POLITYKA BEZPIECZEŃSTWA INFORMACJI URZĘDU MARSZAŁKOWSKIEGO WOJEWÓDZTWA POMORSKIEGO – DOKUMENT GŁÓWNY

Numer referencyjny dokumentu: 1.1

SPIS TREŚCI

§ 1
DEKLARACJA NAJWYŻSZEGO KIEROWNICTWA

Zgodnie z treścią § 20 ust. 1 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, w Urzędzie Marszałkowskim Województwa Pomorskiego (UMWP) realizującym zadania publiczne ustanawia się, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

Wielopoziomowy System Zarządzania Bezpieczeństwem Informacji (SZBI) będący częścią całościowego systemu zarządzania w UMWP, oparty został na podejściu wynikającym z ryzyka i odnosi się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji tj. ochrony informacji w każdym punkcie jej przetwarzania. Wymagania SZBI mają charakter zintegrowany z innymi procesami realizowanymi w UMWP.

SZBI w UMWP opracowany został zgodnie z obowiązującymi przepisami prawa, na podstawie Polskiej Normy PN-ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm z rodziny ISO 27000.

Najwyższe Kierownictwo Urzędu deklaruje, w szczególności:

1. *zapewnienie dostępności zasobów potrzebnych do utrzymania, rozwoju i ciągłego doskonalenia SZBI,*
2. *zaangażowanie w odniesieniu do SZBI, w tym w kompleksową ochronę informacji i aktywów wspierających ich przetwarzanie w UMWP oraz promowanie ciągłego doskonalenia ustanowionego Systemu,*
3. *kierowanie i aktywne wspieranie osób przyczyniających się do osiągnięcia skuteczności SZBI oraz stałe podnoszenie świadomości pracowników Urzędu w zakresie bezpieczeństwa informacji.*

§ 2

WPROWADZENIE

1. Niniejsza Polityka Bezpieczeństwa Informacji jest dokumentem głównym ustanowionego w UMWP Systemu Zarządzania Bezpieczeństwem Informacji.
2. Dokument ma charakter deklaratywny, zawiera ogólne ramy, wymagania, zasady, procedury i instrukcje w zakresie ochrony informacji przetwarzanych w UMWP oraz nadrzędny w stosunku do pozostałych wewnętrznych aktów prawnych dotyczących bezpieczeństwa informacji obowiązujących w Urzędzie, tworząc wspólnie z nimi kompleksową *dokumentację bezpieczeństwa*.
3. *Podstawowy wykaz skrótów i definicji* stosowanych w obowiązującej *dokumentacji bezpieczeństwa* stanowi załącznik nr 1 do niniejszej *Polityki*.
4. *Podstawowy wykaz aktów prawnych, polskich norm i innych dokumentów związanych z bezpieczeństwem informacji* stanowi załącznik nr 2 do niniejszej *Polityki*.
5. *Polityka Bezpieczeństwa Informacji Urzędu Marszałkowskiego Województwa Pomorskiego - dokument głów*ny podlega przeglądom pod kątem aktualności, przydatności i adekwatności, zgodnie z zasadami monitorowania i aktualizacji dokumentacji bezpieczeństwa określonymi w *Polityce monitorowania i nadzoru nad bezpieczeństwem informacji, stanowiąca załącznik nr 16 do niniejszej Polityki.*

§ 3

CELE BEZPIECZEŃSTWA INFORMACJI

1. W Urzędzie Marszałkowskim Województwa Pomorskiego ustanawia się spójne z niniejszym dokumentem, uwzględniające obowiązujące przepisy i wymagania w zakresie bezpieczeństwa informacji oraz wyniki szacowania ryzyka cele bezpieczeństwa informacji.
2. Ustanowione cele bezpieczeństwa wspierają przyjętą strategię i realizację celów ustawowych oraz strategicznych UMWP, jak i zadań wykonywanych przez pracowników UMWP, praktykantów, stażystów, wolontariuszy oraz inne osoby i podmioty zewnętrzne wykonujące czynności w imieniu i na rzecz UMWP i/lub mające dostęp do aktywów informacyjnych Urzędu.
3. Do głównych celów bezpieczeństwa informacji w UMWP należy:
   1) zapewnienie bezpieczeństwa aktywów informacyjnych UMWP (w tym ochrona wizerunku i relacji z podmiotami zewnętrznymi) zgodnie z wymogami obowiązującego prawa oraz adekwatnie do wyników szacowania ryzyka w bezpieczeństwie informacji,
   2) usprawnienie funkcjonowania Urzędu poprzez uporządkowanie zasad przetwarzania informacji oraz zarządzanie aktywami informacyjnymi w zorganizowany sposób, tak aby ułatwić ciągłe doskonalenie i dostosowanie do bieżących celów Urzędu,
   3) minimalizowanie ryzyka i ograniczanie skutków utraty bezpieczeństwa informacji,
   4) stałe podnoszenie świadomości pracowników oraz pozostałych osób i podmiotów, o których mowa w ust.2 w zakresie bezpieczeństwa informacji.
4. W ramach realizacji ww. celów, adekwatnie do poziomu zidentyfikowanych zagrożeń podejmowane są działania w kierunku osiągnięcie poziomu organizacyjnego i technicznego Urzędu, który w szczególności zapewni:
   1) zachowanie poufności przetwarzanych informacji,
   2) integralność informacji oraz ich dostępność,
   3) uwzględnienie dodatkowych atrybutów bezpieczeństwa zgodnie z wymaganiami i decyzjami oraz zapewnienie bezpiecznego przetwarzania informacji, w tym zdolności do podejmowania działań w sytuacjach kryzysowych,
   4) udokumentowane informacje dotyczące celów bezpieczeństwa informacji i stopnia ich realizacji.
5. W UMWP prowadzona jest okresowa ocena stopnia realizacji wyznaczonych celów bezpieczeństwa informacji. Szczegółowe zasady i tryb prowadzenia przedmiotowej oceny określa *Polityka monitorowania i nadzoru nad bezpieczeństwem informacji.*

