Warszawa, dnia 21 lipca 2023 r.

Poz. 34

ZARZĄDZENIE NR 22
MINISTRA ROLNICTWA I ROZWOJU WSI

z dnia 21 lipca 2023 r.

w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji

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. Wprowadza się Politykę Bezpieczeństwa Informacji Ministerstwa Rolnictwa i Rozwoju Wsi, stanowiącą załącznik do niniejszego zarządzenia.

§ 2. Zobowiązuje się dyrektorów komórek organizacyjnych Ministerstwa Rolnictwa i Rozwoju Wsi do zapoznania podległych pracowników z Polityką Bezpieczeństwa Informacji Ministerstwa Rolnictwa i Rozwoju Wsi.

§ 3. Traci moc zarządzenie nr 15 Ministra Rolnictwa i Rozwoju Wsi z dnia 24 maja 2018 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji Ministerstwa Rolnictwa i Rozwoju Wsi.

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

Minister Rolnictwa i Rozwoju Wsi: *R. Telus*

Załącznik do zarządzenia nr 22
Ministra Rolnictwa i Rozwoju Wsi
z dnia 21 lipca 2023 r. (poz. 34)

Polityka Bezpieczeństwa Informacji
Ministerstwa Rolnictwa i Rozwoju Wsi

Bezpieczeństwo informacji oraz systemów, w których są one przetwarzane jest jednym z podstawowych elementów zapewniających realizację zadań statutowych i ustawowych Ministra Rolnictwa i Rozwoju Wsi, zwanego dalej „Ministrem”.

Polityka Bezpieczeństwa Informacji Ministerstwa Rolnictwa i Rozwoju Wsi, zwana dalej „Polityką Bezpieczeństwa Informacji”, jest głównym dokumentem systemu zarządzania bezpieczeństwem informacji, który określa zestaw powiązanych z nią innych dokumentów dotyczących zarządzania bezpieczeństwem informacji, o których mowa w rozdziale VII Polityki Bezpieczeństwa Informacji, zawierającym zasady oraz sposób zarządzania tym bezpieczeństwem i zasobami materialnymi w Ministerstwie Rolnictwa i Rozwoju Wsi, zwanym dalej „Ministerstwem”.

Bezpieczeństwo informacji w Ministerstwie zapewniane jest przez:

1) zarządzanie ryzykiem bezpieczeństwa informacji;
2) zarządzanie zmianami parametrów bezpieczeństwa informacji przez stałe reagowanie na nie, realizowane przez Komitet Bezpieczeństwa oraz Zespół Kryzysowy Bezpieczeństwa Informacji;
3) zarządzanie funkcjonowaniem Ministerstwa przez określenie i wdrożenie instrukcji i procedur zachowania ciągłości przetwarzania informacji;
4) prowadzenie bieżących i okresowych (nie rzadziej niż raz w roku) szkoleń pracowników Ministerstwa zaangażowanych w proces przetwarzania informacji, ze szczególnym uwzględnieniem takich zagadnień jak:
   a) zagrożenia bezpieczeństwa informacji,
   b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,
   c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich.

I. Podstawowe definicje i skróty

Użyte w Polityce Bezpieczeństwa Informacji określenia oznaczają:

1) **Administrator Bezpieczeństwa Systemu Teleinformatycznego (ABST)** – osobę odpowiedzialną za bezpieczeństwo systemu teleinformatycznego. Administrator Bezpieczeństwa Systemu Teleinformatycznego jest wyznaczany przez Głównego Administratora Informacji na wniosek Głównego Administratora Bezpieczeństwa Systemów Teleinformatycznych po uzgodnieniu tego wniosku z właściwym Administratorem Lokalnym Informacji. Funkcję Administratora Bezpieczeństwa Systemu Teleinformatycznego można łączyć, to znaczy, że jedna osoba może pełnić funkcję Administratora Bezpieczeństwa Systemu Teleinformatycznego dla kilku systemów (zasobów) przetwarzania. Jeżeli Administrator Bezpieczeństwa Systemu Teleinformatycznego nie jest wskazany, jego funkcję pełni Główny Administrator Bezpieczeństwa Systemów Teleinformatycznych;
2) **Administrator Danych (AD)** – Ministra, który pełni funkcję administratora w rozumieniu przepisów rozporządzenia 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, z późn. zm.), zwanego dalej „RODO”;
3) **Administrator Bezpieczeństwa Informacji Prawnie Chronionych (ABPC)** – osobę koordynującą bezpieczne przetwarzanie informacji prawnie chronionych oraz informacji istotnych dla funkcjonowania Ministerstwa;
4) **Administratorzy Lokalni Informacji (ALI)** – dyrektorów komórek organizacyjnych Ministerstwa;
5) **Administratorzy Bezpieczeństwa Grupy Informacji (ABGI)** – osoby odpowiedzialne za zarządzanie ochroną informacji z danej grupy informacji chronionych (informacje niejawne, dane osobowe, informacje prawnie chronione). Pełnomocnik ds. Ochrony Informacji Niejawnych, Inspektor Ochrony Danych oraz Administrator Bezpieczeństwa Informacji Prawnie Chronionych są wyznaczani przez Administratora Danych dla każdej grupy informacji chronionych;
6) **bezpieczeństwo informacji** – zachowanie poufności, integralności i dostępności informacji, które oznaczają:

a) poufność informacji – właściwość polegająca na zapewnieniu, że informacja jest udostępniana lub ujawniona tylko osobom lub procesom do tego upoważnionym,

b) integralność informacji – właściwość polegająca na zapewnieniu danym niezmienności, braku dodania innych danych lub usunięcia w nieautoryzowany sposób,

c) dostępność informacji – właściwość bycia dostępnym i możliwym do wykorzystania na żądanie przez upoważnione osoby lub procesy;

7) **cyberbezpieczeństwo** – odporność systemów teleinformatycznych na działania naruszające poufność, integralność, dostępność przetwarzanych danych lub związanych z nimi usług;

8) **Główny Administrator Bezpieczeństwa Informacji (GABI)** – członka Kierownictwa Ministerstwa pełniącego nadzór nad komórką organizacyjną Ministerstwa właściwą do spraw bezpieczeństwa informacji;

