**Warszawa, dnia 18 lipca 2023 r.**

**Poz. 18**

# ZARZĄDZENIE
# MINISTRA AKTYWÓW PAŃSTWOWYCH [1)]

z dnia 18 lipca 2023 r.

## w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji w Ministerstwie Aktywów Państwowych

Na podstawie art. 34 ust. 1 ustawy z dnia 8 sierpnia 1996 r. o Radzie Ministrów (Dz. U. z 2022 r. poz. 1188 oraz z 2023 r. poz. 1195 i 1234) zarządza się, co następuje:

**§ 1**. W Ministerstwie Aktywów Państwowych wprowadza się Politykę Bezpieczeństwa Informacji stanowiącą załącznik do zarządzenia.

**§ 2.** 1. W terminie 30 dni od dnia wejścia w życie zarządzenia pracownicy potwierdzą zapoznanie się z treścią Polityki Bezpieczeństwa Informacji przez złożenie oświadczenia, którego wzór stanowi załącznik do Polityki Bezpieczeństwa Informacji.

2. Oświadczenia włącza się do dokumentacji dotyczącej zatrudnienia, zgodnie z § 28 Polityki Bezpieczeństwa Informacji.

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

Minister Aktywów Państwowych: *J. Sasin*

---

[1)] Minister Aktywów Państwowych kieruje działem administracji rządowej – aktywa państwowe, gospodarka złożami kopalin oraz łączność na podstawie § 1 ust. 2 rozporządzenia Prezesa Rady Ministrów z dnia 3 lipca 2023 r. w sprawie szczegółowego zakresu działania Ministra Aktywów Państwowych (Dz. U. poz. 1263).

Załącznik do zarządzenia
Ministra Aktywów Państwowych
z dnia 18 lipca 2023 r. (poz. 18)

# POLITYKA BEZPIECZEŃSTWA INFORMACJI

## ROZDZIAŁ I

## CEL I DEKLARACJA STOSOWANIA

**§ 1.** 1. Kierownictwo Ministerstwa Aktywów Państwowych mając na uwadze kluczową rolę informacji oraz potrzebę ich ochrony dla właściwego funkcjonowania i realizowania zadań Ministerstwa Aktywów Państwowych, zwanego dalej „ministerstwem”, ustanawia Politykę Bezpieczeństwa Informacji, zwaną dalej „PBI”.

2. Celem opracowania PBI jest efektywne zarządzanie bezpieczeństwem informacji przez określenie: ogólnych wymagań i zasad ochrony informacji oraz podmiotów odpowiedzialnych za ochronę informacji, które stanowią fundament dla wszystkich dokumentów opracowanych do tej pory i w przyszłości w ministerstwie.

3. PBI jest nadrzędnym dokumentem składającym się na obowiązujący w ministerstwie System Zarządzania Bezpieczeństwem Informacji, zwany dalej „SZBI”.

4. Kierownictwo ministerstwa deklaruje:

1) uwzględnianie wymagań w zakresie zarządzania bezpieczeństwem informacji przy definiowaniu i realizacji celów strategicznych i operacyjnych związanych z funkcjonowaniem oraz organizacją bieżącej działalności ministerstwa;
2) zaangażowanie w działania zmierzające do zapewnienia należytego poziomu bezpieczeństwa przetwarzanych informacji oraz wspieranie realizacji tych działań;
3) zapewnianie optymalnych warunków do realizacji celów PBI przez wdrażanie, rozwój i uaktualnianie PBI oraz regulacji wynikających z PBI;
4) wspieranie i inicjonowanie nowych kierunków działań mających na celu ciągłe doskonalenie SZBI przy współpracy z pracownikami ministerstwa realizującymi zadania w zakresie zarządzania bezpieczeństwem informacji;
5) dążenie do osiągnięcia standardów zawartych w normach z rodziny ISO/IEC 27000.

