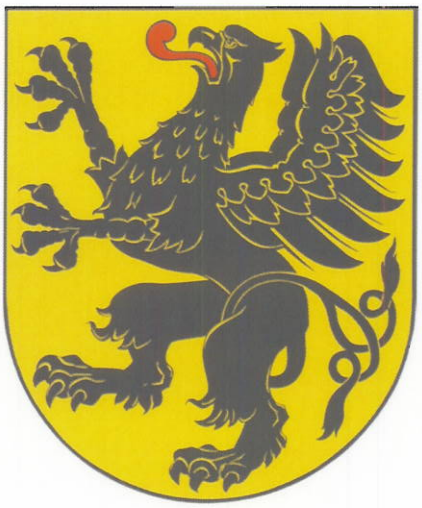
Marszałek Województwa
Mieczysław Struk

Załącznik nr 1
do Zarządzenia Nr 35/19 z dnia 12 sierpnia 2019 roku
zmieniające zarządzenie nr 35/17 z dnia 18 października 2017 roku
w sprawie zatwierdzenia dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Marszałkowskim Województwa Pomorskiego

POLITYKA BEZPIECZEŃSTWA INFORMACJI URZĘDU MARSZAŁKOWSKIEGO WOJEWÓDZTWA POMORSKIEGO – DOKUMENT GŁÓWNY



Numer referencyjny dokumentu: 1.1

ARKUSZ UZGODNIEŃ

Uzgodnienia:	Data:	Podpis i pieczęć:
Anna Szekalska Zastępca Sekretarza Województwa – Zastępca Dyrektora Generalnego Urzędu Marszałkowskiego	07.08.2019	ZASTĘPCA SEKRETARZA WOJEWÓDZTWA ZASTĘPCA DYREKTORA GENERALNEGO URZĘDU Anna Szekalska
Zbigniew Bonarski Dyrektor Departamentu Zamówień Publicznych i Administracji	12.08.2019	DYREKTOR DEPARTAMENTU ZAMÓWIEŃ PUBLICZNYCH I ADMINISTRACJI Zbigniew Bonarski
Michał Potocki Zastępca Dyrektora Departamentu Cyfryzacji	07.08.2019	Z-CA DYREKTORA Departamentu Cyfryzacji Michał Potocki
Anna Drewnowska Dyrektor Departamentu Organizacji	05.08.2019	DYREKTOR DEPARTAMENTU ORGANIZACJI Anna Drewnowska
Małgorzata Falińska Inspektor Ochrony Danych	05.08.2019 r.	Inspektor Ochrony Danych Małgorzata Falińska
Zatwierdzenie:	**Data:**	**Podpis i pieczęć:**
Mieczysław Struk **Marszałek Województwa Pomorskiego**	12.08.2019 r.	Marszałek Województwa Mieczysław Struk

