Warszawa, dnia 20 marca 2019 r.

Poz. 7

Z A R Z Ą D Z E N I E

M I N I S T R A I N W E S T Y C J I I R O Z W O J U

z dnia 20 marca 2019 r.

w sprawie Polityki Bezpieczeństwa Informacji w Ministerstwie Inwestycji i Rozwoju

Na podstawie § 20 rozporządzenia 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) zarządza się, co następuje:

§ 1. W Ministerstwie Inwestycji i Rozwoju wprowadza się Politykę Bezpieczeństwa Informacji, która stanowi załącznik do zarządzenia.

§ 2. Zarządzenie wchodzi w życie z dniem ogłoszenia.

MINISTER INWESTYCJI I ROZWOJU:

WZ. A. SOBOŃ

Załącznik do zarządzenia
Ministra Inwestycji i Rozwoju

POLITYKA BEZPIECZEŃSTWA INFORMACJI W MINISTERSTWIE INWESTYCJI I ROZWOJU

Rozdział 1.

PRZEPISY OGÓLNE

§ 1. 1. Polityka Bezpieczeństwa Informacji, zwana dalej „Polityką”, określa podstawowe zasady zarządzania bezpieczeństwem informacji oraz podmioty odpowiedzialne za ochronę informacji w Ministerstwie Inwestycji i Rozwoju, zwanym dalej „Ministerstwem”.

2. Zasady zarządzania bezpieczeństwem informacji w Ministerstwie zostały opracowane zgodnie z obowiązującymi przepisami oraz w oparciu o wymagania Polskich Norm i standardów w obszarze bezpieczeństwa informacji, w tym w szczególności:

1) rozporządzeniem 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) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), zwanym dalej „RODO”;
2) ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000 i 1669);
3) ustawą z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2018 r. poz. 1330 i 1669);
4) ustawą z dnia 25 lutego 2016 r. o ponownym wykorzystywaniu informacji sektora publicznego (Dz. U. z 2018 r. poz. 1243 i 1669);
5) ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2018 r. poz. 412, z późn. zm.[1)]);
6) ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560);
7) ustawą z dnia 4 lutego1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2018 r. poz. 1191, 1293, 1669, 2245 i 2339);

[1)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U z 2018 r. poz. 650, 1000, 1083 i 1669 oraz z 2019 r. poz. 125.

8) ustawą z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2017 r. poz. 570 oraz z 2018 r. poz. 1000, 1544 i 1669 oraz z 2019 r. poz. 60);
9) rozporządzeniem Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. poz. 948);
10) rozporządzeniem 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);
11) rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 18 stycznia 2007 r. w sprawie Biuletynu Informacji Publicznej (Dz. U. poz. 68);
12) normami:
    a) PN-ISO/IEC 27001,
    b) PN-ISO/IEC 27002,
    c) PN-ISO/IEC 27005,
    d) PN-ISO/IEC 24762.

§ 2. Użyte w Polityce pojęcia oznaczają:

1) aktywa (zasoby) – wszystko, co stanowi wartość dla Ministerstwa i w związku z tym wymaga ochrony, w szczególności:
    a) aktywa informacyjne (informacje) rozumiane jako wiedza, dane oraz wszelkie informacje wpływające na wartość Ministerstwa, w tym informacje udokumentowane,
    b) zasoby ludzkie – pracownicy, wiedza, umiejętności, doświadczenie i kwalifikacje,
    c) usługi i licencje,
    d) wartości niematerialne, w tym wizerunek, kultura organizacyjna, wartości etyczne,
    e) systemy teleinformatyczne i cyberprzestrzeń Ministerstwa,
    f) urządzenia dostępowe i oprogramowanie,
    g) zabezpieczenia fizyczne, środowiskowe, techniczne i organizacyjne,
    h) siedziba i nieruchomości oraz poszczególne pomieszczenia użytkowane przez Ministerstwo;
2) bezpieczeństwo informacji – zabezpieczenie i zachowanie informacji w zakresie integralności, dostępności i poufności przed nieautoryzowanym dostępem lub zmianą; dodatkowo mogą być brane pod uwagę inne atrybuty – rozliczalność, autentyczność, niezaprzeczalność oraz niezawodność;
3) dostępność – właściwość polegająca na tym, że informacja jest dostępna i użyteczna na żądanie upoważnionego podmiotu;