## ROZDZIAŁ II

## POSTANOWIENIA OGÓLNE

**§ 2.** 1. PBI została opracowana w oparciu o przepisy prawa powszechnie obowiązującego oraz zasady zawarte w normach z rodziny ISO/IEC 27000, w szczególności:

1) ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913);
2) rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1, Dz.U.UE.L.2018.127.2, Dz.U.UE.L.2021.74.35);
3) ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781);
4) ustawę z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2023 r. poz. 57, 1123 i 1234);
5) ustawę z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2022 r. poz. 902);
6) ustawę z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz. U. z 2022 r. poz. 1710, z późn. zm.[1)]);
7) ustawę z dnia 26 czerwca 1974 r. – Kodeks pracy (Dz. U. z 2022 r. poz. 1510, 1700 i 2140 oraz z 2023 r. poz. 240 i 641);
8) ustawę z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2020 r. poz. 164);
9) ustawę z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2022 r. poz. 2509);
10) ustawę z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2023 r. poz. 120 i 295);
11) ustawę z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. z 2022 r. poz. 1138, z późn. zm. [2)]);
12) ustawę z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz. U. z 2021 r. poz. 1995);

---

1) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2022 r. poz. 1812, 1933 i 2185 oraz z 2023 r. poz. 412 i 825.
2) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2022 r. poz. 1726, 1855, 2339 i 2600 oraz z 2023 r. poz. 289, 818, 852 i 1234.

13) ustawę z dnia 16 grudnia 2016 r. o zasadach zarządzania mieniem państwowym (Dz. U. z 2023 r. poz. 973);
14) ustawę z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2020 r. poz. 344);
15) 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).

2. PBI określa:

1) zarządzanie bezpieczeństwem informacji;
2) zasady bezpieczeństwa informacji;
3) osoby odpowiedzialne oraz ich zakres odpowiedzialności;
4) klasyfikację informacji;
5) szacowanie ryzyka;
6) odpowiedzialność.

**§ 3.** PBI jest integralną częścią dokumentacji SZBI, w skład której wchodzą w szczególności:

1) zarządzenie nr 102 Dyrektora Generalnego Ministerstwa Aktywów Państwowych z dnia 12 lipca 2021 r. w sprawie wprowadzenia „Regulaminu bezpieczeństwa informacji przetwarzanych w systemach teleinformatycznych w Ministerstwie Aktywów Państwowych”;
2) zarządzenie nr 94 Dyrektora Generalnego Ministerstwa Aktywów Państwowych z dnia 18 czerwca 2021 w sprawie wprowadzenia Polityki Ochrony Danych Osobowych;
3) zarządzenie Ministra Aktywów Państwowych z dnia 18 grudnia 2020 r. w sprawie wprowadzenia instrukcji kancelaryjnej, jednolitego rzeczowego wykazu akt i instrukcji w sprawie organizacji i zakresu działania archiwum zakładowego;
4) zarządzenie nr 96 Dyrektora Generalnego Ministerstwa Aktywów Państwowych z dnia 22 czerwca 2021 r. w sprawie zarządzania ryzykiem w Ministerstwie Aktywów Państwowych;
5) zarządzenie nr 128 Dyrektora Generalnego Ministerstwa Aktywów Państwowych z dnia 28 grudnia 2021 r. w sprawie wprowadzenia Instrukcji organizacji i kontroli ruchu osobowego i samochodowego oraz sposobu przechowywania kluczy w Ministerstwie Aktywów Państwowych;

6) zarządzenie nr 45 Dyrektora Generalnego Ministerstwa Aktywów Państwowych z dnia 22 października 2020 r. w sprawie zasad zarządzania procesami w Ministerstwie Aktywów Państwowych;
7) zarządzenie nr 97 Dyrektora Generalnego Ministerstwa Aktywów Państwowych z dnia 22 czerwca 2021 r. w sprawie zasad zarządzania projektami w Ministerstwie Aktywów Państwowych.

**§ 4.** 1. Dokumentacja SZBI ma strukturę hierarchiczną, w której PBI jest dokumentem nadrzędnym nad innymi dokumentami dotyczącymi bezpieczeństwa informacji.

2. Szczegółowe regulacje dokumentacji SZBI opracowuje się i doskonali przez tworzenie: polityk, procedur, instrukcji, regulaminów oraz innych dokumentów, które dotyczą kwestii korzystania z aktywów ministerstwa.

3. Poszczególne rodzaje dokumentacji SZBI mogą opisywać obszar bezpieczeństwa informacji na różnych poziomach szczegółowości.

**§ 5.** PBI są objęte wszystkie informacje wykorzystywane przez ministerstwo, niezależnie od formy i nośnika przetwarzania lub dystrybucji (ustne, pisemne, nagrania audio i wideo), utrwalone na nośnikach elektronicznych, papierowych, w systemach komputerowych, będące własnością ministerstwa oraz powierzone ministerstwu w ramach umów, porozumień z kontrahentami lub wykonawcami.

