POLITYKA BEZPIECZEŃSTWA INFORMACJI I CIĄGŁOŚCI DZIAŁANIA URZĘDU MARSZAŁKOWSKIEGO WOJEWÓDZTWA POMORSKIEGO – DOKUMENT GŁÓWNY

Numer referencyjny dokumentu: 1.1

SPIS TREŚCI

§ 1

DEKLARACJA NAJWYŻSZEGO KIEROWNICTWA

W Urzędzie Marszałkowskim Województwa Pomorskiego ustanawia się, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali System Zarządzania Bezpieczeństwem Informacji i Ciągłością Działania (SZBIiCD) zapewniający poufność, dostępność i integralność przetwarzanych informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność oraz utrzymanie ciągłości realizacji kluczowych procesów i zadań.

Wielopoziomowy System Zarządzania Bezpieczeństwem Informacji i Ciągłością Działania, będący częścią całościowego systemu zarządzania Urzędem, został oparty na podejściu wynikającym z ryzyka i odnosi się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji oraz ciągłości działania tj. ochrony informacji w każdym punkcie ich przetwarzania oraz skutecznego zarządzania odtworzeniem kluczowych procesów na zdefiniowanym minimalnym akceptowalnym poziomie przed, w trakcie oraz po wystąpieniu sytuacji kryzysowej.

SZBIiCD w UMWP opracowany został zgodnie z obowiązującymi przepisami prawa, na podstawie Norm ISO 27001 i 22301, a jego wymagania mają charakter zintegrowany z innymi procesami funkcjonującymi w UMWP.

Najwyższe kierownictwo Urzędu deklaruje, w szczególności:

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

Marszałek Województwa Pomorskiego

Mieczysław Struk

§ 2

WPROWADZENIE

1. Niniejsza *Polityka Bezpieczeństwa Informacji i Ciągłości Działania* jest dokumentem głównym ustanowionego w Urzędzie Marszałkowskim Województwa Pomorskiego Systemu Zarządzania Bezpieczeństwem Informacji i Ciągłości Działania (SZBIiCD).
2. Polityka, o której mowa w ust. 1, stanowiąca **dokument I poziomu SZBIiCD**, ma charakter deklaratywny, zawiera ogólne ramy, wymagania, zasady, procedury, instrukcje ochrony przetwarzanych informacji i utrzymania ciągłości realizacji procesów krytycznych w UMWP oraz nadrzędny w stosunku do pozostałych wewnętrznych aktów prawnych dotyczących bezpieczeństwa informacji i ciągłości działania.
3. Dokumenty, o których mowa w ust. 2 tworzą kompleksową dokumentację bezpieczeństwa i ciągłości działania (dokumentację SZBIiCD).
4. *Wykaz skrótów i definicji* stosowanych w obowiązującej dokumentacji bezpieczeństwa i ciągłości działania stanowi załącznik nr 1 do niniejszej *Polityki*.
5. *Podstawowy wykaz aktów prawnych, polskich norm i innych dokumentów związanych z bezpieczeństwem informacji i ciągłością działania* stanowi załącznik nr 2 do niniejszej *Polityki*.
6. *Polityka Bezpieczeństwa Informacji i Ciągłości Działania Urzędu Marszałkowskiego Województwa Pomorskiego - dokument główny* podlega przeglądom pod kątem aktualności, przydatności i adekwatności na zasadach określonych w *Polityce monitorowania i nadzoru nad bezpieczeństwem informacji i ciągłością działania*, stanowiącej załącznik nr 17 do niniejszej *Polityki*.

§ 3

CELE BEZPIECZEŃSTWA INFORMACJI I CIĄGŁOŚCI DZIAŁANIA

1. W Urzędzie Marszałkowskim Województwa Pomorskiego ustanawia się spójne cele bezpieczeństwa informacji i ciągłości działania.
2. Cele, o których mowa w ust. 1 uwzględniają obowiązujące przepisy prawa oraz wyniki prowadzonych w Urzędzie szacowania ryzyka w obszarze bezpieczeństwa informacji i oceny ryzyka utraty ciągłości działania.
3. Ustanowione cele bezpieczeństwa informacji i ciągłości działania wspierają realizację celów ustawowych oraz strategicznych UMWP oraz zadań wykonywanych przez pracowników, 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.
4. 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 pracowników w zakresie bezpieczeństwa informacji.

5. Główne cele ciągłości działania obejmują:

1) zapobieganie niezaplanowanym przerwom w realizacja procesów i zadań Urzędu,

2) utrzymywanie właściwej i niezawodnej infrastruktury technicznej niezbędnej do ich realizacji,

3) monitorowanie i ograniczanie potencjalnych zagrożeń w środowisku pracy, w tym identyfikację i ocenę zdarzeń niepewnych, które mogą mieć wpływ na realizowane przez Urząd zadania,

4) stałe podnoszenie świadomości pracowników w zakresie utrzymania ciągłości działania i ich roli w przypadku wystąpienia sytuacji kryzysowej.

6. W ramach realizacji ww. celów, adekwatnie do poziomu zidentyfikowanych zagrożeń podejmowane są działania w kierunku utrzymania w UMWP poziomu organizacyjnego i technicznego, gwarantującego w szczególności:

1) zachowanie poufności przetwarzanych informacji, ich integralności oraz dostępności,

2) uwzględnienie dodatkowych atrybutów bezpieczeństwa oraz gwarancję bezpiecznego przetwarzania informacji, w tym w sytuacjach kryzysowych,

3) identyfikację i ochronę procesów krytycznych, których przerwanie mogłoby niekorzystnie wpływać na jakość i terminowość realizacji usług oraz prowadzić do utraty zaufania klientów, strat finansowych lub wizerunkowych,

4) ograniczenie ryzyka utraty bezpieczeństwa przetwarzanych informacji, opóźnień lub braku realizacji kluczowych procesów i zadań,

5) podnoszenie kompetencji pracowników oraz uwzględnianie ich roli i zaangażowania w SZBIiCD,

6) potwierdzenie realizacji celów bezpieczeństwa informacji i ciągłości działania w udokumentowanej formie.

7. Okresowa ocena stopnia realizacji wyznaczonych celów bezpieczeństwa informacji i ciągłości działania prowadzona jest w trybie i na zasadach określonych w *Polityce monitorowania i nadzoru nad bezpieczeństwem informacji i ciągłością działania,* stanowiącej załącznik nr 17 do niniejszej *Polityki.*

§ 4

KONTEKST URZĘDU MARSZAŁKOWSKIEGO WOJEWÓDZTWA POMORSKIEGO

1. Urząd Marszałkowski Województwa Pomorskiego w Gdańsku jest wojewódzką samorządową jednostką organizacyjną nieposiadająca osobowości prawnej, przy wsparciu której Marszałek Województwa Pomorskiego i Zarząd Województwa

Pomorskiego (ZWP) wykonują swoje zadania i kompetencje niezastrzeżone na rzecz Sejmiku oraz wojewódzkich samorządowych jednostek organizacyjnych.