4) Gestor Systemu – dyrektor komórki organizacyjnej Ministerstwa lub inna, wskazana w uzgodnieniu z Dyrektorem Generalnym Ministerstwa osoba, odpowiedzialna za zainicjowanie powstania systemu, ustalenie założeń i funkcjonalności systemu oraz określanie kierunków jego rozwoju;
5) incydent związany z bezpieczeństwem informacji – pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które zagrażają bezpieczeństwu informacji oraz stwarzają znaczne prawdopodobieństwo utraty aktywów lub zakłócenia realizacji zadań;
6) integralność – właściwość polegająca na zapewnieniu dokładności i kompletności informacji;
7) 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, niedoskonałości zabezpieczeń;
8) poufność – właściwość polegająca na tym, że informacja nie jest udostępniana ani ujawniana nieautoryzowanym osobom, podmiotom lub procesom;
9) ryzyko – potencjalna sytuacja, w której określone zagrożenie wykorzysta podatność aktywa lub grupy aktywów, powodując w ten sposób naruszenie poufności, integralności, dostępności lub innych atrybutów bezpieczeństwa informacji;
10) sytuacja awaryjna – zdarzenie, którego skutki powodują utratę ciągłości działania Ministerstwa; może dotyczyć jednej lub kilku komórek organizacyjnych, których procesy zostały zakłócone;
11) sytuacja kryzysowa – niespodziewane i niepożądane zdarzenie lub seria zdarzeń związanych z bezpieczeństwem przetwarzania informacji, w szczególności w systemach teleinformatycznych, które mogą zakłócić lub zakłócają proces realizacji zadań Ministerstwa (sytuacja może dotyczyć w szczególności bezpieczeństwa ludzi, mienia w znacznych rozmiarach lub środowiska, wywołując znaczne ograniczenia w funkcjonowaniu Ministerstwa);
12) 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;
13) użytkownik – pracownik, stażysta, wolontariusz, praktykant lub inna osoba wykonująca pracę bądź świadcząca usługi na podstawie umów cywilnoprawnych na rzecz Ministerstwa lub Ministra Inwestycji i Rozwoju, zwanego dalej „Ministrem”, która uzyskała uprawnienie albo upoważnienie do przetwarzania danych osobowych w danym zakresie, w tym do przetwarzania informacji w systemach teleinformatycznych;

14) zabezpieczenie – działanie lub rozwiązanie, które ogranicza prawdopodobieństwo wystąpienia zagrożenia lub minimalizuje jego negatywne skutki oraz wpływa na osiągnięcie celów; wyróżnia się trzy rodzaje zabezpieczeń funkcjonujących w Ministerstwie:
   a) organizacyjne (struktury organizacyjne, polityki, procedury postępowania, zarządzenia, regulaminy, klauzule w umowach, 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 (ogrodzenie, drzwi, pomieszczenia plombowane, zamykane szafy, sejfy, strefy ochronne itp.) i środowiskowe (np. bezpieczeństwo okablowania, klimatyzacja);
15) zagrożenie – zdarzenie, zjawisko, działanie lub zaniechanie, które może skutkować naruszeniem integralności, dostępności, poufności informacji albo doprowadzić do szkody lub nieosiągnięcia celów Ministerstwa.

§ 3. 1. Polityka jest podstawowym elementem w 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), utrwalone na nośnikach elektronicznych, systemach komputerowych oraz wytworzone w dokumentach, będące własnością Ministerstwa oraz powierzone w ramach umów lub porozumień z kontrahentami lub wykonawcami.

3. Zapisy Polityki należy uwzględniać w procesie opracowania pozostałej dokumentacji SZBI, w szczególności polityk, procedur, instrukcji i wytycznych obowiązujących w Ministerstwie.

