ZARZĄDZENIE NR 60/25

Wójta Gminy Brudzeń Duży

z dnia 05.09.2025 r.

w sprawie wprowadzenia aktualizacji Systemu Zarządzania Bezpieczeństwem Informacji.

Na podstawie 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) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.), art. 32 ust. 3 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (t.j. Dz. U. z 2023r. poz. 1206), art.13 ust. 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz. U. z 2024 r. poz. 1557 z pozn. zm.) w związku z § 19 Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2024 r. poz. 773), zarządza się, co następuje:

§1.

1. W Urzędzie Gminy Brudzeń Duży, ustanawia się, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali aktualizację Systemu Zarządzania Bezpieczeństwem Informacji, zwanego dalej: SZBI, zapewniającego poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

2. Aktualizacja SZBI odnosi się do ochrony informacji we wszystkich procesach, w których informacje są przetwarzane, w szczególności ustanowienia, wdrażania, eksploatacji, monitorowania, utrzymania i doskonalenia bezpieczeństwa informacji.

§2.

1. Dokumentacja aktualizacji SZBI stanowi załącznik do niniejszego Zarządzenia.

2. Podstawową dokumentację aktualizacji SZBI stanowi:

a) System Zarządzania Bezpieczeństwem Informacji w Urzędzie Gminy Brudzeń Duży - dokument wprowadzający – aktualizacja wydanie 2.0

b) Polityka Bezpieczeństwa Informacji – aktualizacja wydanie 2.0

c) Polityka Bezpieczeństwa Informatycznego – aktualizacja wydanie 2.0

d) Procedura klasyfikacji informacji i analizy ryzyka – aktualizacja wydanie 2.0

W/w dokumenty zostały zatwierdzone przez Wójta Gminy Brudzeń Duży.

§3.

W Urzędzie Gminy Brudzeń Duży przynajmniej raz do roku przeprowadzony zostanie audyt wewnętrzny w zakresie bezpieczeństwa informacji, zgodnie z wymogami określonymi w § 19 ust. 2 pkt. 14 rozporządzenia Rady Ministrów z dnia 21 maja 2024r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów informatycznych.

§4.

1. Pracownicy mają obowiązek zapoznania się z aktualizacjami SZBI (co powinni potwierdzić stosownym oświadczeniem) oraz stosowania jego zapisów.

2. Kierownicy komórek organizacyjnych odpowiadają za wdrożenie i przestrzeganie aktualizacji SZBI w podległych sobie komórkach organizacyjnych.

§ 5.

W związku z wdrożeniem Systemu Zarządzania Bezpieczeństwem Informacji i jego aktualizacji, w Urzędzie Gminy Brudzeń Duży następuje powołanie następujących ról:

Koordynator Bezpieczeństwa Informacji - Pani Beata Banaszczak
Inspektor Ochrony Danych – Pan Konrad Matlęga
Administrator Systemu Informatycznego - Pani Magdalena Śmigrodzka

§ 6.

Traci moc § 5 Zarządzenia Wójta Gminy Brudzeń Duży nr 347/23 z dnia 29.05.2023r. w sprawie wprowadzenia Systemu Zarządzania Bezpieczeństwem Informacji.

§ 7.

Zarządzenie wchodzi w życie z dniem podpisania.

§ 8.

Wykonanie zarządzenia powierza się Sekretarzowi Gminy Brudzeń Duży.

Załącznik nr 1
do zarządzenia nr 60/25
z dnia 05.09.2025

GMINA
BRUDZEŃ DUŻY
MAZOWIECKA SZWAJCARIA

System Zarządzania Bezpieczeństwem Informacji

w Urzędzie Gminy Brudzeń Duży

Dokument wprowadzający

Wydanie 2.0

AKTUALIZACJA

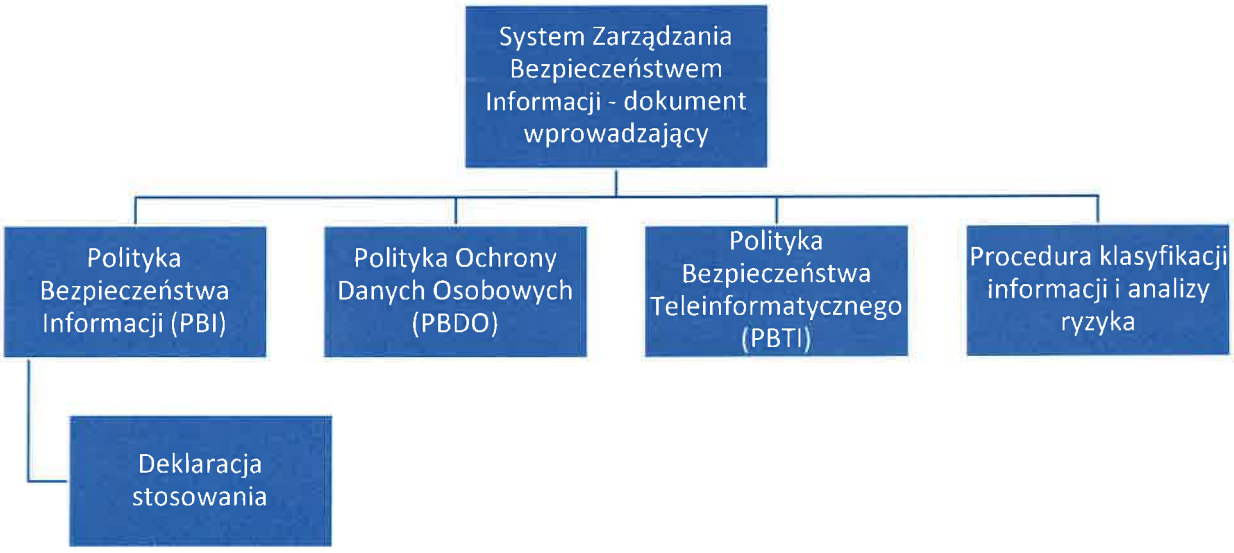
Zatwierdził:

WÓJT GMINY
Brudzeń Duży
Michał Twardy

Wprowadzenie

Niniejszy dokument przedstawia główne założenia w obszarze realizacji kluczowych elementów funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w Urzędzie Gminy Brudzeń Duży, wraz ze wskazaniem wymagań normy ISO/IEC 27001, a także regulacji zewnętrznych, którym podlega Urząd Gminy Brudzeń Duży:

- System Zarządzania Bezpieczeństwem Informacji odnosi się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji przy zachowaniu ich poufności, integralności oraz dostępności,
- Wszystkie komórki organizacyjne Urzędu Gminy Brudzeń Duży zostały objęte Systemem Zarządzania Bezpieczeństwem Informacji,
- Obszary bezpieczeństwa opisane przez System Zarządzania Bezpieczeństwem Informacji przedstawia poniższy schemat:



Role i odpowiedzialność w zarządzaniu bezpieczeństwem informacji

Najwyższe kierownictwo i odpowiedzialność za zarządzanie bezpieczeństwem Informacji.

Podejmowanie kluczowych decyzji dotyczących funkcjonowania Urzędu Gminy Brudzeń Duży jest domeną Wójta.
Podobnie w zakresie bezpieczeństwa informacji, dla najważniejszych zagadnień związanych z artykułowaniem wizji i kierunków rozwoju niezbędne jest wkomponowanie SZBI w struktury zarządzania Urzędem Gminy Brudzeń Duży.
W ramach skutecznego funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji przyjmuje się, iż Wójt Gminy pełni funkcję przedstawiciela najwyższego kierownictwa Systemu Zarządzania Bezpieczeństwem Informacji, a tym samym będzie brał czynny udział w podejmowaniu kluczowych decyzji dotyczących Systemu Zarządzania Bezpieczeństwem Informacji.
Wskazane decyzje odnoszą się do:

- Zatwierdzania wyników oceny ryzyka,
- Zatwierdzania planu postępowania z ryzykiem oraz raportu z przeglądu zarządzania dla Urzędu Gminy Brudzeń Duży ,
- Zatwierdzenie raportu z przeglądu Systemu Zarządzania Bezpieczeństwem Informacji,
- Zatwierdzenia dokumentów wchodzących w skład Systemu Zarządzania Bezpieczeństwem Informacji.

W skład najwyższego kierownictwa SZBI wchodzą:

- Wójt Gminy
- Sekretarz

Do obowiązków najwyższego kierownictwa w szczególności należy:

- Zapewnienie odpowiednich zasobów dla Systemu Zarządzania Bezpieczeństwem Informacji,
- Podejmowanie działań na rzecz ciągłego doskonalenia i rozwoju Systemu Zarządzania Bezpieczeństwem Informacji,
- Ustalanie celów Systemu Zarządzania Bezpieczeństwem Informacji,
- Uczestniczenie w przeglądzie Systemu Zarządzania Bezpieczeństwem Informacji,

Koordynator Bezpieczeństwa

Powołana zarządzeniem Wójta Urzędu Gminy Brudzeń Duży osoba odpowiedzialna za zapewnienie odpowiedniego poziomu bezpieczeństwa informacji, w szczególności:

- Zapewnienie funkcjonowania systemu zarządzania w Urzędzie Gminy Brudzeń Duży opartego o wymagania normy ISO/IEC 27001,
- Nadzorowanie wspólnych dla wszystkich obszarów Urzędu Gminy Brudzeń Duży elementów dokumentacji, zawierającej wymagania dla bezpieczeństwa informacji,
- Realizacja zadań pozwalających na utrzymanie Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Gminy Brudzeń Duży,
- Raportowanie do Wójta wyników analiz dotyczących Systemu Zarządzania Bezpieczeństwem Informacji i opracowań mających na celu doskonalenie SZBI.

Inspektor Ochrony Danych

Do obowiązków Inspektora Ochrony Danych w szczególności należy:

- Sprawdzanie przestrzegania przepisów o ochronie danych osobowych, w szczególności poprzez:
  - Sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych,
  - Wytycza kierunki zmierzające do zapewnienia odpowiedniej ochrony danych osobowych oraz nadzoruje przestrzeganie ustalonych zasad o nadzorowanie opracowania i aktualizowania dokumentacji,
  - Zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
- prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych.

Administrator Systemów Informatycznych

Do obowiązków Administratora Systemów Informatycznych należy w szczególności:

- Bieżące monitorowanie oraz raportowanie stanu bezpieczeństwa systemów teleinformatycznych,
- Implementacja odpowiednich mechanizmów bezpieczeństwa w administrowanej infrastrukturze informatycznej,
- Nadawanie uprawnień użytkownikom systemu informatycznego zgodnie z procedurą nadawania uprawnień,
- Zapewnienie pomocy użytkownikom przy korzystaniu z systemu informatycznego,
- Tworzenie kopii zapasowych danych przechowywanych w systemie informatycznym,

- Instalacja i uaktualnianie oprogramowania oraz zarządzanie licencjami,
- Monitorowanie funkcjonowania systemu informatycznego i przekazywanie informacji o zagrożeniach administratorowi bezpieczeństwa informacji,
- Aktywny udział w procesie reagowania na incydenty w zakresie bezpieczeństwa oraz w usuwaniu ich skutków,
- Rozwój i utrzymanie infrastruktury sprzętowej,
- Zarządzanie polityką dostępu do systemów informatycznych użytkowników i osób trzecich,
- Dokumentowanie procedur eksploatacyjnych, procedur wprowadzania zmian w systemach informatycznych, procedur kopii zapasowych, procedur zarządzania ciągłością działania systemów, procedur odtworzeniowych,
- Zapewnienie zgodności stosowanych rozwiązań z przepisami prawa.

Kierownik komórki organizacyjnej

Kierownicy komórek organizacyjnych, z uwagi na zajmowane stanowisko, stanowią bardzo ważny element w procesie zapewnienia bezpieczeństwa informacji w Urzędzie Gminy Brudzeń Duży. Powinni oni oddziaływać na pracowników, weryfikować spełnienie wymagań Systemu Zarządzani Bezpieczeństwem Informacji w podległych im komórkach oraz brać czynny udział w procesie przeglądu uprawnień. Ponadto kierownicy komórek organizacyjnych zobowiązani są wskazywać odpowiedzialności w odniesieniu do zarządzania systemami teleinformatycznymi.

Pracownicy Urzędu Gminy Brudzeń Duży

Pracownicy Urzędu Gminy Brudzeń Duży są odpowiedzialni za przestrzeganie obowiązujących zasad w zakresie bezpieczeństwa systemów informatycznych oraz bezpieczeństwa informacji. Pracownicy mogą brać udział w projektowaniu, wdrażaniu i stosowaniu systemu zabezpieczeń, aby uniknąć sytuacji, w której pewne mechanizmy ochronne znacznie utrudnią lub niemalże uniemożliwią realizację zadań niektórych użytkowników. Obowiązki pracowników w zakresie bezpieczeństwa informacji obejmują:

- Przestrzeganie zasad bezpieczeństwa informacji, ochrony danych i bezpieczeństwa systemu informatycznego,
- Aktywny udział w szkoleniach dotyczących bezpieczeństwa informacji i systemu informatycznego,
- Informowanie o incydentach w zakresie bezpieczeństwa informacji, w tym systemu informatycznego,

Działania jakie podejmują pracownicy to:

- Udział w analizie ryzyka i klasyfikacji zasobów,

- Raportowanie incydentów bezpieczeństwa informacji,
- Zgłaszanie wniosków o zmianę w dokumentacji.

Zespół Zarządzania Incydentami

Interdyscyplinarny zespół powoływany przez Wójta, w szczególności odpowiedzialny za przeprowadzenie analizy i dalszą reakcję na występujące incydenty bezpieczeństwa informacji w Urzędzie Gminy Brudzeń Duży. Zespół Zarządzania Incydentami (ZZI) przygotowuje niezwłocznie i przedstawia Wójtowi propozycje :

- Klasyfikacji zdarzeń identyfikowanych w Urzędzie Gminy Brudzeń Duży jako incydent lub zdarzenie nie będące incydentem,
- Wskazanie działań jakie należy podjąć, aby zminimalizować skutki wystąpienia incydentu,
- Wskazanie działań pozwalających na zabezpieczenie materiału dowodowego związanego z incydentem,
- Definiowanie działań korygujących, które zapewnią, iż podobne incydenty nie będą zdarzały się w przyszłości.

Należy zapewnić, iż osoby wchodzące w skład Zespołu Zarządzania Incydentami posiadają wiedzę zarówno dotyczącą incydentów teleinformatycznych, jak i niezwiązaną z obszarem IT. Fakultatywne zadania ZZI:

- Alertowanie i ostrzeganie,
- Obsługa incydentów teleinformatycznych,
- Obsługa słabości systemowych,
- Analiza złośliwego oprogramowania,
- Ogłaszanie komunikatów bezpieczeństwa,
- Monitoring technologii bezpieczeństwa,
- Ocena i audyty bezpieczeństwa,
- Dystrybucja informacji związanej z bezpieczeństwem,
- Szkolenia z zakresu bezpieczeństwa,
- Konsultacje z zakresu bezpieczeństwa,
- Budowanie świadomości.

Właściciel informacji

Właścicielem Informacji jest każda osoba wytwarzająca ją na danym stanowisku merytorycznym. Przyjmuje się, iż Właścicielem Informacji będzie osoba na stanowisku kierowniczym, merytorycznie związana z informacjami, których jest właścicielem. Rola ta wykorzystywana będzie do przeprowadzania cyklicznej klasyfikacji informacji i jej oceny pod kątem bezpieczeństwa. Do zadań należących do Właścicieli informacji należy:

- Identyfikowanie i ocena grup informacji istniejących w obszarze merytorycznym Właściciela Informacji,
- Podejmowanie w uzgodnieniu z Koordynatorem Bezpieczeństwa decyzji dotyczących kształtu i sposobu realizacji,
- Działań doskonalących związanych ze zidentyfikowanymi przez niego grupami informacji i zasobami, w których informacje są przetwarzane,
- Dbałość o przetwarzanie informacji zgodnie z zasadami Systemu Zarządzania Bezpieczeństwem Informacji w swoim obszarze merytorycznym.