2. UMWP zapewnia Sejmikowi, Marszałkowi i pozostałym członkom Zarządu Województwa Pomorskiego pomoc w realizacji zadań, w szczególności:
   1) zadań własnych Województwa,
   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, ZWP.
3. Do zadań Samorządu Województwa leżących w kompetencjach Marszałka i/lub Zarządu Województwa Pomorskiego, realizowanych przy wsparciu UMWP należą m.in. 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 wspiera realizację zadań w zakresie promocji województwa i współpracy zagranicznej, rozwoju regionalnego, a także obronności i bezpieczeństwa publicznego, kontroli zarządczej i audytu wewnętrznego oraz zadań związanych z absorpcją 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, w tym strukturę organizacyjną Urzędu, jak i zasady oraz zakres zadań dla poszczególnych komórek organizacyjnych określa *Regulamin Organizacyjny* przyjęty uchwałą ZWP.
7. Głównymi interesariuszami UMWP (stronami zainteresowanymi) są:
   1) mieszkańcy Województwa Pomorskiego,
   2) pracownicy UMWP,
   3) organy administracji rządowej i samorządowej,
   4) dostawcy usług, kontrahenci i inne osoby oraz podmioty realizujące zadania w imieniu i na rzecz UMWP,
   5) organizacje pozarządowe,
   6) instytucje podległe Samorządowi Województwa Pomorskiego.
8. UMWP realizuje swoje zadania z uwzględnieniem określonych uwarunkowań zewnętrznych oraz wewnętrznych, w których funkcjonuje.
9. W ramach uwarunkowań zewnętrznych, uwzględnia się w szczególności:
   1) obowiązujący porządek prawny i konieczność zapewnienie zgodności z przepisami prawa,

2) uwarunkowania ekonomiczne (w tym wpływy z podatków), technologiczne, naturalne, kulturowe, społeczne, polityczne,

3) relacje i kontakty z zewnętrznymi podmiotami publicznymi i prywatnymi (w tym umowy z kontrahentami i dostawcami),

4) wizerunek Urzędu,

5) inne kluczowe czynniki i trendy zewnętrzne mające wpływ na osiągniecie celów strategicznych Urzędu,

10. W ramach uwarunkowań wewnętrznych, uwzględnia się w szczególności:

1) strukturę organizacyjną Urzędu, podział kompetencji, ustanowione role i odpowiedzialność,

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

3) charakter realizowanych procesów i wykonywanych zadań,

4) zasoby wykorzystywane do skutecznej realizacji powierzonych zadań (m.in. budżet, wiedza, pracownicy, budynki i pomieszczenia Urzędu, systemy informatyczne),

5) relacje wewnętrzne i komunikację wewnątrzurzędową (m.in. przepływ informacji w formie tradycyjnej i za pośrednictwem systemu elektronicznego obiegu dokumentów),

6) przyjęte normy, wytyczne i standardy.

11. Celem ciągłego doskonalenia w obszarze ochrony informacji i utrzymania ciągłości działania oraz zapewnienia skuteczności podejmowanych działań, w oparciu o ww. czynniki i wymagania, zidentyfikowane zostały ryzyka i szanse dla ustanowionego w UMWP SZBIiCD.

12. Szczegółowy wykaz głównych interesariuszy UMWP wraz z opisem wzajemnych potrzeb i oczekiwań oraz lista ryzyk i szans, o których mowa w ust. 11 stanowi załącznik nr 3 do niniejszej *Polityki*

13. Kontekst funkcjonowania UMWP oraz lista zidentyfikowanych ryzyk i szans dla SZBIiCD w Urzędzie poddawane są analizie i ocenie oraz aktualizacji w ramach systemu kontroli zarządczej, w tym prowadzonego monitorowania i doskonalenia SZBIiCD

§ 5

ZAKRES SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI I CIĄGŁOSCIĄ DZIAŁANIA

1. Zakres ustanowionego SZBIiCD obejmuje:

1) realizowane w UMWP procesy związane z przetwarzaniem informacji,

2) wyodrębnione w ramach ww. procesów, procesy krytyczne pod kątem zapewnienia ciągłości ich realizacji,

3) 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.

4) aktywa wspierające przetwarzanie informacji i utrzymanie ciągłości działania 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, zapisy dot. ochrony informacji niejawnych i aktywów wspierających ich przetwarzanie, w tym zarządzania ryzykiem zostały określone w treści odrębnych uregulowań wewnętrznych, m.in. w *Planie ochrony informacji niejawnych w Urzędzie Marszałkowskim Województwa Pomorskiego*.

§ 6

PODSTAWOWE ZASADY BEZPIECZEŃSTWA INFORMACJI I CIĄGŁOŚCI DZIAŁANIA

1. Dążąc do skutecznego zabezpieczenia aktywów informacyjnych UMWP i utrzymania ciągłości realizacji kluczowych procesów i zadań, wprowadza się do stosowania podstawowe zasady bezpieczeństwa informacji i ciągłości działania:

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 niezbędne zapisy dot. bezpieczeństwa informacji oraz utrzymania ciągłości realizacji zadań i świadczonych usług na rzecz UMWP,

4) **zasada „czystego biurka** – opuszczając stanowisko pracy należy usunąć z blatu biurka dokumenty oraz zabezpieczyć pozostałe nośniki i urządzenia mobilne 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 nawet krótkotrwałej nieobecności dostęp do komputera należy skutecznie blokować a po zakończeniu pracy komputer wyłączyć, chyba że musi on pracować w trybie ciągłym,

6) **zasada „doskonalenia SZBIiCD”** - system zarządzania bezpieczeństwem informacji i ciągłością działania musi być dostosowywany do zmieniających się uwarunkowań wewnętrznych i zewnętrznych, w oparciu o wyniki prowadzonego monitorowania i nadzoru,

7) **zasada „najsłabszego ogniwa”** – poziom bezpieczeństwa informacji i ciągłość realizacji kluczowych procesów i zadań determinuje najsłabsze ogniwo (najsłabiej zabezpieczony element) SZBIiCD,

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. 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.

§ 7

ROLE I ODPOWIEDZIALNOŚĆ W ZAKRESIE BEZPIECZEŃSTWA INFORMACJI I CIĄGŁOŚCI DZIAŁANIA

1. W ramach ustanowionego SZBIiCD, role i odpowiedzialność w obszarze bezpieczeństwa informacji i ciągłości działania zostały zidentyfikowane i przypisane.
2. Odpowiedzialność za ochronę przetwarzanych informacji i utrzymanie ciągłości realizacji procesów i zadań ponoszą wszyscy pracownicy UMWP, praktykanci, stażyści, wolontariusze oraz inne osoby i podmioty objęte zakresem ustanowionego SZBIiCD.
3. Przedmiotowa odpowiedzialność polega na przestrzeganiu wymagań prawa powszechnie obowiązującego, zapisów niniejszej *Polityki* oraz pozostałych wymogów wskazanych w dokumentacji bezpieczeństwa i ciągłości działania, w szczególności na:
   1) realizacji przypisanych zadań,
   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 i utratę ciągłości działania.