4. Obowiązujące w Ministerstwie regulacje wewnętrzne należy procedować i wdrażać z uwzględnieniem założeń zapewniających ochronę aktywów, w szczególności aktywów informacyjnych.

5. Polityka nie ingeruje w treść dokumentów dedykowanych dla systemów zarządzania bezpieczeństwem informacji, certyfikowanych na zgodność z Polską Normą PN-ISO/IEC 27001, które funkcjonują lub mogą funkcjonować w Ministerstwie, a także w treść dokumentów wynikających z przepisów o ochronie informacji niejawnych.

5. Jeżeli przepisy odrębnych ustaw, które odnoszą się do przetwarzania danych, przewidują dalej idącą ich ochronę, niż wynika to z Polityki, stosuje się przepisy tych ustaw.

§ 4. Polityka ma zastosowanie do wszystkich komórek organizacyjnych Ministerstwa 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 kontekście zdalnego korzystania z sieci komputerowej Ministerstwa, w tym telepracy.

§ 5. 1. Do przestrzegania Polityki zobowiązane są wszystkie osoby korzystające z zasobów Ministerstwa, w szczególności:

1) pracownicy Ministerstwa;
2) osoby świadczące usługi, realizujące dostawy oraz wykonujący roboty budowlane na rzecz Ministerstwa na podstawie umów cywilnoprawnych, w tym umów zlecenia lub umów o dzieło;
3) osoby odbywające praktykę, staż lub wolontariat, w zakresie określonym odpowiednio w umowie o odbywaniu praktyki lub stażu, programie praktyki lub stażu, porozumieniu o świadczeniu wolontariatu;
4) eksperci oraz pracownicy podmiotów zewnętrznych realizujący inne, niż określone w pkt 1-3 zadania na rzecz Ministerstwa.

2. Za zapoznanie z Polityką osób, o których mowa w ust. 1, odpowiada w przypadku:

1) nowo zatrudnionego pracownika – Biuro Zarządzania Zasobami Ludzkimi;
2) pracowników wykonujących obowiązki wynikające ze stosunku pracy na rzecz Ministerstwa – dyrektor lub zastępca dyrektora komórki organizacyjnej Ministerstwa, w której są zatrudnieni, z zastrzeżeniem pkt 1;
3) osób świadczących usługi na podstawie umów cywilnoprawnych (w tym umów zlecenia lub umów o dzieło) – dyrektor lub zastępca dyrektora komórki organizacyjnej Ministerstwa odpowiedzialny za realizację umowy z tą osobą;
4) stażystów, wolontariuszy, praktykantów i ekspertów – dyrektor lub zastępca dyrektora komórki organizacyjnej Ministerstwa, w której będą odbywać staż, wolontariat, praktykę lub wykonywać pracę jako eksperci.

3. Osoby, o których mowa w ust. 1, zobowiązane są do złożenia oświadczenia o zapoznaniu się z treścią Polityki za pomocą dedykowanej aplikacji. W uzasadnionych przypadkach dopuszcza się złożenie oświadczenia własnoręcznie podpisanego, zgodnie z wzorem stanowiącym załącznik do Polityki.

4. Oświadczenia, o których mowa w ust. 3 zdanie drugie, przekazywane są do Biura Polityki Bezpieczeństwa.

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

6. Pełnomocnik do spraw Bezpieczeństwa Informacji w Ministerstwie może wyrazić zgodę lub polecić zapoznanie się z treścią Polityki podmiotom spoza Ministerstwa.

Rozdział 2.

