Polityka bezpieczeństwa informacji w Agencji Badań Medycznych

Obowiązuje od:	**01.06.2022 r.**
Wersja:	**1.0**

Deklaracja Prezesa Agencji Badań Medycznych

Realizacja celu Agencji Badań Medycznych (dalej: ABM) w postaci wspierania działalności innowacyjnej w ochronie zdrowia, ze szczególnym uwzględnieniem rozwoju niekomercyjnych badań klinicznych i eksperymentów badawczych, wiąże się z przetwarzaniem informacji o istotnym znaczeniu dla systemu ochrony zdrowia w Polsce oraz rozwoju innowacyjnych technologii, przyczyniających się do ratowania życia i zdrowia pacjentów.

W związku z powyższym informacje przetwarzane w ABM są chronione przed naruszeniem ich poufności, dostępności oraz integralności, w sposób zgodny z najwyższymi standardami zarządzania bezpieczeństwem informacji.

Polityka bezpieczeństwa informacji w Agencji Badań Medycznych ma na celu określenie podstawowych założeń Systemu Zarządzania Bezpieczeństwem Informacji w ABM, jego najważniejszych celów i stosowanych zabezpieczeń.

Intencją wdrożonego Systemu Zarządzania Bezpieczeństwem Informacji jest w szczególności osiągnięcie przez ABM takiego poziomu organizacyjnego i technicznego, który:

- jest gwarantem najlepszej możliwej ochrony informacji przetwarzanych w ramach działalności ABM;
- pozwala na rozwój działalności ABM oraz wyznaczanie najwyższych standardów w zakresie wpierania innowacji w ochronie zdrowia;
- zapewnia integrację procesów zarządzania bezpieczeństwem informacji z pozostałymi procesami i zadaniami ABM;
- zwiększa zaufanie interesariuszy do ABM i jej działalności w kontekście bezpieczeństwa informacji w niej przetwarzanych.

System Zarządzania Bezpieczeństwem Informacji w ABM został opracowany zgodnie z przepisami prawa powszechnie obowiązującego oraz właściwymi normami, standardami i dobrymi praktykami, w szczególności z normami z rodziny ISO 27000.

W związku z powyższym deklaruję, że kierownictwo ABM:

- jest w pełni zaangażowane w tworzenie i rozwój Systemu Zarządzania Bezpieczeństwem Informacji;
- zapewnia wszelkie zasoby niezbędne do prawidłowego funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji;
- aktywnie promuje wśród pracowników zagadnienia związane z bezpieczeństwem informacji oraz zapewnia szkolenia niezbędne do postępowania zgodnego z wymaganiami Systemu Zarządzania Bezpieczeństwem Informacji;
- wspiera wszystkie osoby przyczyniające się do osiągnięcia skuteczności Systemu Zarządzania Bezpieczeństwem Informacji.

Spis treści

Rozdział 1

Postanowienia ogólne

§ 1.

1. Polityka bezpieczeństwa informacji w Agencji Badań Medycznych (dalej: Polityka) określa zasady funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji w ABM.
2. System Zarządzania Bezpieczeństwem Informacji w ABM stanowi część całościowego systemu zarządzania, opartą na podejściu wynikającym z ryzyka, odnoszącą się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia Bezpieczeństwa informacji.
3. Ilekroć w Polityce oraz innych dokumentach Systemu Zarządzania Bezpieczeństwem Informacji jest mowa o Pracownikach, jej postanowienia stosuje się odpowiednio do innych Użytkowników.

§ 2.

Definicje użyte w Polityce oznaczają:

1) ABM – Agencja Badań Medycznych;
2) Administrator Systemu – Pracownik lub Komórka organizacyjna, którym powierzono nadzór nad Systemem teleinformatycznym ABM;
3) Aktywa – wszystko co ma wartość dla ABM. Aktywa dzielą się na informacje, dane oraz tzw. Aktywa wspierające (w szczególności sprzęt, budynki i pomieszczenia, oprogramowanie, zasoby ludzkie);
4) Bezpieczeństwo informacji – zachowanie Poufności, Integralności i Dostępności informacji;
5) Dostępność – właściwość informacji polegająca na byciu dostępnym i użytecznym na żądanie uprawnionego podmiotu;
6) Incydent bezpieczeństwa – pojedyncze zdarzenie lub seria niepożądanych, niespodziewanych zdarzeń, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych, zagrażają bezpieczeństwu lub stanowią naruszenie obowiązujących zasad bezpieczeństwa;
7) Integralność – właściwość informacji polegająca na jej dokładności i kompletności;
8) Interesariusz – osoba lub organizacja, która może wpływać, podlega wpływowi lub postrzega siebie jako podlegającą wpływowi decyzji lub działalności ABM;
9) Komórka organizacyjna – Wydział, Biuro lub samodzielne stanowisko, wyodrębnione w strukturze organizacyjnej ABM;
10) Nośnik danych – urządzenie wymienne i przenośne umożliwiające zapis, modyfikację lub odczyt danych, takie jak: pendrive, dysk przenośny, dysk wewnętrzny, karta pamięci, taśma magnetyczna, nośnik optyczny itp.;
11) Ocena ryzyka – całościowy proces identyfikacji, analizy oraz ewaluacji ryzyka, rozumianego jako wpływ niepewności na cele, wyrażony jako kombinacja następstw zdarzenia i prawdopodobieństwa jego wystąpienia;
12) Pełnomocnik ds. SZBI – Pełnomocnik ds. Systemu Zarządzania Bezpieczeństwem Informacji; osoba wyznaczona przez Prezesa ABM do nadzoru nad realizacją w ABM obowiązków wynikających z przyjętego SZBI;
13) Podatność – słabość aktywa lub grupy aktywów, która może być wykorzystana przez zagrożenie;
14) Podmiot zewnętrzny – osoba prawna, osoba fizyczna lub inny podmiot, dostarczający na rzecz ABM produkty lub świadczący na rzecz ABM usługi na podstawie umowy lub innego stosunku prawnego, niebędący Pracownikiem, stażystą, wolontariuszem, praktykantem, ekspertem lub współpracownikiem świadczącym pracę na podstawie umów cywilnoprawnych;
15) Poufność – właściwość informacji polegająca na tym, że informacja nie jest udostępniana ani ujawniana nieuprawnionym osobom;
16) Pracownik – osoba zatrudniona w ABM na podstawie stosunku pracy;
17) Prezes ABM – Prezes ABM lub osoba przez niego upoważniona;
18) 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. System teleinformatyczny obejmuje między innymi