4. Kierownictwo Urzędu zapewnia zasoby niezbędne do bieżącego funkcjonowania, utrzymania i ciągłego monitorowania oraz doskonalenia SZBIiCD.
5. Zespół ds. bezpieczeństwa informacji pod kierownictwem Przewodniczącego koordynuje działania związane z eksploatacją, monitorowaniem, przeglądaniem, utrzymywaniem i doskonaleniem Systemu Zarządzania Bezpieczeństwem Informacji, stanowiącego integralną część SZBIiCD.
6. Koordynator ds. ciągłości działania i jego Z-ca koordynują działania związane z eksploatacją, monitorowaniem, przeglądaniem, utrzymywaniem i doskonaleniem Systemu Zarządzania Ciągłością Działania, stanowiącego integralną część SZBIiCD.
7. Zespół ds. bezpieczeństwa informacji oraz Koordynator ds. ciągłości działania/jego Z-ca współpracują w zakresie monitorowania i doskonalenia SZBIiCD na zasadach określonych w dokumentacji bezpieczeństwa i ciągłości działania, w szczególności w *Polityce monitorowania i nadzoru nad bezpieczeństwem informacji i ciągłością działania,* stanowiącej załącznik nr 17 do niniejszej *Polityki.*
8. Departament Organizacji (DO) we współpracy z Zespołem ds. bezpieczeństwa informacji, Koordynatorem ds. ciągłości działania/jego Z-cą i pozostałymi komórkami organizacyjnymi UMWP realizuje działania w zakresie zapewnienia bezpieczeństwa zasobów ludzkich, zarządzania ryzykiem, obsługi ewidencji zdarzeń związanych z bezpieczeństwem informacji i ciągłością działania oraz utrzymania ciągłości działania w obszarze osobowym.
9. Departament Cyfryzacji (DC), we współpracy z Zespołem ds. bezpieczeństwa informacji, Koordynatorem ds. ciągłości działania/jego Z-cą i pozostałymi komórkami organizacyjnymi UMWP realizuje działania w zakresie zapewnienia bezpieczeństwa teleinformatycznego, zarzadzania dostępem logicznym oraz utrzymania ciągłości działania systemów, aplikacji i infrastruktury teleinformatycznej.
10. Departament Zamówień Publicznych i Administracji (DAZ) we współpracy z Zespołem ds. bezpieczeństwa informacji, Koordynatorem ds. ciągłości działania/jego Z-cą i pozostałymi komórkami organizacyjnymi UMWP realizuje działania w zakresie zapewnienia bezpieczeństwa fizycznego i środowiskowego, zarządzania dostępem fizycznym oraz utrzymania dostępności budynków i pomieszczeń, łączności, usług komunalnych i technicznych w UMWP.
11. Kancelaria Marszałka Województwa (KMW) koordynuje wszelkie prace w zakresie komunikacji społecznej, komunikacji z mediami, w tym odpowiada za obsługę strony internetowej Województwa Pomorskiego. Publikowanie informacji dot. Urzędu odbywa się przy ścisłej współpracy z KMW.
12. 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).

13. Kluczowe role i odpowiedzialność w zakresie utrzymania ciągłości działania zostały przypisane do osób funkcyjnych w Urzędzie, w szczególności do:

1) Przewodniczącego i członków Sztabu Kryzysowego,

2) Koordynatora ds. ciągłości działania i jego Z-cy,

3) Właścicieli procesów krytycznych,

4) Właścicieli zasobów krytycznych.

14. Szczegółowy opis kluczowych ról i odpowiedzialności w ustanowionym *Systemie* stanowi załącznik nr 4 do niniejszej *Polityki*.

§ 8

KLASYFIKACJA PRZETWARZANYCH INFORMACJI

1. Przetwarzane w ramach SZBIiCD 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, zostały określone w dedykowanych politykach II poziomu SZBIiCD, stanowiących załączniki nr 5 – 8 do niniejszej *Polityki.*

§ 9

STRUKTURA DOKUMENTACJI BEZPIECZEŃSTWA INFORMACJI I CIĄGŁOŚCI DZIAŁANIA

1. W ramach ustanowionego SZBIiCD wprowadza się trójpoziomową dokumentację bezpieczeństwa i ciągłości działania określającą zasady i tryb zarządzania bezpieczeństwem informacji, ich przetwarzaniem oraz utrzymaniem ciągłości działania Urzędu:

1) W ramach I poziomu SZBIiCD (dokumenty o charakterze publicznym, ogólnodostępnym) wyróżnia się:

a) *Politykę Bezpieczeństwa Informacji i Ciągłości Działania Urzędu Marszałkowskiego Województwa Pomorskiego – dokument główny*:

- dokument nadrzędny w stosunku do pozostałych wewnętrznych aktów prawnych tworzących dokumentację bezpieczeństwa i ciągłości działania,

- określającą ogólne ramy, kierunki, zasady i wymogi bezpieczeństwa informacji i ciągłości działania oraz zakres dokumentacji bezpieczeństwa i ciągłości działania 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 SZBIiCD (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 SZBIiCD,
   b) określające specyficzne wymogi i zasady w kluczowych obszarach bezpieczeństwa informacji i utrzymania ciągłości działania:
      - 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,
      - strategia ciągłości działania,
      - polityka zarządzania incydentami związanymi z bezpieczeństwem informacji i utratą ciągłości działania,
      - polityka monitorowania i nadzoru nad bezpieczeństwem informacji i ciągłością działania,
   c) wprowadzone i aktualizowane w formie załączników do *Polityki Bezpieczeństwa Informacji i Ciągłości Działania Urzędu Marszałkowskiego Województwa Pomorskiego – dokument główny* i/lub na mocy odrębnych zarządzeń Marszałka Województwa Pomorskiego.

3) W ramach III poziomu SZBIiCD (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 SZBIiCD 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 SZBIiCD i/lub dokumentów wewnętrznych wybranych

komórek organizacyjnych UMWP, ewentualnie na mocy odrębnych zarządzeń Marszałka Województwa Pomorskiego,

w tym instrukcje/procedury bezpieczeństwa wybranych komórek organizacyjnych w związku z realizacją projektów unijnych (m.in. regionalnych programów operacyjnych), procedury techniczne dot. zarządzania i ochrony infrastruktury IT,

b) szczegółowe procedury i instrukcje utrzymania ciągłości działania, w tym plany ciągłości działania oraz procedury odtworzeniowe dla procesów krytycznych,

c) wyniki monitorowania SZBIiCD,

d) wybrane umowy z podmiotami zewnętrznymi.