ZASADY DOTYCZĄCE BEZPIECZEŃSTWA INFORMACJI

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

1) zapewnienie odpowiedniej jakości procesów przetwarzania informacji, w szczególności skuteczności i adekwatności działania zabezpieczeń (lub ich grup) i środków chroniących przed nieuprawnionym ujawnieniem, odpowiednich warunków do ich użytkowania oraz sprawności i efektywności ich wykorzystywania;
2) pracowników posiadających odpowiednią wiedzę, umiejętności i doświadczenie adekwatne do powierzonych zadań;
3) ochronę fizyczną, techniczną i organizacyjną aktywów Ministerstwa przed dostępem osób nieupoważnionych, w szczególności przed nieuprawnionym wykorzystaniem, kradzieżą, uszkodzeniem, nieuprawnioną modyfikacją lub zniszczeniem;
4) zabezpieczenie systemów teleinformatycznych eksploatowanych w Ministerstwie przed zagrożeniami;
5) zabezpieczenie aktywów Ministerstwa przed ich uszkodzeniem lub zniszczeniem w wyniku pożaru, zalania, ataku terrorystycznego, zjawisk naturalnych lub innych zagrożeń;
6) zapewnienie ciągłości działania procesów 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 szczególności stosowanie klauzul poufności w umowach cywilnoprawnych z kontrahentami lub wykonawcami;
12) zapewnienie pracownikom szkoleń i innych akcji promocyjno-edukacyjnych z zakresu bezpieczeństwa informacji;
13) zapewnienie działań kontrolnych w zakresie przestrzegania zasad określonych w Polityce;
14) przestrzeganie zasad bezpieczeństwa informacji, o których mowa w § 8.

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

1) zabezpieczenia powinny być adekwatne do wymogów prawnych oraz wyników audytów i analiz ryzyka bezpieczeństwa informacji;
2) zabezpieczenia fizyczne, techniczne i organizacyjne 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-ISO 27002,
   c) uwzględnieniem wyników szacowania ryzyka;
4) świadomość pracowników w zakresie bezpieczeństwa informacji powinna być doskonalona, w szczególności poprzez różne formy podnoszenia kwalifikacji;

5) powinno się unikać niepotrzebnego dublowania zabezpieczeń, przy uwzględnieniu racjonalnego gospodarowania środkami publicznymi, optymalizacji potrzeb oraz ograniczeń i uwarunkowań prawno-organizacyjnych Ministerstwa;
6) należy podejmować działania na rzecz utrzymania standardów współpracy Ministerstwa z osobami i podmiotami zewnętrznymi, poprzez stosowanie zasad regulujących kwestie poufności w ramach realizacji umów, porozumień, listów intencyjnych i innych form relacji, obowiązujących Strony również po ustaniu współpracy.

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

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

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

1) dokonano szacowania ryzyka w odniesieniu do bezpieczeństwa informacji;
2) wdrożono skuteczne zabezpieczenia wymagane przepisami prawa i Polityką.

§ 8. 1. W Ministerstwie stosuje się 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; zasada ta dotyczy np. wydruków z systemu centralnego wydruku;
3) niewygody uzasadnionej – bezpieczeństwo co do zasady opiera się na ograniczeniach oraz jest niewygodne; środki ochrony nie mogą nadmiernie utrudniać realizacji celów i zadań Ministerstwa;
4) czystego biurka i czystego ekranu:
   a) podczas dłuższej nieobecności pracownika na stanowisku pracy dokumenty i informatyczne nośniki danych przechowywane – w miarę możliwości organizacyjno-technicznych – należy przechowywać w odpowiednio zabezpieczonych meblach biurowych lub szafach metalowych/sejfach,
   b) 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 –

np. serwer obsługujący systemy alarmowe; w czasie obecności pracownika monitor powinien być tak ustawiony, aby nie pozwalał na zapoznawanie się z wyświetlanymi treściami przez osoby postronne, nieupoważnione;