sprzęt komputerowy, urządzenia przenośne, oprogramowanie systemowe, systemy (podsystemy), sieć, aplikacje;
19) SZBI – System Zarządzania Bezpieczeństwem Informacji;
20) Środki kontroli – elementy systemu zarządzania, na przykład: procesy, polityki, urządzenia, praktyki, które modyfikują ryzyko (w szczególności ograniczają prawdopodobieństwo wystąpienia ryzyka lub zmniejszają potencjalny wpływ jego materializacji);
21) Urządzenie przenośne – informatyczne urządzenie elektroniczne pozwalające na przetwarzanie, odbieranie lub wysyłanie danych bez konieczności utrzymywania przewodowego połączenia z siecią, takie jak laptop, smartfon, tablet lub Nośnik danych;
22) Użytkownik – Pracownik, stażysta, wolontariusz, praktykant, osoba realizująca zadania na rzecz ABM na podstawie umowy cywilnoprawnej, której w związku z realizacją tej umowy powierzono przetwarzanie informacji, a także osoba, której powierzono przetwarzanie informacji na innej podstawie;
23) Właściciel aktywa – kierujący Komórką organizacyjną lub inna osoba głównie odpowiedzialna za zarządzanie danym Aktywem;
24) Właściciel ryzyka – osoba odpowiedzialna za zarządzanie danym ryzykiem, mająca kompetencje lub zobowiązana do podjęcia działań w stosunku do obszaru, którym zarządza;
25) Zagrożenie – potencjalna przyczyna niepożądanego incydentu bezpieczeństwa, którego skutkiem może być szkoda dla Systemu teleinformatycznego lub ABM.

§ 3.

1. Głównym celem SZBI jest ochrona informacji ABM przed zagrożeniami płynącymi ze źródeł zewnętrznych lub wewnętrznych oraz zachowanie ciągłości procesów i zadań realizowanych przez ABM.
2. Cel, o którym mowa w ust. 1, jest realizowany w szczególności poprzez:
   1) zapewnienie Bezpieczeństwa informacji zgodnie z przepisami prawa powszechnie obowiązującego oraz w sposób adekwatny do wyników Oceny ryzyka Bezpieczeństwa informacji, w tym poprzez:
      a) ochronę fizyczną, techniczną i organizacyjną Aktywów ABM przed dostępem osób nieupoważnionych,
      b) zabezpieczenie Systemu teleinformatycznego ABM przed zagrożeniami,
      c) zabezpieczenie informacji przetwarzanych w ABM przed ich uszkodzeniem, nieautoryzowaną modyfikacją lub zniszczeniem;
   2) wdrożenie oraz utrzymanie właściwych zabezpieczeń technicznych i organizacyjnych informacji, w tym ich regularne testowanie, mierzenie i ocenianie skuteczności;
   3) zarządzanie ryzykiem Bezpieczeństwa informacji;
   4) stałe podnoszenie świadomości Pracowników w zakresie Bezpieczeństwa informacji, w tym opracowanie i prowadzenie szkoleń z zakresu Bezpieczeństwa informacji;
   5) określenie ról i odpowiedzialności związanych z zapewnieniem Bezpieczeństwa informacji, w tym wyznaczenie Właścicieli aktywów oraz Właścicieli ryzyka;
   6) stały nadzór nad dokumentacją SZBI;
   7) zapewnienie nadzoru i kontroli nad przestrzeganiem zasad określonych w SZBI;
   8) zarządzanie Bezpieczeństwem informacji w relacjach z kontrahentami i innymi Podmiotami zewnętrznymi, w szczególności poprzez stosowanie klauzul poufności w umowach;
   9) zapewnienie możliwości odtworzenia informacji w przypadku ich modyfikacji lub zniszczenia;
   10) zapewnienie ciągłości działania ABM, w tym ciągłości procesów przetwarzania informacji;
   11) właściwe reagowanie na Incydenty bezpieczeństwa.