§ 4

KONTEKST URZĘDU MARSZAŁKOWSKIEGO WOJEWÓDZTWA POMORSKIEGO

1. Urząd Marszałkowski Województwa Pomorskiego w Gdańsku jest wojewódzką samorządową jednostką organizacyjną działającą w formie jednostki budżetowej, przy wsparciu której Zarząd i Marszałek Województwa Pomorskiego wykonują swoje zadania i kompetencje niezastrzeżone na rzecz Sejmiku oraz wojewódzkich samorządowych jednostek organizacyjnych.
2. UMWP zapewnia Sejmikowi, Zarządowi i Marszałkowi Województwa Pomorskiego pomoc w realizacji zadań w szczególności:
   1) zadań własnych Województwa Pomorskiego,
   2) zadań administracji rządowej w granicach upoważnień ustawowych,
   3) zadań powierzonych na podstawie porozumień zawartych przez Województwo Pomorskie,
   4) innych zadań, określonych przepisami prawa, uchwałami Sejmiku, Zarządu.
3. Do zadań Samorządu Województwa leżących w kompetencjach Marszałka i/lub Zarządu Województwa Pomorskiego, realizowanych przy wsparciu UMWP należą w szczególności zadania z zakresu edukacji publicznej, ochrony zdrowia, ochrony środowiska i modernizacji terenów wiejskich, gospodarki wodnej, kultury i ochrony dziedzictwa kulturowego, drogownictwa i transportu, sportu i turystyki. Ponadto UMWP realizuje zadania w zakresie promocji województwa i współpracy zagranicznej, rozwoju regionalnego, a także obronności i bezpieczeństwa publicznego, kontroli zarządczej i audytu wewnętrznego oraz zadania dotyczące absorpcji funduszy europejskich.
4. Urząd działa w oparciu o przepisy *ustawy o samorządzie województwa*, a także na podstawie *Statutu Województwa* oraz innych aktów prawnych regulujących zarówno zakres jak i obszar jego funkcjonowania.
5. Główne kierunki działania UMWP określa okresowo przyjmowana na kolejne lata *Strategia Rozwoju Województwa Pomorskiego*.
6. Sposób realizacji ww. zadań oraz wewnętrzne zasady funkcjonowania UMWP określa *Regulamin Organizacyjny* przyjęty uchwałą Zarządu Województwa, w którym określono zarówno strukturę organizacyjną Urzędu, jak i zasady oraz zakres funkcjonowania poszczególnych komórek organizacyjnych, a także inne postanowienia związane z realizacją zadań Urzędu, wynikające z obowiązującego prawa.
7. Interesariuszami UMWP są w szczególności:
   1) mieszkańcy Województwa Pomorskiego,
   2) pracownicy UMWP,
   3) organy administracji publicznej,
   4) dostawcy, kontrahenci i inne osoby oraz podmioty realizujące zadania w imieniu i na rzecz UMWP,
   5) media,
   6) inne podmioty podlegające wpływom decyzji lub działań UMWP.
8. UMWP funkcjonuje oraz realizuje swoje zadania z uwzględnieniem określonych uwarunkowań zewnętrznych jak i wewnętrznych.
9. W ramach uwarunkowań zewnętrznych, uwzględnia się w szczególności:
   1) obowiązujący porządek prawny i konieczność zapewnienie zgodności z obowiązującymi przepisami prawa,
   2) uwarunkowania ekonomiczne (w tym wpływy z podatków), technologiczne, naturalne, kulturowe, społeczne, polityczne,
   3) kluczowe czynniki i trendy zewnętrzne mające wpływ na osiągniecie celów strategicznych Urzędu,
   4) relacje i kontakty z zewnętrznymi podmiotami publicznymi i prywatnymi (w tym umowy z kontrahentami i dostawcami),
   5) wizerunek Urzędu,

10. W ramach uwarunkowań wewnętrznych, uwzględnia się w szczególności:
    1) strukturę organizacyjną UMWP, podział kompetencji, ustanowione role i odpowiedzialności,
    2) strategie, główne cele i kierunki działania i rozwoju, zapisy wewnętrznych aktów prawnych (w tym dokumentacji bezpieczeństwa),
    3) charakter wykonywanych zadań i procesów,
    4) zasoby wykorzystywane do skutecznej realizacji powierzonych zadań i procesów (m.in. budżet, wiedza, pracownicy, budynki i pomieszczenia Urzędu, systemy informatyczne),
    5) relacje wewnętrzne i komunikację w UMWP (m.in. przepływ informacji w formie tradycyjnej i za pośrednictwem systemu elektronicznego obiegu dokumentów),
    6) przyjęte normy, wytyczne i standardy.
11. Kontekst funkcjonowania UMWP jest szczegółowo analizowany, poddawany ocenie i aktualizowany w ramach systemu kontroli zarządczej, w tym prowadzonego monitorowania i doskonalenia SZBI.

§ 5
ZAKRES SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

1. Zakres ustanowionego SZBI obejmuje:
    1) procesy oraz realizowane w UMWP działania i zadania,
    2) wszelkie informacje przetwarzane w ramach ww. procesów i zadań, w tym:
        a) przetwarzane w formie tradycyjnej (m.in. informacje wydrukowane lub zapisane na papierze),
        b) przetwarzane w formie elektronicznej (np. w SI UMWP, przesyłane za pośrednictwem poczty elektronicznej lub urządzeń elektronicznych, elektronicznych nośników informacji),
        c) wypowiadane słownie,

    będące własnością UMWP lub stron zainteresowanych, o ile zostały przekazane na podstawie obowiązujących przepisów prawnych lub umów.
    3) aktywa wspierające przetwarzanie informacji w ramach ww. procesów oraz realizowanych w UMWP działań i zadań, w tym:
        a) personel (wszyscy pracownicy UMWP bez względu na podstawę zatrudnienia, praktykanci, stażyści, wolontariusze oraz inne osoby i podmioty zewnętrzne wykonujące czynności w imieniu i na rzecz UMWP i/lub mające dostęp do aktywów informacyjnych Urzędu),
        b) budynki i pomieszczenia UMWP, w których są lub będą przetwarzane informacje,
        c) sprzęt, w tym sprzęt komputerowy, urządzenia mobilne oraz inne nośniki danych, na których znajdują się informacje podlegające ochronie, oprogramowanie, infrastruktura sieciowa,
        d) technologie służące pozyskiwaniu, selekcjonowaniu, analizowaniu, przetwarzaniu, zarządzaniu i udostępnianiu informacji, do których zalicza się zarówno systemy papierowe jak i elektroniczne wspomagające realizację zadań publicznych,
        e) struktura organizacyjna (wszystkie komórki organizacyjne wskazane w Regulaminie Organizacyjnym UMWP).
2. Z uwagi na szczególny charakter informacji niejawnych wynikający z obowiązujących przepisów prawa, ochrona informacji niejawnych i aktywów wspierających ich przetwarzanie podlega wyłączeniu z ustanowionego SZBI. Zasady i tryb ochrony informacji niejawnych w UMWP określone zostały w treści odrębnych uregulowań wewnętrznych.

§ 6
PODSTAWOWE ZASADY BEZPIECZEŃSTWA INFORMACJI

1. Dążąc do możliwe jak najlepszego zabezpieczenia informacji i aktywów wspierających ich przetwarzanie wprowadza się do stosowania podstawowe zasady bezpieczeństwa informacji:

1) **zasada „adekwatności zabezpieczeń”** – stosowane zabezpieczenia muszą być adekwatne do zidentyfikowanych zagrożeń,

2) **zasada „bezpiecznego przetwarzania”** - przetwarzanie informacji szczególnie chronionych powinno odbywać się wyłącznie w bezpiecznych środowiskach, tj. w wydzielonych systemach informatycznych, zabezpieczonych pomieszczeniach etc.,

3) **zasada „bezpiecznej współpracy z podmiotami zewnętrznymi”** - dokumenty regulujące współpracę z podmiotami zewnętrznymi (m.in. treść umów i porozumień) zawierają zapisy dot. bezpieczeństwa informacji, w tym klauzule bezpieczeństwa o zachowaniu poufności,

4) **zasada „czystego biurka** – w celu wyeliminowania ryzyka przypadkowego lub celowego odczytania informacji, ich skopiowania, zniszczenia lub zmodyfikowania przez osoby nieuprawnione, opuszczając stanowisko pracy należy usunąć z blatu biurka dokumenty zawierające informacje inne niż informacje o charakterze jawnym, umieszczając je w przeznaczonych do tego celu zabezpieczonych meblach biurowych: szafach, szufladach lub sejfach,