**§ 6.** Wymagania określone w PBI uwzględnia się w procesie opracowywania i aktualizacji pozostałej dokumentacji w ramach SZBI.

**§ 7.** Wewnętrzne regulacje proceduje się i wdraża z uwzględnieniem założeń zapewniających ochronę aktywów.

**§ 8.** Jeżeli inne przepisy powszechnie obowiązujące lub regulacje ministerstwa odnoszące się do przetwarzania informacji, przewidują dalej idącą ich ochronę, niż wynika to z PBI, stosuje się te przepisy lub regulacje.

**§ 9.** Użyte w PBI określenia i skróty oznaczają:
1) administrator merytoryczny – dyrektora komórki organizacyjnej lub wyznaczonego przez niego pracownika, który odpowiada za funkcjonalności, wdrożenie, utrzymanie i rozwój systemu teleinformatycznego wykorzystywanego do realizacji celów komórki organizacyjnej lub ministerstwa;
2) ASI (administrator systemu informatycznego) – osobę zarządzającą całością lub częścią systemu teleinformatycznego;

3) ABSI (administrator bezpieczeństwa systemów teleinformatycznych) – dyrektora Biura Dyrektora Generalnego lub osobę przez niego wyznaczoną;
4) aktywa (zasoby) – wszystko, co stanowi wartość dla ministerstwa i w związku z tym wymaga ochrony;
5) autentyczność – właściwość polegającą na tym, że pochodzenie lub zawartość danych opisujących obiekt są takie, jak deklarowane;
6) bezpieczeństwo informacji – proces ochrony zasobów informacyjnych przed nieautoryzowanym dostępem, wykorzystaniem, modyfikacją, ujawnieniem i zniszczeniem, obejmujący wszystkie aspekty ochrony poufności, integralności i dostępności informacji oraz inne własności, takie jak autentyczność, rozliczalność, niezaprzeczalność, niezawodność;
7) dostępność – właściwość polegającą na tym, że informacja jest dostępna i użyteczna na żądanie uprawnionego podmiotu;
8) gestor systemu – osobę pełniącą nadzór nad systemem teleinformatycznym i decydującą we wszelkich sprawach merytorycznych dotyczących tego systemu;
9) incydent bezpieczeństwa informacji – pojedyncze zdarzenie lub serię niepożądanych lub niespodziewanych zdarzeń, które stwarzają znaczne prawdopodobieństwo zakłócenia procesów o istotnym znaczeniu dla ministerstwa albo ujawnienie informacji posiadających wartość dla ministerstwa lub chronionych z mocy przepisów prawa;
10) informacja – to co powiedziano lub napisano o kimś lub o czymś, także zakomunikowanie czegoś, jak również dane przetwarzane przy wykorzystaniu sprzętu teleinformatycznego;
11) integralność – właściwość polegającą na zapewnieniu dokładności i kompletności informacji;
12) Kierownictwo ministerstwa – Ministra, sekretarza stanu, podsekretarza stanu, szefa Gabinetu Politycznego Ministra, dyrektora generalnego;
13) niezaprzeczalność – brak możliwości zanegowania swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie;
14) osoba uprawniona – osobę, która z racji wykonywanych obowiązków służbowych lub na podstawie pełnomocnictwa lub upoważnienia nadano uprawnienia;
15) podatność – słabość lub wrażliwość aktywa lub grupy aktywów która może wpłynąć na wystąpienie zagrożenia i jego ewentualne skutki;
16) niezawodność – stałe, spójne zamierzone zachowania oraz skutki;
17) poufność – właściwość polegającą na tym, że informacja nie jest udostępniana ani ujawniana nieuprawnionym osobom, podmiotom lub procesom;