Rozdział 2
Kontekst funkcjonowania ABM

§ 4.

1. ABM jest państwową osobą prawną, o której mowa w art. 9 pkt 14 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych.

2. ABM działa w szczególności na podstawie ustawy z dnia 21 lutego 2019 r. o Agencji Badań Medycznych (dalej: Ustawa), aktów wykonawczych do Ustawy oraz Statutu.
3. Działalność ABM polega w szczególności na:
   1) dofinansowaniu badań naukowych i prac rozwojowych w dziedzinie nauk medycznych i nauk o zdrowiu oraz projektów interdyscyplinarnych wyłonionych w drodze konkursu, ze szczególnym uwzględnieniem badań klinicznych, obserwacyjnych i epidemiologicznych oraz eksperymentów badawczych;
   2) wydawaniu opinii i ekspertyz w dziedzinie nauk medycznych i nauk o zdrowiu na rzecz organów administracji publicznej lub innych podmiotów w wyniku realizacji zawartych umów;
   3) inicjowaniu i rozwijaniu współpracy międzynarodowej w dziedzinie nauk medycznych i nauk o zdrowiu na podstawie programów, o których mowa w art. 15 ust. 1 pkt 1 Ustawy;
   4) inicjowaniu i realizacji własnych badań naukowych i prac rozwojowych.
4. Strategiczne kierunki działania ABM określa jej roczny plan działalności.
5. Strukturę organizacyjną ABM oraz sposób funkcjonowania jej poszczególnych Komórek organizacyjnych określa jej regulamin organizacyjny.

§ 5.

Do najważniejszych Interesariuszy ABM należą:
1) Minister właściwy do spraw zdrowia;
2) podmioty biorące udział w ogłaszanych i przeprowadzanych przez ABM naborach wniosków na realizację i dofinansowanie projektu;
3) podmioty, który zawarły umowę z ABM na realizację i dofinansowanie projektu (beneficjenci);
4) Ośrodek Przetwarzania Informacji – jednostka podległa Ministrowi właściwemu do spraw szkolnictwa wyższego i nauki, odpowiedzialna za obsługę techniczno-organizacyjną systemu teleinformatycznego, o którym mowa w Ustawie;
5) inne niż ww. organy administracji publicznej, w szczególności Prezes Urzędu Ochrony Danych Osobowych;
6) Pracownicy ABM oraz inni Użytkownicy;
7) kontrahenci oraz inne Podmioty zewnętrzne;
8) media.

§ 6.

1. Na kontekst wewnętrzny ABM składają się w szczególności:
   1) struktura organizacyjna, uwzględniająca podział kompetencji oraz określone role i odpowiedzialności;
   2) zasoby ludzkie;
   3) wiedza, kompetencje i dobre praktyki;
   4) infrastruktura informatyczna;
   5) pomieszczenia i budynki;
   6) regulacje wewnętrzne oraz przyjęte normy i standardy;
   7) kultura organizacyjna;
   8) komunikacja wewnętrzna i zewnętrzna.
2. Na kontekst zewnętrzny ABM składają się w szczególności:
   1) przepisy prawa powszechnie obowiązującego;
   2) uwarunkowania polityczne, ekonomiczne, technologiczne, społeczne oraz dotyczące ochrony zdrowia;
   3) relacje i kontakty z zewnętrznymi Interesariuszami (w tym organami administracji publicznej, dostawcami i innymi kontrahentami);
   4) wizerunek ABM.
3. ABM na bieżąco analizuje kontekst wewnętrzny i zewnętrzny swojej działalności oraz wykorzystuje wyniki tej analizy do planowania i wykonywania powierzonych jej zadań, w tym do opracowania i aktualizacji SZBI.

Rozdział 3
Zakres SZBI

§ 7.

1. SZBI obowiązuje wszystkie Komórki organizacyjne ABM oraz wszystkie procesy i zadania realizowane przez ABM.
2. Polityka obowiązuje wszystkich Użytkowników.

§ 8.

Zasady określone w SZBI mają zastosowanie do wszystkich:

1) informacji przetwarzanych w ramach procesów i zadań realizowanych przez ABM, niezależnie od ich formy oraz sposobu przetwarzania, będących własnością ABM albo powierzonych w ramach umów lub porozumień;
2) Aktywów wspierających przetwarzanie informacji w ramach procesów i zadań realizowanych przez ABM (w szczególności zasobów ludzkich, budynków i pomieszczeń, sprzętu, Nośników danych, oprogramowania, infrastruktury sieciowej, struktury organizacyjnej).

§ 9.

Szczegółowe informacje na temat zakresu SZBI, celów stosowania zabezpieczeń informacji oraz sposobów ich realizacji określa Deklaracja stosowania zabezpieczeń ISO/IEC 27001:2017.

Rozdział 4
Role i odpowiedzialności w ramach SZBI

§ 10.

1. Właściwe zarządzanie Bezpieczeństwem informacji w ABM zapewnia struktura organizacyjna, w której skład wchodzą w szczególności:
   1) Prezes ABM;
   2) Pełnomocnik ds. SZBI;
   3) Inspektor Ochrony Danych;
   4) kierujący Komórkami organizacyjnymi ABM oraz kierownicy działów;
   5) Administrator Systemu;
   6) inni niż ww. Pracownicy oraz inni Użytkownicy.
2. Obowiązki i role są przydzielane w sposób zapobiegający powstaniu konfliktu pomiędzy nimi oraz zapewniający rzetelność i bezstronność wykonywania zadań związanych z Bezpieczeństwem informacji.