9) **Główny Administrator Bezpieczeństwa Systemów Teleinformatycznych (GABST)** – osobę nadzorującą prace wszystkich Administratorów Bezpieczeństwa Systemów Teleinformatycznych, odpowiedzialną za nadzór, koordynację wdrażanych i eksploatowanych systemów teleinformatycznych w zakresie Polityki Bezpieczeństwa Informacji. Główny Administrator Bezpieczeństwa Systemów Teleinformatycznych jest wyznaczany przez Głównego Administratora Informacji. Jeżeli Główny Administrator Bezpieczeństwa Systemów Teleinformatycznych nie jest wyznaczony, rolę jego pełni Pełnomocnik ds. Bezpieczeństwa Cyberprzestrzeni;

10) **Główny Administrator Informacji (GAI)** – Dyrektora Generalnego Ministerstwa;

11) **grupa informacji chronionych** – zbiór informacji podlegających ochronie, obejmujących podobne zagadnienia lub dotyczących jednego tematu. Grupa informacji chronionych może być określona przepisami prawa;

12) **incydent bezpieczeństwa informacji** – pojedyncze zdarzenie lub serię niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia realizacji zadań Ministerstwa i zagrażają bezpieczeństwu informacji;

13) **incydent cyberbezpieczeństwa** – zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo w Ministerstwie;

14) **Inspektor Ochrony Danych (IOD)** – osobę pełniącą funkcję na podstawie art. 37 RODO;

15) **Kierownictwo Ministerstwa** – Kierownictwo Ministerstwa, o którym mowa w regulaminie organizacyjnym Ministerstwa Rolnictwa i Rozwoju Wsi;

16) **Komitet Bezpieczeństwa (KB)** – organ opiniodawczo-doradczy Administratora Danych, w skład którego wchodzą osoby zaangażowane w tworzenie i wdrażanie Systemu Zarządzania Bezpieczeństwem Informacji w Ministerstwie;

17) **Pełnomocnik ds. Ochrony Informacji Niejawnych** – osobę pełniącą funkcję na podstawie art. 14 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2023 r. poz. 756, z późn. zm.);

18) **Pełnomocnik ds. Bezpieczeństwa Cyberprzestrzeni** – osobę do pełnienia tej funkcji wyznaczoną przez Administratora Danych.

Do zadań Pełnomocnika ds. Bezpieczeństwa Cyberprzestrzeni należy:

a) obsługa incydentów cyberbezpieczeństwa, we współpracy z Zespołem Reagowania na Incydenty Bezpieczeństwa Komputerowego prowadzonym przez Szefa Agencji Bezpieczeństwa Wewnętrznego, zwanym dalej „CSIRT GOV”,

b) wyszukiwanie powiązań między incydentami cyberbezpieczeństwa, usuwanie przyczyn ich wystąpienia oraz opracowywanie wniosków wynikających z obsługi tych incydentów,

c) powiadamianie CSIRT GOV niezwłocznie, nie później niż 24 godziny od momentu wykrycia incydentu cyberbezpieczeństwa w Ministerstwie, który jest lub może być zaklasyfikowany jako incydent w podmiocie publicznym,

d) opracowywanie i nadzorowanie realizacji procedur reagowania na incydenty cyberbezpieczeństwa w Ministerstwie,

e) prowadzenie rejestru incydentów cyberbezpieczeństwa w Ministerstwie,

f) identyfikacja i prowadzenie analizy ryzyka systemów teleinformatycznych Ministerstwa,

g) współpraca przy opracowywaniu modułów zadaniowych dla stopni alarmowych i stopni alarmowych CRP;

19) **Polityka Bezpieczeństwa Informacji** – zestaw efektywnych, udokumentowanych zasad i procedur bezpieczeństwa w Ministerstwie wraz z planem ich wdrożenia i egzekwowania. Polityka Bezpieczeństwa Informacji jest częścią składową Systemu Zarządzania Bezpieczeństwem Informacji, zgodnie z przepisami 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);

20) **System Zarządzania Bezpieczeństwem Informacji (SZBI)** – część całościowego systemu postępowania, opartego na zasadach wynikających z zarządzania ryzykiem, odnoszącego się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji, zgodnie z normą ISO 27001;

21) **system teleinformatyczny** – zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2022 r. poz. 1648, z późn. zm);

22) **zdarzenie** – każdą zgłoszoną sytuację, która może mieć potencjalny wpływ na poufność lub integralność lub dostępność informacji;

23) **Zespół Kryzysowy Bezpieczeństwa Informacji (ZKBI)** – organ, w skład którego wchodzą osoby odpowiedzialne za szacowanie zagrożeń i ryzyka dla przetwarzanych informacji oraz rozwiązywanie sytuacji kryzysowych.

II. Cele bezpieczeństwa informacji i sposób ich realizacji

Do celów bezpieczeństwa informacji zalicza się:

1) ochronę zasobów informacji Ministerstwa i podmiotów współpracujących;

2) zapewnienie poufności, integralności i dostępności zasobów informacji;

3) zapewnienie zgodnego z prawem przetwarzania informacji.

Cele Ministerstwa w obszarze bezpieczeństwa informacji realizowane są przez:

1) zapewnienie wsparcia Kierownictwu Ministerstwa w realizacji zadań Systemu Zarządzania Bezpieczeństwem Informacji;

2) organizację Systemu Zarządzania Bezpieczeństwem Informacji opartego na Polityce Bezpieczeństwa Informacji oraz na innych dokumentach, o których mowa w rozdziale VII;

3) zinwentaryzowanie zasobów i grup informacji chronionych oraz przypisanie osób odpowiedzialnych za ich przetwarzanie i ochronę;

4) zarządzanie ryzykiem przez eliminowanie, ograniczanie do akceptowanego poziomu, przeniesienie na inny podmiot lub akceptację ryzyka, zgodnie z normą ISO 27005;

5) ochronę każdej grupy informacji, a w szczególności informacji prawnie chronionych;

6) zapewnienie jak najwyższego poziomu dostępności informacji i niezawodności systemów teleinformatycznych;

7) odtwarzanie techniki informatycznej po katastrofie, opracowanie i wdrożenie awaryjnych planów przetwarzania informacji, zgodnie z normą ISO 24762;

8) ochronę informacji związanych z umowami zawieranymi z innymi podmiotami;

9) ustanowienie i wdrożenie zabezpieczeń, eksploatację i rozwój systemów informacyjnych z zachowaniem zasad bezpieczeństwa informacji, zgodnie z normą ISO 17799;

10) okresowe przeglądy i audyty Systemu Zarządzania Bezpieczeństwem Informacji;

11) zachowanie szczególnej staranności w procesie przetwarzania informacji;

12) podnoszenie poziomu świadomości oraz kwalifikacji osób przetwarzających informacje w zakresie problematyki bezpieczeństwa informacji;

13) traktowanie procesów przetwarzania informacji jako zadań należących do kategorii podstawowych obowiązków pracowniczych oraz egzekwowanie ich prawidłowego wykonywania;

14) podejmowanie w niezbędnym zakresie współpracy z podmiotami powołanymi do ochrony bezpieczeństwa informacji.

