z obowiązującymi w Ministerstwie przepisami kancelaryjno-archiwalnymi. W przypadku oznaczenia dokumentu etykietą związaną z klasyfikacją informacji, umieszcza się ją na każdej stronie dokumentu na środku pierwszego i ostatniego wiersza.

§ 14. 1. W Ministerstwie przyjmuje się następujące zasady postępowania z informacjami w ramach klasyfikacji, o której mowa w § 13 ust. 1:

Informacja nie stanowiąca informacji prawnie chronionej lub wrażliwej	PRZETWARZANIE, PRZECHOWYWANIE, PRZEKAZYWANIE: w sposób gwarantujący zachowanie integralności i dostępności informacji. ZMIANA KLASYFIKACJI I UDOSTĘPNIANIE: na zasadach i w trybie przewidzianych przepisami prawa. NISZCZENIE: zgodnie z wymogami określonymi w przepisach prawa lub zawartych przez Ministerstwo umowach oraz zgodnie z Instrukcją kancelaryjną.
Informacja prawnie chroniona	PRZETWARZANIE: w sposób gwarantujący zapewnienie bezpieczeństwa informacji, ze szczególnym uwzględnieniem atrybutów integralności, dostępności i poufności oraz innych atrybutów bezpieczeństwa, które są wymagane dla danej informacji chronionej na podstawie przepisów prawa. PRZECHOWYWANIE: w sposób gwarantujący zapewnienie bezpieczeństwa informacji. PRZEKAZYWANIE: wyłącznie osobom uprawnionym, w sposób gwarantujący zachowanie integralności i poufności oraz zgodnie z wymaganiami określonymi w przepisach prawa lub zawartych przez Ministerstwo umowach. ZMIANA KLASYFIKACJI: zgodnie z wymaganiami określonymi w przepisach prawa lub zawartych przez Ministerstwo umowach. UDOSTĘPNIANIE: wyłącznie osobom uprawnionym lub uprawnionym podmiotom po uzyskaniu zgody dyrektora właściwej komórki organizacyjnej.

	NISZCZENIE: zgodnie z wymogami określonymi w przepisach prawa lub zawartych przez Ministerstwo umowach oraz zgodnie z Instrukcją kancelaryjną.
Informacja wrażliwa	PRZETWARZANIE: w sposób gwarantujący zapewnienie bezpieczeństwa informacji, ze szczególnym uwzględnieniem atrybutów integralności, dostępności i poufności. PRZECHOWYWANIE: w sposób gwarantujący zapewnienie bezpieczeństwa informacji. PRZEKAZYWANIE: wyłącznie osobom uprawnionym, w sposób gwarantujący zachowanie integralności i dostępności informacji oraz zgodnie z wymaganiami określonymi w zawartych przez Ministerstwo umowach, jeśli określono sposób przekazywania lub udostępniania. ZMIANA KLASYFIKACJI: możliwa po podjęciu decyzji przez osoby uprawnione oraz zgodnie z wymaganiami określonymi w przepisach prawa lub zawartych przez Ministerstwo umowach. UDOSTĘPNIANIE: wyłącznie po uzyskaniu zgody pełnomocnika. NISZCZENIE: zgodnie z wymogami określonymi w przepisach prawa lub zawartych przez Ministerstwo umowach oraz zgodnie z Instrukcją kancelaryjną.
Informacja wymagająca klasyfikacji	Zgodnie z zasadami obowiązującymi dla każdej grupy – po dokonaniu klasyfikacji danej informacji.

2. Klasyfikacja informacji w systemach teleinformatycznych, dla których ustanowiono SZBI certyfikowany za zgodność z PN-EN ISO/IEC 27001, odbywa się w trybie przewidzianym w dokumentacji tego systemu.

Rozdział 5

Szacowanie ryzyka bezpieczeństwa informacji

§ 15. 1. W obszarze bezpieczeństwa informacji szacowanie ryzyka bezpieczeństwa informacji jest obligatoryjne. Przeprowadza się je cykliczne, nie rzadziej niż raz w roku.

2. Dodatkowe szacowanie ryzyka bezpieczeństwa informacji jest przeprowadzane zgodnie z potrzebami, w szczególności przed opracowaniem dokumentacji bezpieczeństwa dla danego obszaru lub systemu teleinformatycznego albo po wystąpieniu istotnych zmian w danym obszarze lub systemie.

3. Szacowanie ryzyka bezpieczeństwa informacji, o którym mowa w ust. 1 i 2:

1) przeprowadza się w oparciu o dostępne metodyki;
2) powinno być udokumentowane.

4. Szacowanie ryzyka bezpieczeństwa informacji w systemach teleinformatycznych, dla których ustanowiono SZBI certyfikowany za zgodność z Polską Normą PN-EN ISO/IEC 27001, odbywa się w trybie przewidzianym w dokumentacji tego systemu.