Właściciel zasobu

Właścicielem Zasobu jest każda osoba zarządzająca danym zasobem, w którym przetwarzane są informacje. Właściciel Zasobu odpowiedzialny jest za proces oceny ryzyka w odniesieniu do zasobu, którego jest właścicielem. Możliwym jest, aby Właścicielem Zasobu był administrator systemu lub inna osoba wskazana przez kierownika komórki organizacyjnej, pracująca w obszarze, w którym zasób jest eksploatowany. Wskazana osoba powinna nie tylko zarządzać, ale i utrzymywać zasób oraz ponosić odpowiedzialność w zakresie zarządzania jego bezpieczeństwem.

Odpowiedzialność za zatwierdzanie dokumentacji

W ramach Systemu Zarządzania bezpieczeństwem informacji zakłada się następujące odpowiedzialności w zatwierdzaniu elementów dokumentacji:

- Wójt – Polityki, Procedury, Instrukcje, Zasady.

Nadzorowanie dokumentacji

Podstawowym założeniem skutecznego wdrożenia dokumentacji i naturalnego korzystania z niej przez pracowników jest wprowadzenie jednego miejsca w Urzędzie Gminy Brudzeń Duży, gdzie źródła najbardziej aktualnej i obowiązującej wiedzy będą dostępne. Z uwagi na wielkość i charakter organizacji a także liczbę dokumentów, wymagane jest umieszczenie dokumentacji w systemie teleinformatycznym, który będzie wspomagał jej publikację, zarządzanie uprawnieniami do poszczególnych elementów dokumentacji, jak również zarządzanie wersją. Powyższe założenia należy w szczególności skutecznie wdrożyć w obszarze bezpieczeństwa teleinformatycznego. Zaleca się również rozszerzenie sposobu nadzorowania dokumentacji o inne wymagania opisujące sposób funkcjonowania działań służb IT (np. procedury zamawiania

usług, realizacji zgłoszeń itp.). Zakłada się również możliwość ograniczenia dostępu do niektórych elementów dokumentacji – np. szczegółowe procedury bezpieczeństwa takie jak instrukcje wykonywania kopii zapasowych, szczegóły zabezpieczeń systemów czy definicje reguł na systemach firewall. Regulacje wewnętrzne Urzędu Gminy Brudzeń Duży są podlegają przeglądowi co najmniej raz w roku, oraz w przypadku potrzeb na bieżąco aktualizowane.

Postanowienia końcowe

Wszystkie zagadnienia uwzględnione w dokumencie ,,System Zarządzania Bezpieczeństwem Informacji w Urzędzie Gminy Brudzeń Duży" mają na celu określenie strategicznych kierunków i odpowiedzialności wynikających z wdrożonego SZBI w Urzędzie Gminy Brudzeń Duży. Wszelkie szczegóły w tym zakresie zostały opisane w dokumentach powiązanych m.in. Polityka Bezpieczeństwa Informacji oraz Polityka Bezpieczeństw Teleinformatycznego.

Załącznik nr 2
do zarządzenia nr 60/25
z dnia 05.09.2025

GMINA
BRUDZEŃ DUŻY
MAZOWIECKA SZWAJCARIA

Polityka Bezpieczeństwa Informacji w Urzędzie Gminy Brudzeń Duży

Wydanie 2.0

AKTUALIZACJA

Zatwierdził:

WÓJT GMINY
Brudzeń Duży
Michał Twardy

Wprowadzenie

Polityka Bezpieczeństwa Informacji w Urzędzie Gminy Brudzeń Duży stanowi zestawienie zasad, praw i reguł oraz wytycznych i dobrych praktyk w zakresie zarządzania i ochrony informacji w szczególności zapewniając ich poufność, dostępność oraz integralność. Polityka określa techniczne i organizacyjne środki służące do osiągnięcia celów stawianych przed Systemem Zarządzania Bezpieczeństwem Informacji (SZBI).

W procesie tym kluczowe jest stosowanie współczesnych technik i technologii, narzędzi oraz systemów informatycznych służących do przetwarzania i zarządzania informacją, która jest jednym z najważniejszych zasobów Urzędzie Gminy Brudzeń Duży i jest chroniona na każdym szczeblu organizacji.

Cele Systemu Zarządzania Bezpieczeństwem Informacji

Głównymi celami Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Gminy Brudzeń Duży są:

- Zapewnienie bezpieczeństwa informacji przez utrzymanie atrybutów dostępności, integralności oraz poufności,
- Spełnienie wymagań prawnych,
- Wzrost świadomości pracowników w zakresie bezpieczeństwa informacji,
- Zapewnienie ciągłości działania świadczonych usług,
- Przygotowanie organizacji na potencjalne incydenty związane z bezpieczeństwem informacji,
- Podniesienie wiarygodności organizacji wśród interesariuszy.

Najwyższe kierownictwo, wdrażając Politykę Bezpieczeństwa Informacji zgodnie z wymaganiami normy PN-EN ISO/IEC 27001:2023 pkt. 5.2; 6.2; 7.5 wykazuje przywództwo i zaangażowanie w kontekście bezpieczeństwa informacji podczas realizowanych procesów w Urzędzie Gminy Brudzeń Duży poprzez zapewnienie, iż wprowadzona Polityka Bezpieczeństwa Informacji:

- Jest zgodna z celami strategicznymi istnienia organizacji,
- Określa cele bezpieczeństwa informacji,
- Zobowiązuje najwyższe kierownictwo do ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji,
- Określa spełnienie wymagań zgodnie z obowiązującymi normami prawnymi,
- Jest zakomunikowana w organizacji,
- Jest dostępna jako udokumentowana i formalnoprawnie wdrożona procedura.

Kontekst organizacji

W oparciu o normę PN-EN ISO/IEC 27001:2023 pkt 4.3, Organizacja, określając zakres Systemu Zarządzania Bezpieczeństwem Informacji, rozważa jej kontekst wewnętrzny oraz zewnętrzny, identyfikuje strony zainteresowane, a także określa interfejsy i zależności między działaniami wykonywanymi wewnątrz organizacji, a także przez inne organizacje.

System Zarządzania Bezpieczeństwem Informacji obejmuje zakresem cały Urząd Gminy Brudzeń Duży ze szczególnym uwzględnieniem relacji z głównymi stronami zainteresowanymi jakimi są przede wszystkim:

- Pracownicy organizacji,
- Osoby fizyczne obsługiwane przez organizację w ramach wykonywanych przez nią zadań,
- Podmioty publiczne,
- Organy kontrolne,
- Kontrahenci organizacji (dostawcy, podwykonawcy, usługodawcy),
- Organizacje pozarządowe, fundacje, stowarzyszenia.

Urząd Gminy Brudzeń Duży zapewnienia ciągłe doskonalenia Systemu Bezpieczeństwa Informacji z uwzględnieniem zapewnienia poufności, integralności, dostępności oraz autentyczności świadczonych usług dla interesariuszy oraz w ramach współpracy z innymi podmiotami i organami nadzoru.

System Zarządzania Bezpieczeństwem Informacji w Urzędzie Gminy Brudzeń Duży został zaprojektowany oraz wdrożony zgodnie z dobrymi praktykami oraz następującymi regulacjami:

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. 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),
- Ustawa z dnia 10 maja 2018 o ochronie danych osobowych,
- Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2024 r. poz. 307)),
- Norma PN-EN ISO/IEC 27001:2023 (Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – Systemy zarządzania bezpieczeństwem informacji - Wymagania),

- Norma PN-EN ISO/IEC 27002:2023 (Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – Zabezpieczanie informacji),
- Norma PN-ISO/IEC 27005:2014-01 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji – Wsparcie do Normy PN-EN ISO/IEC 27001:2017),
- Ustawa o Krajowym Systemie Cyberbezpieczeństwa z dnia 5 lipca 2018 roku.

Zakres Systemu Zarządzania Bezpieczeństwem Informacji

System Zarządzania Bezpieczeństwem Informacji odnosi się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji oraz bezpiecznego świadczenia usług przez Urząd Gminy Brudzeń Duży w oparciu o normę PN-ISO/IEC 27001:2023.

Zakres Systemu Zarządzania Bezpieczeństwem Informacji dotyczy zarządzania informacjami, zachowaniu ich poufności, integralności, dostępności, oraz autentyczności i ma zastosowanie do:

- Wszystkich istniejących, wdrażanych obecnie lub w przyszłości procesów oraz systemów teleinformatycznych, w których przetwarzane są informacje podlegające ochronie,
- Informacji będących własnością organizacji oraz jej kontrahentów,
- Lokalizacji Urzędu Gminy Brudzeń Duży, czyli budynków i pomieszczeń, w których są lub mogą być przetwarzane informacje podlegające ochronie,
- Wszystkich pracowników w rozumieniu przepisów kodeksu pracy, konsultantów, stażystów, współpracowników/pracowników firm zewnętrznych i pozostałych osób mających dostęp do informacji podlegających ochronie,
- Kluczowych czynników zewnętrznych i wewnętrznych mających wpływ na realizację istotnych wymagań stron zainteresowanych.

Nadzorowanie dokumentacji

Wójt Urzędu Gminy Brudzeń Duży zobowiązany jest do zapewnienia nadzoru nad dokumentacją Systemu Zarządzania Bezpieczeństwem Informacji pod kątem aktualności, poprawności oraz dystrybucji. Dokumentacja objęta procedurą nadzoru to:

- Polityka Bezpieczeństwa Informacji (PBI), w tym Deklaracja stosowania zabezpieczeń,
- Polityka Bezpieczeństwa Teleinformatycznego (PBTI),
- Procedura klasyfikacji informacji i analizy ryzyka.

Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji podlega aktualizacji co najmniej raz w roku lub w jednym z poniższych przypadków:

- Wymagania wynikające ze zmian organizacyjnych,
- Incydenty bezpieczeństwa,
- Zmiany prawne,
- Audyty zewnętrzne/wewnętrzne,
- Wyników analizy ryzyka, a tym samym uwzględnienie planu postępowania z ryzykiem.

W celu zapewnienia aktualności obowiązującej dokumentacji, zgodności z wymaganiami regulacyjnymi oraz nadzoru nad zapisami przyjmuje się, że najwyższe kierownictwo odpowiada za zatwierdzanie dokumentacji wchodzącej w skład Systemu Zarządzania Bezpieczeństwem Informacji zgodnie z odpowiedzialnością opisaną w dokumentacji wprowadzającej do SZBI,

Ocena Systemu Zarządzania Bezpieczeństwem Informacji

W celu oceny wyników działań na rzecz bezpieczeństwa informacji oraz skuteczności Systemu Zarządzania Bezpieczeństwem Informacji, Urząd Gminy Brudzeń Duży realizuje:

- Monitorowanie postępu zaleceń wynikających z Planu Postępowania z Ryzykiem (PPR) oraz terminów z nich wynikających,
- Cykliczny przegląd wyników audytów wewnętrznych oraz zewnętrznych, a także poziomu wdrożenia zaleceń z nich wynikających zgodnie z oczekiwanymi terminami,
- Poziom przeszkolenia pracowników Urzędu Gminy Brudzeń Duży z obszaru bezpieczeństwa informacji oraz cyberbezpieczeństwa,
- Cykliczne monitorowanie zaleceń bezpieczeństwa, które powstały jako rekomendacje po zidentyfikowanych incydentach bezpieczeństwa,
- Cykliczne monitorowanie poziomu aktualności systemów teleinformatycznych wykorzystywanych przez Urząd Gminy Brudzeń Duży.

Przegląd zarządzania

W celu zapewnienia ciągłego doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji co najmniej raz do roku planuje się i przeprowadza przegląd zarządzania. Wskazana przez Wójta osoba określa termin oraz formę przeglądu Systemu Zarządzania Bezpieczeństwem Informacji

(spotkanie bezpośrednie, telekonferencja, analiza materiałów na przegląd, opinie i propozycje przesyłane droga elektroniczną).
W ramach przeglądu zarządzania podejmuje się decyzje co do dalszego doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji.
Z każdego przeglądu zarządzania, wskazana przez Wójta osoba przygotowuje sprawozdanie i przekazuje je Wójtowi. W przypadku, gdy w ramach przeglądu zarządzania zostaną wskazane działania doskonalące, należy powiadomić o tym fakcie osoby odpowiedzialne.

W ramach przeglądu zarządzania:

- Weryfikowane są cele bezpieczeństwa informacji,
- Weryfikowane są zmiany czynników wewnętrznych i zewnętrznych, które są istotne dla Systemu Zarządzania Bezpieczeństwem Informacji
- Weryfikacja potrzeb zmian w Systemie Zarządzania Bezpieczeństwem Informacji oraz gdy takie nastąpią ustalenie planu wdrożenia zmiany,
- Omawiane są potrzeby i oczekiwania stron zainteresowanych,
- Weryfikowana jest efektywność Systemu Zarządzania Bezpieczeństwem Informacji,
- Omawiane są zidentyfikowane incydenty,
- Planowane są działania korekcyjne, korygujące lub zapobiegawcze,
- Omawiany jest Plan Postępowania z Ryzykiem (PPR),
- Weryfikowana jest aktualność regulacji wchodzących w zakres Systemu Zarządzania Bezpieczeństwem Informacji,

Planowana jest możliwość ciągłego doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji.

Audyt wewnętrzny

W ramach Systemu Zarządzania Bezpieczeństwem Informacji planuje się i realizuje cykliczny audyt wewnętrzny pod kątem skuteczności wdrożonego systemu zgodnie następującymi zasadami:

- Planowanie audytów wewnętrznych na dany rok kalendarzowy,
- Audytowane obszary są dobierane na podstawie: analizy ryzyka, klasyfikacji informacji, zmian organizacyjnych, miejsc występowania incydentów,
- Kryteriami audytu są: norma PN- ISO/IEC 27001:2023, wymagania prawne, wymagania wewnętrzne oraz zewnętrzne,
- W przypadku pojawienia się niezgodności podejmowane są natychmiastowe działania korygujące,
- Audyt wewnętrzny przeprowadzany jest minimum raz w roku,
- Audytorzy dobierani są w sposób zapewniający zachowanie obiektywności i bezstronności,
- Wyniki audytów przedstawiane są przez audytora Wójtowi

Strategia ciągłości działania

Urząd Gminy Brudzeń Duży dba o zapewnienie ciągłości funkcjonowania usług związanych z przetwarzaniem danych. Celem jest przeciwdziałanie przerwom w działalności oraz ochrona krytycznych usług przed rozległymi awariami lub katastrofami. Realizacja postawionego celu możliwa jest dzięki ustanowionym praktykom i podziałowi odpowiedzialności związanemu z zarządzeniem ciągłością działania tak, aby ograniczyć do akceptowalnego poziomu skutki wypadków i awarii.

W ramach strategii ciągłości działania, Urząd Gminy Brudzeń Duży posiada aktualne plany ciągłości działania systemów, które są własnością Urzędu. W przypadku wykorzystywania usług zewnętrznych obowiązują umowy z zewnętrznymi podmiotami w ramach, których określone są parametry SLA umożliwiające zapewnienie ciągłości działania kluczowych usług Urzędu.

Administrator Systemów Informatycznych lub podmiot świadczący usługi na rzecz Urzędu Gminy Brudzeń Duży zobowiązany jest do opracowania, aktualizacji oraz testowania planów ciągłości działania.