§ 11.

1. Prezes ABM:
   1) zapewnia zasoby niezbędne do prawidłowego funkcjonowania SZBI;
   2) podejmuje strategiczne decyzje w procesie zarządzania Bezpieczeństwem informacji;
   3) wyznacza Inspektora Ochrony Danych oraz Pełnomocnika ds. SZBI;
   4) zatwierdza dokumentację SZBI oraz jej zmiany;
   5) kieruje i wspiera osoby przyczyniające się do osiągnięcia skuteczności SZBI;
   6) promuje ciągłe doskonalenie SZBI.
2. Pełnomocnik ds. SZBI:
   1) odpowiada za zapewnienie zgodności SZBI z właściwymi wymaganiami, w szczególności z wymaganiami norm: PN-EN ISO/IEC 27001, PN-ISO/IEC 27002, PN-ISO/IEC 27005, PN-ISO/IEC 24762;
   2) inicjuje oraz nadzoruje działania wdrożeniowe, korygujące i zapobiegawcze w zakresie Bezpieczeństwa informacji;
   3) koordynuje proces zarządzania ryzykiem Bezpieczeństwa informacji;
   4) nadzoruje opracowanie, przeglądy i aktualizacje dokumentacji SZBI;
   5) opracowuje i przeprowadza szkolenia z zakresu SZBI;
   6) nadzoruje proces zarządzania Incydentami bezpieczeństwa;
   7) nadzoruje lub prowadzi audyty SZBI oraz okresowy przegląd SZBI;

8) prowadzi rejestr Aktywów;
9) wydaje opinie, zalecenia oraz rekomendacje w zakresie związanym z funkcjonowaniem SZBI;
10) odpowiada za utrzymywanie kontaktów z grupami zainteresowanych specjalistów lub innymi specjalistycznymi forami oraz stowarzyszeniami zawodowymi z obszaru Bezpieczeństwa informacji;
11) podejmuje działania w pozostałych kwestiach związanych z Bezpieczeństwem informacji, w zakresie niezastrzeżonym do kompetencji innych osób.

3. Inspektor Ochrony Danych odpowiada za monitorowanie i zapewnienie przestrzegania przepisów o ochronie danych osobowych w ABM.
4. Administrator Systemu odpowiada za zarządzanie Systemem teleinformatycznym ABM.
5. Kierujący Komórkami organizacyjnymi ABM oraz kierownicy działów:
   1) nadzorują realizację obowiązków wynikających z SZBI przez podległych im Pracowników;
   2) identyfikują Aktywa oraz dokonują oceny ich krytyczności oraz klasyfikacji;
   3) dokonują Oceny ryzyka Bezpieczeństwa informacji w podlegających im obszarach;
   4) współpracują z Pełnomocnikiem ds. SZBI, Inspektorem Ochrony Danych oraz Administratorem Systemu, w ramach realizowanych przez nich zadań;
   5) zarządzają ciągłością działania w podlegających im obszarach.
6. Pracownicy:
   1) realizują obowiązki wynikające z SZBI w zakresie powierzonych im zadań;
   2) informują niezwłocznie o wszystkich zdarzeniach mających wpływ na ryzyko Bezpieczeństwa informacji, w tym w szczególności o Incydentach bezpieczeństwa;
   3) współpracują z Pełnomocnikiem ds. SZBI, Inspektorem Ochrony Danych oraz Administratorem w ramach realizowanych przez nich zadań;
   4) odbywają obowiązkowe szkolenia z zakresu SZBI.

§ 12.

1. Szczegółowe obowiązki oraz uprawnienia Inspektora Ochrony Danych określa Polityka ochrony danych osobowych.
2. Szczegółowe obowiązki oraz uprawnienia Administratora Systemu określa Polityka bezpieczeństwa teleinformatycznego.

§ 13.

Pełnomocnikiem ds. SZBI może być osoba, która:

1) posiada właściwe kwalifikacje zawodowe a w szczególności wiedzę fachową nt. zasad bezpieczeństwa informacji lub zarządzania Systemem teleinformatycznym oraz umiejętności wypełnienia zadań określonych w § 11. ust. 2 Polityki;
2) posiada co najmniej trzyletnie doświadczenie w zakresie zarządzania Bezpieczeństwem informacji lub Systemem teleinformatycznym.

Rozdział 5
Dokumentacja SZBI

§ 14.

1. Na dokumentację SZBI w ABM składają się w szczególności:
   1) Polityka bezpieczeństwa informacji;
   2) Deklaracja stosowania zabezpieczeń;
   3) Polityka ochrony danych osobowych;
   4) Polityka bezpieczeństwa teleinformatycznego;
   5) Polityka ciągłości działania;
   6) procedury, regulaminy, opisy, instrukcje i metodyki określające szczegółowe role i obowiązki wynikające z SZBI;
   7) formularze i wzory;
   8) dokumenty stanowiące dowody kompetencji osób zaangażowanych w zarządzanie SZBI.