2. Dokumenty opracowywane na poszczególnych poziomach SZBIiCD uzupełniają się wzajemnie, tworząc kompleksową dokumentację bezpieczeństwa i ciągłości działania:
   1) dokumentacja I poziomu SZBIiCD ma charakter ogólny, a jej zapisy odwołują się wprost do dedykowanych dokumentów II poziomu, w których są uszczegółowione,
   2) poszczególne dokumenty II poziomu SZBIiCD odwołują się do siebie oraz do procedur i instrukcji III poziomu,
   3) procedury i instrukcje III poziomu SZBIiCD uszczegółowiają zapisy dokumentacji II poziomu.
3. Dopuszcza się opracowywanie dodatkowych dokumentów dot. bezpieczeństwa informacji i ciągłości działania, w tym regulaminów, rekomendacji, zasad, wytycznych.
4. Celem zapewnienia właściwości, adekwatności i skuteczności obowiązujących przepisów wewnętrznych, prowadzone są okresowe przeglądy i aktualizacja dokumentacji bezpieczeństwa i ciągłości działania.

   Zasady oraz tryb prowadzenia przeglądów dokumentacji bezpieczeństwa i ciągłości działania określa *Polityka monitorowania i nadzoru nad bezpieczeństwem informacji i ciągłością działania*, stanowiąca załącznik nr 17 do niniejszej *Polityki*.

§ 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 9 do niniejszej *Polityki* oraz *dedykowanych procedurach III poziomu SZBIiCD*.

§ 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 i utrzymania.

2. Szczegółowe zasady dot. ochrony i utrzymania aktywów informacyjnych zostały uregulowane w *Polityce zarządzania aktywami informacyjnymi*, stanowiącej załącznik nr 10 do niniejszej *Polityki* oraz *dedykowanej Procedurze inwentaryzacji aktywów informacyjnych*.

§ 12

ZARZĄDZANIE RYZYKIEM W BEZPIECZEŃSTWIE INFORMACJI I CIĄGŁOŚCI DZIAŁANIA

1. Skuteczne zarządzanie bezpieczeństwem informacji i ciągłością działania wymaga podejmowania regularnych działań w obszarze zarządzania ryzykiem, w szczególności w zakresie szacowania ryzyka w bezpieczeństwie informacji oraz oceny ryzyka utraty ciągłości działania.
2. Szczegółowe zasady dot. zarządzania ryzykiem w bezpieczeństwie informacji zostały uregulowane w *Polityce zarządzania ryzykiem w bezpieczeństwie informacji*, stanowiącej załącznik nr 11 do niniejszej *Polityki*.
3. Szczegółowe zasady dot. zarządzania ryzykiem utraty ciągłości działania zostały uregulowane w *Strategii ciągłości działania*, stanowiącej załącznik nr 14 do niniejszej *Polityki*.

§ 13

BEZPIECZEŃSTWO TELEINFORMATYCZNE

1. W ramach zarządzania bezpieczeństwem teleinformatycznym podejmowane są działania w zakresie szacowania i kontroli ryzyka utraty bezpieczeństwa informacji i ciągłości działania SI UMWP oraz aplikacji, komputerów i urządzeń mobilnych, sieci komputerowych i transmisji danych.
2. Przedmiotowe działania podejmowane są w szczególności w zakresie, monitorowania i rozwoju oraz doskonalenia infrastruktury teleinformatycznej.
3. Szczegółowe zasady bezpieczeństwa teleinformatycznego zostały uregulowane w *Polityce bezpieczeństwa teleinformatycznego*, stanowiącej załącznik nr 12 do niniejszej *Polityki* oraz *dedykowanych procedurach i instrukcjach III poziomu SZBIiCD*.

§ 14

BEZPIECZEŃSTWO FIZYCZNE I ŚRODOWISKOWE

1. W celu zapobieżenia nieuprawnionemu fizycznemu dostępowi, szkodom i zakłóceniom w przetwarzaniu informacji oraz utracie, zniszczeniu, uszkodzeniu, kradzieży aktywów wspierających to przetwarzanie stosuje się dedykowane mechanizmy ochrony fizycznej i środowiskowej.
2. Szczegółowe zasady dot. zarządzania bezpieczeństwem i ciągłością działania w obszarze fizycznym i środowiskowym zostały uregulowane w *Polityce bezpieczeństwa fizycznego i środowiskowego*, stanowiącej załącznik nr 13 do niniejszej *Polityki* oraz *dedykowanych procedurach i instrukcjach III poziomu SZBIiCD*.

§ 15

BEZPIECZEŃSTWO ZASOBÓW LUDZKICH

1. Celem ograniczenia ryzyka błędu ludzkiego, kradzieży lub nadużycia oraz zapewnienia prawidłowej realizacji powierzonych zadań, podejmowane są określone działania, związane w szczególności z:
   1) zapewnieniem wykwalifikowanych pracowników i/lub innych osób oraz podmiotów zewnętrznych do realizacji tych zadań,
   2) weryfikacją formalną kandydatów do pracy,
   3) uwzględnieniem w umowach zawieranych z ww. osobami i podmiotami, odpowiednich zapisów dot. odpowiedzialności w zakresie bezpieczeństwa informacji i utrzymania ciągłości działania obowiązujących w trakcie jak i po zakończeniu stosunku pracy lub umowy,
   4) szkoleniem ww. osób w zakresie bezpieczeństwa informacji i ciągłości działania oraz regularnym informowaniu o aktualizacji polityk i procedur związanych z ich stanowiskiem pracy.
2. Zasady postępowania rekrutacyjnego, w tym weryfikacji kandydatów na wolne stanowiska, sposób postępowania z dokumentami aplikacyjnymi określa *Zarządzenie Marszałka Województwa Pomorskiego w sprawie wprowadzenia procedury naboru pracowników w UMWP*.
3. Umowy z pracownikami i/lub podmiotami zewnętrznymi określają odpowiedzialność stron w zakresie bezpieczeństwa informacji i ciągłości działania, w szczególności:
   1) obowiązek zachowania poufności i nieujawniania informacji, do których otrzymają dostęp,
   2) prawa i obowiązki pracowników oraz osób i podmiotów zewnętrznych np. w odniesieniu do praw autorskich lub ochrony danych osobowych,
   3) dodatkowe wymogi w zakresie bezpieczeństwa informacji i ciągłości działania, które pozostają wiążące po zakończeniu stosunku pracy lub umowy.
4. W ramach przygotowania pracownika do należytego wykonywania obowiązków służbowych, organizowana jest służba przygotowawcza, obejmująca m.in. szkolenia w zakresie bezpieczeństwa informacji i utrzymania ciągłości działania.