WYKAZ ZMIAN

Lp.	Data	Imię i nazwisko	Wersja	Opis i referencja do poprzedniej wersji
1.	07.07.2006	Tomasz Dmitruk	1.0	Opracowanie dokumentu
2.	10.10.2006	Tomasz Dmitruk	2.0	Aktualizacja dokumentu
3.	16.05.2008	Grażyna Kawczyńska Michał Potocki	3.0	Aktualizacja dokumentu
4.	09.07.2008	Grażyna Kawczyńska Michał Potocki	4.0	Aktualizacja dokumentu
5.	09.09.2008	Grażyna Kawczyńska Michał Potocki	5.0	Aktualizacja dokumentu
6.	08.10.2008	Grażyna Kawczyńska Michał Potocki	6.0	Aktualizacja dokumentu
7.	05.05.2009	Grażyna Kawczyńska Michał Potocki	7.0	Aktualizacja dokumentu
8.	24.11.2009	Grażyna Kawczyńska Michał Potocki	8.0	Aktualizacja dokumentu
9.	25.05.2010	Wojciech Piasecki	9.0	Aktualizacja dokumentu
10	28-02-2011	Wojciech Piasecki	10.0	Aktualizacja dokumentu
11	03-10-2011	Wojciech Piasecki	11.0	Aktualizacja dokumentu
12	10-04-2012	Wojciech Piasecki	11.0	Aktualizacja dokumentu
13	19-03-2014	Grażyna Kawczyńska Michał Potocki Wojciech Piasecki	12.0	Nowe opracowanie dokumentu
14	31-07-2014	Grażyna Kawczyńska Wojciech Piasecki	12.1	Aktualizacja dokumentu
15	31-07-2015	Grażyna Kawczyńska Michał Potocki	13.0	Dostosowanie do wymogów audytu wewnętrznego, do zmian do UODO obowiązujących od 1 stycznia 2015 roku z powołanym ABI, polskiej normy PN-ISO/IEC 27002:2014, Zalecenia CM/REC (2015) 5 Komitetu Ministrów dla Państw Członkowskich na temat ochrony danych osobowych wykorzystywanych dla celów zatrudnienia
16	18-10-2017	Zespół ds. Bezpieczeństwa Informacji	14.0	Dostosowanie do wyników audytu bezpieczeństwa przy wdrażaniu Regionalnego Programu Operacyjnego Województwa Pomorskiego w perspektywie 2014-2020, audytu wewnętrznego oraz

				aktualizacja dokumentu polityki bezpieczeństwa informacji w zakresie zapewnienia zgodności ww. dokumentu z aktualnymi aktami prawa powszechnie obowiązującego oraz najnowszymi normami bezpieczeństwa, w tym normami z rodziny ISO 27000.
17	25.05.2018	Zespół ds. Bezpieczeństwa Informacji	15.0	Dostosowanie do wymogów RODO, przepisów prawa powszechnie obowiązującego oraz aktualnych potrzeb i struktury organizacyjnej Urzędu. Aktualizacja dokumentacji i uzupełnienie o dodatkowe treści, pod kątem przydatności i adekwatności. Aktualizacja wzorów raportów i sprawozdań w celu pełnego odzwierciedlenia wyników monitorowania i doskonalenia SZBI. Usunięcie nieaktualnych/powtarzających się treści, redakcja i korekta pod względem językowym i stylistycznym celem zapewnienie większej przejrzystości tekstu.
	08.2019	Zespół ds. Bezpieczeństwa Informacji	16.0	Dostosowanie do zmieniających się przepisów prawa, aktualnych potrzeb i struktury organizacyjnej Urzędu, wyników monitorowania i w celu doskonalenia ustanowionego SZBI. Uzupełnienie treści, pod kątem przydatności i adekwatności. Usunięcie nieaktualnych/powtarzających się treści, redakcja i korekta pod względem językowym i stylistycznym

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 Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Marszałkowskim Województwa Pomorskiego.
2. Dokument ma charakter deklaratywny, zawiera ogólne ramy, wymagania, zasady, procedury i instrukcje ochrony informacji przetwarzanych w UMWP oraz nadrzędny w stosunku do pozostałych wewnętrznych aktów prawnych dotyczących bezpieczeństwa informacji, tworząc wspólnie z nimi kompleksową *dokumentację bezpieczeństwa (dokumentację Systemu Zarządzania Bezpieczeństwem Informacji w UMWP)*.
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 główny* 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*, stanowiącej załącznik nr 16 do niniejszej Polityki.