III. Grupy informacji chronionych

Na potrzeby Polityki Bezpieczeństwa Informacji wyodrębnia się trzy podstawowe grupy informacji chronionych przetwarzanych w Ministerstwie:

1) informacje niejawne;

2) dane osobowe;

3) informacje prawnie chronione oraz informacje istotne dla funkcjonowania Ministerstwa.

Identyfikacja innych niż podstawowe grupy informacji chronionych należy do zadań Komitetu Bezpieczeństwa, który ustala zakres i sposób postępowania z poszczególnymi grupami informacji chronionych. Zidentyfikowane w Polityce Bezpieczeństwa Informacji podstawowe grupy informacji chronionych nie stanowią katalogu zamkniętego i Komitet Bezpieczeństwa może dokonywać aktualizacji grup informacji chronionych.

Ochrona informacji niejawnych stanowi odrębną część systemu zarządzania bezpieczeństwem informacji w Ministerstwie. Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych wraz z rozporządzeniami wykonawczymi w sposób szczegółowy regulują zasady organizacji i funkcjonowania systemu ochrony informacji niejawnych oraz wskazują osoby odpowiedzialne za prawidłowe funkcjonowanie tego systemu.

Ochrona danych osobowych stanowi odrębną część systemu zarządzania bezpieczeństwem informacji w Ministerstwie. RODO oraz przepisy dotyczące ochrony danych osobowych w sposób szczegółowy regulują zasady organizacji i funkcjonowania systemu ochrony danych osobowych oraz wskazują osoby odpowiedzialne za prawidłowe funkcjonowanie tego systemu.

Ochrona informacji prawnie chronionych oraz informacji istotnych dla funkcjonowania Ministerstwa obejmuje swoim zakresem wszystkie informacje (dane) istotne dla funkcjonowania Ministerstwa, z wyłączeniem informacji niejawnych oraz danych osobowych. Polityka bezpieczeństwa informacji prawnie chronionych oraz informacji istotnych dla funkcjonowania Ministerstwa (opracowywana i wdrażana przez Administratora Bezpieczeństwa Informacji Prawnie Chronionych oraz zatwierdzana przez Administratora Danych) w sposób szczegółowy reguluje zasady organizacji i funkcjonowania systemu ochrony tej grupy informacji chronionych oraz wskazuje osoby odpowiedzialne za prawidłowe funkcjonowanie tego systemu.

Informacje (dane) przekazywane lub udostępniane Administratorowi Danych lub Ministerstwu w zakresie, który nie służy do realizacji ich zadań lub obowiązków, są usuwane w sposób trwały, uniemożliwiający ich odzyskanie.

IV. Infrastruktura systemu zarządzania bezpieczeństwem informacji

Przetwarzanie informacji odbywa się w wyznaczonych lokalizacjach, które stanowią obszary przetwarzania informacji. Obszarem przetwarzania informacji jest budynek Ministerstwa oraz obszary przetwarzania informacji wyznaczone na podstawie Porozumienia w sprawie określenia zasad wykonywania pracy zdalnej w Ministerstwie.

Dopuszcza się przetwarzanie informacji w innych obszarach niż budynek Ministerstwa, po ich zatwierdzeniu przez Głównego Administratora Informacji na wniosek złożony przez Administratora Lokalnego Informacji, po uzgodnieniu tego wniosku z właściwymi Administratorami Bezpieczeństwa Grup Informacji.

Udzielanie informacji środkom masowego przekazu, w tym komunikatów i odpowiedzi na zapytania mediów przez właściwe merytorycznie komórki organizacyjne w Ministerstwie, powinno odbywać się za pośrednictwem komórki organizacyjnej właściwej ds. informowania opinii publicznej o polityce prowadzonej przez Ministra.

Ministerstwo zapewnia siły i środki do prawidłowego, niezakłóconego i ustawicznego rozwoju Systemu Zarządzania Bezpieczeństwem Informacji. Celem takiego działania jest zapewnienie poufności, integralności, dostępności, rozliczalności i niezawodności systemu przetwarzającego informacje.

Skuteczna realizacja postawionych celów w odniesieniu do tworzenia Systemu Zarządzania Bezpieczeństwem Informacji w Ministerstwie jest możliwa poprzez:

1) podnoszenie umiejętności i świadomości pracowników;

2) egzekwowanie umów powierzających realizację wybranych zadań stronom zewnętrznym (outsourcing);

3) przestrzeganie zasad konserwacji infrastruktury w celu zapewnienia ciągłości pracy;

4) kontrolowanie wprowadzania wszelkich zmian do infrastruktury;

5) testowanie, a następnie wdrażanie systemów teleinformatycznych przy zastosowaniu przepisów oraz uznanych standardów w tym zakresie;

6) przestrzeganie zasad tworzenia kopii bezpieczeństwa danych i systemów.

Wdrażanie i eksploatowanie systemu teleinformatycznego jest dopuszczalne po uzyskaniu zgody Pełnomocnika ds. Bezpieczeństwa Cyberprzestrzeni na wniosek złożony przez Administratora Lokalnego Informacji lub Administratora Bezpieczeństwa Grupy Informacji po akceptacji i przeprowadzeniu testów bezpieczeństwa przez Głównego Administratora Bezpieczeństwa Systemów Teleinformatycznych.

V. System Zarządzania Bezpieczeństwem Informacji

System Zarządzania Bezpieczeństwem Informacji w Ministerstwie opiera się na podejściu procesowym i został opracowany na podstawie 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 oraz normy ISO 27001.