Zarządzanie incydentami bezpieczeństwa informacji

W celu zapewnienia skuteczności działania Systemu Zarządzania Bezpieczeństwem Informacji w zakresie obsługi incydentów bezpieczeństwa informacji należy:

- Na bieżąco monitorować, czy w organizacji doszło do uchybienia lub naruszenia i podejmować w związku z tym określone stosownymi procedurami czynności,
- Cyklicznie, jednak nie rzadziej niż raz na rok, analizować zidentyfikowane naruszenia bądź uchybienia, ocenia je pod względem istotności w zakresie bezpieczeństwa informacji, wyciąga wnioski, a także podejmuje działania naprawcze względem zidentyfikowanych incydentów,
- Wójt, jeśli uzna to za stosowna, przeprowadza lub zleca przeprowadzenie audytu doraźnego po zidentyfikowaniu i obsłużeniu incydentu bezpieczeństwa,
- Wójt podejmuje decyzje w zakresie kwalifikacji incydentu jako zdarzenia, którego wystąpienie skutkuje koniecznością zgłoszenia tego faktu do organu nadzorczego lub jako zdarzenia, którego wystąpienie nie spowoduje konieczności zgłoszenia do organu nadzorczego (decyzja konsultowana jest z Zespołem Zarządzania Incydentami),
- Wójt podejmuje decyzje w zakresie kwalifikacji incydentu jako zdarzenia, którego wystąpienie skutkuje koniecznością zawiadomienia osób, których dane dotyczą o fakcie ich naruszenia

lub jako zdarzenia, które takich skutków nie wywoła. Każdy pracownik jest zobowiązany do zgłoszenia wójtowi wystąpienie incydentu bezpieczeństwa,

- Względem pracownika, który nie podejmuje czynności poinformowania o potencjalnym incydencie bezpieczeństwa i bagatelizuje zdarzenie, co do którego można mieć podejrzenie, iż wystąpił incydent może zostać zastosowane postępowanie dyscyplinarne.

Ochrona danych osobowych

Ochrona danych osobowych w Urzędzie Gminy Brudzeń Duży w całości nadzorowana jest przez Inspektora Ochrony Danych (IOD). W ramach odpowiedzialności Inspektora Ochrony Danych jest przede wszystkim:

- Zapewnienie, że wszystkie zadania realizowane przez Urząd Gminy Brudzeń Duży są zgodne z wewnętrznymi oraz zewnętrznymi regulacjami m.in. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. 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) oraz Ustawa z dnia 10 maja 2018 o ochronie danych osobowych,
- Jeśli w organizacji zostanie zidentyfikowane zdarzenie, które spowoduje naruszenie ochrony danych osobowych, Inspektor Ochrony Danych zobowiązany jest zgłosić ten fakt organowi nadzorczemu w terminie 72 godzin, chyba, że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych,
- Zgłoszenie, o którym mowa powyżej opisuje co najmniej: charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazanie kategorii i przybliżonej liczby osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie; imię i nazwisko oraz dane kontaktowe Inspektora Ochrony Danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji; możliwe konsekwencje naruszenia ochrony danych osobowych; środki zastosowane lub proponowane przez Inspektora Ochrony Danych w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków,
- Jeżeli w organizacji dojdzie do naruszenia ochrony danych osobowych i zdarzenie to może spowodować wysokie ryzyko naruszenia praw lub wolności osób, których dane dotyczą, Inspektor Ochrony Danych powiadamia o tym fakcie te osoby,
- Inspektor Ochrony Danych informuje osoby fizyczne, których naruszenie dotyczy mając jednocześnie na uwadze zasadę przejrzystości – komunikat powinien być jasny, prosty, zrozumiały dla jego odbiorców,
- Wszystkie czynności opisane powyżej na bieżąco komunikowane są do Wójta.

Odpowiedzialność pracowników organizacji

W oparciu o normę PN-EN ISO/IEC 27001:2023 zał. A. rozdziale 6 (zabezpieczenia osobowe), odpowiedzialność za bezpieczeństwo informacji w organizacji ponoszą wszyscy pracownicy zgodnie z posiadanymi zakresami obowiązków. Każdy pracownik zobowiązany jest dbać o bezpieczeństwo powierzonych mu do przetwarzania, archiwizowania lub przechowywania informacji zgodnie z obowiązującymi w organizacji przepisami wewnętrznymi w tym m. in.:

- Stosować zasady opisane w Polityce Bezpieczeństwa Informacji oraz Polityce Bezpieczeństwa Teleinformatycznego, a także innych dokumentach wewnętrznych organizacji,
- Klasyfikować informacje,
- Chronić informacje podlegające ochronie przed dostępem do nich osób nieuprawnionych,
- Chronić dane przed przypadkowym lub umyślnym zniszczeniem, utratą lub modyfikacją,
- Chronić sprzęt, wydruki komputerowe i inne nośniki zawierające dane chronione,
- Utrzymywać w tajemnicy powierzone hasła, częstotliwość ich zmiany oraz szczegóły technologiczne systemów także po ustaniu zatrudnienia w organizacji,
- Powiadomić Inspektora Ochrony Danych o:
    a) ujawnieniu lub możliwości ujawnienia informacji chronionych osobom nieupoważnionym,
    b) nieautoryzowanej zmianie informacji chronionych lub możliwości wprowadzenia nieautoryzowanych zmian,
    c) zniszczeniu lub możliwości zniszczenia informacji chronionych,
    d) zablokowaniu lub możliwości zablokowania pracy systemu informatycznego przetwarzającego informacje chronione lub uniemożliwienia innego dostępu do informacji chronionych.

Szkolenia w zakresie bezpieczeństwa informacji

- Wszystkie osoby upoważnione do przetwarzania informacji oraz danych osobowych w organizacji są cyklicznie szkolone w zakresie bezpieczeństwa informacji,
- Osoby przetwarzające informacje oraz dane osobowe w organizacji mają znaczący wkład w skuteczność Systemu Zarządzania Bezpieczeństwem Informacji,
- Osoby przetwarzające informacje oraz dane osobowe w organizacji mają świadomość konsekwencji wynikających z niezgodności z wymaganiami Systemu Zarządzania Bezpieczeństwem Informacji oraz regulacjami prawnymi,
- Organizacja zastrzega sobie możliwość zlecenia przeprowadzenia szkolenia z zakresu bezpieczeństwa informacji osobie fizycznej lub podmiotowi spoza organizacji. Najwyższe

kierownictwo wybiera osobę fizyczną lub podmiot spoza organizacji kierując się jednocześnie zasadą konieczności zbadania kompetencji zleceniobiorcy lub osoby oddelegowanej do wykonania zadania przez zleceniobiorcę,

- Inspektor Ochrony Danych w ramach czynności audytowych oraz polityki informacyjnej, o której mowa w rozporządzeniu ogólnym, opracowuje agendę oraz zakres tematyczny szkoleń w zakresie bezpieczeństwa danych osobowych. Inspektor Ochrony Danych, po uprzedniej konsultacji z najwyższym kierownictwem może zlecić przeprowadzenie szkolenia z zakresu bezpieczeństwa informacji osobie fizycznej lub podmiotowi spoza organizacji. Wtedy Inspektor Ochrony Danych wybiera osobę fizyczną lub podmiot spoza organizacji kierując się jednocześnie zasadą konieczności zbadania kompetencji zleceniobiorcy lub osoby oddelegowanej do wykonania zadania przez zleceniobiorcę,
- Agenda oraz zakres tematyczny szkolenia stanowią udokumentowane informacje będące dowodem na ciągłe doskonalenie organizacji w zakresie bezpieczeństwa informacji.
- Zakres merytoryczny szkolenia szczególnie opiewa o zagadnienia takie jak: zagrożenia bezpieczeństwa informacji, skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna, stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich,
- Agenda oraz zakres tematyczny szkolenia jest przez Inspektora Ochrony Danych lub najwyższe kierownictwo skutecznie komunikowane pracownikom w organizacji poprzez udostępnienie tej informacji drogą tradycyjną (papierową) lub za pomocą środków teletransmisji (poczta elektroniczna, elektroniczny obieg dokumentacji) z rozsądnym wyprzedzeniem, tak, aby osoby przetwarzające dane osobowe w organizacji mogły przygotować problematyczne zagadnienia związane z przepływem danych osobowych, które będą bezwzględnie omawiane na każdym szkoleniu z zakresu bezpieczeństwa informacji,
- Osoby przetwarzające dane osobowe w organizacji, w wyniku sprawnie działającej polityki szkoleniowej, mają świadomość pozycji Inspektora Ochrony Danych i jego umocowania w strukturze organizacyjnej,
- Należy zaznaczyć, iż przeprowadzany audyt w zakresie bezpieczeństwa informacji ma charakter edukacyjny, a zatem spotkania z personelem również stanowią element polityki szkoleniowej organizacji,
- Każdy pracownik, który przeszedł szkolenie wstępne stanowiskowe lub cykliczne stanowiskowe w kontekście przetwarzania danych osobowych oraz bezpieczeństwa informacji podpisuje oświadczenie w zakresie zapoznania się z przedstawionym materiałem oraz zobowiązuje się do stosować do regulacji obowiązujących w organizacji.

Bezpieczeństwo w zarządzaniu zasobami ludzkimi

Przechowywanie dokumentów aplikacyjnych – proces rekrutacyjny

- W zakresie przetwarzania danych osobowych złożonych przez osoby aplikujące do pracy w organizacji, Urząd Gminy Brudzeń Duży kieruje się w szczególności zasadą ograniczonego celu, ograniczonego przechowywania oraz poufności,
- Urząd Gminy Brudzeń Duży przechowuje dane osobowe osób składających dokumentację aplikacyjną w trybie ogłoszonego do informacji publicznej konkursu przez okres wskazany w jednolitym rzeczowym wykazie akt osobowych,
- Urząd Gminy Brudzeń Duży zapewnia, żeby dane osobowe osób składających aplikacje były przetwarzane w sposób zapewniający ich bezpieczeństwo oraz stosowną poufność. Dostęp do tego zakresu danych osobowych mogą mieć tylko i wyłącznie pracownicy organizacji upoważnieni do przetwarzania takich danych z racji zajmowanego stanowiska pracy lub miejsca w strukturze organizacji,
- Urząd Gminy Brudzeń Duży zapewnia ochronę przed nieuprawnionym dostępem do tych danych osobowych, a jednocześnie do sprzętu, który służy do przetwarzania takich danych,
- Urząd Gminy Brudzeń Duży zapewnia przetwarzanie danych osobowych zawartych w aplikacjach tylko i wyłącznie w ściśle określonym celu, dla którego osoby składające przedmiotowe dokumenty, wyraziły zgodę (np. tylko i wyłącznie do postępowania konkursowego o konkretnej sygnaturze),
- Urząd Gminy Brudzeń Duży przeprowadza weryfikację czy dane zawarte w dokumentacji aplikacyjnej są zgodne ze stanem faktycznym,
- Urząd Gminy Brudzeń Duży zapewnia, że po zakończonym procesie rekrutacyjnym, wszystkie dane osób aplikujących, które nie podjęły zatrudnienia w organizacji zostają trwale usunięte, chyba, że odrębne przepisy prawne obligują Urząd Gminy Brudzeń Duży do przechowywania powyższych informacji przez określony czas.

Rozwiązanie współpracy z pracownikiem

W przypadku rozwiązania współpracy z pracownikiem Urzędu Gminy Brudzeń Duży należy:

- Odebrać wszystkie uprawnienia do systemów teleinformatycznych,
- Odebrać wszystkie uprawnienia umożliwiające dostęp fizyczny do Urzędu Gminy Brudzeń Duży,
- Zabezpieczyć wszystkie dokumenty fizyczne przed nieuprawnionym wykorzystaniem przez pracownika kończącego współpracę,
- Zabezpieczyć powierzony sprzęt teleinformatyczny przez nieuprawnionym wykorzystaniem przez pracownika kończącego współpracę,

- Wszystkie wymienione powyżej punkty powinny podlegać weryfikacji w zakresie skuteczności wprowadzonych zabezpieczeń przed utratą poufności, integralności oraz dostępności informacji.

Bezpieczeństwo fizyczne i środowiskowe

Bezpieczeństwo fizyczne w Urzędzie Gminy Brudzeń Duży postrzegane jest jako zapewnienie ochrony pomieszczeń, sprzętów, infrastruktury oraz personelu przed bezpośrednim działaniem czynników fizycznych i zdarzeń takich jak: pożar, powódź, kradzież, wandalizm, terroryzm.

Bezpieczeństwo fizyczne realizowane jest poprzez:

- Kontrolę fizycznych wejść i wyjść,
- Zabezpieczenie pomieszczeń, urządzeń i okablowania,
- Ochronę przed zagrożeniami zewnętrznymi i środowiskowymi,
- Uregulowanie zasad postępowania w obiektach w zakresie: ruchu osobowego, ruchu pojazdów, zasad zabezpieczania pomieszczeń, ppoż.

Bezpieczeństwo informacji w relacjach z Dostawcami

W przypadku dostawców zakres Polityki Bezpieczeństwa Informacji ma zastosowanie do:

- Wszystkich systemów, których Urząd Gminy Brudzeń Duży jest dysponentem, dostawcą lub partnerem,
- Informacji będących własnością Urzędu Gminy Brudzeń Duży,
- Wszystkich budynków i pomieszczeń, w których są lub mogą być przetwarzane w systemach teleinformatycznych informacje podlegające ochronie.

Każdy Dostawca niezależnie od przyjętej formy współpracy zobowiązany jest zapoznać się z zasadami / wytycznymi bezpieczeństwa oraz z aktualnymi procedurami ochrony informacji obowiązującymi w Urzędzie Gminy Brudzeń Duży. Działania naruszające Bezpieczeństwo Informacji mogą zostać uznane za ciężkie naruszenie obowiązków i stanowić podstawę do rozwiązania Umowy o współpracy.

Za zapoznanie się pracowników firm zewnętrznych z zapisami dotyczącymi Bezpieczeństwa Informacji odpowiadają właściciele Umów oraz osoby odpowiedzialne za bezpieczeństwo informacji.

Bezpieczeństwo wymiany informacji i współpracy z Dostawcami.

Odpowiedzialność za Bezpieczeństwo informacji w Urzędzie Gminy Brudzeń Duży ponoszą wszyscy Dostawcy zgodnie z posiadanymi zakresami zawartym w Umowach.

Poufność informacji pomiędzy Urzędem Gminy Brudzeń Duży a Dostawcą musi zostać zagwarantowana na etapie negocjacji zawieranej Umowy z Dostawcą (najlepiej już na etapie ofertowania).

Dystrybucja wiadomości e-mail musi być ograniczona jedynie do osób, które powinny znać ich treść lub do osób bezpośrednio związanych z treścią wiadomości. Listy dystrybucyjne nie powinny być używane z wyjątkiem sytuacji, gdy wszyscy adresaci spełniają powyższe kryteria.

Podczas komunikacji elektronicznej z Dostawcą z wykorzystaniem poczty elektronicznej, należy unikać wysyłania wiadomości z dużymi załącznikami do licznego grona osób poprzez listy dystrybucyjne. Należy używać oprogramowania kompresującego pozwalającego zaszyfrować załącznik hasłem. Hasło należy podać innym kanałem komunikacyjnym.

Bezpieczeństwo teleinformatyczne w odniesieniu do Dostawców.

Dostawcy mogą wykonywać swoje zadania na zasobach teleinformatycznych wyłącznie na podstawie aktualnej Umowy.

Dostęp do zasobów teleinformatycznych jest prawem każdego pracownika firmy zewnętrznej świadczącego pracę na rzecz Urzędu Gminy Brudzeń Duży zgodnie z podpisanymi Umowami i służy realizacji celów biznesowych Urzędu Gminy Brudzeń Duży.

Prawo wykorzystania zasobów teleinformatycznych podlega ograniczeniom wynikającym z zakresu obowiązków pracowników firm zewnętrznych na podstawie podpisanych Umów, regulacji wewnętrznych Urzędu Gminy Brudzeń Duży oraz regulacji zewnętrznych obowiązujących na terenie Rzeczpospolitej Polskiej.

Każdy pracownik firmy zewnętrznej odpowiada osobiście za wykonywane przez siebie działania w systemach teleinformatycznych należących do Urzędu Gminy Brudzeń Duży lub których Urząd Gminy Brudzeń Duży jest dostawcą lub partnerem.

Bezpieczeństwo informacji w ramach Krajowych Ram Interoperacyjności

W celu zapewnienia Bezpieczeństwa informacji w ramach Krajowych Ram Interoperacyjności Urzędu Gminy Brudzeń Duży ustanawia, wdraża i doskonali System Zarządzania Bezpieczeństwem Informacji zgodnie z wymaganiami normy ISO 27001 zapewniając tym samym standaryzację systemów i procesów w zakresie zapewnienia integralności, dostępności oraz poufności danych.