5) **zasada „czystego ekranu”** - na czas nieobecności dostęp do komputera należy skutecznie blokować a po zakończeniu pracy komputer wyłączyć, chyba że musi on pracować w trybie ciągłym,

6) **zasada „doskonalenia SZBI”** - system zarządzania bezpieczeństwem informacji jest dostosowywany do zmieniających się warunków w oparciu o wyniki okresowo prowadzonego monitorowania i nadzoru,

7) **zasada „najsłabszego ogniwa”** – poziom bezpieczeństwa informacji wyznacza najsłabsze ogniwo (najsłabiej zabezpieczony element) SZBI,

8) **zasada „segregacji obowiązków i zadań”** - obowiązki i uprawnienia powinny być tak rozdzielone, aby pojedyncza osoba nie dysponowała pełnią uprawnień do wykonywania zadań w całości,

9) **zasada „uprawnionego dostępu”** – korzystanie z aktywów informacyjnych Urzędu odbywać się może tylko w oparciu o formalne uprawnienia do korzystania z wybranych aktywów,

10) **zasada „wiedzy uzasadnionej”** – personel, o którym mowa w § 5 dysponuje wiedzą o aktywach informacyjnych w ograniczonym zakresie, niezbędnym do realizacji powierzonych im zadań.

2. Dodatkowe zasady bezpieczeństwa mogą zostać określone w pozostałych dokumentach wchodzących w skład dokumentacji bezpieczeństwa.

3. Pracownicy UMWP, praktykanci, stażyści, wolontariusze oraz inne osoby i podmioty zewnętrzne wykonujące czynności w imieniu i na rzecz UMWP i/lub mające dostęp do aktywów informacyjnych Urzędu zobowiązani są do przestrzegania obowiązujących w UMWP zasad bezpieczeństwa.

§ 7

ROLE I ODPOWIEDZIALNOŚĆ W ZAKRESIE BEZPIECZEŃSTWA INFORMACJI

1. W ramach ustanowionego SZBI, role i odpowiedzialność w zakresie bezpieczeństwa informacji zostały zidentyfikowane i przypisane.

2. Odpowiedzialność za bezpieczeństwo informacji ponoszą wszyscy pracownicy UMWP, praktykanci, stażyści, wolontariusze oraz inne ww. osoby i podmioty objęte zakresem ustanowionego SZBI.

3. Przedmiotowa odpowiedzialność polega na przestrzeganiu wymagań prawa powszechnie obowiązującego, zapisów niniejszego dokumentu oraz pozostałych wymogów wskazanych w dokumentacji bezpieczeństwa, w szczególności na:

   1) realizacji przypisanych zadań w obszarze bezpieczeństwa informacji,

   2) ochronie powierzonych informacji i zabezpieczeniu aktywów wspierających ich przetwarzanie,

   3) nieudostępnianiu informacji osobom nieuprawnionym,

   4) zachowaniu w tajemnicy chronionych informacji oraz sposobów ich zabezpieczenia,

   5) informowaniu o podejrzeniu/wszelkich zauważonych nieprawidłowościach, które mogą mieć wpływ na bezpieczeństwo informacji.

4. Kierownictwo Urzędu odpowiedzialne jest za zapewnienie zasobów niezbędnych do bieżącego funkcjonowania, utrzymania i ciągłego monitorowania oraz doskonalenia SZBI.
5. Zespół ds. bezpieczeństwa informacji pod kierownictwem Przewodniczącego (Koordynatora Kontroli Zarządczej) odpowiada za realizację działań związanych z eksploatacją, monitorowaniem, przeglądaniem, utrzymywaniem i doskonaleniem ustanowionego Systemu.
6. Referat Bezpieczeństwa Informacji w Departamencie Organizacji współrealizuje ze wszystkim komórkami organizacyjnymi Urzędu działania związane z ustanowionym w UMWP systemem zarządzania bezpieczeństwem informacji.
7. Celem realizacji ww. działań, kluczowe role i odpowiedzialność w zakresie bezpieczeństwa informacji została przypisana do osób funkcyjnych w Urzędzie, w szczególności do:
   1) Administratora Informacji (AI), w osobie Marszałka Województwa Pomorskiego,
   2) Administratora Danych (AD),
   3) Przewodniczącego Zespołu ds. bezpieczeństwa informacji, w osobie Koordynatora Kontroli Zarządczej,
   4) Administratorów Zarządzających (AZ),
   5) Generalnego Administratora Systemu Informatycznego (GASI),
   6) Dyrektora Departamentu Organizacji,
   7) Administratora Bezpieczeństwa Informacji (ABI).
8. W celu rozdzielenia funkcji zarządczych i kontrolnych od funkcji wykonawczych, role i odpowiedzialność w ramach ustanowionego SZBI zostały ustanowione w dwóch obszarach:
   1) Role i odpowiedzialność w obszarze administrowania związane są przede wszystkim z utrzymaniem, bieżącym zarządzaniem i rozwojem SZBI.
   2) Role i odpowiedzialność w obszarze bezpieczeństwa związane są przede wszystkim z nadzorem, monitorowaniem i ciągłym doskonaleniem SZBI.
9. Szczegółowy opis kluczowych ról i odpowiedzialności w obszarze bezpieczeństwa informacji stanowi załącznik nr 3 do niniejszej *Polityki*.

§ 8

KLASYFIKACJA PRZETWARZANYCH INFORMACJI

1. Informacje przetwarzane w UMWP objęte zakresem ustanowionego SZBI klasyfikowane są w następujących grupach:
   1) dane osobowe (w rozumieniu przepisów dot. ochrony danych osobowych),
   2) tajemnice prawnie chronione (tajemnice powołane na mocy ustaw, których obowiązek ochrony wynika z tychże ustaw),
   3) tajemnice Urzędu (informacje, których ujawnienie mogłoby narazić UMWP na szkodę oraz informacje wewnętrzne udostępniane na zasadzie „wiedzy uzasadnionej”),
   4) informacje jawne (w tym informacje udostępniane w trybie informacji publicznej).
2. Szczegółowe zasady dot. bezpieczeństwa i ochrony poszczególnych grup informacji, w tym ich zakres, tryb udostępniania i dystrybucji oraz archiwizacji i niszczenia zostały określone w dedykowanych politykach bezpieczeństwa, stanowiących załączniki nr 4-7 do niniejszej *Polityki.*

§ 9

STRUKTURA DOKUMENTACJI SZBI

1. W ramach ustanowionego SZBI wprowadza się trójpoziomową dokumentację bezpieczeństwa określającą zasady i tryb zarządzania bezpieczeństwem informacji oraz aktywów wspierających przedmiotowe przetwarzanie w UMWP:
   1) W ramach I poziomu SZBI (dokumenty o charakterze publicznym, ogólnodostępnym) wyróżnia się:
      a) „Politykę Bezpieczeństwa Informacji Urzędu Marszałkowskiego Województwa Pomorskiego – dokument główny”:

- dokument nadrzędny w stosunku do pozostałych wewnętrznych aktów prawnych dotyczących bezpieczeństwa informacji obowiązujących w UMWP, tworzących wspólnie dokumentację bezpieczeństwa,
- określającą ogólne ramy, kierunki, zasady i wymogi bezpieczeństwa informacji w UMWP oraz zakres dokumentacji bezpieczeństwa na pozostałych poziomach,
- wprowadzaną i aktualizowaną w formie zarządzenia Marszałka Województwa Pomorskiego.