Na podejście procesowe Systemu Zarządzania Bezpieczeństwem Informacji składają się następujące działania:

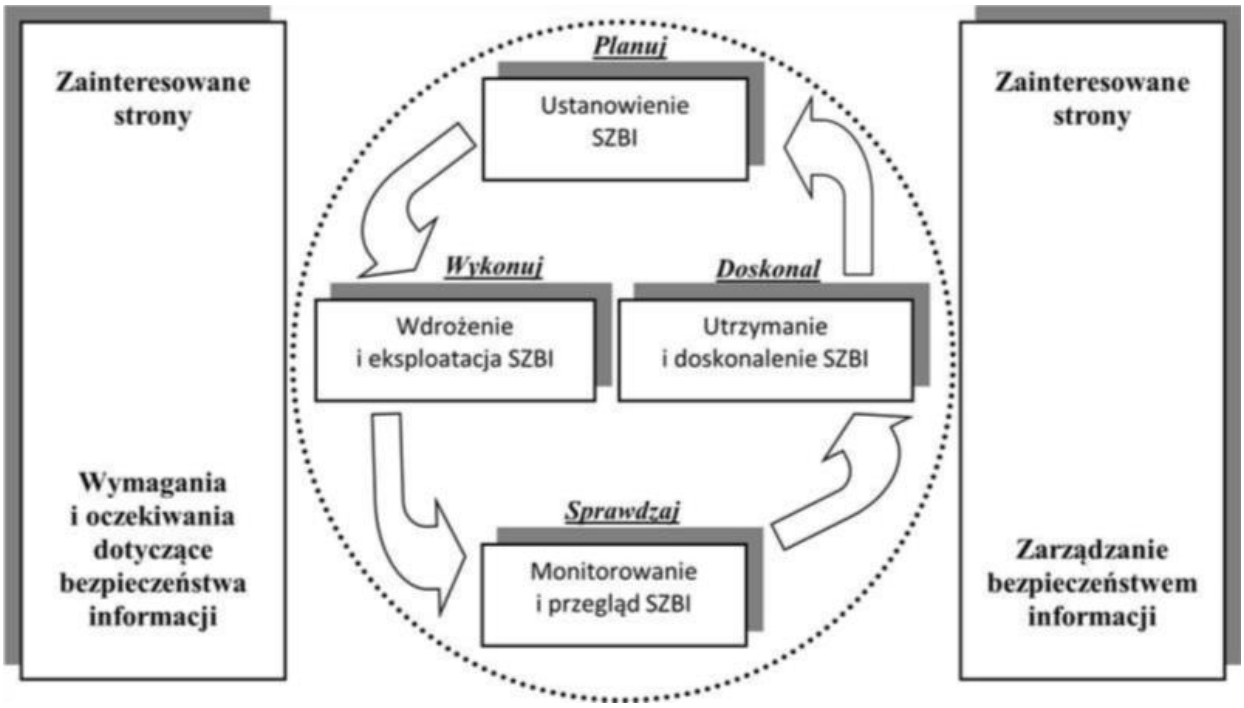
1) przygotowanie i wdrożenie systemu;

2) funkcjonowanie systemu;

3) zarządzanie ciągłością działania systemu;

4) doskonalenie.

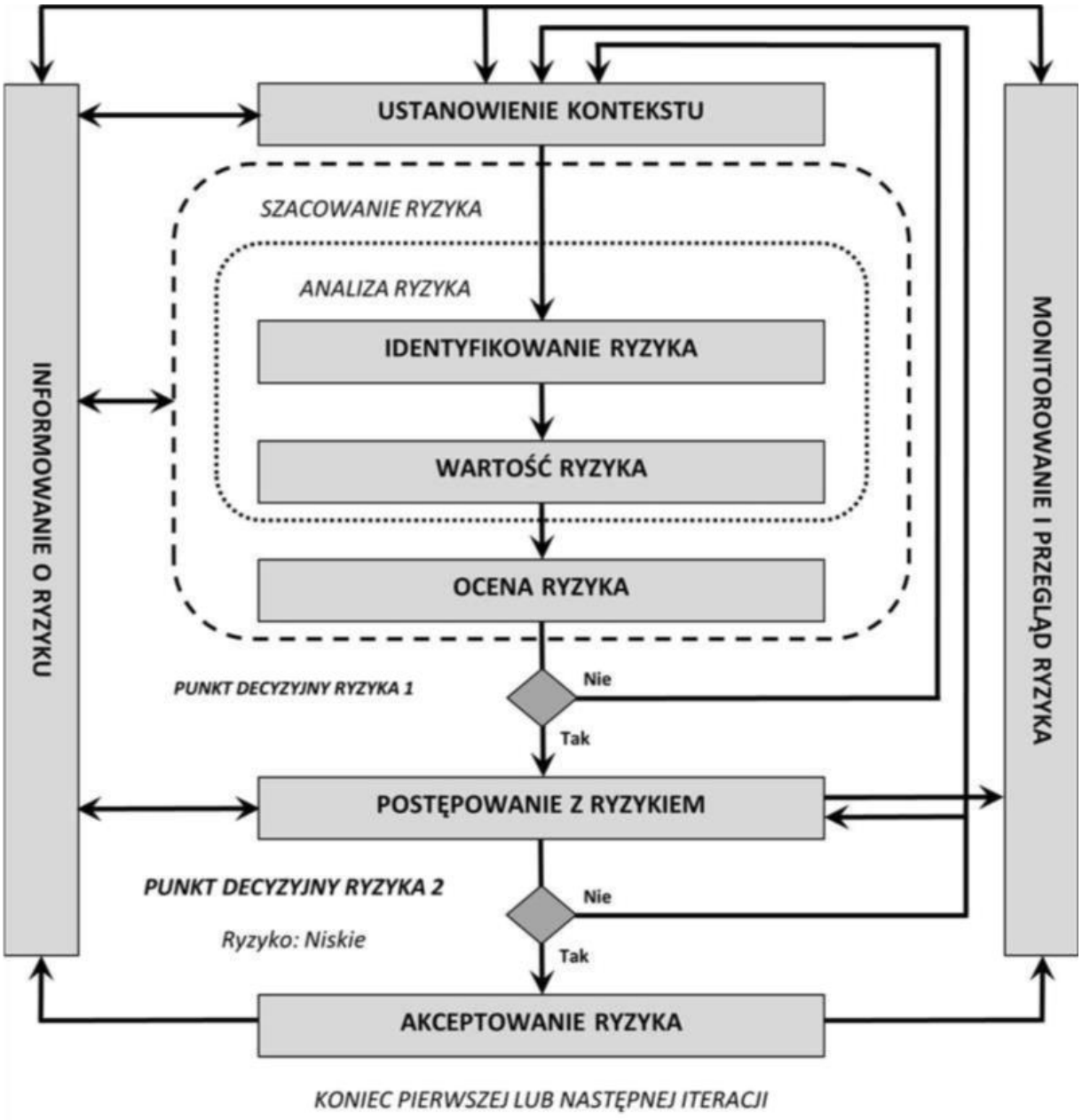
Sposób funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji określają dokumenty, o których mowa w rozdziale VII. Wszelkie działania mające wpływ na System Zarządzania Bezpieczeństwem Informacji oparte są na modelu związanym z czterema etapami zarządzania bezpieczeństwem informacji, którymi są: planowanie, wykonywanie, sprawdzanie i doskonalenie systemu. Model Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) stosowany w Ministerstwie przedstawia rysunek nr 1.