2. Podział dokumentacji SZBI oraz przyznawanie dostępu do niej odbywa się zgodnie z zasadą wiedzy koniecznej.

§ 15.

1. Dokumentacja SZBI podlega ochronie, w szczególności przed utratą Dostępności, Poufności, Integralności lub niewłaściwym użyciem.
2. Dokumentacja SZBI podlega okresowemu oraz bieżącemu przeglądowi i aktualizacji, z uwzględnieniem w szczególności zmian w przepisach prawa powszechnie obowiązującego, regulacjach wewnętrznych, obowiązujących normach oraz innych wymaganiach lub celach bezpieczeństwa.
3. Szczegółowe zasady przeglądu i aktualizacji dokumentacji SZBI określa Procedura oceny wyników i doskonalenia SZBI.

§ 16.

1. Wszyscy Pracownicy, a także inne osoby mające dostęp do informacji przetwarzanych w ABM, są zobowiązani do zapoznania się z Polityką oraz pozostałą dokumentacją SZBI, do której otrzymali dostęp, oraz do ich przestrzegania.
2. Dokumentacja SZBI może być udostępniana osobom innym niż Pracownicy tylko w zakresie niezbędnym do prawidłowego wykonania przez nich zadań na rzecz ABM.

Rozdział 6
Ogólne zasady zarządzania Bezpieczeństwem informacji

§ 17.

Wszyscy Pracownicy zobowiązani są do należytego postępowania z informacjami, do których mają dostęp, w szczególności do:

1) zachowania w poufności informacji, których ujawnienie jest niezgodne z przepisami prawa powszechnie obowiązującego, regulacjami wewnętrznymi oraz zawartymi przez ABM umowami lub mogłoby narazić ABM na szkodę;
2) postępowania z informacjami, do których posiadają dostęp w ramach wykonywanych obowiązków, w sposób adekwatny do kategorii i poziomu ochrony informacji;
3) przestrzegania zasad, o których mowa w § 18.

§ 18.

W celu zapewnienia odpowiedniego poziomu Bezpieczeństwa informacji stosuje się zasady:

1) odpowiedzialności za Aktywa – dla każdego Aktywa określono Właściciela aktywa, który jest odpowiedzialny w szczególności za jego należyte zabezpieczenie;
2) przywilejów koniecznych – prawa dostępu do informacji są ograniczone wyłącznie do takich informacji, które są niezbędne do realizacji powierzonych obowiązków;
3) wiedzy koniecznej – pracownicy ABM posiadają wiedzę o informacjach ograniczoną do zagadnień, które są konieczne do realizacji powierzonych obowiązków;
4) asekuracji zabezpieczeń – w celu ochrony informacji dla każdej informacji stosowane jest co najmniej jedno zabezpieczenie;
5) adekwatności – wykorzystywane Środki kontroli muszą być adekwatne do rodzaju informacji i sytuacji;
6) kompletności – w celu zabezpieczenia informacji stosowane jest kompleksowe podejście, uwzględniające wszystkie elementy procesu przetwarzania informacji.

Rozdział 7
Zarządzanie Aktywami

§ 19.

ABM identyfikuje informacje i inne Aktywa związane z informacjami oraz środkami przetwarzania informacji oraz opracowuje, utrzymuje i aktualizuje ewidencję tych Aktywów.

§ 20.

1. Wszelkie informacje wytworzone, przekazywane i przetwarzane w ABM podlegają ochronie.
2. Informacje, o których mowa w ust. 1, stanowiące własność ABM, podlegają grupowaniu poprzez przypisanie do poziomu ochrony, adekwatnego do ich znaczenia oraz wpływu na ciągłość działania ABM.

§ 21.

Szczegółowe zasady dotyczące zarządzania Aktywami w tym identyfikacji, klasyfikacji i ewidencji Aktywów określają: Procedura identyfikacji i wartościowania aktywów oraz zarządzania ryzykiem bezpieczeństwa informacji, Procedura klasyfikowania informacji oraz postępowania z określonymi grupami informacji oraz Polityka bezpieczeństwa teleinformatycznego.

Rozdział 8
Zarządzanie ryzykiem Bezpieczeństwa informacji

§ 22.

1. W celu zapewnienia odpowiedniego poziomu Bezpieczeństwa informacji oraz realizacji ustanowionych w ABM celów bezpieczeństwa w ABM wdrożony został kompleksowy system zarządzania ryzykiem Bezpieczeństwa informacji.
2. Na system, o którym mowa w ust. 1, składa się w szczególności okresowa i bieżąca Ocena ryzyka Bezpieczeństwa informacji, jego raportowanie oraz opracowywanie planów postępowania z ryzykiem.
3. Wyniki analizy ryzyka są uwzględniane we wszystkich procesach w ramach SZBI.

§ 23.

Wszyscy Pracownicy mają obowiązek:

1) uwzględniania ryzyka Bezpieczeństwa informacji w realizowanych zadaniach, procesach oraz projektach, niezależnie od ich rodzaju i etapu zaawansowania;
2) informowania, w zakresie ich właściwości, Pełnomocnika ds. SZBI, Inspektora Ochrony Danych oraz Administratora Systemu o wszystkich zdarzeniach, które mogą mieć wpływ na ryzyko Bezpieczeństwa informacji.

§ 24.