2) W ramach II poziomu SZBI (dokumenty dedykowane i udostępniane wszystkim pracownikom UMWP, praktykantom, stażystom, wolontariuszom, w uzasadnionych przypadkach wybranym osobom i podmiotom zewnętrznym wykonującym czynności w imieniu i na rzecz UMWP i/lub mającym dostęp do aktywów informacyjnych Urzędu) wyróżnia się dedykowane polityki tematyczne:
   a) zawierające uszczegółowienie zapisów polityki I poziomu SZBI,
   b) określające specyficzne wymogi i zasady bezpieczeństwa w kluczowych obszarach bezpieczeństwa informacji:
      - polityki bezpieczeństwa dedykowane dla poszczególnych grup informacji wskazanych w § 8 niniejszego dokumentu,
      - polityka kontroli dostępu,
      - polityka zarządzania aktywami informacyjnymi,
      - polityka zarządzania ryzykiem w bezpieczeństwie informacji,
      - polityka bezpieczeństwa teleinformatycznego,
      - polityka bezpieczeństwa fizycznego i środowiskowego,
      - polityka zarządzania ciągłością działania,
      - polityka bezpieczeństwa w relacjach z podmiotami zewnętrznymi,
      - polityka zarządzania incydentami związanymi z bezpieczeństwem informacji,
      - polityka monitorowania i nadzoru nad bezpieczeństwem informacji,
   c) wprowadzane i aktualizowane w formie załączników do polityki I poziomu SZBI i/lub na mocy odrębnych zarządzeń Marszałka Województwa Pomorskiego.

3) W ramach III poziomu SZBI (dokumenty dedykowane i udostępniane wybranym osobom i podmiotom na zasadzie „wiedzy uzasadnionej") wyróżnia się:
   a) wybrane procedury i instrukcje wykonawcze:
      - określające zasady i sposób realizacji wymogów w obszarach uregulowanych na II poziomie SZBI w danej komórce organizacyjnej/przez dany podmiot zewnętrzny wykonujący czynności w imieniu i na rzecz UMWP,
      - wprowadzane i aktualizowane w formie załączników do dokumentów II poziomu SZBI i/lub dokumentów wewnętrznych wybranych komórek organizacyjnych UMWP, ewentualnie na mocy odrębnych zarządzeń Marszałka Województwa Pomorskiego,
   b) instrukcje/procedury bezpieczeństwa dla wybranych komórek organizacyjnych w związku z realizacją projektów unijnych, w tym regionalnych programów operacyjnych,
   c) wybrane umowy ze stronami trzecimi,

2. Dokumenty opracowywane na poszczególnych poziomach SZBI uzupełniają się wzajemnie, tworząc kompleksową dokumentację Systemu Zarządzania Bezpieczeństwem Informacji w UMWP (dokumentację bezpieczeństwa):
   1) dokumentacja I poziomu SZBI ma charakter ogólny, a jej zapisy odwołują się wprost do dedykowanych dokumentów II poziomu SZBI, w których przedmiotowe zapisy są uszczegółowione,
   2) poszczególne dokumenty II poziomu SZBI odwołują się do siebie oraz do procedur i instrukcji III poziomu SZBI.

3) procedury i instrukcje III poziomu SZBI uszczegółowiają wybrane kwestie zidentyfikowane w ramach dokumentacji II poziomu.

3. W przyjętym w UMWP modelu bezpieczeństwa dopuszcza się opracowywanie dodatkowych dokumentów dot. bezpieczeństwa informacji, w tym regulaminów, rekomendacji, zasad, wytycznych.

4. Celem zapewnienia właściwości, adekwatności i skuteczności obowiązujących przepisów wewnętrznych w zakresie bezpieczeństwa, prowadzone są okresowe przeglądy i aktualizacja ww. dokumentacji. Zasady oraz tryb prowadzenia przedmiotowych przeglądów dokumentacji SZBI uregulowano w *Polityce monitorowania i nadzoru nad bezpieczeństwem informacji*.

§ 10

KONTROLA DOSTĘPU DO INFORMACJI

1. W ramach zapewnienia ograniczonego dostępu do aktywów informacyjnych UMWP, w tym do budynków i pomieszczeń, sprzętu i urządzeń oraz systemów informatycznym tylko dla osób i podmiotów uprawnionych, prowadzona jest kontrola dostępu fizycznego i logicznego.

2. Szczegółowe zasady zarządzania dostępem do aktywów informacyjnych UMWP zostały uregulowane w *Polityce kontroli dostępu*, stanowiącej załącznik nr 8 do niniejszej *Polityki* oraz *dedykowanych procedurach III poziomu SZBI*.

§ 11

ZARZĄDZANIE AKTYWAMI INFORMACYJNYMI

1. W celu zapewnienia adekwatnego poziomu bezpieczeństwa aktywów informacyjnych, przedmiotowe aktywa są inwentaryzowane, klasyfikowane i zarządzane zgodnie z obowiązującymi wymaganiami w zakresie ich ochrony.

2. Szczegółowe zasady dot. identyfikowania, klasyfikowania, postępowania z aktywami oraz odpowiedzialności za aktywa informacyjne zostały uregulowane w *Polityce zarządzania aktywami informacyjnymi*, stanowiącej załącznik nr 9 do niniejszej *Polityki* oraz *dedykowanej Procedurze inwentaryzacji aktywów informacyjnych*.

§ 12

ZARZĄDZANIE RYZYKIEM W BEZPIECZEŃSTWIE INFORMACJI

1. Skuteczne zarządzanie bezpieczeństwem informacji wymaga podejmowania okresowych działań w obszarze zarządzania ryzykiem, w szczególności w zakresie szacowania tj. identyfikowania, analizy i oceny ryzyka w bezpieczeństwie informacji, zmierzających do ograniczenia oraz eliminacji przedmiotowego ryzyka.

2. Działania związane z zarządzaniem ryzykiem mającym wpływ na bezpieczeństwo informacji obejmują w szczególności:

   1) przygotowanie oraz okresową aktualizację dokumentów dot. zarządzania ryzykiem,

   2) prowadzenie okresowego szacowania ryzyka,

   3) postępowanie z ryzykiem,

   4) podejmowanie działań korygujących.

3. Szczegółowe zasady dot. zarządzania ryzykiem w bezpieczeństwie informacji zostały uregulowane w *Polityce zarządzania ryzykiem w bezpieczeństwie informacji*, stanowiącej załącznik nr 10 do niniejszej *Polityki* oraz *dedykowanej Procedurze szacowania i postępowania z ryzykiem w bezpieczeństwie informacji*.

§ 13

BEZPIECZEŃSTWO TELEINFORMATYCZNE

1. W ramach zarządzania bezpieczeństwem teleinformatycznym podejmowane są działania w zakresie szacowania i kontroli ryzyka utraty poufności, integralności, dostępności informacji w związku z korzystaniem z SI UMWP oraz aplikacji, komputerów i urządzeń mobilnych, sieci komputerowych i transmisji danych.