§ 3

CELE BEZPIECZEŃSTWA INFORMACJI

1. W Urzędzie Marszałkowskim Województwa Pomorskiego ustanawia się spójne, uwzględniające obowiązujące przepisy i wymagania w zakresie bezpieczeństwa informacji oraz wyniki szacowania ryzyka cele bezpieczeństwa informacji.
2. Ustanowione cele bezpieczeństwa wspierają realizację celów ustawowych oraz strategicznych UMWP, zadań wykonywanych przez pracowników Urzędu, 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. Główne cele bezpieczeństwa informacji obejmują:
   1) zapewnienie bezpieczeństwa aktywów informacyjnych UMWP (w tym ochronę wizerunku i współpracy 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 potrzeb,
   3) minimalizację ryzyka i ograniczanie potencjalnych skutków utraty bezpieczeństwa informacji,
   4) stałe podnoszenie świadomości w zakresie bezpieczeństwa informacji.
4. W ramach realizacji ww. celów, adekwatnie do poziomu zidentyfikowanych zagrożeń podejmowane są działania w kierunku utrzymania poziomu organizacyjnego i technicznego Urzędu, który w szczególności zapewnia:
   1) zachowanie poufności przetwarzanych informacji,
   2) ich integralność oraz dostępność,
   3) uwzględnienie dodatkowych atrybutów bezpieczeństwa zgodnie z wymaganiami i decyzjami oraz gwarancję bezpiecznego przetwarzania, w tym zdolność do realizacji działań w sytuacjach kryzysowych,
   4) udokumentowane informacje w zakresie stopnia realizacji celów bezpieczeństwa informacji.
5. Okresowa ocena stopnia realizacji wyznaczonych celów bezpieczeństwa informacji prowadzona jest w trybie i na zasadach określonych w *Polityce 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. Główne kierunki działania UMWP określa okresowo przyjmowana na kolejne lata *Strategia Rozwoju Województwa Pomorskiego*.
5. Urząd działa w oparciu o przepisy *ustawy o samorządzie województwa*, na podstawie *Statutu Województwa* oraz innych aktów prawnych regulujących zakres i obszar jego funkcjonowania.
6. Sposób realizacji ww. zadań oraz wewnętrzne zasady funkcjonowania UMWP określa *Regulamin Organizacyjny* przyjęty uchwałą Zarządu Województwa, określający strukturę organizacyjną Urzędu, jak i zasady oraz zakres zadań dla poszczególnych komórek organizacyjnych.
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 realizuje swoje zadania z uwzględnieniem określonych uwarunkowań zewnętrznych oraz 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 odpowiedzialność,

2) strategie, główne cele i kierunki działania i rozwoju, zapisy wewnętrznych aktów prawnych (w tym dokumentacji bezpieczeństwa),

3) charakter wykonywanych zadań i realizowanych procesów,

4) zasoby wykorzystywane do skutecznej realizacji powierzonych zadań (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 poddawany jest analizie i ocenie oraz aktualizacji w ramach systemu kontroli zarządczej, w tym prowadzonego monitorowania i doskonalenia SZBI.

§ 5

ZAKRES SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

1. Zakres ustanowionego SZBI obejmuje:

   1) realizowane w UMWP procesy związane z przetwarzaniem informacji,

   2) wszelkie informacje przetwarzane w ramach ww. procesów, w tym:

      a) przetwarzane w formie tradycyjnej (wydrukowane lub zapisane na papierze),

      b) przetwarzane w formie elektronicznej (np. w systemie informatycznym/aplikacjach, przesyłane za pośrednictwem poczty elektronicznej lub urządzeń elektronicznych),

      c) wypowiadane słownie,

   będące własnością UMWP lub stron zainteresowanych, o ile zostały przekazane na podstawie obowiązujących przepisów lub umów.

   3) aktywa wspierające przetwarzanie informacji w ramach ww. procesów m.in.:

      a) personel (w tym wszystkich pracowników UMWP bez względu na podstawę zatrudnienia, praktykantów, stażystów, wolontariuszy),

      b) budynki i pomieszczenia Urzędu,

      c) sprzęt, w tym sprzęt komputerowy, urządzenia mobilne oraz inne nośniki danych,

      d) oprogramowanie, infrastrukturę sieciową oraz technologie służące pozyskiwaniu, selekcjonowaniu, analizowaniu, przetwarzaniu, zarządzaniu i udostępnianiu informacji,

      e) strukturę organizacyjną (w tym komórki organizacyjne wskazane w *Regulaminie Organizacyjnym*).