Rozdział 6

Zapoznanie z Polityką

§ 16. 1. Wszystkie osoby posiadające dostęp do aktywów mają obowiązek zapoznania się z treścią Polityki.

2. Za zapoznanie się z treścią Polityki odpowiada w przypadku:

1) nowo zatrudnionych pracowników – Biuro Zarządzania Zasobami Ludzkimi;
2) pozostałych pracowników – dyrektor komórki organizacyjnej, w której są zatrudnieni;
3) stażystów, wolontariuszy i praktykantów – dyrektor komórki organizacyjnej, w której będą odbywać albo odbywają staż, wolontariat lub praktykę;
4) osób świadczących usługi lub wykonujących inne zadania na rzecz Ministerstwa lub Ministra na podstawie umów cywilnoprawnych – dyrektor komórki organizacyjnej odpowiedzialny za realizację danej umowy;
5) osób, o których mowa w ust. 4 – dyrektor komórki organizacyjnej odpowiedzialny za udzielenie dostępu do aktywów;
6) pozostałych osób – dyrektor komórki organizacyjnej właściwej do spraw bezpieczeństwa informacji.

3. Każda osoba posiadająca dostęp do aktywów jest obowiązana do złożenia oświadczenia o zapoznaniu się z treścią Polityki za pomocą dedykowanej aplikacji. W przypadku braku dostępu do aplikacji dopuszcza się złożenie własnoręcznie podpisanego oświadczenia w postaci papierowej, zgodnie ze wzorem stanowiącym załącznik do Polityki.

4. W przypadku konieczności udzielenia dostępu do aktywów osobie spoza Ministerstwa niebędącej użytkownikiem, dyrektor komórki organizacyjnej odpowiedzialny za udzielenie

dostępu niezwłocznie informuje o tym pełnomocnika. Pełnomocnik poleca takiej osobie zapoznanie się z treścią Polityki i złożenie oświadczenia, o którym mowa w ust. 3. W takiej sytuacji oświadczenie jest składane wyłącznie w postaci papierowej, a dostęp do aktywów jest udzielany po jego złożeniu.

5. Pełnomocnik może udzielić zgody na zapoznanie się z treścią Polityki lub jej częścią osobie spoza Ministerstwa niebędącej użytkownikiem, której nie zostanie udzielony dostęp do aktywów. Zgoda może być udzielona po złożeniu przez taką osobę własnoręcznie podpisanego oświadczenia o zachowaniu w poufności treści Polityki lub jej części. Wzór oświadczenia zostanie opracowany przez pełnomocnika.

6. Oświadczenia, o których mowa w ust. 3 zdanie drugie oraz ust. 4 i 5, są przekazywane do komórki organizacyjnej właściwej do spraw bezpieczeństwa informacji.

7. Użytkowników serwisów internetowych Ministerstwa obowiązują zapisy dedykowanych dla tych serwisów polityk prywatności.

Załącznik do Polityki
bezpieczeństwa informacji

Oświadczenie o zapoznaniu się z Polityką bezpieczeństwa informacji w Ministerstwie Funduszy i Polityki Regionalnej

Niniejszym oświadczam, że zapoznałem/am* się z obowiązującą w Ministerstwie Funduszy i Polityki Regionalnej Polityką bezpieczeństwa informacji i zobowiązuję się do jej przestrzegania.

Ponadto zobowiązuję się do zachowania w tajemnicy informacji prawnie chronionych, do których mam lub będę miał/a* dostęp w związku z wykonywaniem przeze mnie obowiązków pracowniczych lub innych zadań na rzecz Ministerstwa Funduszy i Polityki Regionalnej lub Ministra Funduszy i Polityki Regionalnej, a także sposobów zabezpieczenia tych informacji, zarówno w trakcie wykonywania tych obowiązków/zadań, jak i po ich zakończeniu.

Mam świadomość, że celem Polityki bezpieczeństwa informacji jest zapewnienie odpowiedniego poziomu bezpieczeństwa informacji przetwarzanych w Ministerstwie Funduszy i Polityki Regionalnej, a naruszenia bezpieczeństwa informacji mogą skutkować odpowiedzialnością karną lub dyscyplinarną na zasadach i w trybie przewidzianych w przepisach prawa, w tym w ustawie z dnia 21 listopada 2008 r. o służbie cywilnej (Dz. U. z 2024 r. poz. 409) i ustawie z dnia 26 czerwca 1974 r. – Kodeks pracy (Dz. U. z 2023 r. poz. 1465, z późn. zm.).

…….. …….

imię i nazwisko data i podpis

*niepotrzebne skreślić