18) pracownik – osobę zatrudnioną w ministerstwie na podstawie umowy o pracę, powołania, mianowania, a także stażystę, wolontariusza, praktykanta lub osobę świadczącą usługi na podstawie umowy cywilnoprawnej na rzecz ministerstwa;
19) RODO – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);
20) rozliczalność – właściwość systemu pozwalającą przypisać określone działanie w systemie do osoby fizycznej lub procesu oraz umiejscowić je w czasie;
21) 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;
22) SZBI – część systemu zarządzania ministerstwem odnoszący się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji, w szczególności obejmujący strukturę organizacyjną, polityki, planowane działania, odpowiedzialności, zasady, procedury, procesy i aktywa mające bezpośredni wpływ na zapewnienie ciągłości działania;
23) zabezpieczenie – działanie lub rozwiązanie, które ogranicza prawdopodobieństwo wystąpienia zagrożenia lub minimalizuje jego negatywne skutki oraz wpływa na osiągnięcie celów, realizowane w ramach jednego z trzech jego rodzajów funkcjonujących w ministerstwie:
    a) organizacyjne (struktury organizacyjne, polityki, procedury, zarządzenia, regulaminy, klauzule w umowach, opisy stanowisk, zakresy obowiązków pracowników, szkolenia, audyty, kontrole itp.),
    b) techniczne (systemy bezpieczeństwa teleinformatycznego, systemy kontroli dostępu, depozytory kluczy, urządzenia alarmowe, sygnalizacyjne lub monitoringu, oprogramowanie antywirusowe itp.),
    c) fizyczne (pracownicy ochrony, kontrola dostępu, drzwi, pomieszczenia plombowane, zamykane szafy, strefy ochronne itp.);
24) zagrożenie – potencjalną przyczynę zdarzenia lub incydentu naruszenia bezpieczeństwa informacji, którego skutkiem może być szkoda (strata) dla ministerstwa.

## ROZDZIAŁ III

## ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI

**§ 10.** Zarządzanie bezpieczeństwem informacji jest realizowane przez:

1) zapewnianie aktualizacji regulacji w zakresie uwzględniającym zmieniające się otoczenie;
2) utrzymywanie aktualności inwentaryzacji sprzętu i oprogramowania;
3) przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowanie działań minimalizujących to ryzyko, odpowiednio do wyników przeprowadzonej analizy;
4) podejmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają niezbędne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji;
5) bezzwłoczną zmianę uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4;
6) zapewnianie szkolenia osób zaangażowanych w przetwarzanie informacji;
7) zapewnianie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami;
8) ustanawianie zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy zdalnej;
9) zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie;
10) zawieranie w umowach podpisanych ze stronami trzecimi uregulowań gwarantujących odpowiedni poziom bezpieczeństwa informacji;
11) ustalanie zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;
12) zapewnianie odpowiedniego poziomu bezpieczeństwa podczas wytwarzania, przetwarzania, przechowywania, przekazywania oraz usuwania informacji;
13) bezzwłoczne zgłaszanie naruszeń zasad bezpieczeństwa informacji w określony sposób, umożliwiający szybkie podjęcie działań korygujących;
14) zapewnianie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok;
15) przestrzeganie zasad bezpieczeństwa informacji, o których mowa w § 14.

**§ 11.** Szczegółowe metody i sposoby implementacji zabezpieczeń, o których mowa w § 10, mogą być określane w innych dokumentach stanowiących dokumentację SZBI.

**§ 12.** 1. Funkcjonowanie SZBI wymaga stałego monitorowania. Mierzenie skuteczności SZBI obejmuje w szczególności przeglądy wdrożonych w ministerstwie zabezpieczeń (organizacyjnych, technicznych i fizycznych) zgodnie z kompetencjami wynikającymi z obszarów działań poszczególnych komórek organizacyjnych.

2. Na system oceny wyników i doskonalenia SZBI składają się, w szczególności:

1) wewnętrzne i zewnętrzne audyty SZBI;
2) kontrole;
3) okresowy przegląd zarządzania SZBI;
4) podejmowanie działań korygujących;
5) przegląd dokumentacji SZBI.

**§ 13.** Na poziom bezpieczeństwa informacji ma wpływ, w szczególności:

1) szacowanie ryzyka w odniesieniu do bezpieczeństwa informacji;
2) ciągłe monitorowanie i doskonalenie systemów i usług wspierających zapewnienie należytego poziomu bezpieczeństwa przetwarzanych informacji;
3) wdrażanie zabezpieczeń wymaganych przepisami prawa i PBI;
4) doskonalenie zabezpieczeń w SZBI;
5) prowadzenie szkoleń w zakresie bezpieczeństwa informacji.