Szczegółowe zasady zarządzania ryzykiem Bezpieczeństwa informacji, w tym jego oceny oraz opracowywania planów postępowania z ryzykiem określa Procedura identyfikacji i wartościowania aktywów oraz zarządzania ryzykiem bezpieczeństwa informacji.

Rozdział 9
Bezpieczeństwo zasobów ludzkich

§ 25.

1. Zarządzanie bezpieczeństwem zasobów ludzkich w ABM obejmuje podejmowanie odpowiednich działań przed, w trakcie oraz po zakończeniu lub zmianie zatrudnienia.
2. Zawierając umowy z Pracownikami lub innymi podmiotami należy zapewnić, aby w umowach tych znalazły się postanowienia określające obowiązki stron w zakresie Bezpieczeństwa informacji.

§ 26.

1. Kandydaci do pracy podlegają weryfikacji zgodnie z obowiązującymi przepisami prawa i regulacjami wewnętrznymi ABM oraz z uwzględnieniem informacji, które będą przetwarzać i ryzyka dla ich bezpieczeństwa, związanych z wykonywanymi obowiązkami.
2. Przed rozpoczęciem wykonywania przez Pracownika obowiązków służbowych:
   1) Pracownik, który nie otrzymał jeszcze stosownego upoważnienia, nie powinien pozostawać na terenie ABM bez nadzoru osoby upoważnionej;
   2) Pracownik zapoznaje się z dokumentacją SZBI oraz podpisuje oświadczenie o zapoznaniu się z dokumentacją oraz o zachowaniu poufności. Oświadczenie podlega dołączeniu do akt osobowych Pracownika;
   3) Pracownik zostaje przeszkolony w zakresie obowiązków wynikających z SZBI.

§ 27.

1. W chwili rozpoczęcia wykonywania pracy Pracownik otrzymuje uprawnienia dostępu niezbędne do realizowania powierzonych mu zadań.
2. W przypadku zmiany warunków zatrudnienia uprawnienia dostępu podlegają stosownej modyfikacji.

§ 28.

1. W przypadku zmiany albo ustania zatrudnienia uprawnienia dostępu są odbierane lub zmieniane Pracownikowi najpóźniej w chwili odpowiednio zmiany albo ustania zatrudnienia. Odbiór albo zmiana uprawnień dotyczy każdego rodzaju dostępu, w tym dostępu fizycznego i logicznego (wirtualnego).
2. W przypadku zakończenia zatrudnienia Pracownicy zobowiązani są do zwrotu wszelkich posiadanych Aktywów ABM.

§ 29.

Zasady nadawania uprawnień, ich modyfikacji oraz odbioru określa Polityka bezpieczeństwa teleinformatycznego oraz Procedura bezpieczeństwa fizycznego i środowiskowego.

Rozdział 10
Szkolenia

§ 30.

1. W ABM obowiązuje system szkoleń poświęconych zagadnieniom Bezpieczeństwa informacji.
2. Szkolenia obejmują w szczególności tematykę:
   1) SZBI, w tym obowiązków Pracownika związanych z Bezpieczeństwem informacji – prowadzone przez Pełnomocnika ds. SZBI;
   2) ochrony danych osobowych – prowadzone przez Inspektora Ochrony Danych;
   3) korzystania z Systemu teleinformatycznego ABM – prowadzone przez Administratora Systemu.
3. Szkolenia uwzględniają w szczególności następujące zagadnienia:
   1) zagrożenia Bezpieczeństwa informacji;
   2) skutki naruszenia zasad Bezpieczeństwa informacji, w tym odpowiedzialność prawna;
   3) stosowanie środków zapewniających Bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich.
4. Szkolenia są prowadzone jako:
   1) szkolenia wstępne – prowadzone przy rozpoczęciu zatrudnienia;
   2) szkolenia okresowe – prowadzone w określonych (przez komórkę organizacyjną lub osobę odpowiedzialną za dane szkolenie) odstępach czasu, mające na celu przypomnienie i aktualizację wiedzy uczestników na temat wybranych zagadnień z zakresu bezpieczeństwa;
   3) szkolenia doskonalące – prowadzone w przypadku istotnych zmian w SZBI lub obowiązkach dotyczących Bezpieczeństwa informacji.
5. Szkolenia okresowe są prowadzone nie rzadziej niż raz na 2 lata.
6. Odbycie szkoleń wstępnych jest warunkiem otrzymania dostępu do Aktywów ABM.

Rozdział 11
Bezpieczeństwo fizyczne i środowiskowe

§ 31.

1. System zarządzania bezpieczeństwem fizycznym i środowiskowym został wdrożony w celu redukcji ryzyka wynikającego z zagrożeń fizycznych i środowiskowych oraz zapobieżenia:
   1) nieuprawnionemu fizycznemu dostępowi, szkodom i zakłóceniom w informacjach i środkach przetwarzania informacji należących do ABM;
   2) utracie, uszkodzeniu, kradzieży lub naruszeniu Integralności Aktywów należących do ABM;
   3) zakłóceniu działalności ABM.
2. Zarządzanie bezpieczeństwem fizycznym i środowiskowym w ABM odbywa się w szczególności poprzez:

1) określenie obszarów bezpieczeństwa fizycznego wraz z ustanowieniem i utrzymywaniem stosownych zabezpieczeń, adekwatnych do informacji i innych Aktywów przechowywanych w danym obszarze;
2) kontrolę ruchu osobowego w budynkach i pomieszczeniach ABM;
3) zarządzanie dostępem fizycznym do obszarów, pomieszczeń i innych miejsc przechowywania informacji;
4) stosowanie adekwatnych zabezpieczeń środowiskowych, chroniących informacje i inne Aktywa przechowywane w poszczególnych obszarach przed zniszczeniem albo uszkodzeniem wywołanym zjawiskami naturalnymi.