Rysunek nr 1 – Model Systemu Zarządzania Bezpieczeństwem Informacji.

VI. Zarządzanie ryzykiem bezpieczeństwa informacji

Proces zarządzania ryzykiem bezpieczeństwa informacji został opracowany na podstawie normy ISO 27005. Model zarządzania ryzykiem bezpieczeństwa informacji został przedstawiony na rysunku nr 2. Zarządzanie ryzykiem bezpieczeństwa informacji jest procesem ciągłym i dynamicznym. Za zarządzanie ryzykiem bezpieczeństwa informacji jest odpowiedzialny Zespół Kryzysowy Bezpieczeństwa Informacji.



Rysunek nr 2 – Model zarządzania ryzykiem bezpieczeństwa informacji.

Zarządzanie ryzykiem bezpieczeństwa informacji odbywa się na podstawie Instrukcji zarządzania ryzykiem przetwarzania informacji. Zespół Kryzysowy Bezpieczeństwa Informacji raz w roku oraz w przypadku wystąpienia zagrożenia bezpieczeństwa informacji dokonuje analizy ryzyka przetwarzania informacji.

VII. Dokumenty dotyczące Systemu Zarządzania Bezpieczeństwem Informacji

1. Na dokumenty dotyczące Systemu Zarządzania Bezpieczeństwem Informacji składają się w szczególności:

1) Polityka Bezpieczeństwa Informacji;

2) dokumenty bezpieczeństwa poszczególnych grup informacji chronionych, określające szczegółowe wymagania bezpieczeństwa dla tych grup informacji;

3) dokumenty bezpieczeństwa systemów teleinformatycznych przetwarzających informacje, opisujące szczegółowe wymagania dla tych systemów, tworzone przez Głównego Administratora Bezpieczeństwa Systemów Teleinformatycznych;

4) dokumenty dotyczące zasad zarządzania bezpieczeństwem informacji, opisujące te zasady, w skład których wchodzą:

a) regulaminy opisujące szczegółowe zasady postępowania użytkowników systemów lub zasobów teleinformatycznych Ministerstwa,

b) instrukcje opisujące zasady wykonywania poszczególnych zadań,

c) dokumenty procedur opisujących szczegółowe etapy działań podejmowanych w systemach przetwarzania informacji,

d) dokumenty dotyczące zarządzania ryzykiem bezpieczeństwa informacji.

2. Dokumenty bezpieczeństwa grup informacji chronionych są opracowywane i wdrażane przez Administratora Bezpieczeństwa Grup Informacji danej grupy informacji chronionych po ich zatwierdzeniu przez Administratora Danych.

3. Dokumenty dotyczące organizacji zarządzania ryzykiem bezpieczeństwa informacji są opracowywane oraz wdrażane przez Zespół Kryzysowy Bezpieczeństwa Informacji po ich zatwierdzeniu przez Administratora Danych.

4. Dokumenty opisujące zasady zarządzania bezpieczeństwem informacji są zatwierdzane przez Głównego Administratora Bezpieczeństwa Informacji.

5. Niezbędne dokumenty procedur bezpiecznego przetwarzania informacji w komórkach organizacyjnych Ministerstwa są opracowywane i wdrażane przez Administratorów Lokalnych Informacji po uzgodnieniu z Administratorami Bezpieczeństwa Grup Informacji poszczególnych grup informacji chronionych i zatwierdzane przez Głównego Administratora Informacji.

6. Dokumenty dotyczące szacowania ryzyka w podległych komórkach organizacyjnych prowadzone są przez Administratorów Lokalnych Informacji co najmniej raz w roku oraz po każdej istotnej zmianie w zakresie zidentyfikowanego ryzyka, które mogą mieć wpływ na zmianę poziomu zagrożenia dla realizacji założonych celów.

7. Administratorzy Bezpieczeństwa Grup Informacji kontrolują poprawność prowadzenia przez Administratorów Lokalnych Informacji szacowanie ryzyka. W sposób szczególny za bezpieczeństwo informacji odpowiedzialny jest: Komitet Bezpieczeństwa oraz Zespół Kryzysowy Bezpieczeństwa Informacji, które prowadzą ostateczną analizę zestawienia szacowania ryzyka dokonanych przez Administratorów Lokalnych Informacji oraz podejmują decyzję w stosunku do wszystkich ryzyk kluczowych. Szczegółowy zakres realizowanych zadań i odpowiedzialności w zakresie zarządzania ryzykiem bezpieczeństwa informacji w Ministerstwie odbywa się na podstawie Instrukcji zarządzania ryzykiem przetwarzania informacji.

8. Dokumenty związane z bezpieczeństwem systemów teleinformatycznych przetwarzających informacje jawne (regulaminy, instrukcje, procedury) są opracowywane przez Pełnomocnika ds. Bezpieczeństwa Cyberprzestrzeni, przy udziale Głównego Administratora Bezpieczeństwa Systemów Teleinformatycznych i zatwierdzane przez Administratora Danych. Dokumenty te są dokumentami o charakterze wewnętrznym komórki właściwej do spraw informatyki i podlegają udostępnieniu pracownikom Ministerstwa, jedynie w zakresie niezbędnym do bezpiecznego użytkowania systemów teleinformatycznych.