5) separacji obowiązków – pojedyncze osoby nie mogą wykonywać krytycznych zadań w całości;
6) 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; zasada ta ma ograniczone znaczenie dla pewnych grup informacji, np. informacji dostępnych publicznie;
7) obecności koniecznej – prawo przebywania w określonych miejscach - istotnych dla bezpieczeństwa informacji - powinny mieć tylko osoby upoważnione;
8) zamykania pomieszczeń – 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 powinna zamknąć wszystkie okna i drzwi oraz zabezpieczyć klucze do pomieszczenia;
9) nadzorowania dokumentów – po godzinach pracy wszystkie dokumenty zawierające informacje podlegające ochronie powinny być przechowywane w miejscach zabezpieczonych przed dostępem osób nieuprawnionych;
10) stałej gotowości – niedopuszczalne jest tymczasowe wyłączanie mechanizmów zabezpieczających system funkcjonujący w Ministerstwie bez zastosowania alternatywnych mechanizmów; system powinien być sprawny i przygotowany na zidentyfikowane zagrożenia;
11) zachowania prywatności kont w systemach – każdy pracownik zobowiązany jest do pracy w systemach teleinformatycznych na przypisanych lub udostępnionych mu kontach; zabronione jest udostępnianie własnych kont osobom trzecim;
12) poufności haseł – każdy pracownik zobowiązany jest do zachowania poufności udostępnionych mu haseł i kodów dostępu, w szczególności do systemów teleinformatycznych;
13) legalnego oprogramowania – na stacjach roboczych zainstalowane jest wyłącznie legalne oprogramowanie umożliwiające automatyczne aktualizacje;
14) zgłaszania incydentów bezpieczeństwa informacji – każdy użytkownik ma obowiązek niezwłocznie zgłosić wystąpienie lub podejrzenie wystąpienia incydentu bezpieczeństwa informacji;
15) automatyzacji backupu – procesy tworzenia kopii zapasowych powinny być zautomatyzowane oraz niemożliwe do przerwania przez pracownika;
16) ochrony nośników danych – dane kopiowane na nośniki i wynoszone poza Ministerstwo powinny być odpowiednio zabezpieczone w czasie transportu i przechowywania, co najmniej poprzez szyfrowanie;

17) adekwatności zabezpieczeń – używane mechanizmy zabezpieczeń powinny być adekwatne do zagrożeń, podatności, wartości aktywów oraz innych istotnych okoliczności;
18) 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;
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;
20) bezpiecznej współpracy z podmiotami zewnętrznymi – dokumenty regulujące współpracę powinny zawierać stosowne klauzule bezpieczeństwa, w tym o zachowaniu poufności, zasadach postępowania z pozyskaną informacją, niszczenia lub zwrotu dokumentacji po ich 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) czystej tablicy – po zakończonym spotkaniu należy uprzątnąć wszystkie materiały oraz wyczyścić tablice;
24) czystego kosza – dokumenty papierowe, z wyjątkiem materiałów promocyjnych, marketingowych i innych publicznie dostępnych, powinny być niszczone w sposób uniemożliwiający ich odczytanie.

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

Rozdział 3.

ODPOWIEDZIALNOŚĆ I UPRAWNIENIA W ZAKRESIE BEZPIECZEŃSTWA INFORMACJI

§ 9.1. Właściwe zarządzanie bezpieczeństwem informacji w Ministerstwie zapewnia wewnętrzna struktura organizacyjna, w której skład wchodzą, w szczególności:

1) Minister;
2) Sekretarze Stanu, Podsekretarze Stanu i Dyrektor Generalny Ministerstwa;
3) Szef Gabinetu Politycznego Ministra;
4) Zespół do spraw SZBI;

5) Pełnomocnik do spraw bezpieczeństwa informacji;
6) Inspektor Ochrony Danych;
7) Pełnomocnicy do spraw ochrony danych osobowych;
8) Pełnomocnik do spraw bezpieczeństwa cyberprzestrzeni;
9) Pełnomocnik do spraw ochrony informacji niejawnych;
10) Pełnomocnik do spraw otwartości danych;
11) Inspektor Bezpieczeństwa Teleinformatycznego;
12) dyrektorzy komórek organizacyjnych Ministerstwa;
13) użytkownicy.