3. Szczegółowe zasady zarządzania bezpieczeństwem fizycznym i środowiskowym określa Procedura bezpieczeństwa fizycznego i środowiskowego.

Rozdział 12

Bezpieczeństwo Systemu teleinformatycznego

§ 32.

W celu zapewnienia należytego poziomu bezpieczeństwa Systemu teleinformatycznego ABM stosuje się w szczególności następujące zabezpieczenia:

1) dostęp do Systemu teleinformatycznego jest ograniczony wyłącznie do elementów tego systemu niezbędnych do prawidłowej realizacji zadań przez Użytkownika;
2) dostęp do Systemu teleinformatycznego jest przyznawany, modyfikowany i odbierany oraz podlega ochronie zgodnie z określonymi zasadami;
3) Aktywa stanowiące element Systemu teleinformatycznego są należycie ewidencjonowane, monitorowane i chronione przed utratą, uszkodzeniem, nieuprawnioną modyfikacją lub naruszeniem w inny sposób;
4) stosowana jest ochrona przed złośliwym oprogramowaniem;
5) określone zostały procedury wprowadzania oraz modyfikacji oprogramowania;
6) określone zostały zasady postępowania z Urządzeniami przenośnymi, w tym Nośnikami danych;
7) kopie zapasowe i archiwalne są tworzone i testowane;
8) określone zostały zasady nadzoru nad usługami dostarczanymi przez Podmioty zewnętrzne;
9) określone zostały zasady zarządzania zmianami w Systemie teleinformatycznym i jego elementach;
10) określono szczegółowe zasady zarządzania hasłami i innymi poufnymi informacjami uwierzytelniającymi.

§ 33.

Szczegółowe zasady bezpieczeństwa Systemu teleinformatycznego ABM i kontroli dostępu do tego systemu określa Polityka bezpieczeństwa teleinformatycznego.

§ 34.

Szczegółowe prawa i obowiązki Użytkowników Systemu teleinformatycznego określają: Regulamin użytkownika systemu teleinformatycznego oraz Instrukcja użytkowania urządzeń przenośnych, stanowiące załączniki do Polityki bezpieczeństwa teleinformatycznego.

Rozdział 13

Zarządzanie Incydentami bezpieczeństwa

§ 35.

1. Celem kompleksowego zarządzania Incydentami bezpieczeństwa jest w szczególności zapewnienie spójnego i skutecznego systemu reagowania na Incydenty oraz minimalizacja ryzyka ich wystąpienia.
2. W tym celu wszyscy Pracownicy są zobowiązani do informowania Pełnomocnika ds. SZBI o wszelkich zdarzeniach stanowiących albo mogących stanowić Incydent bezpieczeństwa lub zwiększających ryzyko wystąpienia Incydentu bezpieczeństwa.
3. Szczegółowe zasady zarządzania Incydentami bezpieczeństwa w ABM określa Procedura zarządzania incydentami bezpieczeństwa.

§ 36.

System zarządzania Incydentami bezpieczeństwa w ABM jest zintegrowany z innymi systemami zgłaszania naruszeń lub ich podejrzeń, w szczególności z wewnętrznym systemem zgłaszania naruszeń oraz systemem informowania o zagrożeniach lub naruszeniach ochrony danych osobowych.

Rozdział 14
Zarządzanie ciągłością działania

§ 37.

1. Zarządzanie ciągłością działania w obszarze Bezpieczeństwa informacji stanowi element obowiązującego w ABM, całościowego systemu zarządzania ciągłością działania.
2. Podstawowym celem systemu zarządzania ciągłością działania w ABM jest utrzymanie jej zdolności do prawidłowej i terminowej realizacji zadań ustawowych oraz ochrona organizacji i jej Interesariuszy przed negatywnymi konsekwencjami zakłócenia ciągłości jej działania.

§ 38.

1. Zarządzanie ciągłością działania opiera się w szczególności na:
   1) analizie wpływu;
   2) Ocenie ryzyka;
   3) określeniu wymagań szczególnych dla danego obszaru i procesów, w szczególności wynikających z przepisów prawa powszechnie obowiązującego, regulacji wewnętrznych, wytycznych, norm lub dobrych praktyk;
   4) opracowaniu i regularnym testowaniu planów ciągłości działania.
2. Szczegółowe zasady zarządzania ciągłością działania określa Polityka ciągłości działania.

Rozdział 15
Ocena wyników i doskonalenie SZBI

§ 39.

SZBI podlega ciągłemu doskonaleniu, aby zapewnić jego adekwatność i przydatność do realizacji celów, o których mowa w § 3.

§ 40.