VIII. Komitet Bezpieczeństwa i Zespół Kryzysowy Bezpieczeństwa Informacji

W Ministerstwie funkcjonuje Komitet Bezpieczeństwa, w którego skład wchodzą:

1) Przewodniczący – Główny Administrator Bezpieczeństwa Informacji;

2) Zastępca Przewodniczącego – Główny Administrator Informacji;

3) Sekretarz – dyrektor komórki organizacyjnej Ministerstwa właściwej do spraw zarządzania bezpieczeństwem informacji;

4) członkowie:

a) dyrektor komórki organizacyjnej Ministerstwa właściwej do spraw kadrowych,

b) dyrektor komórki organizacyjnej Ministerstwa właściwej do spraw administracyjnych,

c) Pełnomocnik ds. Ochrony Informacji Niejawnych,

d) Pełnomocnik ds. Bezpieczeństwa Cyberprzestrzeni,

e) Inspektor Ochrony Danych,

f) Administrator Bezpieczeństwa Informacji Prawnie Chronionych,

g) Główny Administrator Bezpieczeństwa Systemów Teleinformatycznych,

h) zastępca dyrektora komórki organizacyjnej Ministerstwa właściwej do spraw zarządzania bezpieczeństwem informacji,

i) inne osoby powołane przez Przewodniczącego niezbędne w procesie zarządzania bezpieczeństwem informacji.

Do głównych zadań Komitetu Bezpieczeństwa należy:

1) koordynacja działań wspólnych dotyczących organizacji i funkcjonowania zidentyfikowanych grup informacji chronionych;

2) rekomendowanie do wdrożenia projektów działań związanych z zapewnieniem bezpieczeństwa informacji;

3) dokonywanie przeglądów systemu zarządzania bezpieczeństwem informacji oraz monitorowanie wykonania działań doskonalących;

4) składanie według potrzeb Administratora Danych raportów ze stanu bezpieczeństwa informacji;

5) ustalanie hierarchii działań lub procesów realizowanych w Ministerstwie na wypadek konieczności ograniczeń ich realizacji, wynikających z dostępności zasobów;

6) identyfikacja grup informacji chronionych.

W Ministerstwie funkcjonuje Zespół Kryzysowy Bezpieczeństwa Informacji, w którego skład wchodzą:

1) Przewodniczący – dyrektor komórki organizacyjnej Ministerstwa właściwej do spraw zarządzania bezpieczeństwem informacji;

2) Zastępca Przewodniczącego – zastępca dyrektora komórki organizacyjnej Ministerstwa właściwej do spraw zarządzania bezpieczeństwem informacji;

3) Sekretarz – osoba wyznaczona przez Przewodniczącego;

4) członkowie:

a) Pełnomocnik ds. Ochrony Informacji Niejawnych,

b) Pełnomocnik ds. Bezpieczeństwa Cyberprzestrzeni,

c) Inspektor Ochrony Danych,

d) Administrator Bezpieczeństwa Informacji Prawnie Chronionych,

e) Główny Administrator Bezpieczeństwa Systemu Teleinformatycznego,

f) inne osoby powołane przez Przewodniczącego niezbędne w procesie rozwiązywania sytuacji kryzysowych bezpieczeństwa informacji.

Do głównych zadań Zespołu Kryzysowego Bezpieczeństwa Informacji należy:

1) szacowanie zagrożeń i ryzyka dla przetwarzanych informacji oraz rozwiązywanie sytuacji kryzysowych;

2) zarządzanie ryzykiem oraz przeprowadzanie analizy ryzyka;

3) wybór kryteriów szacowania skutków, oceny ryzyka oraz akceptowania ryzyka;

4) akceptowanie sposobu postępowania z ryzykiem;

5) opracowanie programu systematycznego przeglądu ryzyka bezpieczeństwa informacji w stałym cyklu przeglądowym;

6) doradzanie Komitetowi Bezpieczeństwa w rozwiązywaniu sytuacji kryzysowych;

7) przyjmowanie przez Administratorów Bezpieczeństwa Grup Informacji (wg właściwości) zgłoszeń incydentów dotyczących naruszeń bezpieczeństwa informacji zgłaszanych przez osoby, które zauważyły lub doświadczyły zdarzeń naruszających bezpieczeństwo informacji;

8) przyjmowanie przez Pełnomocnika ds. Bezpieczeństwa Cyberprzestrzeni zgłoszeń incydentów dot. cyberbezpieczeństwa zgłaszanych przez osoby, które zauważyły lub doświadczyły zdarzeń naruszających bezpieczeństwo.

Sporządzone przez Zespół Kryzysowy Bezpieczeństwa Informacji analizy i wnioski wynikające z okresowego przeglądu ryzyka bezpieczeństwa informacji są przedstawiane Komitetowi Bezpieczeństwa do akceptacji.

IX. Odpowiedzialność za bezpieczeństwo informacji

1. Za bezpieczeństwo informacji odpowiedzialny jest każdy pracownik Ministerstwa i jest on obowiązany do przestrzegania zasad bezpieczeństwa wynikających z Polityki Bezpieczeństwa Informacji oraz do zgłaszania wystąpienia incydentów bezpieczeństwa informacji lub incydentów cyberbezpieczeństwa w przypadku powzięcia takiej informacji.

2. W przypadku wystąpienia incydentu bezpieczeństwa informacji lub incydentu cyberbezpieczeństwa powiadamiany jest właściwy dla zaistniałego incydentu Administrator Lokalny Informacji oraz właściwy Administrator Bezpieczeństwa Grupy Informacji, a także Pełnomocnik ds. Bezpieczeństwa Cyberprzestrzeni (w przypadku incydentu cyberbezpieczeństwa).

3. Każde zdarzenie naruszenia bezpieczeństwa informacji (incydent bezpieczeństwa informacji) posiada swoją dokumentację, przechowywaną przez właściwego Administratora Bezpieczeństwa Grupy Informacji, w postaci opisu zdarzenia, działań mających na celu usunięcie skutków zdarzenia oraz propozycję rozwiązań zaradczych.

4. Ostateczną decyzję o sposobie usunięcia skutków zdarzenia mającego wpływ na realizację głównych celów Ministerstwa i na bezpieczeństwo informacji, podejmuje Komitet Bezpieczeństwa przy współpracy z Zespołem Kryzysowym Bezpieczeństwa Informacji.