2. Dane osób pełniących funkcje, o których mowa w ust. 1 pkt 5-11, są opublikowane w Intranecie.

3. Pełnomocnik, o którym mowa w ust. 1 pkt 8, jest jednocześnie osobą wyznaczoną przez Ministra do utrzymywania kontaktów Ministerstwa, jako użytkownika cyberprzestrzeni, z podmiotami krajowego systemu cyberbezpieczeństwa, w rozumieniu ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

4. Odpowiedzialność za bezpieczeństwo informacji w Ministerstwie ponoszą wszystkie osoby, o których mowa w § 5 ust. 1, w zakresie odpowiednim do nałożonych na nich obowiązków, posiadanych uprawnień lub zapisów określonych w umowach, porozumieniach i innych pisemnych formach współpracy regulujących obszar bezpieczeństwa informacji.

5. Niezależnie od zakresu, o którym mowa w ust. 4, pracownicy są zobowiązani do przestrzegania obowiązku zachowania tajemnicy pracodawcy zgodnie z przepisami prawa pracy.

§ 10. 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 bezpieczeństwa cyberprzestrzeni,
   d) Pełnomocnika do spraw otwartości danych.

2. Sekretarze Stanu, Podsekretarze Stanu oraz Dyrektor Generalny Ministerstwa odpowiadają, w zakresie swojej właściwości, za nadzorowanie bezpieczeństwa informacji w Ministerstwie.

3. Dyrektor Generalny Ministerstwa:

1) akceptuje wyniki przeglądów zarządzania bezpieczeństwem informacji oraz raporty z incydentów bezpieczeństwa;

2) wydaje wewnętrzne akty normatywne regulujące zasady funkcjonowania i zarządzania bezpieczeństwem informacji;
3) określa dyrektorom komórek organizacyjnych Ministerstwa zadania mające na celu zapewnienie bezpieczeństwa informacji, w przypadku wystąpienia takiej potrzeby;
4) egzekwuje odpowiedzialność pracowników Ministerstwa za naruszenia związane z bezpieczeństwem informacji, w zakresie adekwatnym do nałożonych na nich obowiązków i posiadanych uprawnień.

4. Zadania Zespołu do spraw SZBI określają odrębne przepisy.

5. Pełnomocnik do spraw bezpieczeństwa informacji:

1) zapewnia koordynację spraw z zakresu bezpieczeństwa informacji;
2) nadzoruje opracowanie dokumentacji SZBI;
3) współpracuje z dyrektorem komórki organizacyjnej Ministerstwa właściwej do spraw szkoleń przy realizacji szkoleń, o którym mowa w ust. 9;
4) inicjuje oraz nadzoruje działania wdrożeniowe, korygujące i zapobiegawcze w zakresie bezpieczeństwa informacji;
5) nadzoruje działania związane z wykrytymi incydentami;
6) organizuje przeglądy SZBI, nie rzadziej niż raz na dwa lata, oraz nadzoruje realizację ustaleń wynikających z przeglądów;
7) jest zobowiązany do:
   a) wydawania zaleceń w zakresie związanym z funkcjonowaniem SZBI,
   b) uzyskania wyjaśnień od pracowników Ministerstwa, w szczególności w przypadku wystąpienia incydentów i nieprawidłowości w zakresie funkcjonowania SZBI,
   c) podejmowania działań w kwestiach bezpieczeństwa informacji, w zakresie niezastrzeżonym do kompetencji innych osób,
   d) rekomendowania rozwiązań organizacyjno-technicznych zwiększających skuteczność zarządzania w obszarze SZBI.

6. Zadania Inspektora Ochrony Danych określa art. 39 RODO.

7. Uprawnienia i obowiązki:

1) Pełnomocników do spraw ochrony danych osobowych;
2) Pełnomocnika do spraw bezpieczeństwa cyberprzestrzeni;
3) Pełnomocnika do spraw ochrony informacji niejawnych;
4) Pełnomocnika do spraw otwartości danych;
5) Inspektora Bezpieczeństwa Teleinformatycznego

określają odrębne upoważnienia.

8. Dyrektor komórki organizacyjnej Ministerstwa właściwej do spraw kontroli i audytu wewnętrznego zapewnia przeprowadzanie przynajmniej raz w roku audytu SZBI.