   Szczegółowe zapisy dot. organizacji i przebiegu służby przygotowawczej określa *Zarządzenie Marszałka Województwa Pomorskiego w sprawie sposobu przeprowadzania służby przygotowawczej i organizowania egzaminu kończącego tę służbę*.
5. Szkolenia z zakresu bezpieczeństwa informacji i utrzymania ciągłości działania dla pracowników UMWP odbywają się zgodnie z procedurą szkoleniową określoną w *Zarządzeniu Marszałka Województwa Pomorskiego w sprawie wprowadzenia procedury szkoleniowej dla pracowników UMWP w Gdańsku*.
6. Szkolenia mają charakter powtarzalny, adekwatnie do zidentyfikowanych potrzeb, w formie szkoleń stacjonarnych (nie rzadziej niż raz na 4 lata), jak i poprzez bieżące udostępnianie materiałów szkoleniowych za pośrednictwem pozastacjonarnych kanałów m.in. poczty służbowej, Intranet-u (samokształcenie pracowników UMWP).

§ 16

UTRZYMANIE CIĄGŁOŚCI DZIAŁANIA

1. W UMWP podejmowane są działania w zakresie utrzymania ciągłości realizacji kluczowych procesów i zadań.
2. Szczegółowe zasady dot. zarządzania ciągłością działania zostały uregulowane w *Strategii ciągłości działania*, stanowiącej załącznik nr 14 do niniejszej *Polityki* oraz *dedykowanych procedurach i instrukcjach III poziomu SZBIiCD*.

§ 17

RELACJE Z PODMIOTAMI ZEWNĘTRZNYMI

Wymogi bezpiecznej współpracy, w tym ochrony aktywów informacyjnych Urzędu udostępnianych usługodawcom, dostawcom oraz innym osobom i podmiotom zewnętrznym wykonującym czynności w imieniu i na rzecz UMWP zostały uregulowane w *Polityce bezpieczeństwa w relacjach z podmiotami zewnętrznymi* stanowiącej załącznik nr 15 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, 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 pod kątem praw własności intelektualnej i użytkowania prawnie zastrzeżonego oprogramowania.
3. Kierownicy komórek organizacyjnych, w zakresie określonym w *Regulaminie Organizacyjnym* prowadzą bieżący nadzór nad zgodnością 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 Koordynatorem ds. ciągłości działania/jego Z-cą i kierownikami poszczególnych komórek organizacyjnych UMWP dokonuje okresowych przeglądów regulacji wewnętrznych dotyczących bezpieczeństwa informacji i ciągłości działania w zakresie ich zgodności z przepisami prawa i zapisami umownymi,

   Przeglądy prowadzone są na zasadach i w trybie określonym w *Polityce monitorowania i nadzoru nad bezpieczeństwem informacji i ciągłością działania,* stanowiącej załącznik nr 17 do niniejszej *Polityki.*
6. Departament Kontroli i Audytu Wewnętrznego, nie rzadziej niż raz na rok, zapewnia okresowy audyt wewnętrzny w zakresie bezpieczeństwa informacji oraz w obszarze utrzymania ciągłości działania Urzędu.
7. Dokumentacja bezpieczeństwa i ciągłości działania jest zgodna z obowiązującymi przepisami prawa oraz wybranymi standardami międzynarodowymi, określonymi

m.in. w *Podstawowym wykazie aktów prawnych, polskich norm i innych dokumentów związanych z bezpieczeństwem informacji i ciągłością działania.*

§ 19

NARUSZENIE BEZPIECZEŃSTWA INFORMACJI I CIĄGŁOŚCI DZIAŁANIA

1. Podstawową konsekwencją naruszenia bezpieczeństwa informacji i/lub ciągłości działania jest obniżenie poziomu ochrony przetwarzanych informacji oraz aktywów wspierających ich przetwarzanie w UMWP i/lub przerwanie ciągłości realizacji kluczowych procesów i zadań.
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 i zakłócenia/przerwania ciągłości działania.
3. Nieprzestrzeganie wymogów dokumentacji bezpieczeństwa i ciągłości działania stanowi naruszenie obowiązków pracowniczych i może skutkować sankcjami natury dyscyplinarnej.
4. Naruszenie postanowień ww. dokumentacji 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 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 i/lub ciągłości działania Urzędu na adres incydent@pomorskie.eu.
7. Szczegółowe zasady dot. identyfikowania, zgłaszania, reagowania i obsługi zdarzeń i incydentów związanych z bezpieczeństwem informacji i utratą ciągłości działania zostały uregulowane w *Polityce zarządzania incydentami związanymi z bezpieczeństwem informacji i utratą ciągłości działania*, stanowiącej załącznik nr 16 do niniejszej *Polityki*.

§ 20

DOBÓR ZABEZPIECZEŃ

1. Identyfikacja celów stosowania i dobór zabezpieczeń w SZBIiCD prowadzony jest w oparciu o aktualne wymogi prawa, zalecenia polskich norm z rodziny ISO 27000 oraz normy ISO 22301, wyniki monitorowania *Systemu*, w szczególności wyniki szacowania ryzyka w bezpieczeństwie informacji i oceny ryzyka utraty ciągłości działania.

2. 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 SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI I CIĄGŁOŚCIĄ DZIAŁANIA

1. Działania w zakresie utrzymania, monitorowania i doskonalenia *Systemu* podejmowane są w szczególności w zidentyfikowanych na II poziomie SZBIiCD obszarach bezpieczeństwa i ciągłości działania.
2. Działania, o których mowa w ust. 1 mają charakter bieżący i okresowy.
3. W oparciu o wyniki prowadzonego monitorowania i nadzoru nad bezpieczeństwem informacji i ciągłością działania, 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 SZBIiCD.
5. Szczegółowe zasady dot. monitorowania i doskonalenia SZBIiCD zostały określone w *Polityce monitorowania i nadzoru nad bezpieczeństwem informacji i ciągłością działania,* stanowiącej załącznik nr 17 do niniejszej *Polityki.*

§ 22

INFORMOWANIE O TREŚCI DOKUMENTACJI BEZPIECZEŃSTWA I CIĄGŁOŚCI DZIAŁANIA

1. Niniejszy dokument *Polityki* wraz z załącznikami nr 1, 2 i 15 stanowią dokumentację I poziomu SZBIiCD, mają charakter jawny i są ogólnodostępne.
2. Załączniki nr 3-14 oraz 16-17 do niniejszej *Polityki*, stanowiące dokumentację II poziomu SZBIiCD, 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 SZBIiCD 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 i ciągłością działania
3. Kontekst Urzędu Marszałkowskiego Województwa Pomorskiego
4. Kluczowe role i odpowiedzialność w zakresie bezpieczeństwa informacji i utrzymania ciągłości działania.
5. Polityka bezpieczeństwa danych osobowych