2. Z uwagi na szczególny charakter 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 skutecznego zabezpieczenia aktywów informacyjnych UMWP, 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 chronionych odbywa się wyłącznie w bezpiecznych środowiskach, tj. w zabezpieczonych 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 musi być dostosowywany do zmieniających się warunków w oparciu o wyniki prowadzonego monitorowania i nadzoru nad bezpieczeństwem informacji,

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”** – dostęp i dalsze korzystanie z aktywów informacyjnych Urzędu odbywać się może tylko w oparciu o formalnie przyznane uprawnienia,

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

2. Dodatkowe zasady bezpieczeństwa mogą zostać ustanowione 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 ww. 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 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) koordynuje działania związane z eksploatacją, monitorowaniem, przeglądaniem, utrzymywaniem i doskonaleniem ustanowionego Systemu.

6. Departament Organizacji (DO) współrealizuje w ramach Zespołu ds. Bezpieczeństwa Informacji ze wszystkimi komórkami organizacyjnymi urzędu działania związane z Systemem Zarządzania Bezpieczeństwem Informacji opracowanym na podstawie Polskiej Normy PN-ISO/IEC 27001, w szczególności w zakresie bezpieczeństwa zasobów ludzkich, zarządzania ryzykiem, obsługi ewidencji zdarzeń związanych z bezpieczeństwem informacji oraz ciągłości działania.

7. Departament Cyfryzacji (DC) współrealizuje w ramach Zespołu ds. Bezpieczeństwa Informacji ze wszystkimi komórkami organizacyjnymi urzędu działania związane z Systemem Zarządzania Bezpieczeństwem Informacji opracowanym na podstawie Polskiej Normy PN-ISO/IEC 27001, w szczególności w zakresie bezpieczeństwa teleinformatycznego, kontroli dostępu logicznego oraz ciągłości działania.
8. Departament Zamówień Publicznych i Administracji (DAZ) współrealizuje w ramach Zespołu ds. Bezpieczeństwa Informacji ze wszystkimi komórkami organizacyjnymi urzędu działania związane z Systemem Zarządzania Bezpieczeństwem Informacji opracowanym na podstawie Polskiej Normy PN-ISO/IEC 27001, w szczególności w zakresie bezpieczeństwa fizycznego i środowiskowego, kontroli dostępu fizycznego oraz ciągłości działania.
9. Kluczowe role i odpowiedzialność w zakresie bezpieczeństwa informacji zostały przypisane do osób funkcyjnych w Urzędzie, w szczególności do:
   1) Administratora Informacji (AI), tj. Marszałka Województwa Pomorskiego,
   2) Administratora Danych (AD),
   3) Przewodniczącego Zespołu ds. bezpieczeństwa informacji, tj. Koordynatora Kontroli Zarządczej,
   4) Administratorów Zarządzających (AZ),
   5) Generalnego Administratora Systemu Informatycznego (GASI),
   6) Inspektora Ochrony Danych (IOD).
10. W celu rozdzielenia funkcji zarządczych i kontrolnych od funkcji wykonawczych, przedmiotowe role i odpowiedzialność zostały ustanowione w dwóch pionach:
    1) w pionie administrowania, odpowiedzialnym za utrzymanie, bieżące zarządzanie i eksploatację SZBI,
    2) w pionie bezpieczeństwa, odpowiedzialnym za nadzór, monitorowanie i ciągłe doskonalenie SZBI.
11. Szczegółowy opis kluczowych ról i odpowiedzialności w obszarze bezpieczeństwa informacji stanowi załącznik nr 3 do niniejszej *Polityki*.

§ 8

KLASYFIKACJA PRZETWARZANYCH INFORMACJI

1. W ramach SZBI, przetwarzane informacje 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 dostępu do 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 ich przetwarzanie w Urzędzie:
   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 tworzących *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.

b) *Politykę bezpieczeństwa w relacjach z podmiotami zewnętrznymi*.