2. Przedmiotowe działania podejmowane są w szczególności w zakresie rozwoju, monitorowania i doskonalenia infrastruktury teleinformatycznej.

3. Szczegółowe zasady i wymogi w zakresie bezpieczeństwa teleinformatycznego zostały uregulowane w *Polityce bezpieczeństwa teleinformatycznego*, stanowiącej załącznik nr 11 do niniejszej *Polityki* oraz *dedykowanych procedurach i instrukcjach III poziomu SZBI*.

§ 14

BEZPIECZEŃSTWO FIZYCZNE I ŚRODOWISKOWE

1. W celu zapobieżenia nieuprawnionemu fizycznemu dostępowi, szkodom i zakłóceniom w przetwarzaniu informacji i środkach przetwarzania informacji oraz utracie, zniszczeniu, uszkodzeniu, kradzieży aktywów informacyjnych UMWP stosowane są mechanizmy ochrony w obszarze bezpieczeństwa fizycznego i środowiskowego.
2. Szczegółowe zasady dot. zarządzania bezpieczeństwem fizycznym i środowiskowym zostały uregulowane w *Polityce bezpieczeństwa fizycznego i środowiskowego*, stanowiącej załącznik nr 12 do niniejszej *Polityki* oraz *dedykowanych procedurach i instrukcjach, w tym procedurach III poziomu SZBI*.

§ 15

BEZPIECZEŃSTWO ZASOBÓW LUDZKICH

1. Celem ograniczenia ryzyka błędu ludzkiego, kradzieży lub nadużycia oraz zapewnienia, że pracownicy UMWP, praktykanci, stażyści, wolontariusze, zleceniobiorcy oraz inne osoby i podmioty wykonujące czynności w imieniu i na rzecz UMWP i/lub mające dostęp do aktywów informacyjnych Urzędu są świadomi odpowiedzialności i swoich obowiązków dotyczących bezpieczeństwa informacji oraz wypełniają je w odpowiedni sposób i z uwzględnieniem interesów UMWP, podejmowane są określone działania w obszarze bezpieczeństwa zasobów ludzkich, w szczególności:
   1) zapewnienie wykwalifikowanych pracowników i/lub innych osób oraz podmiotów zewnętrznych do realizacji zadań,
   2) uwzględnienie odpowiednich zapisów dot. odpowiedzialności w zakresie bezpieczeństwa informacji w umowach zawieranych z ww. osobami i podmiotami,
   3) szkolenie ww. osób i podmiotów w zakresie bezpieczeństwa informacji oraz regularne informowanie o aktualizacji polityk i procedur związanych z ich stanowiskiem pracy.
2. Szczegółowe zasady dot. zarządzania bezpieczeństwem zasobów ludzkich zostały uregulowane w *Polityce bezpieczeństwa danych osobowych*, stanowiącej załącznik nr 4 do niniejszej *Polityki* oraz *dedykowanych procedurach i instrukcjach, w tym procedurach III poziomu SZBI.*

§ 16

ZAPEWNIENIE CIĄGŁOŚCI DZIAŁANIA

1. W UMWP podejmowane są działania w zakresie planowania, weryfikowania, zapewnienia, przeglądu i oceny ciągłości działania i postępowania w przypadku wystąpienia sytuacji kryzysowych.
2. Szczegółowe zasady dot. zarządzania ciągłością działania zostały uregulowane w *Polityce zarządzania ciągłością działania*, stanowiącej załącznik nr 13 do niniejszej *Polityki* oraz *dedykowanych procedurach i instrukcjach, w tym procedurach III poziomu SZBI*.

§ 17

RELACJE Z PODMIOTAMI ZEWNĘTRZNYMI

1. Celem zapewnienia ochrony aktywów informacyjnych udostępnianych usługodawcom, dostawcą i innym osobom i podmiotom zewnętrznym wykonującym czynności w imieniu i na rzecz UMWP i/lub mającym dostęp do aktywów Urzędu, wprowadza się zasady postępowania w przypadku współpracy związanej z dostępem do aktywów informacyjnych UMWP i korzystania z usług ww. osób i podmiotów.
2. W przypadku wykonywania zadań delegowanych i/lub korzystania z aktywów, w tym przetwarzania informacji powierzonych przez podmioty zewnętrzne w drodze stosownej umowy i/lub porozumienia, poza wymogami określonymi w obowiązującej w UMWP dokumentacji bezpieczeństwa dopuszcza się stosowanie wymogów i zaleceń bezpieczeństwa określonych przez ww. podmioty zewnętrzne, o ile wskazane wymogi i zalecenia „zewnętrzne” nie obniżają poziomu bezpieczeństwa pozostałych informacji przetwarzanych w Urzędzie.

3. Przedmiotowe zasady i wymogi współpracy zostały uregulowane w P*olityce bezpieczeństwa w relacjach z podmiotami zewnętrznymi* stanowiącej załącznik nr 14 do niniejszej *Polityki*.

§ 18

ZGODNOŚĆ Z PRZEPISAMI PRAWA I ZAPISAMI UMOWNYMI

1. W celu uniknięcia naruszenia obowiązujących przepisów prawa, zobowiązań ustawowych, zapisów zawartych umów i porozumień, w UMWP prowadzona jest bieżąca kontrola zgodności regulacji wewnętrznych, przyjętych zasad bezpieczeństwa i ich stosowania z ww. przepisami, w tym identyfikowanie, dokumentowanie i aktualizowanie wszystkich istotnych wymagań prawnych, regulacyjnych, umownych oraz podejścia organizacji do ich przestrzegania.
2. Przedmiotowa kontrola dotyczy również zgodności z wymaganiami prawnymi, regulacyjnymi i umownymi, związanymi z prawami własności intelektualnej i użytkowaniem prawnie zastrzeżonego oprogramowania.
3. Kierownicy komórek organizacyjnych, w zakresie zadań realizowanych zgodnie z *Regulaminem Organizacyjnym* prowadzą bieżący nadzór w swoich komórkach w zakresie zgodności z przepisami prawa i zapisami umownymi.
4. Administrator Bezpieczeństwa Informacji w UMWP odpowiedzialny jest za zapewnienia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych.
5. Zespół ds. bezpieczeństwa informacji, we współpracy z kierownikami poszczególnych komórek organizacyjnych UMWP dokonuje okresowych przeglądów regulacji wewnętrznych dotyczących bezpieczeństwa informacji w zakresie ich zgodności z przepisami prawa i zapisami umownymi, na zasadach i w trybie określonym w *Polityce monitorowania i nadzoru nad bezpieczeństwem informacji i dedykowanych procedurach.*
6. Departament Kontroli i Audytu Wewnętrznego zapewnia okresowy audyt wewnętrzny w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.
7. *Polityka Bezpieczeństwa Informacji Urzędu Marszałkowskiego Województwa Pomorskiego - dokument główny* oraz opracowywane dokumenty II i III poziomu SZBI są zgodne z obowiązującymi przepisami prawa oraz wybranymi standardami międzynarodowymi dot. bezpieczeństwa informacji, w szczególności ze wskazanymi w *Podstawowym wykazie aktów prawnych, polskich norm i innych dokumentów związanych z bezpieczeństwem informacji.*