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

WYKAZ SKRÓTÓW I DEFINICJI

Pojęcie	Definicja
Akceptacja ryzyka	Decyzja uprawnionej osoby o zaniechaniu działań mających na celu zmianę poziomu ryzyka;
Aktywa	Wszystko, co ma wartość dla organizacji (UMWP) i z tego powodu wymaga ochrony;
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*;*
Analiza ryzyka	Proces identyfikacji ryzyka, określenia jego wielkości i wyodrębnienia obszarów wymagających zabezpieczeń; Proces dążący do poznania charakteru ryzyka oraz określenia poziomu ryzyka;
Analiza wpływu na biznes (BIA)	Proces analizy wpływu działalności oraz skutków, jakie zakłócenia mogą wywierać na te działalności;
Anonimizacja	To proces polegający na przekształceniu danych osobowych, w sposób uniemożliwiający przyporządkowanie poszczególnych informacji osobistych lub rzeczowych do określonej czy możliwej do zidentyfikowania osoby fizycznej lub w przypadku, kiedy można tego dokonać jedynie niewspółmiernie dużym nakładem czasu, kosztów i sił. Polega na trwałym usunięciu ze wszystkich nośników (papierowych, elektronicznych, systemów informatycznych) wszystkich informacji pozwalających na identyfikację osób fizycznych; Zatem anonimizacja jest procesem nieodwracalnym;
Apetyt na ryzyko	Ważność i rodzaj ryzyka, które organizacja jest skłonna monitorować lub które podlega retencji;
Arkusz BIA	Narzędzie wykorzystywane do przeprowadzenia analizy wpływu na biznes, w którym zostały określone wymagane dane oraz sposób przeprowadzania BIA;
Arkusz RA	Narzędzie wykorzystywane do oceny ryzyka, w którym zostały określone wymagane dane oraz sposób przeprowadzania przedmiotowej oceny;
Atak DDoS	Atak na system komputerowy lub usługę sieciową mający na celu uniemożliwienie działania poprzez wygenerowanie bardzo dużej ilości fałszywych zapytań, skutkujących przeciążaniem serwera, a w konsekwencji brakiem dostępu do systemu/usługi;
Atak socjotechniczny	Oparty o techniki manipulacji atak ukierunkowany na użytkownika, mający na celu skłonić go do określonego działania np. ujawnienia określonych informacji;

Pojęcie	Definicja
Autentyczność	Właściwość, która polega na tym, że podmiot jest tym, za kogo się podaje*;* Właściwość polegająca na tym, że pochodzenie lub zawartość danych opisujących obiekt są takie jak deklarowane*;*
Bezpieczeństwo Informacji	Zachowanie poufności, integralności i dostępności Informacji; Dodatkowo, mogą być brane pod uwagę inne własności, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność;
Budynek	Budynek UMWP położony w Gdańsku pod następującymi adresami: ul. Okopowa 19, ul. Okopowa 21/27, ul. Augustyńskiego 1, ul. Augustyńskiego 2, ul. Rzeźnicka 54/56, ul. Równa 19/21 oraz w Słupsku, ul. Jaracza 18a*;*
Ciągłość działania	Zdolność UMWP do kontynuowania świadczenia usług na akceptowalnych, zdefiniowanych poziomach po wystąpieniu incydentu zakłócającego*;*
Czynność/ proces przetwarzania	Zespół powiązanych ze sobą operacji na danych, wykonywanych przez jedną lub kilka osób, które można określić w sposób zbiorczy, w związku z celem, w jakim te czynności są podejmowane;
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;
Deklaracja stosowania	Dokument określający, które zabezpieczenia zostały wdrożone, jakie są cele stosowania tych zabezpieczeń, wraz z uzasadnieniem ich wyboru/wykluczenia;
Dokumentacja bezpieczeństwa i ciągłości działania (dokumentacja SZBIiCD)	Zespół powiązanych ze sobą spójnych dokumentów określających zasady i sposoby zarządzania bezpieczeństwem informacji i aktywów wspierających przetwarzanie informacji w UMWP oraz utrzymaniem ciągłości działania Urzędu*;*
Dostępność	Właściwość bycia dostępnym i użytecznym na żądanie autoryzowanego podmiotu; Właściwość określająca, że zasób systemu teleinformatycznego jest możliwy do wykorzystania na żądanie, w założonym czasie, przez podmiot uprawniony do pracy w systemie teleinformatycznym*;*
Działania korygujące	Działania mające na celu wyeliminowanie przyczyny określonego stanu rzeczy (niezgodności) i zapobieżenie jego powtórzeniu*;*
Działania naprawcze	Działania podejmowane w celu wyeliminowania określonego stanu rzeczy i przywrócenia stanu pożądanego*;*
Identyfikowanie ryzyka	Proces wyszukiwania, rozpoznawania i opisywania ryzyka;

Pojęcie	Definicja
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*;*
Incydent związany z utratą ciągłości działania	Sytuacja, która może prowadzić do zakłócenia, straty, sytuacji awaryjnej lub kryzysu;
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*;*
Informacje objęte tajemnicą przedsiębiorcy	Informacje znane jedynie określonemu kręgowi osób i związane z prowadzoną przez przedsiębiorcę działalnością (informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą), wobec których podjął on wystarczające środki ochrony w celu zachowania ich poufności*;*
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*;*
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*;*
Informowanie o ryzyku	Wymiana lub dzielenie się informacjami o ryzyku między uczestnikami procesu zarządzania ryzykiem w bezpieczeństwie informacji;
Integralność	Właściwość informacji polegająca na tym, że informacja nie została zmieniona, dodana lub usunięta w nieautoryzowany sposób*;* Właściwość polegająca na zapewnieniu dokładności i kompletności*;* Właściwość polegająca na tym, ze zasób systemu teleinformatycznego nie został zmodyfikowany w sposób nieuprawniony*;*
Interesariusz, Strona zainteresowana	Osoba lub organizacja, która może na decyzję lub działalność wpływać, być nią dotknięta lub dostrzegać jej oddziaływanie na siebie;
IOD	Inspektor Ochrony Danych;
Kategoria incydentu	Rodzaj zidentyfikowanego zagrożenia, przypisywany do incydentu zgodnie z załącznikiem nr 3 do *Procedury obsługi i postępowania z incydentami związanymi z bezpieczeństwem informacji i utratą ciągłości działania*;

Pojęcie	Definicja
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*;*
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*;*
Kluczowe aktywa informacyjne	Aktywa informacyjne niezbędne do realizacji procesów krytycznych;
Komórki organizacyjne	Departamenty, samodzielne biura oraz stanowisko ds. bezpieczeństwa, higieny pracy i ppoż., Inspektor Ochrony Danych;
Kryteria ryzyka	Poziomy odniesienia, względem których określa się ważność ryzyka;
Materiał dowodowy	Każda okoliczność, rzecz świadcząca o czymś, potwierdzająca lub wykluczająca określone postępowanie;
MTPD (Maximum Tolerable Period of Disruption)	Maksymalny tolerowany czas zakłócenia, czas, po którym niekorzystne skutki powstałe w wyniku niedostarczenia wyrobu lub usług albo nierealizowania działalności stają się nieakceptowalne;
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*;* Naruszenie lub podejrzenie naruszenia dostępności, poufności i/lub integralności informacji*;*
Naruszenie ochrony danych osobowych	Naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub przetwarzanych w inny sposób;
Naruszenie przepisów o ochronie danych osobowych	Zachowanie naruszające RODO, akty delegowane i wykonawcze przyjęte na mocy RODO lub prawo państwa członkowskiego;
Niezaprzeczalność	Zdolność do udowodnienia, że wystąpiły deklarowane zdarzenia lub działania oraz, że wywołał je dany podmiot*;* Brak możliwości zanegowania swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie*;*
Niezawodność	Właściwość informacji oznaczająca spójne, zamierzone zachowanie i skutki*;*
Niezgodność	Niespełnienie wymagań bezpieczeństwa informacji/utrzymania ciągłości działania*;*
Ocena ryzyka w bezpieczeństwie informacji	Proces porównywania wyników analizy ryzyka z kryteriami ryzyka w celu stwierdzenia, czy ryzyko i/lub jego wielkość są akceptowalne lub tolerowane;