Do stanowisk, których zakres obowiązków obejmuje odpowiedzialność za zarządzanie bezpieczeństwem informacji w Ministerstwie należą:

1) **Główny Administrator Informacji (GAI)**

Główny Administrator Informacji ustala, jakie rodzaje informacji będą przetwarzane. Określa grupy informacji przetwarzanych w Ministerstwie oraz ich własność (czy należą do Ministerstwa, czy też do innego podmiotu). Ustala grupy informacji stanowiących tajemnicę służbową Ministerstwa. Określa czas i miejsce, narzędzia, metody przetwarzania, przechowywania, tworzenia i udostępniania oraz niszczenia informacji;

2) **Główny Administrator Bezpieczeństwa Informacji (GABI)**

Główny Administrator Bezpieczeństwa Informacji jest odpowiedzialny za zarządzanie bezpieczeństwem informacji w Ministerstwie. Główny Administrator Bezpieczeństwa Informacji nadzoruje pracę wszystkich Administratorów Lokalnych Informacji oraz Administratorów Bezpieczeństwa Grup Informacji;

3) **Administratorzy Bezpieczeństwa Grup Informacji (ABGI)**

Administratorzy Bezpieczeństwa Grup Informacji są to kontrolerzy jakości administrowanych grup informacji chronionych. Są oni odpowiedzialni za organizację i zabezpieczenie ochrony informacji z danej grupy informacji chronionych (informacje niejawne, dane osobowe, informacje prawnie chronione) przed kradzieżą, nieautoryzowanym dostępem i modyfikacją, zatajeniem oraz utratą lub zniszczeniem informacji.

Do tych administratorów zalicza się:

a) Pełnomocnika ds. ochrony informacji niejawnych,

b) Inspektora Ochrony Danych,

c) Administratora Bezpieczeństwa Informacji Prawnie Chronionych.

Wyznaczani są oni przez Administratora Danych;

4) **Administratorzy Lokalni Informacji (ALI)**

Administratorzy Lokalni Informacji, są to dyrektorzy komórek organizacyjnych Ministerstwa.

Administratorzy Lokalni Informacji:

a) decydują o narzędziach, metodach, miejscu i czasie przetwarzania, przechowywania, tworzenia, udostępniania i niszczenia przetwarzanych grup informacji chronionych, z wyjątkiem grupy informacji niejawnych,

b) decydują, które osoby w podległej komórce organizacyjnej i na jakich prawach mają dostęp do danej grupy informacji,

Grupą informacji może zarządzać kilku Administratorów Lokalnych Informacji, jeżeli są oni odpowiedzialni za wspólny zakres informacji i tylko do niego przyznają dostęp podległym pracownikom (użytkownikom informacji). Jeden Administrator Lokalny Informacji może zarządzać wieloma grupami informacji,

c) opracowują i wdrażają niezbędne procedury bezpiecznego przetwarzania grup informacji w podległej komórce organizacyjnej. Procedury te są zatwierdzane przez Głównego Administratora Informacji,

d) odpowiadają za realizację szkolenia oraz uzyskanie niezbędnych upoważnień, zaświadczeń

do zgodnego z prawem przetwarzania informacji chronionych przez podległych mu pracowników,

e) zgłaszają do komórki organizacyjnej Ministerstwa odpowiedzialnej za zarządzanie bezpieczeństwem informacji nowoprzyjętych pracowników oraz osoby wykonujące usługi na podstawie umów cywilno-prawnych, w celu objęcia ich szkoleniem podstawowym z zakresu bezpieczeństwa informacji (w tym również z ochrony danych osobowych),

f) decydują o konieczności dodatkowego przeszkolenia pracowników z podległej komórki organizacyjnej.

Praktykanci, stażyści oraz wolontariusze zgłaszani są na szkolenia do komórki organizacyjnej Ministerstwa odpowiedzialnej za zarządzanie bezpieczeństwem informacji przez komórkę organizacyjną Ministerstwa właściwą do spraw rozwoju zasobów ludzkich.

Wszystkie osoby przed rozpoczęciem pracy w Ministerstwie zapoznają się z przepisami dotyczącymi bezpieczeństwa informacji, a następnie podpisują oświadczenie potwierdzające zapoznanie się z nimi oraz zobowiązują się do ich przestrzegania, a także zachowania poufności przetwarzanych danych osobowych i innych informacji prawnie chronionych przetwarzanych w Ministerstwie.

Zarządzanie bezpieczeństwem informacji realizowane przez Administratorów Lokalnych Informacji w podległych komórkach organizacyjnych jest nadzorowane przez Administratorów Bezpieczeństwa Grup Informacji oraz przez Głównego Administratora Bezpieczeństwa Informacji.

W przypadku dokonania znaczącej aktualizacji uregulowań wewnętrznych z zakresu bezpieczeństwa informacji, wdrażany jest cykl ogólnodostępnych szkoleń pracowników Ministerstwa, na których prezentowane są nowe, niezbędne informacje. Szkolenia te realizuje komórka organizacyjna Ministerstwa właściwa do spraw zarządzania bezpieczeństwem informacji;

5) **Główny Administrator Bezpieczeństwa Systemów Teleinformatycznych (GABST)**

Główny Administrator Bezpieczeństwa Systemów Teleinformatycznych jest odpowiedzialny za koordynację i nadzór nad wdrażaniem oraz eksploatacją systemów teleinformatycznych służących do przetwarzania informacji (z wyłączeniem systemu teleinformatycznego służącego do przetwarzania informacji niejawnych), z uwzględnieniem ich funkcjonalności, niezawodności, używalności, wydajności, migracji oraz konserwacji przy zastosowaniu norm oraz uznanych standardów w tym zakresie.

W zakresie Polityki Bezpieczeństwa Informacji Główny Administrator Bezpieczeństwa Systemów Teleinformatycznych dopuszcza system teleinformatyczny do eksploatacji w Ministerstwie za zgodą Głównego Administratora Informacji po wcześniejszej uzgodnieniach i akceptacji Administratorów

Lokalnych Informacji lub Administratorów Bezpieczeństwa Grup Informacji (zgodnie z ich kompetencjami).