W celu zapewnienia interoperacyjności na poziomie organizacyjnym stosuje się:

- Opis usług świadczonych przez Urząd Gminy Brudzeń Duży wraz ze sposobem dostępu do tych usług,
- Umieszczenie opisu dotyczącego świadczonych usług na stronie WWW BIP (Biuletynu Informacji Publicznej),
- Publikacji opisu świadczonych usług na zasobie wskazanym przez ministra właściwego do spraw informatyzacji,
- Zapewnienie standardu w zakresie dokumentowania procesów i procedur dotyczących świadczonych usług.

W celu zapewnienia interoperacyjności na poziomie semantycznym stosuje się:

- Standaryzację w zakresie struktur danych i znaczenia danych zawartych w tych strukturach publikowanych w repozytorium interoperacyjności
- Opublikowana informacja w repozytorium interoperacyjności nie może być modyfikowana lub usunięta z repozytorium. W przypadku, gdy informacja podlega aktualizacji należy umieścić w repozytorium kolejną wersję przedmiotowej informacji.

W celu zapewnienia interoperacyjności na poziomie technologicznym stosuje się:

- Wymagania dla systemów teleinformatycznych uwzględnione w Polityce Bezpieczeństwa Teleinformatycznego,
- Wymagania w zakresie normy ISO 27001,
- Wymagania w zakresie zapewnienia ciągłości działania systemów teleinformatycznych.

Urząd Gminy Brudzeń Duży stosuje minimalne wymagania dla rejestrów publicznych i wymiany informacji w postaci elektronicznej zgodnie z wymaganiami rozdziału III Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności oraz wytycznych stanowiących załącznik nr 1 do Rozporządzenia.

Urzędu Gminy Brudzeń Duży w celu zapewnienia odpowiedniego bezpieczeństwa informacji zapewnia:

- Rozliczalność operacji w ramach, których następuje wymiana informacji z rejestru,
- Ochronę informacji pozyskanych od innych podmiotów na poziomie nie gorszym niż dane przechowywane we własnych rejestrach,
- Wymianę minimalnych informacji, które są niezbędne do świadczenia usług publicznych,
- Wymiana informacji odbywa się zgodnie ze strukturami referencyjnymi danych,
- Umieszczenie w repozytorium interoperacyjności niezbędnych opisów usług oraz ich schematów XML, a także innych wzorów jeżeli mają zastosowanie do prawidłowej interpretacji usługi.

Załącznik nr 3
do zarządzenia nr 60/25
z dnia 05.09.2025

GMINA
BRUDZEŃ DUŻY
MAZOWIECKA SZWAJCARIA

Polityka Bezpieczeństwa Teleinformatycznego w Urzędzie Gminy Brudzeń Duży

Wydanie 2.0

AKTUALIZACJA

Zatwierdził:

WÓJT GMINY
Brudzeń Duży
Michał Twardy

Wprowadzenie

Polityka Bezpieczeństwa Teleinformatycznego w Urzędzie Gminy Brudzeń Duży stanowi zestawienie zasad, praw i reguł oraz wytycznych i dobrych praktyk w zakresie zarządzania bezpieczeństwem teleinformatycznym oraz stanowi integralną część Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).

Polityka Bezpieczeństwa Teleinformatycznego w Urzędzie Gminy Brudzeń Duży została zaprojektowana oraz wdrożona zgodnie z dobrymi praktykami oraz następującymi regulacjami:

- 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 (Dz.U. 2017 poz. 2247),
- Norma PN-EN ISO/IEC 27001:2023 (Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – Systemy zarządzania bezpieczeństwem informacji - Wymagania),
- Norma PN-EN ISO/IEC 27002:2023 (Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – Zabezpieczanie informacji),
- Ustawa o Krajowym Systemie Cyberbezpieczeństwa z dnia 5 lipca 2018 roku.

Stosowanie zasad bezpieczeństwa określonych w niniejszym dokumencie ma na celu zapewnienie prawidłowej ochrony informacji przetwarzanych w systemach teleinformatycznych, jednocześnie przeciwdziałając zagrożeniom jakimi są:

- Udostępnianie danych osobom nieupoważnionym,
- Zmiana lub pozyskanie danych przez osobę nieuprawnioną,
- Przetwarzanie z naruszeniem przepisów,
- Utrata, uszkodzenie lub zniszczenie danych.

Zakres stosowania

Polityka Bezpieczeństwa Teleinformatycznego dotyczy wszystkich pracowników Urzędu Gminy Brudzeń Duży i podmiotów zewnętrznych wykonujących prace w infrastrukturze teleinformatycznej Urzędu Gminy Brudzeń Duży.

Kontrola dostępu do systemów teleinformatycznych

Identyfikacja i uwierzytelnianie się użytkowników w systemach teleinformatycznych:

- Danymi uwierzytelniającymi użytkownika w systemie teleinformatycznym są atrybuty jego konta: identyfikator i hasło,
- Konto jest jednoznacznie przyporządkowane do danego użytkownika,
- Konto użytkownika należy wykorzystywać wyłącznie do celów służbowych,
- Zabrania się stosowania kont przypisanych do więcej niż jednego użytkownika,
- Identyfikator danego użytkownika nie może być przypisany innemu użytkownikowi,
- Identyfikator konta zwykłego składa się z co najmniej 8 znaków,
- Identyfikator użytkownika wprowadzającego dane oraz data wykonania operacji na danych są automatycznie rejestrowane w dzienniku systemu operacyjnego.

System zarządzania hasłami:

- Hasła nie mogą być powszechnie używanymi słowami. Jako haseł nie należy wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, itp.
- W przypadku podejrzenia lub stwierdzenia ujawnienia hasła należy je niezwłocznie zmienić,
- Hasło do systemu teleinformatycznego należy przekazać użytkownikowi w sposób poufny,
- Początkowe hasło nadawane jest przy założeniu konta użytkownika w systemie teleinformatycznym,
- Użytkownik niezwłocznie po uzyskaniu hasła do systemu teleinformatycznego zobowiązany jest do jego zmiany,

Ograniczenie czasu trwania połączenia

W celu wymuszenia ochrony systemu teleinformatycznego w przypadku stwierdzenia braku aktywności użytkownika stosuje się następujące mechanizmy ochronne:

- Blokowanie lub wyłączanie stacji roboczej / sesji połączeniowej,
- Żądanie powtórnej identyfikacji i uwierzytelniania użytkownika,
- Powrót do stanu aktywności wymaga podania hasła,
- Czas braku aktywności użytkownika jest definiowany na poziomie każdego systemu teleinformatycznego.

Zarządzanie urządzeniami mobilnymi

W celu zapewnienia ochrony urządzeń mobilnych przyjęto następujące zasady:

- Urząd Gminy Brudzeń Duży prowadzi rejestr urządzeń mobilnych wraz z przypisanymi pracownikami,
- Każdy pracownik jest odpowiedzialny za wszystkie operacje prowadzone na zarejestrowanych urządzeniach mobilnych, które zostały mu powierzone,
- Każdy pracownik jest odpowiedzialny za ochronę urządzenia na okoliczność kradzieży,
- Zabronione jest udostępnianie urządzeń mobilnych innym osobą,
- Zabronione jest wykorzystywanie urządzeń mobilnych do celów prywatnych,
- Dostęp do urządzenia mobilnego typu smartfon jest zabezpieczony poprzez uwierzytelnianie użytkownika za pośrednictwem kodu PIN lub danych biometrycznych,
- W urządzeniach mobilnych typu smartfon wykorzystywane są zabezpieczeń kryptograficznych dostarczane przez producenta urządzenia mobilnego,
- Zabronione jest instalowanie przez aplikacji, które nie są wykorzystywane do obowiązków służbowych,

Kopie zapasowe

Organizacja wprowadziła i stosuje następujące zasady dotyczące kopii zapasowych:

- Instrukcja, o której mowa powyżej może stanowić zapis z konfiguracji systemów wykonujących kopie zapasowe opatrzony stosownym komentarzem i uzupełniony o niezbędne dla administratora zagadnienia,
- Okres przechowywania kopii zapasowych nie powinien być krótszy niż 24 miesiące,
- Kopie zapasowe powinny być przechowywane w pomieszczeniach szczególnie chronionych przed nieuprawnionym dostępem i szkodliwym wpływem środowiska. Zalecane jest przechowywanie kopii zapasowych w specjalnych sejfach,
- Każde testowe odtworzenie danych powinno być odnotowywane w dzienniku administracyjnym systemu teleinformatycznego.

Zarządzanie zmianami w systemach teleinformatycznych

Organizacja wprowadziła i stosuje następujące zasady w zakresie zarządzania zmianami w systemach teleinformatycznych:

- Przed dokonaniem zmiany, jeżeli ma to zastosowanie, należy wykonać kopię zapasową środowiska systemu teleinformatycznego (oprogramowania, konfiguracji i danych) celem umożliwienia, w przypadku wystąpienia problemów, powrotu do pierwotnego stanu systemu teleinformatycznego,
- Wszystkie modyfikacje powinny być przetestowane w środowisku testowym, w przypadku jego braku osoba odpowiedzialna za utrzymanie systemu teleinformatycznego zobowiązana jest do podjęcia wszelkich możliwych kroków pozwalających zapewnić bezawaryjną pracę systemu teleinformatycznego podczas wprowadzania zmian,
- Weryfikacja modyfikacji obejmuje sprawdzenie poprawności działania systemu, aktualizację dokumentacji oraz zabezpieczenie nowej (zmienionej) wersji środowiska teleinformatycznego,
- Przed produkcyjnym uruchomieniem system może zostać poddany testom bezpieczeństwa. Decyzja w zakresie testów bezpieczeństwa systemu powinna być uwarunkowana od jego krytyczności, wpływu na usługi, weryfikację czy system komunikuje się z siecią publiczną oraz wpływu systemu na inne zasoby teleinformatyczne organizacji. Wszystkie wymienione czynniki powinny zostać uwzględnione podczas analizy ryzyka systemu teleinformatycznego. Decyzja w zakresie konieczności przeprowadzenia testów bezpieczeństwa powinna wynikać z rekomendacji koordynatora bezpieczeństwa przy współpracy z właścicielem systemu, administratorem systemu oraz w oparciu o wyniki analizy ryzyka,
- Negatywny wynik testów bezpieczeństwa może być podstawą do wstrzymania produkcyjnego uruchomienia danego rozwiązania teleinformatycznego do czasu usunięcia usterek i podatności.

Obsługa nośników

Zarządzanie nośnikami wymiennymi:

- Nośniki informacji należy przechowywać i eksploatować zgodnie z zaleceniami producenta, z uwzględnieniem wymagań w zakresie ochrony informacji,
- Nośniki zawierające informacje wrażliwe należy przechowywać w specjalnych szafach zapewniających ochronę przed:
  - pożarem,
  - eksplozją towarzyszącą pożarowi,
  - działaniem gazów powstałych podczas pożaru,
  - zalaniem,
  - włamaniem,
  - działaniem pola elektromagnetycznego.

Wycofanie z eksploatacji nośników informacji:

- Wycofanie z eksploatacji wymiennych nośników informacji, przekazanie do naprawy lub ponownego użycia jest poprzedzone archiwizacją, a następnie skutecznym usunięciem zapisanych danych,
- Uszkodzone wymienne nośniki informacji zawierające informacje wrażliwe są niszczone w sposób uniemożliwiający odczytanie zapisanych na nich informacji.

Bezpieczeństwo dokumentacji systemowej:

- Ochronie podlega dokumentacja powykonawcza, techniczna, administratora i użytkownika,
- Dokumentacja systemów teleinformatycznych jest udostępniana na zasadzie „wiedzy koniecznej".

Zasady monitorowania w systemach teleinformatycznych

W celu zapewnienia monitorowania zdarzeń w systemach teleinformatycznych wykorzystywane są dzienniki zdarzeń (logi) generowane zgodnie ze specyfikacją danego systemu.

Ochrona informacji zawartych w dziennikach (logi) zdarzeń:

- Dzienniki należy objąć standardową procedurą tworzenia kopii zapasowych,
- Dzienniki należy utrzymywać i przechowywać dla wszystkich krytycznych systemów teleinformatycznych przez okres nie krótszy niż 24 miesiące,
- Dzienniki dla wszystkich systemów teleinformatycznych należy zabezpieczyć przed nieuprawnionym dokonywaniem zmian.

Dzienniki administracyjne:

- Dla każdego systemu teleinformatycznego lub grupy jednorodnych systemów teleinformatycznych ich administrator prowadzi dziennik, w którym odnotowywane są istotne zdarzenia związane z ich zarządzaniem,
- Dzienniki stanowią dowody audytowe i umożliwiają weryfikację poprawności realizacji procedur przez administratorów systemów teleinformatycznych, a także służą budowaniu bazy wiedzy,
- W dziennikach administracyjnych administrator odnotowuje:
  - nazwę lub identyfikator systemu teleinformatycznego,
  - datę i czas wpisu,
  - opis czynności lub zdarzenia,

- imię i nazwisko osoby, która dokonuje wpisu.

Synchronizacja zegarów:

Odpowiednią dokładność i możliwość korelacji dzienników zdarzeń należy zapewnić przez synchronizację zegarów urządzeń teleinformatycznych względem wzorcowego źródła czasu – wskazanego serwera NTP.

Ochrona przed szkodliwym oprogramowaniem

Organizacja wprowadziła i stosuje następujące środki bezpieczeństwa przed szkodliwym oprogramowaniem i wyciekom informacji:

- Zakaz korzystania z nieautoryzowanego oprogramowania na terenie całej organizacji,
- Zabezpieczenia wykrywające lub zapobiegające użyciu znanych szkodliwych stron WWW poprzez stosowanie tzw. ,,*black list*",
- Skanowanie za pośrednictwem oprogramowania antywirusowego załączników poczty elektronicznej oraz ściąganych danych pod kątem obecności szkodliwego oprogramowania,
- Przeprowadzanie regularnych przeglądów oprogramowania i danych zawartych w systemach obsługujących krytyczne procesy organizacji,
- Ręczna aktualizacja systemów operacyjnych na komputerach osobistych,
- Włączenie funkcji automatycznej aktualizacji oprogramowania antywirusowego,
- Wykonywanie kopii zapasowych danych znajdujących się na stacji przed przeprowadzeniem procedury aktualizacji oprogramowania,
- Skanowanie zewnętrznych nośników podłączanych do komputera za pośrednictwem oprogramowania antywirusowego,
- Zakaz podłączania nośników zewnętrznych, które nie są wykorzystywane do realizacji obowiązków służbowych przez pracowników Urzędu Gminy Brudzeń Duży.