2) W ramach II poziomu SZBI (dokumenty 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 dokumentów I poziomu SZBI,

b) określające specyficzne wymogi i zasady 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 zarządzania incydentami związanymi z bezpieczeństwem informacji,
- polityka monitorowania i nadzoru nad bezpieczeństwem informacji,

c) wprowadzone i aktualizowane w formie załączników do *Polityki Bezpieczeństwa Informacji Urzędu Marszałkowskiego Województwa Pomorskiego – dokument główny* i/lub na mocy odrębnych zarządzeń Marszałka Województwa Pomorskiego.

3) W ramach III poziomu SZBI (dokumenty 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 z podmiotami zewnętrznymi.

2. Dokumenty opracowywane na poszczególnych poziomach SZBI uzupełniają się wzajemnie, tworząc kompleksową *dokumentację bezpieczeństwa (dokumentację Systemu Zarządzania Bezpieczeństwem Informacji w UMWP)*:

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 *dokumentacji bezpieczeństwa*. Zasady oraz tryb prowadzenia przeglądów *dokumentacji bezpieczeństwa* uregulowano w *Polityce monitorowania i nadzoru nad bezpieczeństwem informacji*.

§ 10

KONTROLA DOSTĘPU DO INFORMACJI

1. W ramach zarządzania dostępem do aktywów informacyjnych UMWP, w tym dostępu do budynków i pomieszczeń, sprzętu i urządzeń oraz systemów informatycznym i aplikacji, prowadzona jest kontrola dostępu fizycznego i logicznego.

2. Szczegółowe zasady zarządzania dostępem 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 wysokiego poziomu bezpieczeństwa aktywów informacyjnych, przedmiotowe aktywa są inwentaryzowane, klasyfikowane i eksploatowane zgodnie z obowiązującymi wymaganiami w zakresie ich ochrony.

2. Szczegółowe zasady dot. ochrony aktywów informacyjnych 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 regularnych działań w obszarze zarządzania ryzykiem, w szczególności w zakresie szacowania tj. identyfikowania, analizy i oceny ryzyka w bezpieczeństwie informacji,

2. Działania związane z zarządzaniem ryzykiem w bezpieczeństwie informacji obejmują w szczególności:

   1) przygotowanie oraz okresową aktualizację dokumentów,

   2) prowadzenie okresowego szacowania ryzyka,

   3) postępowanie z ryzykiem nieakceptowalnym,

   4) podejmowanie działań zmierzających do ograniczenia oraz eliminacji przedmiotowego ryzyka.

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 bezpieczeństwa 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 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 stosuje się dedykowane mechanizmy ochrony fizycznej i środowiskowej.
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 obowiązków oraz wypełniają je w odpowiedni sposób i z uwzględnieniem interesów UMWP, podejmowane są określone działania w obszarze bezpieczeństwa zasobów ludzkich, związane w szczególności z:
   1) zapewnieniem wykwalifikowanych pracowników i/lub innych osób oraz podmiotów zewnętrznych do realizacji zadań,
   2) uwzględnieniem odpowiednich zapisów dot. odpowiedzialności w zakresie bezpieczeństwa informacji w umowach zawieranych z ww. osobami i podmiotami,
   3) szkoleniem ww. osób i podmiotów w zakresie bezpieczeństwa informacji oraz regularnym informowaniu 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 Urzędu udostępnianych usługodawcom, dostawcom oraz innym osobom i podmiotom zewnętrznym wykonującym czynności w imieniu i na rzecz UMWP, zasady i wymogi bezpiecznej współpracy zostały uregulowane w *Polityce bezpieczeństwa w relacjach z podmiotami zewnętrznymi* stanowiącej załącznik nr 14 do niniejszej *Polityki*.
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.