Praca Głównego Administratora Bezpieczeństwa Systemów Teleinformatycznych jest wspomagana przez stanowiska do spraw bezpieczeństwa teleinformatycznego. W przypadku braku takich stanowisk Główny Administrator Bezpieczeństwa Systemów Teleinformatycznych może korzystać z zewnętrznych specjalistów w tym zakresie lub wdrażać rozwiązania technologiczne wspierające jego pracę. Praca Głównego Administratora Bezpieczeństwa Systemów Teleinformatycznych jest nadzorowana przez Pełnomocnika ds. Bezpieczeństwa Cyberprzestrzeni;

6) **Administratorzy Bezpieczeństwa Systemów Teleinformatycznych (ABST)**

Administratorzy Bezpieczeństwa Systemów Teleinformatycznych (jeżeli są powołani) odpowiedzialni są za przestrzeganie zasad bezpieczeństwa w stosunku do administrowanych systemów teleinformatycznych przetwarzających informacje chronione (z wyłączeniem systemu teleinformatycznego służącego do przetwarzania informacji niejawnych). Dbają o bezpieczeństwo pracy systemów, na bieżąco monitorując stan bezpieczeństwa, przeglądają rejestry zdarzeń systemowych, instalują i konfigurują sprzęt oraz oprogramowanie. Ich obowiązkiem jest zapewnienie, żeby do informacji chronionych miały dostęp wyłącznie osoby upoważnione i żeby mogły one wykonywać wyłącznie uprawnione operacje (kontrolują proces przyznawania praw dostępu). Administratorzy Bezpieczeństwa Systemów Teleinformatycznych są wyznaczani dla każdego systemu teleinformatycznego przetwarzającego informacje chronione. Praca Administratorów Bezpieczeństwa Systemów Teleinformatycznych jest nadzorowana przez Głównego Administratora Bezpieczeństwa Systemów Teleinformatycznych;

7) **Administrator Bezpieczeństwa Informacji Prawnie Chronionych (ABPC)**

Administrator Bezpieczeństwa Informacji Prawnie Chronionych zarządza przetwarzaniem informacji prawnie chronionych istotnych dla funkcjonowania Ministerstwa (z wyjątkiem informacji niejawnych i danych osobowych) zgodnie z obowiązującymi przepisami prawa, normującego zasady przetwarzania tych informacji.

X. Zakres stosowania i rozpowszechniania Polityki Bezpieczeństwa Informacji

Polityka Bezpieczeństwa Informacji jest głównym dokumentem bezpieczeństwa informacji w Ministerstwie dotyczącym Systemu Zarządzania Bezpieczeństwem Informacji.

W przypadku wystąpienia kolizji postanowień Polityki Bezpieczeństwa Informacji z postanowieniami innych dokumentów wewnętrznych, pierwszeństwo mają postanowienia Polityki Bezpieczeństwa Informacji.

Zasady określone przez Politykę Bezpieczeństwa Informacji mają zastosowanie do całości systemu przetwarzania informacji Ministerstwa, w szczególności do:

1) wszystkich sposobów przetwarzania, w których są lub będą przetwarzane informacje podlegające ochronie;

2) informacji będących w dyspozycji Ministerstwa lub innych podmiotów, o ile zostały przekazane na podstawie umów;

3) wszystkich nośników, na których są lub będą znajdować się informacje podlegające ochronie;

4) wszystkich obszarów przetwarzania informacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie.

Do stosowania zasad określonych w Polityce Bezpieczeństwa Informacji oraz w innych dokumentach Systemu Zarządzania Bezpieczeństwem Informacji określonymi w rozdziale VII zobowiązani są wszyscy pracownicy w rozumieniu przepisów Kodeksu Pracy, konsultanci, stażyści i inne osoby mające dostęp do informacji podlegającej ochronie.

Polityka Bezpieczeństwa Informacji może być przedstawiana podmiotom, z którymi Ministerstwo związane jest umowami, lub innym podmiotom (jednostkom) współpracującym w niezbędnym zakresie za zgodą Głównego Administratora Bezpieczeństwa Informacji.

Zapoznanie osób nieuprawnionych ze szczegółami rozwiązań w zakresie bezpieczeństwa danych i architekturą systemów teleinformatycznych stosowanych do ich przetwarzania jest zabronione.

Dokumenty Systemu Zarządzania Bezpieczeństwem Informacji, w tym Polityka Bezpieczeństwa Informacji, podlegają szczególnej ochronie, ponieważ ich ujawnienie może mieć negatywny wpływ na wykonywanie zadań w zakresie bezpieczeństwa informacji. Nieuprawniony dostęp do wymienionych dokumentów mógłby nieść ze sobą zagrożenie dla praw i poufności danych osobowych obywateli.

Polityka Bezpieczeństwa Informacji oraz dokumenty z niej wynikające są dokumentami o charakterze wewnętrznym, niepodlegającym udostępnieniu do wiedzy publicznej.

Osoby, które posiadają informacje na temat sposobu zabezpieczania danych, zobowiązane są zachować te informacje w tajemnicy.

XI. Przegląd i aktualizacja dokumentów dotyczących Systemu Zarządzania Bezpieczeństwem Informacji

Przegląd Polityki Bezpieczeństwa Informacji oraz innych dokumentów dotyczących Systemu Zarządzania Bezpieczeństwem Informacji, o których mowa w rozdziale VII, dokonywany jest okresowo (raz na 5 lat) oraz w razie potrzeby. Przeglądu dokonuje Komitet Bezpieczeństwa, uwzględniając uwagi osób, o których mowa w rozdziale IX.

XII. Podstawy prawne, normy i standardy będące podstawą Polityki Bezpieczeństwa Informacji w Ministerstwie

1. Polityka Bezpieczeństwa Informacji oraz inne dokumenty dotyczące Systemu Zarządzania Bezpieczeństwem Informacji, o których mowa w rozdziale VII, są zgodne z:

1) RODO;

2) ustawą z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2023 r. poz. 57, z późn. zm.);

3) ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781);

4) ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych;

5) ustawą z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2022 r. poz. 902);

6) 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;

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

2. Polityka Bezpieczeństwa Informacji będzie aktualizowana w przypadku zmiany przepisów oraz zmian organizacyjnych mających wpływ na jej postanowienia.

3. Do tworzenia i rozwijania Polityki Bezpieczeństwa Informacji wykorzystywane będą obowiązujące w tym zakresie normy i standardy, w szczególności:

1) „PN-EN ISO/IEC-27001:2022 (wersja angielska) Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania”;

2) „PN-ISO/IEC-27005:2014-01 Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji”;

3) „PN-EN ISO/IEC 27002:2022 (wersja angielska) Technika informatyczna – Praktyczne zasady zarządzania bezpieczeństwem informacji”.