Zasady eksploatacji systemów teleinformatycznych

Zasady ogólne:

- Wszelkie zmiany w konfiguracji sprzętu komputerowego wykonują wyznaczeni administratorzy,

- Zasoby teleinformatyczne Urzędu Gminy Brudzeń Duży podlegają ewidencjonowaniu i przypisaniu właścicieli tych zasobów, a także ewidencjonowaniu podlega wynoszenie sprzętu poza organizację,
- Uprawnienia do systemów teleinformatycznych mogą zostać nadane użytkownikowi, który posiada odpowiednie upoważnienia i uprawnienia do informacji jakie w danym systemie teleinformatycznym są przetwarzane,
- Uprawnienia uprzywilejowane do systemów teleinformatycznych powinni posiadać tylko i wyłącznie osoby na stanowiskach administratora danego systemu teleinformatycznego,
- Administrator systemu teleinformatycznego podczas codziennej pracy w systemach teleinformatycznych powinien używać konta standardowego, które nie posiada podwyższonych uprawnień,
- Uprawnienia uprzywilejowane powinny być wykorzystywane tylko i wyłącznie w sytuacjach zmian konfiguracyjnych systemów teleinformatycznych, do których takie uprawnienia są niezbędne,
- Wykorzystywanie uprawnień uprzywilejowanych powinno być rejestrowane w dziennikach zdarzeń systemu teleinformatycznego i umożliwiać przeprowadzenie audytu wykonywanych czynności,
- Uprawnienia do systemów teleinformatycznych dla firm zewnętrznych możliwe jest tylko i wyłącznie w sytuacji zabezpieczenia prawnego,
- Wszelkie działania firm zewnętrznych w infrastrukturze teleinformatycznej Urzędu Gminy Brudzeń Duży musi podlegać monitorowaniu oraz nadzorowaniu,
- W przypadku zakończenia współpracy z firmą zewnętrzną, administrator systemu zobowiązany jest do niezwłocznego odebrania uprawnień dla pracowników firmy zewnętrznej,
- Wszelkie działania zmierzające do niestabilności systemów teleinformatycznych oraz próby nieautoryzowanego podsłuchu ruchu w sieci teleinformatycznej są zabronione,
- Użytkownicy zobowiązani są do wykorzystywania przekazanego im oprogramowania zgodnie z warunkami licencji,
- Przekazywanie numerów seryjnych, kodów aktywacyjnych, kluczy zabezpieczających w celu nielegalnego zainstalowania bądź uruchomienia programu na innym komputerze jest zabronione,
- Zaleca się przetwarzanie i przechowywanie danych (w tym danych osobowych) na zasobach objętych systemem kopii zapasowych,
- Użytkownik ma obowiązek uniemożliwić podglądanie ekranu lub klawiatury przez osoby nieupoważnione,
- Kierownicy komórek organizacyjnych mają obowiązek bezzwłocznego wnioskowania o odebranie uprawnień do zasobów teleinformatycznych podległego im pracownika z powodu rozwiązania współpracy lub zmiany zakresu obowiązków, o ile nowe obowiązki pracownika nie wymagają posiadania wcześniej nabytych uprawnień,

- Zabronione jest pozostawianie komputerów przenośnych bez opieki w miejscach szczególnie narażonych na kradzież takich jak: samochód oraz w innych miejscach, gdzie pracownik nie ma możliwości sprawowania nad nim skutecznego nadzoru,
- Wszyscy pracownicy Urzędu Gminy Brudzeń Duży zobowiązani są do stosowania zasady tzw. ,,czystego biurka",
- Wszelkie informacje prawnie chronione umieszczone na komputerach przenośnych, należy przechowywać w postaci zaszyfrowanej,
- Użytkownicy korzystający z komputerów przenośnych mają zakaz ich udostępniania osobom trzecim,
- W razie utraty komputera przenośnego należy niezwłocznie poinformować przełożonego,
- W sytuacji kradzieży zdarzenie należy niezwłocznie zgłosić policji,
- Zagubienie / kradzież sprzętu wiąże się z wygenerowaniem incydentu bezpieczeństwa,
- Podczas zakończenia współpracy z Urzędem Gminy Brudzeń Duży, pracownik zobowiązany jest do zwrotu wszystkich aktywów powierzonych przez Urzędu Gminy Brudzeń Duży,
- W sytuacjach, gdy zmiany w środowiskach teleinformatycznych mogą wpływać na ciągłość działania usług, rekomenduje się wykorzystywanie oddzielnych środowisk testowych i produkcyjnych,
- Wszystkie audyty przeprowadzane w środowiskach teleinformatycznych Urzędu Gminy Brudzeń Duży muszą odbywać się z zapewnieniem ciągłości działania tych środowisk,
- Środowiska teleinformatyczne w Urzędzie Gminy Brudzeń Duży w zależności od przeznaczenia powinny zostać odseparowane na poziomie fizycznym lub logicznym w celu ochrony przez zagrożeniami i zapewnieniem ciągłości działania,
- W przypadku projektowania, wdrażania i rozwoju systemów teleinformatycznych, pracownicy Urzędu Gminy Brudzeń Duży oraz firmy zewnętrzne realizujące przedmiotowe prace na rzecz Urzędu zobowiązane są do stosowania niniejszej Polityki Bezpieczeństwa Teleinformatycznego, a także dobrych praktyk w zakresie zapewnienia odpowiedniego bezpieczeństwa,
- W przypadku wdrażania i rozwoju systemów teleinformatycznych w środowiskach testowych zarówno Urzędu Gminy Brudzeń Duży jak i firmy zewnętrznej zabrania się przetwarzania danych produkcyjnych. W celu weryfikacji funkcjonalności danego systemu powinny być wykorzystywane dane testowe tj. dane podlegające całkowitej anonimizacji lub maskowania, uniemożliwiające ich odtworzenie lub też dane fikcyjne wygenerowane na potrzeby danego systemu,
- Dostęp do kodów źródłowych jest ograniczony wyłącznie do osób zajmujących się tworzeniem oprogramowania lub uczestniczących przy tworzeniu oprogramowania przez firmę zewnętrzną.

Użytkownikom systemów teleinformatycznych zabrania się:

- Transferu danych do nieautoryzowanych przez Urząd Gminy Brudzeń Duży lokalizacji sieciowych, przetwarzanie ich w nieautoryzowanej publicznej chmurze obliczeniowej lub przesyłanie na prywatne adresy pocztowe,
- Korzystania z nieautoryzowanych portali społecznościowych, wykorzystując systemy teleinformatyczne należące do Urzędu Gminy Brudzeń Duży,
- Łączenia zasobów teleinformatycznych Urzędu Gminy Brudzeń Duży z obcymi systemami teleinformatycznym. Powyższe ograniczenie nie dotyczy przypadków, w których połączenie takie stanowi realizację stosownej umowy,
- Komentowania, umieszczania swoich opinii na forach internetowych, nieautoryzowanych portalach społecznościach z wykorzystaniem sprzętu służbowego,
- Wykorzystywania do celów służbowych zewnętrznej poczty elektronicznej w zakresie wysyłania i odbierania wiadomości i dokumentów,
- Drukowania, kopiowania i przetwarzania dokumentów niezwiązanych z obowiązkami służbowymi przy wykorzystaniu systemów teleinformatycznych należących do Urzędu Gminy Brudzeń Duży,
- Korzystania z serwisów internetowych niezwiązanych z pełnieniem obowiązków służbowych,
- Przetwarzania treści szkodliwych lub obraźliwych takich jak pornografia, przemoc, rasizm, terroryzm, środki odurzające itp.,
- Przetwarzania treści naruszających dobra osobiste osób trzecich,
- Przetwarzania treści naruszających prawa autorskie i pokrewne osób trzecich,
- Przetwarzanie danych zawierających szkodliwe oprogramowanie.

Niestosowanie się użytkownika do postanowień Polityki Bezpieczeństwa Teleinformatycznego może być podstawą do odebrania użytkownikowi uprawnień do pracy w systemach teleinformatycznych, niezależnie od innych sankcji przewidzianych w Kodeksie Pracy, Kodeksie Karnym i obowiązujących regulacjach wewnętrznych i zewnętrznych.

Obowiązki administratora systemów teleinformatycznych:

- Zapewnienie prawidłowego funkcjonowania, planowania, konserwacji oraz konfiguracji systemu teleinformatycznego,
- Nadzór nad oprogramowaniem instalowanym na stacjach użytkowników końcowych oraz ewidencjonowanie zgodności licencyjnych,
- Konserwację sprzętu teleinformatycznego zgodnie z zaleceniami producenta,
- Nadzór i kontrolę zmian w systemach teleinformatycznych, w tym monitorowanie zdarzeń w zakresie bezpieczeństwa infrastruktury teleinformatycznej,

- Nadzór nad standardem technologicznym wykorzystywanym w Urzędzie Gminy Brudzeń Duży, w tym również przygotowywanie wytycznych do postępowań zakupowych realizowanych przez Urząd Gminy Brudzeń Duży w zakresie zakupu nowej technologii,
- Nadawanie dostępu użytkownikom do systemu teleinformatycznego zgodnie z wytycznymi zawartymi we wniosku bezpośredniego przełożonego pracownika o nadanie dostępu do zasobów teleinformatycznych,
- Monitorowanie pojemności systemu teleinformatycznego, jego wydajności, a także odpowiednie planowanie w zakresie konieczności zwiększenia przedmiotowych parametrów w celu zapewnienia efektywnego i stabilnego funkcjonowania,
- Realizację przeglądu uprawnień w systemie teleinformatycznym, przy czym przegląd uprawnień nie powinien być wykonywany rzadziej niż raz w roku,
- Zarządzanie kontami technicznymi w systemach teleinformatycznych,
- Dokumentowanie procedur eksploatacyjnych,
- Prowadzenie dzienników administracyjnych systemów teleinformatycznych,
- Instalację oprogramowania w systemach produkcyjnych,
- Weryfikację podatności w systemach teleinformatycznych oraz w przypadku zidentyfikowania takich zdarzeń niezwłocznego podjęcia działań mających na celu ich wyeliminowanie,
- Przygotowanie sprzętu teleinformatycznego dla pracowników Urzędu Gminy Brudzeń Duży,
- W przypadku, gdy sprzęt teleinformatyczny wykorzystywany jest do ponownego użycia, administrator systemu odpowiedzialny jest za skuteczne usunięcie danych po poprzednim użytkowniku przed udostępnieniem zasobów nowemu pracownikowi,
- W przypadku, gdy sprzęt teleinformatyczny podlega wycofaniu z eksploatacji, administrator systemu odpowiedzialny jest za skuteczne usunięcie danych umieszczonych na zasobie teleinformatycznym poprzez wybranie odpowiedniej metody. W sytuacji, gdy sprzęt wycofany z eksploatacji będzie przekazywany do odsprzedaży lub udostępniany innym podmiotom, administrator zobowiązany jest do wymontowania ze sprzętu nośników danych, poddania nośników skutecznemu procesowi niszczenia lub też zarchiwizowania nośników w Urzędzie Gminy Brudzeń Duży,
- Prowadzi rejestr skutecznego usunięcia danych,
- Zarządzanie i nadzorowanie sieci w celu ochrony informacji w podłączonych do sieci systemach teleinformatycznych i aplikacjach,
- Aktualizację planów ciągłości działania oraz procedur odtworzeniowych.

Minimalne wymagania dla rejestrów publicznych i wymiany informacji w postaci elektronicznej

Zgodnie z Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej:

- Organizacja realizuje usługi elektroniczne wobec obywateli i innych podmiotów celem załatwiania spraw urzędowych w sposób elektroniczny za pomocą elektronicznej skrzynki podawczej (ESP) udostępnionej na platformie ePUAP,
- Organizacja zamieszcza na swojej głównej stronie WWW (BIP) odesłania do opisów usług, które zawierają wymagane informacje dotyczące:
    - Aktualnej podstawy prawnej świadczonych usług,
    - Nazwy usług, miejsca świadczenia usług (złożenia dokumentów),
    - Terminu składania i załatwiania spraw,
    - Nazwy komórek odpowiedzialnych za załatwienie spraw,
- Organizacja prowadzi listę świadczonych usług w formie elektronicznej,
- Organizacja zgodnie z ww. rozporządzeniem stosuje się do:
    - Zasad tworzenia i oznaczania metadanych opisujących wzór,
    - Trybu przekazywania wzorów dokumentów elektronicznych do centralnego repozytorium,
    - Sposobu oznaczania w pismach w postaci elektronicznej niezbędnych elementów struktury,
- Organizacja kompletuje i archiwizuje wnioski przekazania wzorów dokumentów elektronicznych do centralnego repozytorium wniosków dokumentacji elektronicznej (CRWDE) za pomocą elektronicznej skrzynki podawczej (ESP) udostępnionej na platformie ePUAP,
- Organizacja zapewnia pełną rozliczalność wymiany informacji oraz stosuje odpowiednie mechanizmy bezpieczeństwa opisane w niniejszym dokumencie,
- Organizacja udostępnia tylko niezbędne informacje wynikające z realizacji usług kanałami elektronicznymi.

Minimalne wymagania dla systemów teleinformatycznych

- Systemy teleinformatyczne wykorzystywane przez Urzżd Gminy Brudzeń Duży są projektowane, wdrażane oraz eksploatowane z uwzględnieniem ich funkcjonalności, niezawodności, używalności, wydajności, przenoszalności i pielęgnowalności z uwzględnieniem dobrych praktyk oraz Polskich Norm m.in. PN-ISO/IEC 20000-1 i PN-ISO/IEC 20000-2,
- Wszystkie usługi realizowane przez Urząd Gminy Brudzeń Duży za pośrednictwem systemów teleinformatycznych monitorowane są pod względem zachowania odpowiedniego poziomu dostępności w oparciu o obowiązującą dokumentację eksploatacyjną,
- Zasoby teleinformatyczne Urzędu Gminy Brudzeń Duży (sprzęt, oprogramowanie, protokoły komunikacyjne, szyfrujące) projektowane są i wdrażane zgodnie z najlepszymi praktykami w celu odpowiedniego zabezpieczenia przetwarzanych informacji. Podczas projektowania systemów zarówno pracownicy Urzędu Gminy Brudzeń Duży jak i firmy zewnętrzne zobowiązane są do weryfikacji standardów międzynarodowych takich jak m.in. Internet Engineering Task Force (IETF) i publikowane w postaci Request For Comments (RFC) oraz World Wide WebConsortium (W3C) i publikowane w postaci W3C Recommendation (REC).
- Organizacja stosuje kodowanie znaków według standardu Unicode UTF-8 lub/oraz UTF-16 w dokumentach wysyłanych z systemu teleinformatycznego (także w odniesieniu do informacji wymienianej przez te systemy z innymi systemami na drodze teletransmisji). W przypadku systemów z rodziny Windows dopuszcza się normy zamienne, kompatybilne ze standardem UTF-8.
- System teleinformatyczny organizacji udostępnia zasoby informacyjne co najmniej w jednym z formatów danych określonych w załączniku nr 2 (formaty danych oraz standardy zapewniające dostęp do zasobów informacji udostępnianych za pomocą systemów teleinformatycznych używanych do realizacji zadań publicznych) do Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2017 poz. 2247).
- System teleinformatyczny organizacji umożliwia przyjmowanie dokumentów elektronicznych służących do załatwiania spraw należących do zakresu działania podmiotu w formatach danych określonych w załącznikach nr 2 (formaty danych oraz standardy zapewniające dostęp do zasobów informacji udostępnianych za pomocą systemów teleinformatycznych używanych do realizacji zadań publicznych) i 3 (formaty danych obsługiwane przez podmiot realizujący zadanie publiczne w trybie odczytu) do Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2024 r. poz. 307)),

- W projektowanych i wdrażanych systemach teleinformatycznym służących prezentacji zasobów informacji należy zapewnić spełnienie przez ten system wymagań Web Content Accessibility Guidelines (WCAG 2.0), z uwzględnieniem poziomu AA,
- Każdy system teleinformatyczny wraz z wykorzystywanym sprzętem oraz konfiguracją podlega obowiązkowemu ewidencjonowaniu i przypisaniu właściciela,
- Konfiguracje sprzętu, oprogramowania, usług i sieci są rejestrowane, a wszystkie zmiany konfiguracji są prowadzone w rejestrze.
- Wszelkie zmiany w konfiguracjach są monitorowane i są przeglądane w celu weryfikacji właściwych ustawień konfiguracji, oceny siły haseł i oceny wykonanych działań,
- Każdy system teleinformatyczny podlega analizie ryzyka w zakresie utraty poufności, integralności oraz dostępności przetwarzanych informacji, a następnie wprowadzane są działania mające na celu mitygację zidentyfikowanych ryzyk,
- Każdy system teleinformatyczny musi zapewniać ochronę informacji przed kradzieżą, nieuprawnionym dostępem, uszkodzeniem lub zakłóceniem przez monitorowanie dostępu do informacji, wykrywanie nieautoryzowanych działań związanych z przetwarzaniem informacji oraz zapewnienia środków uniemożliwiających nieautoryzowany dostęp do zasobów teleinformatycznych Urzędu Gminy Brudzeń Duży,
- Zapewnienie cyklicznej aktualizacji oprogramowania, w tym aktualizacji poprawek bezpieczeństwa,
- Minimalizacja ryzyk związanych z awariami poprzez stosowanie szeregu działań opisanych w ramach Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Gminy Brudzeń Duży m.in. ciągłość działania, dokumentacja eksploatacyjna, kopie zapasowe, odpowiednie zarządzanie i modyfikacja systemów teleinformatycznych,
- Cykliczna realizacja testów bezpieczeństwa systemów teleinformatycznych w zakresie identyfikacji podatności systemowych oraz zgodności z normami o dobrymi praktykami,
- Systemy teleinformatyczne wykorzystywane do realizacji zadań publicznych powinny posiadać opis protokołów i struktur wymiany danych usług sieciowych zgodnie z Web Services Description Language (WSDL),
- Powyżej wymieniony opis powinien zostać umieszczony w centralnym repozytorium wniosków dokumentacji elektronicznej (CRWDE).