§ 18

ZGODNOŚĆ Z PRZEPISAMI PRAWA I ZAPISAMI UMOWNYMI

1. W celu uniknięcia naruszenia obowiązujących przepisów prawa, zobowiązań ustawowych, zapisów zawartych umów i porozumień, prowadzona jest bieżąca kontrola zgodności, w tym identyfikowanie, dokumentowanie i aktualizacja wszystkich istotnych wymagań prawnych, regulacyjnych, umownych oraz podejścia Urzędu do ich przestrzegania.
2. Przedmiotowa kontrola dotyczy również kontroli zgodności z wymaganiami związanymi z prawami własności intelektualnej i użytkowaniem prawnie zastrzeżonego oprogramowania.
3. Kierownicy komórek organizacyjnych, w zakresie określonym w *Regulaminie Organizacyjnym* prowadzą bieżący nadzór zgodności z przepisami prawa i zapisami umownymi.
4. Inspektor Ochrony Danych w UMWP informuje, doradza oraz monitoruje zgodność przetwarzania danych osobowych w UMWP 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.*
6. Departament Kontroli i Audytu Wewnętrznego zapewnia okresowy audyt wewnętrzny w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.
7. *Dokumentacja bezpieczeństwa (Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w UMWP)* jest zgodna z obowiązującymi przepisami prawa oraz wybranymi standardami międzynarodowymi dot. bezpieczeństwa informacji, w szczególności 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 ma obowiązek informowania podmiotów odpowiedzialnych za ich bezpieczeństwo w Urzędzie o podejrzeniu/każdym zidentyfikowanym przypadku naruszenia bezpieczeństwa.
3. Nieprzestrzeganie zasad zawartych w *dokumentacji bezpieczeństwa (dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji w UMWP)* stanowi naruszenie obowiązków pracowniczych i może skutkować sankcjami natury dyscyplinarnej.
4. Naruszenie postanowień dokumentacji bezpieczeństwa 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 tym dot. przetwarzania danych osobowych), grożą odrębne kary określone w szczególności w:
   1) kodeksie pracy,
   2) kodeksie cywilnym,
   3) kodeksie karnym,
   4) RODO oraz w ustawie o ochronie danych osobowych.
6. Osoby bądź podmioty zewnętrzne, niezwiązane bezpośrednio 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, 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 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 SZBI.
5. Szczegółowe zasady dot. monitorowania i doskonalenia SZBI zostały określone w *Polityce monitorowania i nadzoru nad bezpieczeństwem informacji.* .

§ 22

INFORMOWANIE O TREŚCI DOKUMENTACJI BEZPIECZEŃSTWA

1. Niniejszy dokument *Polityki* wraz z załącznikami nr 1, 2 i 14 mają charakter jawny i są ogólnodostępne.
2. Załączniki nr 3-13 oraz 15-16 do niniejszej *Polityki*, 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 na zasadzie „wiedzy uzasadnionej" w zakresie, pozwalającym na realizację powierzonych zadań wybranym pracownikom/innym osobom i podmiotom zewnętrznym.

§ 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*
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 związane z przetwarzaniem informacji, informacje przetwarzane w dowolnej formie, w tym papierowej i elektronicznej w ramach ww. procesów oraz aktywa wspierające przedmiotowej 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 1, ul. Augustyńskiego 2, ul. Rzeźnicka 54/56, ul. Równa 19/21 oraz w Słupsku, ul. Jaracza 18a *(definicja własna);*
Dane osobowe	wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej (*Rozporządzenie 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* (RODO) *ogólne rozporządzenie o ochronie danych);*
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 (dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w UMWP)	Zespół powiązanych ze sobą spójnych dokumentów określających zasady i sposoby zarządzania bezpieczeństwem informacji oraz aktywów wspierających przetwarzanie informacji w UMWP *(definicja własna);*