Pojęcie	Definicja
Ocena ryzyka w ciągłości działania	Całościowy proces identyfikacji ryzyka, analizy ryzyka oraz ewaluacji w obszarze ciągłości działania
Oprogramowanie złośliwe	Wszelkie aplikacje, skrypty itp. mające szkodliwe, przestępcze, groźne lub destrukcyjne działanie w stosunku do infrastruktury teleinformatycznej i użytkownika końcowego;
PBI	Polityka Bezpieczeństwa Informacji i Ciągłości Działania Urzędu Marszałkowskiego Województwa Pomorskiego – dokument główny określająca zestaw praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji i informacji oraz utrzymania ciągłości działania w UMWP*;*
Plan ciągłości działania (PCD)	Udokumentowane procedury, które ukierunkowują UMWP jak odpowiednio reagować na zakłócenia oraz wznawiać, odzyskiwać i przywracać usługi zgodnie z celami ciągłości działania;
Podatność	Słabość aktywu (zasobu) lub zabezpieczenia, która może być wykorzystana przez co najmniej jedno zagrożenie;
Postępowanie z ryzykiem	Proces modyfikowania ryzyka;
Poufność	Właściwość polegająca na tym, że informacja nie jest udostępniana ani ujawniana nieautoryzowanym osobom, podmiotom lub procesom;
Poziom ryzyka	Wielkość ryzyka, wyrażona w postaci kombinacji następstw oraz ich prawdopodobieństwa;
Pracownik	Osoba zatrudniona w UMWP na podstawie umowy o pracę, powołania lub wyboru;
Prawdopodobieństwo	Możliwość, szansa wystąpienia zdarzenia;
Prezes UODO	Prezes Urzędu Ochrony Danych Osobowych;
Priorytet incydentu	Krytyczność/pilność obsługi incydentu, określana w oparciu o analizę potencjalnych skutków incydentu i częstotliwości występowania danego typu incydentu w przeszłości, determinująca max. czas reakcji po powzięciu informacji o incydencie, zgodnie z załącznikiem nr 1 do *Procedury obsługi i postępowania z incydentami związanymi z bezpieczeństwem informacji i utratą ciągłości działania;*
Proces	Zbiór powiązanych ze sobą lub wzajemnie oddziałujących działań, które przekształcają dane wejściowe na dane wyjściowe;
Proces krytyczny	Każdy proces podstawowy dla którego MTPD <= 2 tygodnie oraz proces, bez którego proces krytyczny nie może działać (czyli proces wspierający, który powoduje zatrzymanie procesu krytycznego w takim samym czasie).
Proces podstawowy	Proces związany z przetwarzaniem informacji w ramach realizacji zadań merytorycznych w danej komórce organizacyjnej, identyfikowany i aktualizowany podczas okresowej inwentaryzacji aktywów informacyjnych za pośrednictwem dedykowanego narzędzia

Pojęcie	Definicja
Przetwarzanie danych osobowych	Operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, tj. 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;
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*;*
Pseudonimizacja	Przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej; W założeniu proces pseudonimizacji powinien być odwracalny;
RODO	Rozporządzenie 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 (Dz.U. UE. L Nr 119, s.1);
Rozliczalność	Właściwość informacji, polegająca na tym, że określone działanie dowolnego podmiotu może być jednoznacznie przypisane temu podmiotowi; Właściwość systemu pozwalająca przypisać określone działanie w systemie do osoby fizycznej lub procesu oraz umiejscowić je w czasie;
RPO	Docelowy punkt odtworzenia danych, punkt w czasie, z którego informacja używana przez konkretną działalność musi być przywrócona, aby umożliwić tej działalności wznowienie funkcjonowania;
RTO (Recovery Time Objective)	Docelowy czas wznowienia działalności, okres następujący po incydencie, w czasie którego wyrób lub usługa musi zostać ponownie dostarczona lub działalność musi zostać wznowiona, lub zasoby muszą być odtworzone;
Ryzyko	Wpływ niepewności na cele; Prawdopodobieństwo wykorzystania podatności przez zagrożenie i spowodowania szkody dla organizacji;
Ryzyko szczątkowe	Ryzyko pozostające po zastosowaniu działań określonych w postępowaniu z ryzykiem;
SI UMWP	System informatyczny UMWP
Skutek/następstwo	Rezultat zdarzenia mający wpływ na cele; negatywna zmiana w wyniku oddziaływania zagrożenia;