## ROZDZIAŁ IV

## ZASADY BEZPIECZEŃSTWA INFORMACJI

**§ 14.** 1. W ministerstwie stosuje się w szczególności następujące zasady dotyczące bezpieczeństwa informacji:

1) wiedzy koniecznej (ograniczonego dostępu do informacji) – pracownicy posiadają dostęp tylko do tych informacji, które są konieczne do realizacji powierzonych im zadań; zasada ta dotyczy głównie informacji wrażliwych; zasada ta ma ograniczone znaczenie dla pewnych 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;
3) ograniczonej wygody – bezpieczeństwo co do zasady opiera się na ograniczeniach oraz jest niewygodne;
4) czystego biurka – przechowywanie dokumentów odbywa się poza zasięgiem wzroku i dłoni osób postronnych, dokumentów nie należy pozostawiać bez nadzoru;

5) bezpiecznego przechowywania – przechowywanie dokumentów w odpowiednio zabezpieczonych meblach biurowych lub szafach metalowych/sejfach;
6) czystego ekranu – ustawienie sprzętu komputerowego w sposób uniemożliwiający zapoznanie się z informacjami przez osoby nieuprawnione, blokowanie sprzętu podczas nieobecności pracownika, wyłączanie po zakończeniu pracy;
7) separacji obowiązków – pojedyncze osoby nie mogą wykonywać krytycznych zadań w całości;
8) dyskrecji (ograniczonego zaufania i odpowiedzialnej konwersacji) – wszelkie informacje służbowe mogą być przekazywane wyłącznie w celu wykonywania zadań w zakresie do tego niezbędnym oraz osobom uprawnionym do pozyskania tych informacji;
9) obecności koniecznej – prawo przebywania w określonych miejscach, istotnych dla bezpieczeństwa informacji, powinny mieć tylko osoby uprawnione;
10) zamkniętych pomieszczeń – niedopuszczalne jest pozostawienie pod nieobecność pracownika niezabezpieczonego pomieszczenia, 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 klucze do pomieszczenia;
11) nadzorowania dokumentów – po godzinach pracy wszystkie dokumenty zawierające informacje podlegające ochronie powinny być przechowywane w miejscach zabezpieczonych przed dostępem osób nieuprawnionych;
12) stałej gotowości – SZBI jest przygotowany na wszelkie zagrożenia; niedopuszczalne jest tymczasowe wyłączanie mechanizmów zabezpieczających system funkcjonujący w ministerstwie bez zastosowania alternatywnych mechanizmów; system powinien być sprawny i przygotowany na zidentyfikowane zagrożenia;
13) zachowania prywatności kont w systemach – każdy pracownik jest obowiązany do pracy w systemach teleinformatycznych na przypisanych lub udostępnionych mu kontach; zabronione jest udostępnianie własnych kont osobom trzecim;
14) poufności haseł – każdy pracownik jest obowiązany do zachowania poufności udostępnionych mu haseł i kodów dostępu, w szczególności do systemów teleinformatycznych;
15) legalnego oprogramowania – na stacjach roboczych jest zainstalowane wyłącznie legalne oprogramowanie;
16) zgłaszania incydentów bezpieczeństwa informacji – każdy pracownik ma obowiązek niezwłocznie zgłosić wystąpienie lub podejrzenie wystąpienia incydentu bezpieczeństwa informacji;

17) automatyzacji backupu – procesy tworzenia kopii zapasowych powinny być zautomatyzowane;
18) ochrony nośników danych – dane kopiowane na nośniki i wynoszone poza ministerstwo powinny być odpowiednio zabezpieczone w czasie transportu i przechowywania, co najmniej przez szyfrowanie;
19) adekwatności zabezpieczeń – używane mechanizmy zabezpieczeń powinny być adekwatne do zagrożeń, podatności, wartości aktywów oraz innych istotnych okoliczności;
20) kompleksowości ochrony (asekuracji zabezpieczeń) – ochrona aktywów systemu przetwarzania informacji powinna opierać się na stosowaniu różnych mechanizmów ochrony, w tym ochrony prawnej, fizycznej, technicznej oraz organizacyjnej;
21) 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;
22) bezpiecznej współpracy z podmiotami zewnętrznymi – dokumenty regulujące współpracę powinny zawierać odpowiednie klauzule bezpieczeństwa, w tym o zachowaniu poufności, zasadach postępowania z pozyskaną informacją, niszczenia lub zwrotu dokumentacji po jej wykorzystaniu;
23) ewolucji – SZBI jest stale monitorowany i dostosowywany do zmieniających się warunków wewnętrznych i zewnętrznych;
24) podwyższonego poziomu ochrony zbiorów informacji – w szczególnie uzasadnionych przypadkach zbiór informacji powinien być bardziej chroniony niż poszczególne informacje, które się na niego składają;
25) czystego kosza – dokumenty papierowe przeznaczone do zniszczenia nie powinny być umieszczane w koszach na śmieci, a niszczone w przeznaczonych do tego urządzeniach (niszczarkach), w sposób uniemożliwiający ich odczytanie;
26) minimalnych uprawnień do danych przetwarzanych w systemach teleinformatycznych – przydzielanie wyłącznie uprawnień, które są konieczne do pracy na zajmowanym stanowisku;
27) wielowarstwowych zabezpieczeń – aktywa powinny być chronione równolegle na wielu poziomach: organizacyjnym, technicznym i fizycznym;
28) udostępniania infrastruktury teleinformatycznej ministerstwa – nie korzysta się z infrastruktury ministerstwa do celów prywatnych;