Mechanizmy kryptograficzne

Mechanizmy kryptograficzne będące sposobem wykorzystania technik lub algorytmów kryptograficznych, wykorzystywane są w celu realizacji bezpieczeństwa pod względem:

- Poufności,
- Integralności,
- Uwierzytelniania,

- Niezaprzeczalności,
- Kontroli dostępu,
- Rozliczalności i audytu.

Właściciel systemu teleinformatycznego jest odpowiedzialny za określenie usług danego systemu teleinformatycznego oraz wraz z administratorem systemu dobór narzędzi i mechanizmów kryptograficznych umożliwiających zapewnienie adekwatnych mechanizmów bezpieczeństwa.

Cykl życia kluczy i certyfikatów wykorzystywanych w narzędziach kryptograficznych musi uwzględniać:

- Sposób generowania,
- Sposób użytkowania,
- Kopia bezpieczeństwa w tym odzyskiwanie,
- Wymiana i odnowienie,
- Odwołanie i wycofanie z użytku,
- Klucze i certyfikaty powinny mieć określony okres użytkowania, jednak nie dłuższy niż 24 miesiące,
- Klucze oraz certyfikaty muszą być generowanie z wykorzystaniem algorytmów, które nie zostały skompromitowane i ich długość odpowiada standardom i dobrym praktyką.
- W przypadku wykorzystywania algorytmu AES minimalna długość klucza powinna wynosić 128 bit. Jeżeli istnieją możliwości techniczne rekomendowana długość klucza wynosi 256 bit.
- W przypadku wykorzystania algorytmu RSA minimalna długość klucza powinna wynosić 1024 bit. Jeżeli istnieją możliwości techniczne rekomendowana długość klucza wynosi 2048 bit.

Zasady wykorzystywania poczty elektronicznej

- Użytkownicy, którzy posiadają dostęp do służbowej poczty elektronicznej zobowiązani są do zachowania należytej staranności w zakresie zachowania poufności, integralności oraz dostępności informacji,
- Wymiana informacji szczególnie chronionych (w tym danych osobowych) powinna odbywać się z wykorzystaniem metod szyfrowania np. poprzez wymianę kluczy kryptograficznych lub wykorzystania mechanizmów szyfrujących wbudowanych w oprogramowanie archiwizujące np. 7-ZIP,
- W przypadku szyfrowania załączników z wykorzystaniem oprogramowania 7-ZIP lub podobnego, użytkownik zobowiązany jest do przekazania hasła dostępu do zaszyfrowanego pliku innym kanałem komunikacji niż poczta e-mail,

- Użytkownicy zobowiązani są do wykorzystywania poczty elektronicznej tylko i wyłącznie do realizacji zadań służbowych,
- Użytkownicy poczty elektronicznej w celu ochrony przed atakami cybernetycznymi typu phishing powinni odbyć szkolenie z bezpieczeństwa teleinformatycznego oraz zachować szczególną ostrożność w zakresie korespondencji otrzymanej z podejrzanych domen, korespondencji zawierającej błędy językowe lub też podejrzane załączniki,
- W przypadku podejrzenia, że otrzymana wiadomość może stanowić atak phishingowy, użytkownik zobowiązany jest to powiadomienia o tym fakcie koordynatora bezpieczeństwa oraz administratora systemu teleinformatycznego,
- Koordynator bezpieczeństwa wspólnie z administratorem systemu informatycznego przeprowadzają weryfikację korespondencji pod względem potencjalnych zagrożeń bezpieczeństwa.

Zasady publikacji informacji na stronie WWW

- Publikacja informacji na stronie WWW może być realizowana tylko i wyłącznie przez pracowników Urzędu Gminy Brudzeń Duży do tego uprawnionych,
- Publikacja informacji musi zapewniać pełną rozliczalność tj. zawierać kompletną informację kto dokonał publikacji, w jakim zakresie oraz kiedy czynność została zrealizowana,
- W celu publikacji informacji na stronie WWW konieczne jest wykorzystywanie mechanizmów uwierzytelniających (login i hasło),
- Wytyczne w zakresie złożoności loginu i hasła, a także przypisania danych uwierzytelniających do pracownika Urzędu Gminy Brudzeń Duży zostały określone w rozdziale 3 dotyczącym kontroli dostępu do systemów teleinformatycznych,
- Wszelkie informacje przed publikacją powinny zostać zweryfikowane w zakresie kompletności oraz poufności,
- W sytuacji opublikowania informacji, która nie stanowi informacji publicznej, zdarzenie takie należy zakwalifikować jako incydent bezpieczeństwa oraz obsłużyć zgodnie z obowiązującymi regulacjami.

Bezpieczeństwo systemów teleinformatycznych

- Wszystkie systemy teleinformatyczne i komponenty wchodzące w ich skład podlegają ewidencjonowaniu,
- W ewidencji systemów teleinformatycznych należy uwzględniać nazwę komponentu, datę aktualizacji, wersję oraz właściciela,

- Każdy system teleinformatyczny uwzględniony w ewidencji podlega monitorowaniu przez administratora systemu w zakresie pojawienia się informacji o podatnościach bezpieczeństwa,
- Monitorowanie, o którym mowa powyżej może odbywać się z wykorzystaniem m.in. informacji od producenta rozwiązania w postaci komunikatów, bazy znanych podatności CVE, skanerów podatności,
- W przypadku zidentyfikowania podatności bezpieczeństwa, administrator systemu niezwłocznie informuje właściciela systemu oraz wspólnie ustalają termin zaimplementowania poprawek bezpieczeństwa. Jeżeli jest to możliwe i nie wpływa na ciągłość działania usług, poprawki bezpieczeństwa powinny zostać zaimplementowane natychmiast,
- Czynności dotyczące implementacji poprawek bezpieczeństwa powinny zostać uwzględnione w dzienniku administracyjnym danego systemu teleinformatycznego,
- Każdy pracownik Urzędu Gminy Brudzeń Duży w momencie zidentyfikowania podatności w systemach teleinformatycznych zobowiązany jest do powiadomienia o tym fakcie administratora lub właściciela systemu,
- Każdy system teleinformatyczny wykorzystywany do świadczenia usług publicznych podlega audytowi bezpieczeństwa nie rzadziej niż raz na 24 miesiące,
- Administrator systemu zobowiązany jest do uwzględnienia w dokumentacji eksploatacyjnej systemu wytycznych w zakresie bezpieczeństwa systemu, zarządzania podatnościami w danym systemie, bezpieczeństwo fizyczne i kontrolę dostępu do systemu, plan ciągłości działania i jego wpływ na świadczone usługi,
- Dokumentacja, o której mowa powyżej musi być przechowywania minimum przez 24 miesiące od dnia jej wycofania lub zastąpienia nowszą wersją,
- Każdy system teleinformatyczny wykorzystywany do świadczenia usług publiczny powinien zostać objęty monitorowaniem w trybie ciągłym,
- Pracownicy Urzędu Gminy Brudzeń Duży wykorzystujący w ramach obowiązków służbowych systemy teleinformatyczne powinni odbyć szkolenie w zakresie bezpiecznego wykorzystywania systemów i cyberzagrożeń z nimi związanych.

Załącznik nr 1 – Ewidencja kopii zapasowych

L.P	Oznaczenie systemu/ zbioru danych	Określenie procesu archiwizacji (oprogramowanie automatyczne/ kopia ręczna)	Określenie nośnika, na którym wykonano kopię awaryjną	Nazwisko i imię osoby sporządzającej kopię	Data	Podpis	Uwagi

Załącznik nr 4
do zarządzenia nr 60/25
z dnia 05.09.2025

GMINA BRUDZEŃ DUŻY MAZOWIECKA SZWAJCARIA

Metodyka szacowania i postępowania z ryzykiem w obszarze bezpieczeństwa informacji w Urzędzie Gminy Brudzeń Duży

Wydanie 2.0

AKTUALIZACJA

Zatwierdził:

WÓJT GMINY
Brudzeń Duży
Michał Twardy

Wprowadzenie

Niniejszy dokument określa metodykę szacowania oraz postępowania z ryzykami związanymi z przetwarzaniem informacji w Urzędzie Gminy Brudzeń Duży, zgodnie z normą PN-ISO/IEC 27001:2023, rozdziały 6.1.2, 6.1.3, 8.2 oraz 8.3

Metodyka szacowania i postępowania z ryzykiem w Urzędzie Gminy Brudzeń Duży została zaprojektowana oraz wdrożona zgodnie z dobrymi praktykami oraz następującymi regulacjami:

- Norma PN-ISO/IEC 27001:2023 Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – Systemy zarządzania bezpieczeństwem informacji – Wymagania,
- Norma PN-ISO/IEC 27005 Technika Informatyczna, Techniki bezpieczeństwa, Zarządzanie ryzykiem w bezpieczeństwie informacji,
- Norma PN-ISO 31000 Zarządzanie ryzykiem, Zasady i wytyczne,
- Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r. poz. 1560 z późn. zm.),
- 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 (ogólne rozporządzenie o ochronie danych) - stosowane od dnia 25 maja 2018 r.

Dokumenty powiązane:

- Polityka Bezpieczeństwa Informacji w Urzędzie Gminy Brudzeń Duży
- Polityka Bezpieczeństwa Teleinformatycznego Urzędzie Gminy Brudzeń Duży
- Deklaracja Stosowania Zabezpieczeń.

Definicje

Aktywa informacyjne to wszelkie urządzenia, oprogramowanie, informacje czy elementy infrastruktury, które mają znaczenie dla organizacji i wpływają na bezpieczeństwo informacji,

Poufność informacji - właściwość zapewniająca, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom,

Integralność informacji - właściwość polegająca na zapewnieniu dokładności i kompletności informacji,

Dostępność informacji - właściwość bycia dostępnym i możliwym do wykorzystania na żądanie w założonym czasie, przez autoryzowany podmiot,

Polityka Bezpieczeństwa Informacji - zbiór reguł i procedur określających organizację i zarządzanie bezpieczeństwem informacji w Urzędzie,

SZBI - część całościowego systemu zarządzania, oparty na podejściu wynikającym ze zidentyfikowanego ryzyka, odnoszący się do ustanawiania, wdrażania, eksploatacji, monitorowania,

Ryzyko - kombinacja następstw zdarzenia bezpieczeństwa informacji i związanego z nim prawdopodobieństwa wystąpienia,

Ryzyko w bezpieczeństwie informacji – sytuacja, w której określone zdarzenie może wykorzystać podatność (słabość) aktywów powodując szkodę w organizacji,

Ryzyko szczątkowe – ryzyko pozostające po zastosowaniu działań określonych w postępowaniu z ryzykiem,

Wpływ ryzyka – potencjalne skutki materializacji ryzyka, które mogą wpłynąć na obszar finansowy, strategiczny, operacyjny lub prawno-regulacyjny. Przy wycenie istotności ryzyka brana jest pod uwagę wycena finansowego wpływu,

Prawdopodobieństwo wystąpienia ryzyka - częstotliwość występowania zdarzenia objętego ryzykiem;

Postępowanie z ryzykiem – proces modyfikacji ryzyka,

Incydent - pojedyncze niepożądane lub niespodziewane zdarzenie związane z bezpieczeństwem informacji lub seria takich zdarzeń, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji,

Istotność ryzyka - kombinacja wpływu ryzyka i prawdopodobieństwa jego wystąpienia,

Właściciel ryzyka – osoba w organizacji, której przypisano własność ryzyka. Odpowiada za plan działań i ograniczenie wystąpienia ryzyka,

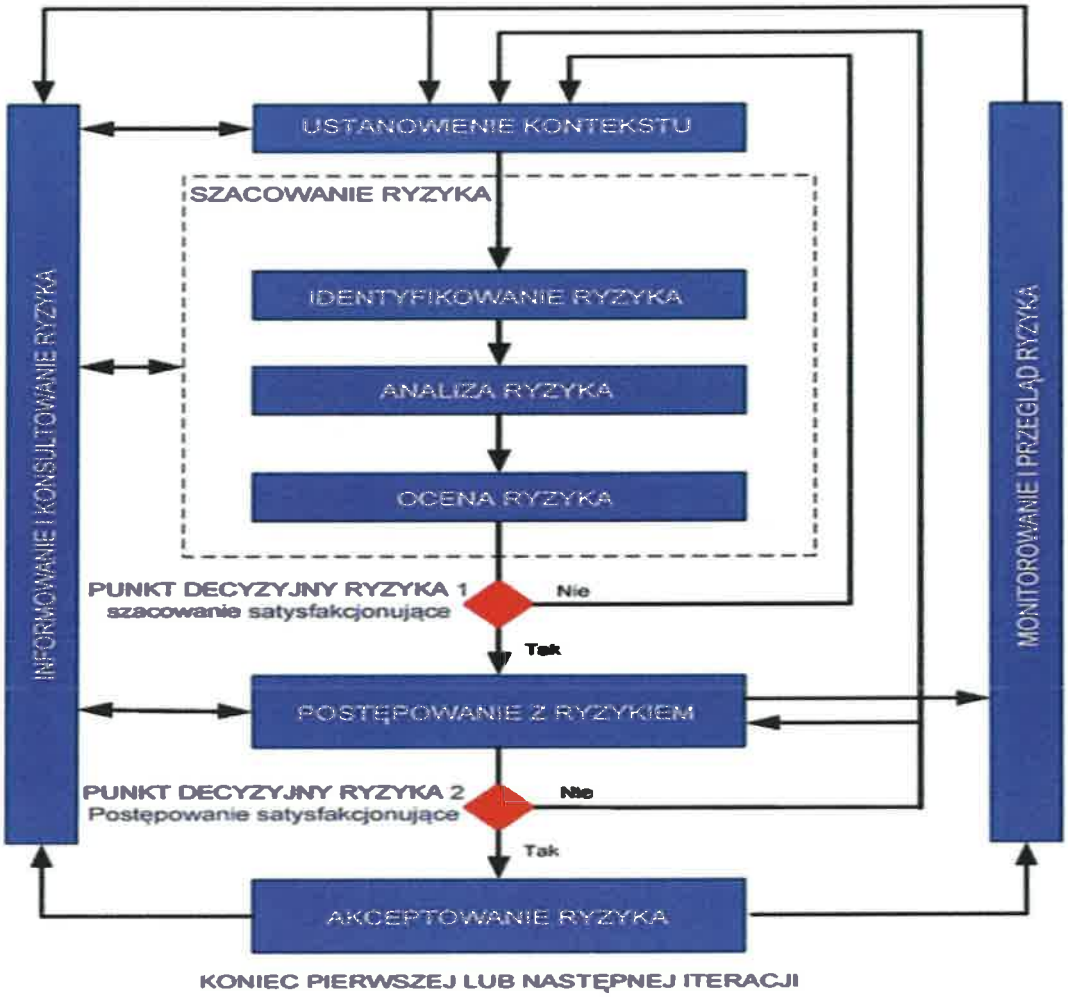
Zarządzanie ryzykiem – skoordynowane działania dotyczące kierowania i nadzorowania organizacji w odniesieniu do ryzyka.

Proces zarządzania ryzykiem

Proces zarządzania ryzykiem w bezpieczeństwie informacji w Urzędzie Gminy Brudzeń Duży składa się z:

- ustanowienia kontekstu,

- szacowania ryzyka,
- postępowania z ryzykiem,
- akceptowania ryzyka,
- monitorowania i przeglądu ryzyka.



Rys 1. Etapy procesu zarządzania ryzykiem wg Normy PN-ISO/IEC 27005:2014-01

Zakres i granice procesu zarządzania ryzykiem

Proces zarządzania ryzykiem w bezpieczeństwie informacji w Urzędzie Gminy Brudzeń Duży jest stosowany w całej organizacji i obejmuje wszystkie aktywa informacyjne Urzędu.