Pojęcie	Definicja
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);*
Działania naprawcze	Działanie podejmowane w celu wyeliminowania określonego stanu rzeczy i przywrócenia stanu pożądanego *(definicja własna);*
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);*
Informacje objęte tajemnicą przedsiębiorstwa	Informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, które jako całość lub w szczególnym zestawieniu i zbiorze ich elementów nie są powszechnie znane osobom zwykle zajmującym się tym rodzajem informacji albo nie są łatwo dostępne dla takich osób, o ile uprawniony do korzystania z informacji lub rozporządzania nimi podjął, przy zachowaniu należytej staranności, działania w celu utrzymania ich w poufności *(ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji);*
Informacje objęte tajemnicą przedsiębiorcy	Informacje znane jedynie określonemu kręgowi osób i związane są z prowadzoną przez przedsiębiorcę działalnością (informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub innej informacji posiadającej wartość gospodarczą), wobec których podjął on wystarczające środki ochrony w celu zachowania ich poufności *(definicja własna);*
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);*

Pojęcie	Definicja
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);*
IOD	Inspektor Ochrony Danych;
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., Inspektor Ochrony Danych *(definicja własna w oparciu o Regulamin Organizacyjny UMWP);*
Komórki organizacyjne	Departamenty, samodzielne biura oraz stanowisko ds. bezpieczeństwa, higieny pracy i ppoż., Inspektor Ochrony Danych *(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);*
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);*

Pojęcie	Definicja
Pracownik	Osoba zatrudniona w UMWP na podstawie umowy o pracę, powołania lub wyboru *(Regulamin Pracy UMWP);*
Przetwarzanie informacji	Jakiekolwiek operacje wykonywane na informacjach obejmujące zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie *(definicja własna);*
Prezes UODO	Prezes Urzędu Ochrony Danych Osobowych;
RODO	Rozporządzenie 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);
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);*
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 10 maja 2018 r. o ochronie danych osobowych / aktualnie obowiązująca ustawa o ochronie danych osobowych;

Pojęcie	Definicja
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. Rozporządzenie 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;
2. Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy;
3. Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach;
4. Ustawa z dnia 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych;
5. Ustawa z dnia 29 września 1994 roku o rachunkowości;
6. Ustawa z dnia 6 czerwca 1997 r. - Kodeks karny;
7. Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia;
8. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych;
9. Ustawa z dnia 27 lipca 2001 roku o ochronie baz danych;
10. Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej;
11. Ustawa z dnia 18 lipca 2002 roku o świadczeniu usług drogą elektroniczną;
12. Ustawa z dnia 17 lutego 2005 roku o informatyzacji działalności podmiotów realizujących zadania publiczne;
13. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych;
14. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;
15. Ustawa z dnia 22 listopada 2018 r. o dokumentach publicznych
16. Ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);
17. Ustawa z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych
18. Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego;
19. 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;
20. 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;
21. 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;

Wykaz Polskich Norm związanych z bezpieczeństwem informacji:

1. PN-ISO/IEC 27000 Technika informatyczna -- Techniki bezpieczeństwa -- Systemy zarządzania bezpieczeństwem informacji -- Przegląd i terminologia;
2. PN-ISO/IEC 27001 Technika informatyczna -- Techniki bezpieczeństwa -- Systemy zarządzania bezpieczeństwem informacji – Wymagania;
3. PN-ISO/IEC 27002 Technika informatyczna -- Techniki bezpieczeństwa -- Praktyczne zasady zabezpieczania informacji;
4. PN-ISO/IEC 27005 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 "zasad i trybu wykonywania czynności kancelaryjnych w Urzędzie Marszałkowskim Województwa Pomorskiego" 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. Zarządzenie Marszałka Województwa Pomorskiego w sprawie utworzenia stałych dyżurów w Samorządzie Województwa Pomorskiego;
11. Zarządzenie Marszałka Województwa Pomorskiego w sprawie wyznaczenia osób do zadań w zakresie zwalczania pożarów i ewakuacji osób;
12. Zarządzenie 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.