29) czystego wydruku – w przypadku używania przez pracownika ogólnodostępnej drukarki niedozwolone jest pozostawianie urządzenia w trakcie pracy (drukowania/skanowania/kopiowania) bez nadzoru;
30) wyłączenia portów USB – nie można wykorzystywać portów USB DATA do przetwarzania, przechowywania i przenoszenia danych.

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

## ROZDZIAŁ V

## OSOBY ODPOWIEDZIALNE ORAZ ICH ZAKRES OBOWIĄZKÓW

**§ 15.** PBI ma zastosowanie do pracowników ministerstwa i obejmuje swoim zakresem nie tylko siedzibę 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 systemu teleinformatycznego ministerstwa.

**§ 16.** Zarządzanie bezpieczeństwem informacji w ministerstwie jest realizowane w ramach wewnętrznej struktury organizacyjnej, w której skład wchodzą, w szczególności:
1) Kierownictwo ministerstwa;
2) Inspektor Ochrony Danych;
3) Pełnomocnik do spraw Ochrony Informacji Niejawnych;
4) dyrektorzy komórek organizacyjnych ministerstwa;
5) administrator merytoryczny;
6) ASI;
7) ABSI;
8) pracownicy.

**§ 17.** Minister:
1) ustanawia PBI oraz zapewnia wdrożenie oraz doskonalenie SZBI;
2) zapewnia przeprowadzanie okresowego audytu wewnętrznego lub zewnętrznego w zakresie bezpieczeństwa informacji;
3) zatwierdza wyniki przeglądów SZBI.

**§ 18.** Sekretarze stanu i podsekretarze stanu oraz szef Gabinetu Politycznego Ministra odpowiadają, w zakresie swojej właściwości, za nadzorowanie bezpieczeństwa informacji.

**§ 19.** Dyrektor Generalny:
1) akceptuje wyniki przeglądów SZBI;

2) wyznacza dyrektorom komórek organizacyjnych ministerstwa zadania mające na celu zapewnienie bezpieczeństwa informacji, w przypadku wystąpienia takiej potrzeby;
3) w przypadku naruszenia bezpieczeństwa informacji, dokonuje czynności z zakresu prawa pracy wobec pracowników, w zakresie adekwatnym do nałożonych na nich obowiązków i posiadanych uprawnień.

**§ 20.** Zadania Inspektora Ochrony Danych określa art. 39 RODO oraz obowiązująca w ministerstwie Polityka Ochrony Danych Osobowych.

**§ 21.** Pełnomocnik do spraw ochrony informacji niejawnych realizuje zadania wynikające z ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2023 r. poz. 756 i 1030).

**§ 22.** 1. Dyrektorzy komórek organizacyjnych ministerstwa, w zakresie swojej właściwości, odpowiadają za:
1) wdrożenie i przestrzeganie PBI;
2) ochronę aktywów;
3) realizację procedur zapewniających ciągłość funkcjonowania komórki organizacyjnej w sytuacjach awaryjnych i kryzysowych;
4) wdrażanie i aktualizowanie dokumentacji bezpieczeństwa informacji w zakresie swojego obszaru działania;
5) umożliwianie pracownikom udziału w organizowanych szkoleniach z zakresu bezpieczeństwa informacji;
6) przestrzeganie zasad ochrony informacji przez podległych im pracowników;
7) właściwy tryb zgłaszania, postępowania i dokumentowania zdarzeń i incydentów bezpieczeństwa informacji, zgodnie z wewnętrznymi regulacjami w tym zakresie;
8) wyznaczenie administratorów merytorycznych.