Określając zakres i granice zarzadzania ryzykiem organizacja wzięła pod uwagę:

- cele realizowane przez Urząd Gminy Brudzeń Duży,
- Wymagania prawne i kontraktowe,
- Obowiązującą w Urzędzie Gminy Brudzeń Duży Politykę Bezpieczeństwa Informacji,
- Aktywa informacyjne,
- Kontekst zewnętrzny i wewnętrzny organizacji i oczekiwania stron zainteresowanych.

Użytkownikami niniejszego dokumentu są wszyscy pracownicy Urzędu Gminy Brudzeń Duży, którzy biorą udział w szacowaniu ryzyka oraz postępowaniu z ryzykiem.

Cele zarządzania ryzykiem

Celem zarządzania ryzykiem w Urzędzie Gminy Brudzeń Duży jest:

- Wsparcie SZBI,
- Zgodność z prawem oraz poświadczenie należytej staranności,
- Zwiększenie prawdopodobieństwa realizacji zadań i osiągania celów Urzędu Gminy Brudzeń Duży,
- Uzyskanie bezpieczeństwa informacji, w tym danych osobowych;
- Minimalizacja skutków wpływy incydentów na działalność Urzędu Gminy Brudzeń Duży.

Kontekst zewnętrzny i wewnętrzny Urzędu

Kontekst działalności Urzędu Gminy Brudzeń Duży stanowią strony i ich oczekiwania. Kontekst działalności jest podstawą do ustalenia kryterium dla oceny ryzyka. Kontekst wraz z dokonaną klasyfikacją zasobów informacyjnych stanowią punkt wyjściowy do identyfikacji ryzyk oraz wynikających z nich zagrożeń.

Kontekst zewnętrzny

- Mieszkańcy Gminy - oczekiwanie sprawnego działania urzędu, racjonalne kosztowo realizowanie zadań administracji publicznej,
- Urząd Gminy Brudzeń Duży– sprawna realizacja zadań powierzonych urzędowi,

- Urząd Marszałkowski, Urząd Wojewódzki - sprawna realizacja powierzonych zadań administracyjnych,
- Instytucje publiczne regulujące pracę administracji (Krajowe Biuro Wyborcze, Główny Urząd Statystyczny, itp.) - sprawna realizacja zadań powierzonych Urzędowi,
- Jednostki organizacyjne: własne (szkoły, przedszkole, dom kultury, GOPS, świetlica środowiskowa, biblioteka, spółki gminne) - wsparcie dla własnych jednostek organizacyjnych,
- Organizacje pozarządowe na terenie gminy - wsparcie dla działalności organizacji, patronat.

Kontekst wewnętrzny

- Rada Urzędu Gminy Brudzeń Duży - realizacja zadań Urzędu wynikających ze statutu oraz uchwał Rady, nadzorowanie pracy Burmistrza oraz podległych mu jednostek organizacyjnych,
- Burmistrz i kadra Kierownicza Urzędu Gminy Brudzeń Duży - bezpieczeństwo zasobów informacyjnych, unikanie i zapobieganie incydentom bezpieczeństwa informacji,
- Pracownicy Urzędu Gminy Brudzeń Duży - bezpieczeństwo pracy użytkowników, dostępność środków wymiany informacji, uzyskiwanie informacji na poziomie umożliwiającym sprawne realizowanie powierzonych zadań,
- Systemy wsparcia informacji - sprawna infrastruktura telekomunikacyjna i teleinformatyczna zapewniająca bezpieczne i sprawne przekazywanie danych między aplikacjami i bazami danych a terminalami,
- Obsługa informatyczna – zapewnienie wsparcia informatycznego pracowników w realizacji obowiązków służbowych.

Wymagania prawne i regulacyjne mające zastosowanie w Urzędzie

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. 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),
- Ustawa z dnia 10 maja 2018 o ochronie danych osobowych,
- 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 (Dz.U. 2017 poz. 2247),
- Ustawa z dnia 27 sierpnia 2009 roku o finansach publicznych (Dz. U. z 2017 r. poz. 2077),

- Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U. z 2017 r. poz. 1875, ze zm.)

Odpowiedzialność i uprawnienia

W celu zapewnienia aktualności obowiązującej dokumentacji, zgodności z wymaganiami regulacyjnymi oraz nadzoru nad zapisami przyjmuje się następujący podział ról i odpowiedzialności:

1. Wójt Urzędu Gminy Brudzeń Duży:
    - Zatwierdza Metodykę,
    - Określa poziom ryzyka, powyżej którego należy rozpocząć działania zapobiegające ryzyku.

2. Właściciel ryzyka:
    - Odpowiada za zarządzanie ryzykiem w nadzorowanym przez siebie obszarze,
    - Odpowiada za przypisaną grupę aktywów i szacują ryzyko utraty poufności, integralności, dostępności aktywów,
    - Odpowiada za utrzymanie ryzyka zgodnie z określonym poziomem tolerancji,
    - Odpowiada za monitorowanie czynników i skutków ryzyka, jego istotności oraz skuteczności stosowanych mechanizmów kontrolnych ryzyka,
    - Podejmuje działania zaradcze w stosunku do zasobów, którymi zarządza,
    - Monitoruje poziom ryzyka.

3. Koordynator Bezpieczeństwa:
    - Koordynuje prace w zakresie zarządzania ryzykiem,
    - Odpowiada za wdrożenie, realizację i nadzór nad niniejszą procedurą,
    - Prowadzi Rejestr ryzyk,
    - Aktualizuje dokumentację wraz z zapewnieniem kontroli wersji,
    - Zapewnia udostępnienie dokumentu i stronom zainteresowanym.

Szacowanie ryzyka

Celem procesu szacowania ryzyka jest określenie co może się zdażyć i spowodować potencjalną stratę. Organizacja identyfikuje źródła ryzyka, obszary wpływów, zdarzenia oraz ich przyczyny i potencjalne następstwa. Analizowane są zdarzenia mające negatywny wpływ na osiąganie celów Urzędu Gminy Brudzeń Duży.

Szacując ryzyko Urząd Gminy Brudzeń Duży:

- Określa wartość aktywów informacyjnych,
- Identyfikuje zagrożenia,
- Identyfikuje istniejące podatności,
- Określa ryzyka w bezpieczeństwie informacji, związane z utratą poufności, integralności i dostępności informacji, z uwzględnieniem wpływu istniejących zabezpieczeń,
- Określa prawdopodobieństwo wystąpienia ryzyka oraz skutki jego zmaterializowania się.
- Identyfikuje właścicieli ryzyka,
- Ustanawia i utrzymuje kryteria ryzyka w bezpieczeństwie informacji,
- Zapewnia porównywalność wyników w kolejnych szacowaniach ryzyka,

Proces szacowania ryzyka jest koordynowany przez Koordynatora Bezpieczeństwa.

Wyniki szacowania ryzyka są podstawa do określenia właściwych opcji postępowania z ryzykiem oraz wyboru adekwatnych zabezpieczeń.

Stosowane przez Urzędu Gminy Brudzeń Duży zabezpieczenia zostały określone w Deklaracji Stosowania.

Dla działań szacowania i postępowania z ryzykiem w Urzędzie Gminy Brudzeń Duży stosuje się podejście iteracyjne, polegające na zwiększeniu szczegółowości analizy w każdej iteracji.

Identyfikacja aktywów

Urząd Gminy Brudzeń Duży identyfikuje wszystkie zasoby / aktywa związane z procesami funkcjonującymi w Urzędzie, czyli wszystkie aktywa, które mogą wpływać na poufność, integralność i dostępność informacji w Urzędzie Gminy Brudzeń Duży.

Aktywa informacyjne to wszelkie urządzenia, oprogramowanie, informacje czy elementy infrastruktury, które mają znaczenie dla danej organizacji i wpływ na bezpieczeństwo informacji.

1) Aktywa podstawowe:
   - Procesy i działania biznesowe, których utrata lub pogorszenie uniemożliwia wypełnienie misji organizacji,
   - Procesy zawierające poufne informacje,
   - Procesy mające na celu osiągnięcie zgodności z wymaganiami prawnymi lub umownymi,
   - Informacje wrażliwe, w tym dane osobowe.
2) Aktywa wspierające:
   - Sprzęt (np. laptop, serwer, komputer, drukarka, dysk wymienny, nośniki danych),

- Oprogramowanie (np. aplikacje, oprogramowanie systemowe),
- Sieć (media, urządzenia telekomunikacyjne),
- Personel,
- Siedziba (lokalizacja, budynki, linie telefoniczne, usługi komunalne i techniczne,
- Organizacja (struktura organizacyjna, dostawcy).

W klasyfikacji uwzględnia się kto jest właścicielem danego zasobu informacyjnego.

Analizując wartość zasobów informacyjnych dla organizacji, bierze się pod uwagę przetwarzane informacje objęte zakresem ustanowionego SZBI.

Klasyfikacja informacji

Informacje przetwarzane w Urzędzie Gminy Brudzeń Duży klasyfikowane są w następujących grupach:

Informacje publiczne (przeznaczone dla wszystkich):

- Informacje udostępniane na stronach internetowych Urzędu Gminy Brudzeń Duży,
- Informacje opracowywane na potrzeby działań marketingowych

Informacje wewnętrzne (przeznaczone wyłącznie dla pracowników):

- Informacje przetwarzane przez podmioty zewnętrzne (np. firmy telekomunikacyjne, dostawców mediów),
- Chronione informacje wewnętrzne organizacji, których ujawnienie nie wiąże się z sankcjami karnymi lub odszkodowawczymi, jednak może wiązać się z niewielkimi stratami firmy,
- Zasoby zgromadzone na dyskach sieciowych poszczególnych jednostek organizacyjnych,
- Zawartość korespondencji e-mailowej zgromadzonej w skrzynkach pocztowych,
- Dokumentacja papierowa zgromadzona w pomieszczeniach Urzędu Gminy Brudzeń Duży,
- Dane zawarte w systemach informatycznych.

Informacje poufne (przeznaczone wyłącznie dla wybranego grona osób):

- Informacje chronione artykułem 27 Ustawy o ochronie danych osobowych (tzw. dane wrażliwe),
- Informacje objęte tajemnicą, wynikającą z innych aktów prawnych (np. ordynacji podatkowej, tajemnicy bankowej, tajemnicy przedsiębiorstwa I pozostałych),
- Informacje, których ujawnienie może wiązać się z sankcjami karnymi lub odszkodowawczymi oraz mogą zagrozić funkcjonowaniu Urzędu Gminy Brudzeń Duży (faktury, dane przetwarzane w dziale

księgowości, dane kadrowe, osobowe, dane związane z utrzymaniem systemów teleinformatycznych).

Identyfikacja zagrożeń

Zagrożenia mogą stanowić przyczynę utraty poufności, integralności, dostępności aktywów oraz zagrażać realizacji poszczególnych celów i zadań realizowanych przez Urząd Gminy Brudzeń Duży i Jednostki Organizacyjne.

W Urzędzie Gminy Brudzeń Duży identyfikuje się zagrożenia dla każdego aktywu. Niektóre zagrożenia mogą odnosić się do różnych aktywów.

Zagrożenia można przyporządkować do obszarów:

- zagrożenia ludzkie - wynikające z działania czynnika ludzkiego, mające wpływ na bezpieczeństwo systemu teleinformatycznego Urzędu Gminy Brudzeń Duży,
- zagrożenia naturalne - zjawiska klimatyczne, pogodowe,
- zagrożenia techniczne - awarie urządzeń, niewłaściwe funkcjonowanie komponentów.

Lista typowych zagrożeń wraz z identyfikacją typów źródeł znajduje się w Zał. Nr.1

Zasady oceny wpływu ryzyka

Określenie wpływu ryzyka polega na określeniu przewidywanych skutków jakie będzie miało wystąpienie zdarzenia objętego ryzykiem dla realizacji zadania lub osiągania celu działania Urzędu Gminy Brudzeń Duży. W tym celu dokonuje się oceny następstwa (wpływu) w skali 1-5 dla każdego z zagrożonych aktywów. Do określenia wpływu używany jest opis jakościowy przy zastosowaniu skali ocen: wysoki, poważny, średni, mały, nieznaczny, zgodnie z opisem w Tabeli nr.1.

Efektem przeprowadzonej analizy zagrożeń jest lista aktywów i ich wartości w odniesieniu do ujawnienia (zachowanie poufności), modyfikacji (zapewnienie integralności, niedostępności).

Jako podstawę do wartościowania aktywów przyjęto koszty poniesione w wyniku utraty poufności, integralności i dostępności następstw incydentu.

Tabela nr. 1 Wpływ zagrożenia na aktywa

Wpływ zagrożenia	Odpowiednik punktowy	Skutek
Wysoki	5	Brak realizacji zadania i brak realizacji celu, bardzo poważne i rozległe konsekwencje prawne, naruszenie bezpieczeństwa pracowników (ujemne konsekwencje dla zdrowia i życia pracowników), wysokie straty finansowe, utrata dobrego wizerunku Gminy. (Wysoka strata finansowa – powyżej 1% budżetu Gminy)
Poważny	4	Poważny wpływ na realizacje zadania w tym poważne zagrożenie terminu jego realizacji i osiągniecia celu, poważne konsekwencje prawne, zagrożenie bezpieczeństwa pracowników, poważne straty finansowe, poważny wpływ na wizerunek Gminy (Poważny skutek finansowy – od 0,5% do 1% budżetu Gminy)
Średni	3	Średni wpływ na realizację zadań i celów, umiarkowane konsekwencje prawne, średni skutek finansowy, brak wpływu na bezpieczeństwo pracowników, średni wpływ na wizerunek Gminy. (Średni skutek finansowy – od 0,2% do 5% budżetu Gminy)
Mały	2	Mały wpływ na realizację celów i zadań, bez skutków prawnych, mały skutek finansowy, brak wpływu na bezpieczeństwo pracowników, niewielki wpływ na wizerunek Gminy. (Mały skutek finansowy – od 0,1% do 0,2% budżetu Gminy)
Nieznaczny	1	Znikomy wpływ na realizację zadań i celów, brak skutków prawnych, nieznaczny skutek finansowy, brak wpływu na bezpieczeństwo pracowników, brak wpływu na wizerunek Gminy. (Nieznaczny skutek finansowy do 0,1 % budżetu Gminy)

Analiza prawdopodobieństwa wystąpienia zagrożenia

Każde z ocenianych zagrożeń dla grup informacji/aktywów jest oceniane pod kątem prawdopodobieństwa wystąpienia. Skala oceny jest pięciostopniowa (od bardzo niskiego do bardzo wysokiego). Kryteria oceny określono w Tabeli nr. 2 - Tabela oceny prawdopodobieństwa. Prawdopodobieństwo wystąpienia zagrożenia są oceniane uwzględniając funkcjonujące zabezpieczenia.

Przy szacowaniu prawdopodobieństwa wystąpienia danego zagrożenia są brane pod uwagę:

- statystyki wystąpienia takich zdarzeń,
- motywację i zasoby dostępne dla atakujących,
- czynniki geograficzne,
- atrakcyjność i podatność aktywów,
- istniejące zabezpieczenia i ich skuteczność.

W Urzędzie Gminy Brudzeń Duży przyjęto ilościowe prawdopodobieństwo scenariuszy incydentów.

Tabela nr.2 Tabela oceny prawdopodobieństwa

Waga prawdopodobieństwa zagrożenia	Prawdopodobieństwo wystąpienia	Zasady oceny prawdopodobieństwa urzeczywistnienia się zagrożenia
5	Bardzo wysokie	Ryzyko może się spełnić co najmniej raz w ciągu najbliższego kwartału
4	Wysokie	Ryzyko może się spełnić co najmniej raz w ciągu najbliższych 12 miesięcy
3	Średnie	Ryzyko może się spełnić co najmniej raz w ciągu najbliższych 2 lat
2	Niskie	Ryzyko może się spełnić co najmniej raz w ciągu najbliższych 5 lat
1	Bardzo niskie	Ryzyko najprawdopodobniej nie spełni się lub może spełnić się rzadziej niż raz na 5 lat

Analiza i ocena ryzyka

W Urzędzie Gminy Brudzeń Duży w celu określenia ryzyk dla zasobów, przyjęto metodykę powiązania czynników następstw oraz prawdopodobieństwa urzeczywistnienia się zagrożenia (biorąc pod uwagę aspekty podatności).