1. Na system oceny wyników i doskonalenia SZBI składają się w szczególności
   1) wewnętrzne i zewnętrzne audyty SZBI;
   2) audyt wewnętrzny;
   3) okresowy przegląd zarządzania SZBI;
   4) podejmowanie działań korygujących;
   5) przegląd dokumentacji SZBI.
2. Szczegółowe zasady oceny wyników i doskonalenia SZBI określa Procedura oceny wyników i doskonalenia SZBI.

Rozdział 16
Zgodność

§ 41.

1. SZBI w ABM został opracowany zgodnie z obowiązującymi przepisami oraz wymaganiami odpowiednich norm i standardów w obszarze Bezpieczeństwa informacji, w tym w szczególności zgodnie z:
   1) Ustawą oraz aktami wykonawczymi do Ustawy;
   2) 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);
   3) ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych;
   4) ustawą z dnia 6 września 2001 r. o dostępie do informacji publicznej;
   5) ustawą z dnia 25 lutego 2016 r. o ponownym wykorzystywaniu informacji sektora publicznego;

6) ustawą z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne;
7) ustawą z dnia 26 czerwca 1974 r. Kodeks pracy;
8) 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;
9) rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 18 stycznia 2007 r. w sprawie Biuletynu Informacji Publicznej;
10) normami: PN-ISO/IEC 27001, PN-ISO/IEC 27002, PN-ISO/IEC 27005, PN-ISO/IEC 24762.

§ 42.

1. ABM na bieżąco identyfikuje wymagania prawne, regulacyjne i umowne oraz inne obowiązki związane z Bezpieczeństwem informacji.
2. Za bieżącą identyfikację i realizację wymagań, o których mowa w ust. 1, odpowiadają kierujący Komórkami organizacyjnymi w zakresie podlegających im obszarów. Osoby, o których mowa w zdaniu poprzednim, mogą powierzyć realizację obowiązku wskazanego w zdaniu poprzednim podległym im osobom.
3. Pełnomocnik ds. SZBI, we współpracy z osobą lub Komórką organizacyjną realizującą funkcję zgodności (compliance), wspierają proces identyfikacji, o którym mowa w ust. 2 poprzez stałe monitorowanie zmian w przepisach prawa powszechnie obowiązującego, regulacjach wewnętrznych, normach oraz innych źródłach obowiązków w zakresie Bezpieczeństwa informacji.
4. Pełnomocnik ds. SZBI prowadzi i aktualizuje listę wymagań prawnych, regulacyjnych i umownych związanych z Bezpieczeństwem informacji.
5. W przypadku stwierdzenia zmian w obowiązkach w zakresie Bezpieczeństwa informacji Komórki organizacyjne i osoby, o których mowa w ustępach powyżej, informują się wzajemnie o takich zmianach. W takim przypadku Pełnomocnik ds. SZBI informuje o zmianach także Komórki organizacyjne, na których działalność zmiany te mogą mieć wpływ.

§ 43.

1. Za zgodność odpowiadają wszyscy Pracownicy w ramach powierzonych im zadań i Aktywów.
2. Kierujący Komórkami organizacyjnymi lub osoby przez nich wyznaczone nadzorują przestrzeganie przez Pracowników zasad określonych w dokumentacji SZBI.

§ 44.

W związku z wykonywaniem powierzonych im zadań Pracownicy mają obowiązek przestrzegania praw własności intelektualnej (w tym związanych z użytkowaniem prawnie zastrzeżonego oprogramowania) należących do ABM oraz innych podmiotów, jak również niezwłocznego informowania o naruszeniu tych praw Pełnomocnika ds. SZBI oraz Komórki właściwej ds. prawnych.

Rozdział 17
Relacje z Podmiotami zewnętrznymi

§ 45.

1. ABM zarządza relacjami z Podmiotami zewnętrznymi w sposób zapewniający należyty poziom Bezpieczeństwa informacji i innych Aktywów
2. Od Podmiotów zewnętrznych ABM wymaga przestrzegania obowiązków i wymagań związanych z zapewnieniem Bezpieczeństwa informacji, w tym przestrzegania Polityki oraz innych dokumentów, istotnych z punktu widzenia stosunku prawnego łączącego ABM z danym Podmiotem zewnętrznym.

§ 46.

Określając odpowiedzialność Podmiotu zewnętrznego za Bezpieczeństwo informacji uwzględniane są działania, które mają miejsce w siedzibie ABM oraz wszelkie sytuacje, w których informacje związane z działalnością ABM są przetwarzane poza jej siedzibą (obejmuje to w szczególności zdalny dostęp do Systemu teleinformatycznego ABM).

§ 47.

Szczegółowe zasady dotyczące zarządzania relacjami z Podmiotami zewnętrznymi w kontekście SZBI określają Wytyczne dotyczące bezpieczeństwa informacji w relacjach z podmiotami zewnętrznymi.

Rozdział 18
Postanowienia końcowe

§ 48.

Naruszenie Polityki oraz innych obowiązków z zakresu Bezpieczeństwa informacji może być podstawą odpowiedzialności Pracownika lub innego Użytkownika, w szczególności odpowiedzialności karnej, odpowiedzialności przewidzianej w przepisach prawa pracy lub przepisach Kodeksu cywilnego, w tym może skutkować rozwiązaniem stosunku prawnego łączącego Pracownika lub innego Użytkownika z ABM.