2. Dyrektor komórki organizacyjnej pełni rolę gestora systemu informatycznego będącego w jego właściwości.

**§ 23.** Administrator merytoryczny jest odpowiedzialny w szczególności za:
1) zarządzanie, we współpracy z ASI, zmianą w zakresie wdrażania, utrzymania i rozwoju systemu teleinformatycznego;
2) zapewnianie ciągłości działania systemów teleinformatycznych (pod względem struktury, zmian, uregulowań prawnych itp.).

**§ 24.** ASI jest odpowiedzialny w szczególności za:

1) monitorowanie systemów teleinformatycznych;
2) wykonywanie kopii zapasowych;
3) czynności związane z wprowadzaniem zmian w systemie teleinformatycznym;
4) czynności związane z zarządzaniem systemami teleinformatycznymi;
5) prowadzenie rejestru uprawnień pracowników ministerstwa w administrowanym przez siebie systemie;
6) opiniowanie zmian w zakresie utrzymania i rozwoju systemu teleinformatycznego;
7) bieżącą aktualizację systemów teleinformatycznych;
8) wdrażanie zaleceń mających wpływ na podwyższenie poziomu bezpieczeństwa systemu teleinformatycznego.

**§ 25.** ABSI jest odpowiedzialny w szczególności za:
1) ochronę i monitorowanie wykorzystywania systemów teleinformatycznych ministerstwa;
2) autoryzację nowych środków przetwarzania informacji;
3) akceptację planów wdrożenia nowych systemów, urządzeń i oprogramowania;
4) przeglądy uprawnień ASI oraz weryfikacje wdrażanych przez ASI zaleceń mających wpływ na podwyższenie poziomu bezpieczeństwa systemu teleinformatycznego.

**§ 26.** Pracownicy odpowiadają w szczególności za:
1) przestrzeganie PBI;
2) ochronę aktywów, w zakresie swojej właściwości;
3) niezwłoczne reagowanie w przypadku wystąpienia lub podejrzenia wystąpienia incydentu bezpieczeństwa informacji oraz postępowanie zgodnie z wewnętrznymi regulacjami w tym zakresie;
4) zabezpieczanie informacji w taki sposób by nie doszło do ich utraty, uszkodzenia, zniszczenia lub dostępu osób nieuprawnionych;
5) zachowanie w tajemnicy informacji pozyskanych w ramach wykonywania obowiązków służbowych w ministerstwie oraz przestrzegania zasad bezpiecznego ich przetwarzania, w tym w systemach teleinformatycznych, w zakresie nadanych uprawnień lub wskazanym w upoważnieniu do przetwarzania danych osobowych.

**§ 27**. Za zapoznanie z PBI, odpowiada w przypadku:
1) pracownika wykonującego obowiązki wynikające ze stosunku pracy na rzecz ministerstwa – dyrektor komórki organizacyjnej ministerstwa, w której jest zatrudniony pracownik;

2) osoby świadczącej usługi, realizującej dostawy oraz wykonującej pracę na rzecz ministerstwa na podstawie umów cywilnoprawnych – dyrektor lub zastępca dyrektora komórki organizacyjnej ministerstwa odpowiedzialny za realizację umowy;
3) stażysty, praktykanta, wolontariusza – komórka organizacyjna właściwa do spraw kadr.

**§ 28.** 1. Osoby, o których mowa w § 16, są obowiązane do złożenia oświadczenia o zapoznaniu się z treścią PBI, którego wzór stanowi załącznik do PBI. Oświadczenia przekazuje się do komórki organizacyjnej właściwej do spraw kadr w celu dołączenia do akt osobowych pracownika lub akt związanych z zawartą z pracownikiem umową.

2. Oświadczenia osób wskazanych w § 27 pkt 2 są przechowywane w komórkach organizacyjnych odpowiedzialnych za realizację umowy.

## ROZDZIAŁ VI

## KLASYFIKACJA INFORMACJI

**§ 29.** 1. Każda informacja, która jest przetwarzana w celu realizacji zadań wynikających z przepisów prawa powszechnie obowiązującego i regulacji ministerstwa, w tym udostępniona ministerstwu lub w nim wytworzona, stanowi informację służbową i podlega ochronie.

2. Przy klasyfikowaniu uwzględnia się wymagania prawne w zakresie zapewnienia bezpieczeństwa informacjom oraz ich znaczenie dla ministerstwa.