§ 19

NARUSZENIE BEZPIECZEŃSTWA INFORMACJI I ODPOWIEDZIALNOŚĆ Z TYTUŁU PRZEDMIOTOWEGO NARUSZENIA

1. Podstawową konsekwencją naruszenia bezpieczeństwa informacji jest obniżenie poziomu ochrony przetwarzanych informacji i aktywów wspierających ich przetwarzanie w UMWP.
2. Każdy, kto posiada dostęp do informacji i aktywów wspierających ich przetwarzanie w UMWP (pracownicy UMWP, jak również praktykanci, stażyści, wolontariusze, zleceniobiorcy oraz inne osoby i podmioty zewnętrzne wykonujące czynności w imieniu i na rzecz UMWP i/lub mające dostęp do aktywów informacyjnych Urzędu) ma obowiązek informowania podmiotów odpowiedzialnych za bezpieczeństwo UMWP o podejrzeniu/każdym zidentyfikowanym przypadku naruszenia bezpieczeństwa.
3. Nieprzestrzeganie zasad zawartych w dokumentacji bezpieczeństwa stanowi naruszenie obowiązków pracowniczych i może skutkować sankcjami natury dyscyplinarnej.
4. Naruszenie postanowień PBI przez kontrahenta UMWP lub jego pracowników stanowi podstawę do odstąpienia od umowy i żądania pokrycia powstałej szkody lub zapłaty kary umownej, jeżeli taki obowiązek wynika z zawartej umowy.
5. Z tytułu działań pracowników/kontrahentów UMWP i innych osób i podmiotów, o których mowa w ust. 2, niezgodnych z przepisami prawa powszechnie obowiązującego (w szczególności dot. przetwarzania danych osobowych), grożą odrębne kary określone w szczególności w:
   1) kodeksie pracy,
   2) kodeksie cywilnym,
   3) kodeksie karnym,
   4) ustawie o ochronie danych osobowych.

6. W celu uzyskania możliwie pełnej informacji o naruszeniu bądź też podejrzeniu naruszenia bezpieczeństwa informacji w UMWP, osoby bądź podmioty niezwiązane z UMWP mogą zgłaszać przypadki bądź podejrzenie naruszenia bezpieczeństwa aktywów informacyjnych Urzędu na adres incydent@pomorskie.eu.
7. Szczegółowe zasady dot. identyfikowania, zgłaszania, reagowania i obsługi zdarzeń i incydentów związanych z bezpieczeństwem informacji zostały uregulowane w *Polityce zarządzania incydentami związanymi z bezpieczeństwem informacji*, stanowiącej załącznik nr 15 do niniejszej *Polityki* oraz dedykowanej *Procedurze postępowania i obsługi incydentów związanych z bezpieczeństwem informacji,* stanowiącej dokument III poziomu SZBI.

§ 20

DOBÓR ZABEZPIECZEŃ

1. Cele i dobór zabezpieczeń w SZBI prowadzony jest w oparciu o aktualne wymogi prawa powszechnie obowiązującego, zalecenia polskich norm z rodziny ISO 27000 oraz wyniki monitorowania Systemu, w szczególności wyniki szacowania ryzyka w bezpieczeństwie informacji.
2. Stosowane zabezpieczenia fizyczne, techniczne i organizacyjne powinny uzupełniać się wzajemnie, zapewniając wymagany poziom bezpieczeństwa informacji.
3. Wykaz stosowanych zabezpieczeń wraz z celami ich stosowania i uzasadnieniem ich wyboru/wyłączenia ma charakter udokumentowanej informacji, opracowanej w formie *Deklaracji Stosowania*.

§ 21

UTRZYMANIE, MONITOROWANIE I DOSKONALENIE SZBI

1. Działania w zakresie utrzymania, monitorowania i doskonalenia SZBI podejmowane są w szczególności w zidentyfikowanych na II poziomie SZBI obszarach bezpieczeństwa.
2. Działania, o których mowa w ust. 1 mają charakter działań bieżących i okresowych.
3. W oparciu o wyniki prowadzonego monitorowania i nadzoru nad bezpieczeństwem informacji, w przypadku zidentyfikowania niezgodności podejmowane są adekwatne działania doskonalące, w tym działania korygujące mające na celu wyeliminowanie przyczyn niezgodności.
4. W UMWP prowadzone jest ciągłe doskonalenie przydatności, adekwatności i skuteczności ustanowionego systemu zarządzania bezpieczeństwem informacji.
5. Szczegółowe zasady dot. monitorowania i doskonalenia SZBI zostały określone w *Polityce monitorowania i nadzoru nad bezpieczeństwem informacji* oraz *dedykowanych procedurach*.

§ 22

INFORMOWANIE O TREŚCI DOKUMENTACJI BEZPIECZEŃSTWA

1. Niniejszy dokument *Polityki* wraz z załącznikami nr 1 i 2 mają charakter jawny i są ogólnodostępne.
2. Załączniki nr 3-16 do niniejszej *Polityki*, w tym zawierające dokumentację II poziomu SZBI udostępniane są wszystkim pracownikom UMWP, praktykantom, stażystom, wolontariuszom, w uzasadnionych przypadkach wybranym osobom/podmiotom zewnętrznym wykonującym czynności w imieniu i na rzecz UMWP i/lub mającym dostęp do aktywów informacyjnych Urzędu.
3. Dokumentacja III poziomu SZBI udostępniana jest w ograniczonym zakresie, wybranym pracownikom/innym osobom i podmiotom zewnętrznym na zasadzie „wiedzy uzasadnionej”, pozwalającym na realizację powierzonych zadań.

§ 23

ZAŁĄCZNIKI

1. *Wykaz skrótów i definicji.*
2. *Podstawowy wykaz aktów prawnych, polskich norm i innych dokumentów związanych z bezpieczeństwem informacji.*
3. *Kluczowe role i odpowiedzialność w zakresie bezpieczeństwa informacji.*

DOKUMENTACJA II POZIOMU SZBI

4. *Polityka bezpieczeństwa danych osobowych.*
5. *Polityka bezpieczeństwa informacji – tajemnice prawnie chronione.*
6. *Polityka bezpieczeństwa informacji – tajemnice Urzędu.*
7. *Polityka bezpieczeństwa informacji jawnych.*
8. *Polityka kontroli dostępu.*
9. *Polityka zarządzania aktywami informacyjnymi.*
10. *Polityka zarządzania ryzykiem w bezpieczeństwie informacji.*
11. *Polityka bezpieczeństwa teleinformatycznego.*
12. *Polityka bezpieczeństwa fizycznego i środowiskowego.*
13. *Polityka zarządzania ciągłością działania.*
14. *Polityka bezpieczeństwa w relacjach z podmiotami zewnętrznymi.*
15. *Polityka zarządzania incydentami związanymi z bezpieczeństwem informacji.*
16. *Polityka monitorowania i nadzoru nad bezpieczeństwem informacji.*