Pojęcie	Definicja
System informacyjny	Uporządkowany układ odpowiednich elementów, charakteryzujących się pewnymi właściwościami i połączonych wzajemnie określonymi relacjami*;* Aplikacje, usługi, aktywa technik informacyjnych lub inne komponenty przetwarzające informacje*;*
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*);*
System zarządzania bezpieczeństwem informacji (SZBI)	Część zintegrowanego systemu zarządzania bezpieczeństwem informacji i ciągłością działania (SZBIiCD), która dotyczy ustanowienia, wdrażania, funkcjonowania, monitorowania, przeglądu, utrzymania i ciągłego doskonalenia bezpieczeństwa informacji w Urzędzie;
System zarządzania bezpieczeństwem informacji i ciągłością działania (SZBIiCD)	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 i ciągłości działania;
System zarządzania ciągłością działania (SZCD)	Część zintegrowanego systemu zarządzania bezpieczeństwem informacji i ciągłością działania (SZBIiCD), która dotyczy ustanowienia, wdrażania, funkcjonowania, monitorowania, przeglądu, utrzymania i ciągłego doskonalenia ciągłości działania Urzędu;
Sytuacja kryzysowa (kryzys)	Nieplanowane zdarzenie lub seria zdarzeń, będąca następstwem materializacji zagrożenia lub incydentów, której wystąpienie ma negatywny wpływ życie lub zdrowie ludzkie, realizację kluczowych procesów w UMWP lub wizerunek Urzędu; Sytuacja wpływająca negatywnie na poziom bezpieczeństwa ludzi, mienia w znacznych rozmiarach, wywołująca poważne ograniczenia w działaniu UMWP z uwagi na nieadekwatność posiadanych sił i środków;
Szacowanie ryzyka	Całościowy proces identyfikowania ryzyka, analizy ryzyka i oceny ryzyka w bezpieczeństwie informacji;
Środek przetwarzania informacji	Każdy system przetwarzania informacji, usługa lub infrastruktura albo ich fizyczna lokalizacja;
Świadczenie usług drogą elektroniczną	Wykonanie usługi świadczonej bez jednoczesnej obecności stron (na odległość), poprzez przekaz danych na indywidualne żądanie usługobiorcy, przesyłanej i otrzymywanej za pomocą urządzeń do elektronicznego przetwarzania, włącznie z kompresją cyfrową, i przechowywania danych, która jest w całości nadawana, odbierana lub transmitowana za pomocą sieci telekomunikacyjnej w rozumieniu ustawy – Prawo telekomunikacyjne;
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*;*
Użytkownik	Każdy, kto posiada upoważnienie do korzystania z systemu informatycznego i dzięki określonym uprawnieniom uczestniczy w przetwarzaniu Informacji*;*
Właściciel aktywa	Kierownik komórki organizacyjnej UMWP i inne osoby odpowiedzialne za zarządzanie aktywami informacyjnymi, ich bieżącą eksploatacją, rozwój, utrzymanie oraz ochronę. Właściciel aktywa może nie dysponować rzeczywistym prawem własności aktywów;
Właściciel ryzyka	Właściciel aktywa/aktywów odpowiedzialny za zarządzanie, monitorowanie i kontrolowanie wszystkich aspektów przypisanego ryzyka związanego z zarządzaniem danym aktywem/grupą aktywów, który jest władny do podejmowania wiążących decyzji w celu zapewnienia bezpieczeństwa ww. aktywa/aktywów;
Właściciel zasobu krytycznego	Osoba kierującą pracą komórki organizacyjnej Urzędu, odpowiedzialną za wskazane w Analizie wpływu na biznes (BIA) zasoby niezbędne do realizacji poszczególnych procesów krytycznych tj.: Dyrektor DO lub jego Z-ca w obszarze osobowym i organizacyjnym, Dyrektor DAZ lub jego Z-ca w obszarze fizycznym i środowiskowym, Dyrektor DC lub jego Z-ca w obszarze infrastruktury teleinformatycznej;
Wpływ	Wynik zakłóceń mający wpływ na cele;
Zabezpieczenie	Wszystko to, co modyfikuje ryzyko;
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;
Zakłócenie	Incydent związany z utratą ciągłości działania, przewidywany lub nieprzewidziany, który powoduje nieplanowane, negatywne odchylenie od oczekiwanej dostawy wyrobów i usług zgodnie z celami UMWP;
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;
Zarządzanie ryzykiem	Skoordynowane działania dotyczące kierowania organizacją i nadzorowania jej w odniesieniu do ryzyka;
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*;*

Pojęcie	Definicja
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*;*
Zespół CSIRT NASK	Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym prowadzony przez Naukową i Akademicką Sieć Komputerową - Państwowy Instytut Badawczy;
Zespół ds. Bezpieczeństwa Informacji	Zespół zarządczo-doradczy powołany Zarządzeniem Marszałka Województwa Pomorskiego w celu realizacji działań związanych z eksploatacją, monitorowaniem, przeglądaniem, utrzymywaniem i doskonaleniem bezpieczeństwa informacji w UMWP;

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

Wykaz podstawowych aktów prawa powszechnie obowiązującego związanych z bezpieczeństwem informacji i ciągłością działania:

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 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. Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych;
13. Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej;
14. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych;
15. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;
16. Ustawa z dnia 22 listopada 2018 r. o dokumentach publicznych
17. 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);
18. Ustawa z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych
19. Ustawa z dnia 18 listopada 2020 r. o doręczeniach elektronicznych;
20. Ustawa z dnia 28 kwietnia 2022 r. o zmianie niektórych ustaw w związku z rozwojem publicznych systemów teleinformatycznych;
21. Ustawa z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej
22. Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego;
23. 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;

24. 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;
25. 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 i ciągłością działania:

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;
5. PN-ISO/IEC 29151 Technika informatyczna -- Techniki bezpieczeństwa -- Praktyczne zasady ochrony informacji o identyfikowalnych osobach
6. PN-ISO/IEC 22301 Bezpieczeństwo i odporność -- Systemy zarządzania ciągłością działania – Wymagania

Inne dokumenty związane z bezpieczeństwem informacji i ciągłością działania, 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 wprowadzenia do stosowania Karty audytu wewnętrznego, Kodeksu etyki audytora wewnętrznego i Podręcznik procedur audytu wewnętrznego w Urzędzie Marszałkowskim Województwa Pomorskiego ;
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. Zarządzenie MWP w sprawie postępowania w przypadku zagrożenia terrorystycznego w Urzędzie Marszałkowskim Województwa Pomorskiego.
14. Zarządzenie MWP w sprawie opracowania "Planu Operacyjnego Funkcjonowania Urzędu Marszałkowskiego Województwa Pomorskiego w warunkach zewnętrznego zagrożenia bezpieczeństwa państwa i w czasie wojny".
15. Zarządzenie MWP w sprawie wprowadzenia Regulaminu postępowania w przypadku przeprowadzenia czynności przez organy prowadzące postępowanie kontrolne i karne.
16. Zarządzenie MWP w sprawie wprowadzenia Procedury dotyczącej postępowania w przypadku uzyskiwania informacji i materiałów, wstępu do pomieszczeń oraz wglądu w działalność Urzędu Marszałkowskiego przez Radnych Województwa.
17. Zarządzenie MWP w sprawie powołania oraz określenia zakresu zadań Zespołu ds. Bezpieczeństwa Informacji.
18. Zarządzenie MWP w sprawie ustalenia stawki ryczałtu za jedną godzinę zużycia energii elektrycznej oraz korzystania z usług telekomunikacyjnych (Internetu) dla potrzeb określenia kosztów w związku z wykonywaniem pracy zdalnej przez pracowników UMWP, z którymi zostało zawarte Indywidualne porozumienie w sprawie wykonywania pracy zdalnej oraz określenia wzoru Indywidualnego porozumienia w sprawie wykonywania pracy zdalnej
19. Zarządzenie MWP w sprawie powołania Sztabu Kryzysowego w Urzędzie Marszałkowskim Województwa Pomorskiego.
20. Zarządzenie MWP w sprawie wprowadzenia jednolitych wzorów dokumentów procedowanych przez Zarząd Województwa Pomorskiego
21. Zarządzenie MWP w sprawie wprowadzenia Polityki zarządzania zasobami ludzkimi w Urzędzie Marszałkowskim Województwa Pomorskiego
22. Zarządzenie MWP w sprawie wprowadzenia do użytku służbowego ,,Regulaminu korzystania z intranetu” w Urzędzie Marszałkowskim Województwa Pomorskiego
23. Zarządzenie MWP w sprawie Polityki zarządzania zasobami ludzkimi
24. Instrukcje bhp, p.poż.