Zidentyfikowane i ocenione ryzyka o określonym stopniu istotności zostają zarejestrowane i udokumentowane w *Arkuszu identyfikacji, oceny oraz metody przeciwdziałania ryzyku*. Przyjmuje się, że ponowna ocena zidentyfikowanego ryzyka nie może być rzadsza niż raz na 12 miesięcy.

Tabela nr 3 Istotność ryzyka

Wpływ					
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
	1	2	3	4	5
	Prawdopodobieństwo				

	Skala akceptacji ryzyka
13-25	Ryzyko wysokie
5-12	Ryzyko umiarkowane
1-4	Ryzyko niskie

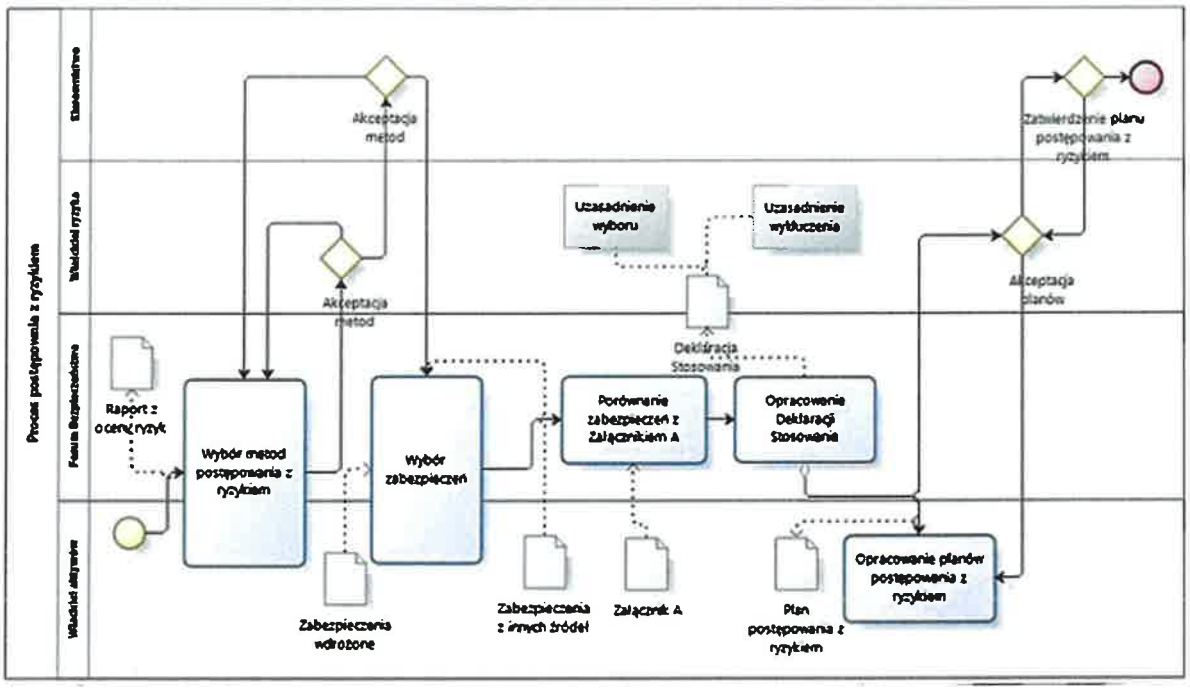
- Ryzykiem akceptowanym jest ryzyko niskie oraz ryzyko umiarkowane. Ryzyko wysokie przekracza akceptowany poziom ryzyka.
- Ryzyko przekraczające akceptowany poziom ryzyka wymaga ustalenia i podjęcia działań ograniczających je do poziomu umiarkowanego lub niskiego poprzez zmniejszenie jego wpływu lub prawdopodobieństwa ziszczenia się (przeciwdziałanie ryzyku).

Urząd Gminy Brudzeń Duży listę ryzyk wraz z przypisanymi poziomami wartości poddaje ocenie oraz nadaje priorytety dla celów postępowania z ryzykiem. Podjęte decyzje uwzględniają cele organizacji, jej kontekst, wymagania prawne, regulacyjne, umowne.

Uzyskana w ten sposób lista ryzyk jest zgodna z kryteriami oceny ryzyka, w odniesieniu do scenariuszy incydentów powodujących te ryzyka.

Postępowanie z ryzykiem

Schemat procesu postępowania z ryzykiem w Urzędzie Gminy Brudzeń Duży.



Dla wszystkich zasobów/działań, których poziom ryzyka będzie wyższy niż dopuszczalny, Urząd Gminy Brudzeń Duży wdraża środki ograniczające ryzyko lub stosuje jedną z następujących metod postępowania:

- **Modyfikowanie ryzyka** - obniżenie ryzyka do poziomu akceptowalnego (tzw. ryzyko szczątkowe) poprzez wybór oraz zastosowanie odpowiednich zabezpieczeń zgodnie z wytycznymi określonymi w normie PN-EN ISO/IEC 27001, Załącznik A,
- **Zachowanie (akceptacja) ryzyka** - podjęciem decyzji w zakresie odmowy zastosowania zabezpieczeń minimalizujących ryzyko oraz przyjęcie konsekwencji wynikających z ewentualnych sytuacji kryzysowych,
- **Unikanie ryzyka** - podjęcia działań polegających na wycofaniu się z danej działalności, lub zmianę warunków prowadzenia aktywności powodującej powstawanie określonych zagrożeń,

- **Dzielenie (transfer) ryzyka** -przeniesienie konsekwencji wystąpienia szkody lub jej skutków finansowych na inny podmiot np. ubezpieczenie się od jakiegoś zagrożenia bądź przekazanie odpowiedzialności za obszar ryzyka na podmioty zewnętrzne.

Właściciel ryzyka mając na uwadze oczekiwane koszty wdrożenia poszczególnych wariantów, oczekiwane korzyści, a także dotychczasowe zabezpieczenia, wybiera wariant optymalny kosztowo.

Stosowne zabezpieczenia opisano w Deklaracji Stosowania.

Monitorowanie oraz przegląd ryzyka

W Urzędzie Gminy Brudzeń Duży monitorowanie ryzyka jest prowadzone w trybie ciągłym. Monitorowanie ma na celu weryfikację, czy system zarządzania ryzykiem spełnia założone cele, czy polityki i procedury ustanowione w jego ramach są nadal aktualne, odpowiednie i wydajne.

Monitorowanie ryzyk gwarantują, że wszystkie nowe ryzyka zostaną w odpowiednim czasie zidentyfikowane oraz ustanowione wobec nich priorytety działania.

Każdy Właściciel ryzyka jest odpowiedzialny za:

- Niezbędne modyfikacje wartości aktywów,
- Cykliczne monitorowanie zdefiniowanych czynników ryzyka,
- Monitorowanie mechanizmów kontrolnych pod kątem ich adekwatności i skuteczności,
- Weryfikację oceny prawdopodobieństwa wystąpienia ryzyka i jego skutków

Monitorowanie ryzyk ma na celu zapewnienie, że wszystkie nowe ryzyka zostaną w odpowiednim czasie zidentyfikowane oraz ustanowione wobec nich priorytety działania. W sytuacji odnotowania jakichkolwiek zmian czynników wpływających na ryzyko, należy dokonać ponownego przeglądu ryzyk oraz zaktualizowania ich wartości, jeżeli jest to uzasadnione.

Monitorowanie i przegląd ryzyka pozwalają na ciągłe dostosowywanie procesu zarzadzania ryzykiem do celów biznesowych organizacji.

Wykaz załączników

Załącznik 1: Zbiorczy rejestr ryzyk i plan postępowania z ryzykiem w roku……
Załącznik 2: Lista typowych zagrożeń wraz z identyfikacją typów źródeł (wg Normy PN-ISO/IEC 27005:2017-06),
Załącznik 3: Przykłady podatności (wg Normy PN-ISO/IEC 27005:2017-06),

Załącznik nr 1
Zbiorczy rejestr ryzyk i plan postępowania z ryzykiem w roku...

Zbiorczy rejestr ryzyk i plan postępowania z ryzykiem w roku.....

L.P.	Aktywo / zasób	Ryzyko*	Reakcja na ryzyko	Wybrane zabezpieczenie	Właściciel ryzyka odpowiedzialny za mitygację ryzyka	Termin realizacji wdrożenia zabezpieczenia
1.						
2.						
3.						
4.						

*Skala ryzyka: wysokie i średnie

Rejestr sporządzono na podstawie arkuszy identyfikacji, oceny oraz określenia metod przeciwdziałaniu ryzyku poszczególnych komórek organizacyjnych Urzędu Gminy Brudzeń Duży.

.....
Podpis

Załącznik nr.2

Lista typowych zagrożeń wraz z identyfikacją typów źródeł

Zniszczenia fizyczne
Pożar
Zalanie
Zanieczyszczenie
Poważny wypadek
Zniszczenie urządzeń lub nośników
Pył, korozja, wychłodzenie
Atak bombowy
Atak terrorystyczny
Zjawiska naturalne
Zjawiska klimatyczne
Zjawiska sejsmiczne
Zjawiska wulkaniczne
Zjawiska pogodowe
Powódź
Utrata podstawowych usług
Awaria systemu klimatyzacji lub dostaw wody
Utrata dostaw prądu
Awaria urządzenia telekomunikacyjnego
Zakłócenia spowodowane promieniowaniem
Promieniowanie elektromagnetyczne
Promieniowanie cieplne
Impuls elektromagnetyczny
Naruszenie bezpieczeństwa informacji
Przechwycenie sygnałów na skutek zjawiska interferencji
Szpiegostwo zdalne
Podsłuch
Kradzież nośników lub dokumentów
Kradzież urządzenia
Odtworzenie z powtórnie wykorzystanych lub wyrzuconych nośników
Ujawnienie

Dane z niewiarygodnych źródeł
Manipulowanie urządzeniem
Sfałszowanie oprogramowania
Detekcja umiejscowienia
Szkody spowodowane działaniem strony trzeciej
Szkody spowodowane testami penetracyjnymi
Zużycie nośników informacji
Utrata usług wsparcia (np. technicznego)
Awarie techniczne
Awaria urządzenia
Niewłaściwe funkcjonowanie urządzeń
Przeciążenie systemu informacyjnego
Niewłaściwe funkcjonowanie oprogramowania
Naruszenie zdolności utrzymania systemu informacyjnego
Nieautoryzowane działania
Nieautoryzowane użycie urządzeń
Nieuprawnione kopiowanie oprogramowania
Użycie fałszywego lub skopiowanego oprogramowania
Zniekształcenie danych
Nielegalne przetwarzanie danych
Nieautoryzowany dostęp do sieci
Nieautoryzowany dostęp fizyczny
Naruszenie bezpieczeństwa funkcji
Błąd użytkownika
Naruszenie praw
Fałszowanie praw
Odmowa działania
Naruszenie dostępności personelu

Załącznik nr 3: Przykłady podatności

Rodzaj	Przykłady podatności
Sprzęt	Niewystarczające utrzymanie / błędna instalacja nośników pamięci
	Brak planów okresowej wymiany
	Wrażliwość na wilgoć, pył, zanieczyszczenie
	Wrażliwość na promieniowanie elektromagnetyczne
	Brak skutecznej kontroli zmian konfiguracji
	Brak planu wymiany zużywających się części, sprzęt niskiej jakości
	Zła obsługa
	Wrażliwość na zmiany napięcia
	Wrażliwość na zmiany temperatury
	Brak lub niewłaściwa kontrola zmian, błędnie napisana instrukcja, brak przeszkolenia pracowników
	Niekontrolowane kopiowanie
Oprogramowanie	
	Brak lub niewystarczające testowanie oprogramowania
	Brak wylogowania przy opuszczaniu stacji roboczej
	Pozbywanie się lub ponowne używanie nośników bez właściwego kasowania informacji
	Błędne przypisanie praw dostępu
	Szeroko dystrybuowane oprogramowanie
	Zastosowanie programów aplikacyjnych do nieaktualnych danych
	Skomplikowany interfejs użytkownika
	Nieprawidłowe ustawienie parametrów
	Brak mechanizmów identyfikacji i uwierzytelniania użytkownika
	Niezabezpieczone hasła
	Złe zarządzanie hasłami
	Uruchomione zbędne usługi
	Brak skutecznej kontroli zmian
	Niekontrolowane ściąganie i użytkowanie oprogramowania
	Brak kopii zapasowych
Sieć	
	Brak dowodu wysłania lub odebrania wiadomości
	Niezabezpieczone linie telekomunikacyjne

	Niechroniony wrażliwy ruch
	Złe łączenie kabli
	Pojedynczy punkt uszkodzenia
	Brak identyfikacji i uwierzytelniania nadawcy i odbiorcy
	Niebezpieczna architektura sieciowa
	Przesyłanie hasła w jawnej postaci
	Nieodpowiednie zarządzanie siecią
	Niezabezpieczone połączenia z siecią publiczną
Personel	
	Nieobecność personelu
	Nieodpowiednie procedury rekrutacji
	Niewystarczające szkolenie z bezpieczeństwa
	Niepoprawne użycie oprogramowania lub sprzętu
	Brak świadomości w zakresie bezpieczeństwa
	Brak mechanizmów monitorowania
	Praca personelu zewnętrznego lub sprzątającego bez nadzoru
	Brak polityki w zakresie poprawnego użytkowania środków telekomunikacyjnych i komunikatorów
Siedziba	
	Nieodpowiednie lub niestaranne użytkowanie fizycznej kontroli dostępu do budynków i pomieszczeń
	Lokalizacja na obszarach zagrożonych powodzią
	Niestabilna sieć elektryczna
	Brak fizycznej ochrony budynków, drzwi i okien
Organizacja	
	Brak formalnej procedury rejestrowania i wyrejestrowywania użytkowników
	Naruszenie formalnego procesu przeglądu praw dostępu
	Brak lub niewystarczające zapisy odnoszące się do bezpieczeństwa w umowach z klientami i/lub stronami trzecimi
	Brak procedur monitorowania środków przetwarzania informacji
	Brak regularnych audytów
	Brak procedur identyfikowania i szacowania ryzyka
	Brak raportowania błędów rejestrowanych w dziennikach administratorów i operatorów
	Nieodpowiednia reakcja utrzymania serwisowego
	Brak lub niewystarczająca umowa o poziomie usług
	Brak procedury kontroli zmian
	Brak formalnej procedury nadzoru nad dokumentacją SZBI

	Brak formalnej procedury nad zapisami SZBI
	Brak formalnego procesu autoryzacji dla informacji publicznie dostępnych
	Brak właściwego przypisania zakresów odpowiedzialności związanych z bezpieczeństwem informacji
	Brak planów ciągłości
	Brak polityki korzystania z poczty elektronicznej
	Brak procedur instalowania oprogramowania w systemach produkcyjnych
	Brak zapisów w dziennikach administratorów i operatorów
	Brak procedur przetwarzania informacji klasyfikowanych
	Brak odpowiedzialności związanej z bezpieczeństwem informacji w zakresach obowiązków
	Brak lub niewystarczające zapisy odnoszące się do bezpieczeństwa informacji w umowach z pracownikami
	Brak zdefiniowanego postępowania dyscyplinarnego w przypadku incydentu związanego z bezpieczeństwem informacji
	Brak formalnej polityki korzystania z komputerów przenośnych
	Brak nadzoru nad aktywami znajdującymi się poza siedzibą
	Brak lub niewystarczająca polityka czystego biurka i czystego ekranu
	Brak autoryzacji środków przetwarzania informacji
	Brak ustanowionych mechanizmów monitorowania naruszeń bezpieczeństwa
	Brak regularnych przeglądów realizowanych przez kierownictwo
	Brak procedur raportowania o słabościach bezpieczeństwa
	Brak procedur zapewniających zgodność z prawem własności intelektualnej