3. Przyjmuje się następującą klasyfikację informacji służbowych:
1) informacje wewnętrzne – informacje wytworzone, pozyskane i przetworzone w ramach wykonywanej pracy, których obowiązek ochrony wynika z regulacji ministerstwa;
2) informacje publiczne – 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;
3) informacje prawnie chronione – informacje, których obowiązek ochrony wynika z przepisów prawa lub umów zawartych przez ministerstwo (np. dane osobowe, informacje niejawne, tajemnica przedsiębiorstwa, tajemnica statystyczna).

4. Przy postępowaniu ze sklasyfikowanymi informacjami uwzględnia się wymogi określone w przepisach prawa, regulacjach ministerstwa oraz zawartych umowach przy zachowaniu poufności, integralności i dostępności danych.

## ROZDZIAŁ VII

## SZACOWANIE RYZYKA

**§ 30.** 1. W obszarze bezpieczeństwa informacji identyfikacja i analiza ryzyka jest obligatoryjna i przeprowadza się ją cykliczne, nie rzadziej niż raz w roku.

2. Identyfikacja i analiza ryzyka powinna być dodatkowo realizowana zgodnie z potrzebami, w szczególności przed opracowaniem dokumentacji bezpieczeństwa dla danego obszaru lub systemu oraz po wystąpieniu istotnych zmian w danym obszarze lub systemie.

3. Identyfikację i analizę ryzyka przeprowadza się w oparciu o dostępne metodyki.

4. Identyfikacja i analiza ryzyka powinna być udokumentowana.

5. Identyfikacja i analiza ryzyka w systemach teleinformatycznych odbywa się w trybie przewidzianym w dokumentacji tego systemu.

## ROZDZIAŁ VIII

## ODPOWIEDZIALNOŚĆ

**§ 31.** 1. Odpowiedzialność za przestrzeganie PBI ponoszą wszystkie osoby, o których mowa w § 16, w zakresie odpowiednim do nałożonych na nie obowiązków, posiadanych uprawnień lub postanowień określonych w umowach, porozumieniach i innych pisemnych formach współpracy regulujących obszar bezpieczeństwa informacji.

2. Nieprzestrzeganie postanowień PBI może zostać uznane za naruszenie obowiązków pracowniczych w rozumieniu ustawy z dnia 26 czerwca 1974 r. – Kodeks pracy oraz ustawy z dnia 21 listopada 2008 r. o służbie cywilnej (Dz. U. z 2022 r. poz. 1691 oraz z 2023 r. poz. 1195).

## ROZDZIAŁ IX

## POSTANOWIENIA KOŃCOWE

**§ 32.** 1. Dokumentacja z zakresu SZBI jest wprowadzana odrębnymi regulacjami.

2. Obowiązujące dokumenty SZBI, opracowane przed wejściem w życie PBI, zostaną do niej sukcesywnie dostosowane.

**§ 33.** W celu zapewnienia aktualności dokumentacja SZBI, w szczególności PBI, podlega cyklicznym przeglądom i zmianom w przypadku wystąpienia innych istotnych zdarzeń.

Załącznik do Polityki Bezpieczeństwa Informacji

*WZÓR*

OŚWIADCZENIE

Niniejszym oświadczam, że zapoznałam/em* się z Polityką Bezpieczeństwa Informacji w Ministerstwie Aktywów Państwowych, stanowiącą załącznik do zarządzenia Ministra Aktywów Państwowych z dnia 18 lipca 2023 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji w Ministerstwie Aktywów Państwowych i zobowiązuję się do przestrzegania zawartych w niej zasad.

Zobowiązuję się do zachowania w tajemnicy informacji prawnie chronionych oraz informacji służbowych, do których miałam/em*, mam lub będę miał/a* dostęp w związku z wykonywaniem przeze mnie obowiązków pracowniczych lub innych zadań wykonywanych na rzecz Ministerstwa Aktywów Państwowych, a także sposobów zabezpieczenia tych informacji, zarówno w trakcie ich wykonywania, jak i po ich zakończeniu.

Jestem świadoma/y*, że nieprzestrzeganie postanowień ww. regulacji może skutkować odpowiedzialnością karną lub dyscyplinarną na zasadach i w trybie przewidzianym w przepisach prawa, w tym w ustawie z dnia 26 czerwca 1974 r. – Kodeks pracy oraz ustawy z dnia 21 listopada 2008 r. o służbie cywilnej.

_____

data i czytelny podpis

* niewłaściwe skreślić