WYKAZ SKRÓTÓW I DEFINICJI

Pojęcie	Definicja
Aktywa	Wszystko, co ma wartość dla organizacji (UMWP) i z tego powodu wymaga ochrony *(PN-ISO/IEC 27005);*
Aktywa informacyjne	Kluczowe procesy i zadania, informacje przetwarzane w dowolnej formie, w tym papierowej i elektronicznej w ramach ww. procesów i zadań oraz aktywa wspierające przedmiotowe przetwarzanie, posiadające wartość dla UMWP i wymagające właściwej ochrony przed utratą dostępności, poufności i integralności *(definicja własna);*
Autentyczność	Właściwość, która polega na tym, że podmiot jest tym, za kogo się podaje *(PN-ISO/IEC 27000);* Właściwość polegająca na tym, że pochodzenie lub zawartość danych opisujących obiekt są takie jak deklarowane *(Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych);*
Bezpieczeństwo Informacji	Zachowanie poufności, integralności i dostępności Informacji; dodatkowo, mogą być brane pod uwagę inne własności, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność *(PN-ISO/IEC 27000);*
Budynek	Budynek UMWP położony w Gdańsku pod następującymi adresami: ul. Okopowa 21/27, ul. Augustyńskiego 2, ul. Rzeźnicka 54/56, ul. Żabi Kruk 12, ul. Równa 19/21, ul. Długi Targ 1-10 oraz w Słupsku, ul. Jaracza 18a *(definicja własna);*
Dane osobowe	Wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, przy czym osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne (*ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych);*
Deklaracja stosowania	Dokument określający, które zabezpieczenia zostały wdrożone, jakie są cele stosowania tych zabezpieczeń, wraz z uzasadnieniem ich wyboru/wykluczenia *(PN-ISO/IEC 27001);*
Dokumentacja bezpieczeństwa	Zespół powiązanych ze sobą spójnych dokumentów określających zasady i sposoby zarządzania bezpieczeństwem informacji oraz aktywów wspierających przetwarzanie informacji w UMWP *(definicja własna);*
Dostępność	Właściwość bycia dostępnym i użytecznym na żądanie autoryzowanego podmiotu *(PN-ISO/IEC 27000)*; Właściwość określająca, że zasób systemu teleinformatycznego jest możliwy do wykorzystania na żądanie, w założonym czasie, przez podmiot uprawniony do pracy w systemie teleinformatycznym *(Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych);*
Działania korygujące	Działanie mające na celu wyeliminowanie przyczyny określonego stanu rzeczy (niezgodności) i zapobieżenie jego powtórzeniu *(PN-ISO/IEC 27000);*

Pojęcie	Definicja
Działania naprawcze	Działanie podejmowane w celu wyeliminowania określonego stanu rzeczy i przywrócenia stanu pożądanego *(definicja własna);*
GIODO	Generalny Inspektor Ochrony Danych Osobowych;
Incydent związany z bezpieczeństwem informacji	Pojedyncze niepożądane lub niespodziewane zdarzenie związane z bezpieczeństwem informacji lub seria takich zdarzeń, które stwarzają znaczne prawdopodobieństwo zakłócenia działań i zagrażają bezpieczeństwu przetwarzanych informacji *(PN-ISO/IEC 27000);*
Informacje niejawne	Informacje, których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne, także w trakcie ich opracowywania oraz niezależnie od formy i sposobu ich wyrażania *(ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182 poz.1228 ze zm.);*
Informacje objęte tajemnicą przedsiębiorstwa	Nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, co do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności *(ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji);*
Informacje objęte tajemnicą skarbową	Informacje wskazane szczegółowo w *ustawie z dnia 29 sierpnia 1997 r. Ordynacja podatkowa*;
Informacje publiczne	Każda informacja o sprawach publicznych odnosząca się do organu władzy publicznej i dotycząca sfery jego działalności, w tym treść dokumentów, treść wystąpień, opinii i ocen przez nie dokonywanych *(ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej);*
Integralność	Właściwość informacji polegająca na tym, że nie została zmienione, dodana lub usunięta w nieautoryzowany sposób *(definicja własna);* Właściwość polegająca na zapewnieniu dokładności i kompletności *(PN-ISO/IEC 27000);* Właściwość polegająca na tym, ze zasób systemu teleinformatycznego nie został zmodyfikowany w sposób nieuprawniony *(Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych);*
Kierownik	Osoba kierująca pracą komórki organizacyjnej Urzędu, tj. dyrektor i jego zastępcy, kierownik biura, radca prawny-koordynator oraz osoby zajmujące następujące stanowiska pracy: Samodzielne Stanowisko ds. bezpieczeństwa, higieny pracy i ppoż., Pełnomocnik ds. ochrony informacji niejawnych, Administrator Bezpieczeństwa Informacji *(definicja własna w oparciu o Regulamin Organizacyjny UMWP);*
Komórki organizacyjne	Departament, samodzielne biuro oraz stanowisko ds. bezpieczeństwa, higieny pracy i ppoż., Pełnomocnik ds. ochrony informacji niejawnych, Administrator Bezpieczeństwa Informacji *(definicja własna w oparciu o Regulamin Organizacyjny UMWP)*;
Kierownictwo Urzędu/Osoby zarządzające	najwyższe kierownictwo, osoba lub grupa osób, która określa kierunek i steruje organizacją na najwyższym poziomie, tj. Sejmik, Zarząd, Marszałek, Sekretarz Województwa - Dyrektor Generalny Urzędu, Zastępca Sekretarza Województwa – Zastępca Dyrektora Generalnego Urzędu, Skarbnik Województwa *(definicja własna w oparciu o Regulamin Organizacyjny UMWP);*

Pojęcie	Definicja
Naruszenie bezpieczeństwa informacji	Przypadek, w którym użytkownik lub inna osoba pomija lub niszczy ustanowione zabezpieczenia lub środki ochrony w celu pozyskania nieuprawnionego dostępu do informacji lub do pozostałych zasobów Systemu *(definicja własna);* Naruszenie lub podejrzenie naruszenia dostępności, poufności i /lub integralności informacji *(definicja własna);*
Niezaprzeczalność	Zdolność do udowodnienia, że wystąpiły deklarowane zdarzenia lub działania oraz że wywołał je dany podmiot *(PN-ISO/IEC 27000);* Brak możliwości zanegowania swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie *(Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych);*
Niezawodność	Właściwość informacji oznaczająca spójne, zamierzone zachowanie i skutki *(PN-ISO/IEC 27000);*
Niezgodność	Niespełnienie wymagań bezpieczeństwa informacji *(PN-ISO/IEC 27000);*
PBI	Polityka Bezpieczeństwa Informacji Urzędu Marszałkowskiego Województwa Pomorskiego – dokument główny określająca zestaw praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji i informacji w UMWP *(definicja własna);*
Poufność	Właściwość polegająca na tym, że informacja nie jest udostępniana ani ujawniana nieautoryzowanym osobom, podmiotom lub procesom *(PN-ISO/IEC 27000);*
Pracownik	Osoba zatrudniona w UMWP na podstawie umowy o pracę, powołania lub wyboru *(Regulamin Pracy UMWP):*
Przetwarzanie informacji	Jakiekolwiek operacje wykonywane na informacjach obejmujące ich zbieranie, gromadzenie, utrwalanie, przechowywanie, opracowywanie, zmienianie, wytwarzanie, udostępnianie, przekazywanie i usuwanie *(definicja własna);*
Rozliczalność	Właściwość informacji, polegająca na tym, że określone działanie dowolnego podmiotu może być jednoznacznie przypisane temu podmiotowi *(definicja własna)*; Właściwość systemu pozwalająca przypisać określone działanie w systemie do osoby fizycznej lub procesu oraz umiejscowić je w czasie *(Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych);*
System informacyjny	Uporządkowany układ odpowiednich elementów, charakteryzujących się pewnymi właściwościami i połączonych wzajemnie określonymi relacjami *(definicja własna);* Aplikacje, usługi, aktywa technik informacyjnych lub inne komponenty przetwarzające informacje *(PN-ISO/IEC 27000);*
System informatyczny (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 *(ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne);*