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

10. Dyrektor komórki organizacyjnej Ministerstwa właściwej do spraw komunikacji działa na rzecz zapewnienia skutecznej komunikacji oraz bierze udział w zarządzaniu dostępem do informacji zgodnie z przepisami prawa i polityką informacyjną Ministerstwa.

11. Dyrektor komórki organizacyjnej Ministerstwa właściwej do spraw ochrony fizycznej zapewnia zabezpieczenia fizyczne, techniczne i organizacyjne aktywów.

12. Dyrektor komórki organizacyjnej Ministerstwa właściwej do spraw informatyki zapewnia bezpieczeństwo systemów teleinformatycznych Ministerstwa i łączności telefonicznej w Ministerstwie, jak również budowę, rozwój i utrzymanie tych systemów, a także środki techniczne i organizacyjne umożliwiające przetwarzanie informacji w tych systemach.

13. Gestorzy Systemów zapewniają, w zakresie swojej właściwości, bezpieczeństwo systemów teleinformatycznych Ministerstwa.

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

15. Dyrektorzy komórek organizacyjnych Ministerstwa, 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 komórki w sytuacjach awaryjnych i kryzysowych;
5) umożliwienie pracownikom udziału w organizowanych szkoleniach z zakresu bezpieczeństwa informacji;
6) właściwy tryb zgłaszania, postępowania i dokumentowania incydentów, zgodnie z wewnętrznymi regulacjami w tym zakresie.

16. Użytkownicy odpowiadają w szczególności za:

1) przestrzeganie Polityki;
2) ochronę aktywów, w zakresie swojej właściwości;
3) niezwłoczne reagowanie w przypadku wystąpienia lub podejrzenia wystąpienia incydentu oraz postępowanie zgodnie z wewnętrznymi regulacjami w tym zakresie;
4) zabezpieczanie informacji przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, 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 przestrzegania zasad bezpiecznego ich przetwarzania, w tym w systemach teleinformatycznych, w zakresie nadanych uprawnień lub wskazanym w upoważnieniu do przetwarzania danych osobowych.

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

Rozdział 4.

KLASYFIKACJA INFORMACJI I ZASADY POSTĘPOWANIA Z INFORMACJAMI

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

Grupa informacji	Opis
Informacja publiczna	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. Informacje udostępniane w szczególności na stronach internetowych 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 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 ogólnie dostępne wewnątrz Ministerstwa, oraz przeznaczone do użytku wewnętrznego.
Informacja wymagająca klasyfikacji	Informacje, których ewentualne udostępnienie poza Ministerstwo wymaga złożenia stosownego wniosku oraz analizy prawnej dotyczącej możliwości udostępnienia informacji wskazanej we wniosku oraz analizy ewentualnych konsekwencji związanych z jej udostępnieniem.

2. Wprowadzenie klasyfikacji informacji, o której mowa w ust. 1 nie powoduje konieczności specjalnego fizycznego oznaczania informacji udokumentowanych, dokonuje się w nich jedynie odwzorowania literowo-cyfrowego zgodnie z Instrukcją kancelaryjną lub oznaczenia identyfikujące dokument w systemie Elektronicznego Zarządzania Dokumentacją (EZD).

3. W Ministerstwie przyjmuje się następujące zasady postępowania z informacjami:

Informacja publiczna	PRZETWARZANIE, PRZECHOWYWANIE, PRZEKAZYWANIE: w sposób gwarantujący zachowanie integralności i dostępności informacji. ZMIANA KLASYFIKACJI i UDOSTĘPNIANIE: na zasadach i w trybie przewidzianym przepisami prawa. NISZCZENIE: zgodnie z wymogami określonymi w przepisach prawa lub zawartych przez Ministerstwo umowach oraz 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 właściwej ustawy. 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 uprawnionym osobom lub podmiotom po uzyskaniu zgody dyrektora lub zastępcy dyrektora właściwej komórki organizacyjnej Ministerstwa. NISZCZENIE: zgodnie z wymogami określonymi w przepisach prawa lub zawartych przez Ministerstwo umowach oraz 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 (pracownikom Ministerstwa, osobom/pracownikom podmiotów, z którymi Ministerstwo zawarło stosowne umowy), w sposób gwarantujący zachowanie integralności i dostępności informacji oraz zgodnie z wymaganiami określonymi w przepisach prawa lub zawartych przez Ministerstwo