Pojęcie	Definicja
SZBI UMWP	System Zarządzania Bezpieczeństwem Informacji w Urzędzie Marszałkowskim Województwa Pomorskiego - część całościowego systemu zarządzania (struktura polityki, procedur, wytycznych i związanych z tym zasobów służących do osiągnięcia celów organizacji) oparta na podejściu wynikającym z ryzyka, odnosząca się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji *(definicja własna w oparciu o PN-ISO/IEC 27000);*
SI UMWP	System informatyczny UMWP
Środek przetwarzania informacji	Każdy system przetwarzania informacji, usługa lub infrastruktura albo ich fizyczna lokalizacja (*PN-ISO/IEC 27000);*
UMWP, Urząd	Urząd Marszałkowski Województwa Pomorskiego;
UODO	*Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych;*
Urządzenia mobilne	Komputery przenośne (notebooki, palmtopy), a także urządzenia multimedialne (projektory oraz aparaty i kamery cyfrowe) i telefony komórkowe, smartfony, tablety (*definicja własna);*
Użytkownik	Każdy, kto posiada upoważnienie do korzystania z systemu informatycznego i dzięki określonym uprawnieniom uczestniczy w przetwarzaniu Informacji *(definicja własna);*
Zagrożenie	Potencjalna przyczyna niepożądanego incydentu, który może wywołać szkodę w systemie lub organizacji np. kradzież, nieautoryzowana modyfikacja, szpiegostwo, sabotaż, wandalizm, zniszczenie w wyniku pożaru lub powodzi (*PN-ISO/IEC 27000);*
Zarządzanie ryzykiem w bezpieczeństwie informacji	Systematyczne stosowanie zasad zarządzania, procedur i praktyk na rzecz działań w zakresie informowania, konsultowania, tworzenia kontekstu oraz identyfikowania, analizy, oceny, postępowania z ryzykiem, monitorowania i przeglądania ryzyka związanego z przetwarzaniem informacji (*PN-ISO/IEC 27000);*
Zarządzanie ciągłością działania	Całościowy proces zarządzania identyfikujący potencjalne zagrożenia i skutki, jakie te zagrożenia mogą wywierać na działalność UMWP w przypadku ich wystąpienia, który zapewnia kształtowanie odporności Urzędu i umożliwia skuteczną reakcję w celu ochrony interesów kluczowych interesariuszy tj. osób zaangażowanych w działalność UMWP, reputacji i wizerunku Urzędu *(definicja własna w oparciu o PN-EN ISO 22301:2014);*
Zdarzenie związane z bezpieczeństwem informacji	Stwierdzone wystąpienie stanu systemu, usługi lub sieci, który wskazuje na możliwe naruszenie polityki bezpieczeństwa informacji lub błąd zabezpieczenia, lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem informacji (*PN-ISO/IEC 27000);*

PODSTAWOWY WYKAZ AKTÓW PRAWNYCH, POLSKICH NORM I INNYCH DOKUMENTÓW ZWIĄZANYCH Z BEZPIECZEŃSTWEM INFORMACJI

Wykaz podstawowych aktów prawa powszechnie obowiązującego związanych z bezpieczeństwem informacji:

1. Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy;
2. Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach;
3. Ustawa z dnia 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych;
4. Ustawa z dnia 29 września 1994 roku o rachunkowości;
5. Ustawa z dnia 6 czerwca 1997 r. - Kodeks karny;
6. Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia;
7. Ustawa z dnia 29 sierpnia 1997 roku o ochronie danych osobowych;
8. Ustawa z dnia 27 lipca 2001 roku o ochronie baz danych;
9. Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej;
10. Ustawa z dnia 18 lipca 2002 roku o świadczeniu usług drogą elektroniczną;
11. Ustawa z dnia 17 lutego 2005 roku o informatyzacji działalności podmiotów realizujących zadania publiczne;
12. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych;
13. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 roku w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych;
14. Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego;
15. Rozporządzenie Prezesa Rady Ministrów z dnia 14 września 2011 r. w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych;
16. Rozporządzenie Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych;
17. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych;
18. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji;
19. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych;
20. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji;

Wykaz Polskich Norm związanych z bezpieczeństwem informacji:

1. PN-ISO/IEC 27000:2014 Technika informatyczna -- Techniki bezpieczeństwa -- Systemy zarządzania bezpieczeństwem informacji -- Przegląd i terminologia;
2. PN-ISO/IEC 27001:2014 Technika informatyczna -- Techniki bezpieczeństwa -- Systemy zarządzania bezpieczeństwem informacji – Wymagania;
3. PN-ISO/IEC 27002:2014 Technika informatyczna -- Techniki bezpieczeństwa -- Praktyczne zasady zabezpieczania informacji;
4. PN-ISO/IEC 27005:2014 Technika informatyczna -- Techniki bezpieczeństwa -- Zarządzanie ryzykiem w bezpieczeństwie informacji;

Inne dokumenty związane z bezpieczeństwem informacji, w szczególności:

1. Statut Województwa Pomorskiego;
2. Strategia Rozwoju Województwa Pomorskiego,
3. Regulamin Organizacyjny UMWP;
4. Regulamin Pracy UMWP;
5. Zarządzenie Marszałka Województwa Pomorskiego w sprawie wprowadzenia procedury naboru pracowników UMWP;
6. Zarządzenie Marszałka Województwa Pomorskiego w sprawie sposobu przeprowadzania służby przygotowawczej i organizowania egzaminu kończącego tę służbę;
7. Zarządzenie Marszałka Województwa Pomorskiego w sprawie "Instrukcji postępowania z dokumentami w systemie elektronicznego obiegu dokumentów" w Urzędzie Marszałkowskim Województwa Pomorskiego;
8. Zarządzenie Marszałka Województwa Pomorskiego w sprawie opisu systemu kontroli zarządczej funkcjonującej w Urzędzie Marszałkowskim Województwa;
9. Zarządzenie Marszałka Województwa Pomorskiego w sprawie opisu systemu kontroli zarządczej funkcjonującej w Urzędzie Marszałkowskim Województwa Pomorskiego w zakresie audytu wewnętrznego;
10. Zarządzeniu Marszałka Województwa Pomorskiego w sprawie utworzenia stałych dyżurów w Samorządzie Województwa Pomorskiego;
11. Zarządzeniu Marszałka Województwa Pomorskiego w sprawie wyznaczenia osób do zadań w zakresie zwalczania pożarów i ewakuacji osób;
12. Zarządzeniu Marszałka Województwa Pomorskiego w sprawie sposobu planowania i realizacji zadań w sytuacjach kryzysowych przez komórki organizacyjne UMWP i wyznaczone wojewódzkie samorządowe jednostki organizacyjne;
13. Instrukcje bhp, p.poż.