	umowach. ZMIANA KLASYFIKACJI: możliwa po podjęciu decyzji przez uprawnione osoby oraz zgodnie z wymaganiami określonymi w przepisach prawa lub zawartych przez Ministerstwo umowach. UDOSTĘPNIANIE: wyłącznie po uzyskaniu zgody dyrektora lub zastępcy dyrektora właściwej komórki organizacyjnej Ministerstwa. NISZCZENIE: zgodnie z wymogami określonymi w przepisach prawa lub zawartych przez Ministerstwo umowach oraz Instrukcją kancelaryjną.
Informacja wymagająca klasyfikacji	PRZETWARZANIE: w sposób gwarantujący zachowanie integralności, dostępności i poufności informacji. PRZECHOWYWANIE: w sposób gwarantujący zapewnienie bezpieczeństwa informacji. PRZEKAZYWANIE: możliwe wysyłanie adresatom zewnętrznym po dokonaniu analizy prawnej dotyczącej możliwości udostępnienia informacji oraz analizy ewentualnych konsekwencji z tym związanych. Przekazywanie wewnątrz Ministerstwa na zasadach określonych przez dyrektora lub zastępcę dyrektora właściwej komórki organizacyjnej Ministerstwa. ZMIANA KLASYFIKACJI: po dokonaniu analizy w tym zakresie. UDOSTĘPNIANIE: wyłącznie po uzyskaniu zgody dyrektora lub zastępcy dyrektora właściwej komórki organizacyjnej Ministerstwa. NISZCZENIE: zgodnie z Instrukcją kancelaryjną.

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

Rozdział 5.

SZACOWANIE RYZYKA

§ 12. 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, w których ustanawiano SZBI certyfikowany za zgodność z Polską Normą PN-ISO/IEC 27001, odbywa się w trybie przewidzianym w dokumentacji tego systemu.

Rozdział 6.

POSTANOWIENIA KOŃCOWE

§ 13. Dokumentacja z zakresu bezpieczeństwa informacji, o której mowa w § 3 ust. 3, jest wprowadzana odrębnymi regulacjami.

§ 14. 1. W terminie miesiąca od dnia wejścia w życie Polityki osoby, o których mowa w § 5 ust. 1, mają obowiązek zapoznać się z jej treścią zgodnie z trybem określonym w § 5 ust. 2-6.

2. W terminie 6 miesięcy od dnia wejścia w życie Polityki należy dostosować lub opracować dokumentację SZBI.

Załącznik
do Polityki Bezpieczeństwa Informacji
w Ministerstwie Inwestycji i Rozwoju

Oświadczenie o zapoznaniu się z Polityką Bezpieczeństwa Informacji w Ministerstwie Inwestycji i Rozwoju

Niniejszym oświadczam, że zapoznałem/am* się z Polityką Bezpieczeństwa Informacji w Ministerstwie Inwestycji i Rozwoju i zobowiązuję się do przestrzegania zawartych w niej zasad.

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

Mam świadomość, że celem Polityki Bezpieczeństwa Informacji jest zapewnienie odpowiedniego poziomu bezpieczeństwa informacji przetwarzanych w Ministerstwie, a naruszenia związane z bezpieczeństwem informacji mogą skutkować odpowiedzialnością karną lub dyscyplinarną na zasadach i w trybie przewidzianym w przepisach prawa, w tym w ustawie z dnia 21 listopada 2008 r. o służbie cywilnej (Dz. U. z 2018 r. poz. 1559) i ustawie z dnia z dnia 26 czerwca 1974 r. - Kodeks pracy (Dz. U. z 2018 r. poz. 917, 1000, 1076, 1629 i 2245).

……..

Data i podpis

*niepotrzebne skreślić