ZARZĄDZENIE NR 347 /23

Wójta Gminy Brudzeń Duży

z dnia 29.05.2023 r.

w sprawie wprowadzenia 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 2018r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019r. poz. 125), art.13 ust. 1 ustawy z dnia 17 lutego 2005r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz. U. z 2021 r. poz. 2070 z późn. zm.) w związku z§ 20 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t.j. Dz. U. z 2017r. poz. 2247), zarządza się, co następuje:

§1.

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

2. 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 SZBI stanowi załącznik do niniejszego Zarządzenia.
2. Podstawową dokumentację SZBI stanowi:

a) System Zarządzania Bezpieczeństwem Informacji w Urzędzie Gminy Brudzeń Duży - dokument wprowadzający,

b) Polityka Bezpieczeństwa Informacji (PBI),

c) Polityka Bezpieczeństwa Teleinformatycznego (PBTI),

d) Polityka Bezpieczeństwa Danych Osobowych (PBDO),

e) Procedura klasyfikacji informacji i analizy ryzyka.

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 § 20 ust. 2 pkt. 14 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012r. w sprawie Krajowych Ram

Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

§4.

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

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

§ 5.

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

Koordynator Bezpieczeństwa Informacji - Pani Maria Maraszek

Zastępca Koordynatora Bezpieczeństwa Informacji - Pan Piotr Sieczkowski

Inspektor Ochrony Danych - Pani Edyta Wasilewska,

Administrator Systemu Informatycznego - Pan Piotr Sieczkowski.

§ 6.

Zarządzenie wchodzi w życie z dniem podpisania.

§ 7.

Traci moc Zarządzenie **Nr** 36/19 Wójta Gminy Brudzeń Duży z dnia 30 kwietnia 2019 r.

Wójt Gminy Brudzeń Duży

Andrzej Dwojnych

System Zarządzania Bezpieczeństwem Informacji

w Gminie Brudzeń Duży

Dokument wprowadzający

Wydanie 1.0

Historia dokumentu

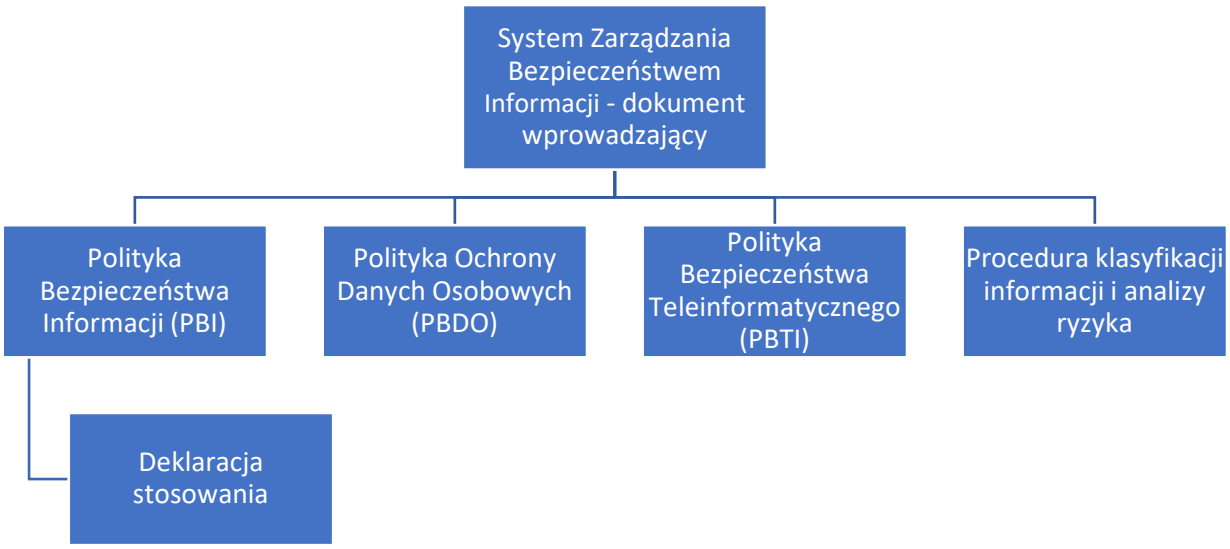
Numer zmiany		Imię i Nazwisko	Zdarzenie	Data zdarzenia
1	Opracował:		Utworzenie v.1.0	
	Zatwierdził:			
2				
3				

Spis treści

1. Wprowadzenie

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

- 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:



2. Role i odpowiedzialność w zarządzaniu bezpieczeństwem informacji

Najwyższe kierownictwo i odpowiedzialność za zarządzanie bezpieczeństwem Informacji.

Podejmowanie kluczowych decyzji dotyczących funkcjonowania Gminy 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 Gminą.
W ramach wdrożenia SZBI przyjmuje się, iż Wójt Gminy będzie brał czynny udział w podejmowaniu kluczowych decyzji dotyczących Systemu Zarządzania Bezpieczeństwem Informacji.

Wskazane decyzje odnoszą się do:

- Powołania Koordynatora Bezpieczeństwa,
- Zatwierdzania wyników oceny ryzyka,
- Zatwierdzania planu postępowania z ryzykiem oraz raportu z przeglądu zarządzania dla Gminy,
- Zatwierdzenia dokumentów wchodzących w skład Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).

Koordynator Bezpieczeństwa

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

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

Zastępca Koordynator Bezpieczeństwa

Koordynator Bezpieczeństwa wspierany jest przez zastępcę, powołanego na wniosek Koordynatora Bezpieczeństwa zarządzeniem Wójta. Do odpowiedzialności Zastępcy Koordynatora należy utrzymanie Systemu Zarządzania Bezpieczeństwem Informacji na terenie Gminy, w szczególności:

- Zapewnienie funkcjonowania systemu zarządzania w Gminie opartego o wymagania normy ISO/IEC 27001,
- Wypełnienie wymagań zdefiniowanych we wspólnej dla całej Gminy dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji,
- Realizacja zadań pozwalających na utrzymanie Systemu Zarządzania Bezpieczeństwem Informacji,
- Raportowanie do Koordynatora Bezpieczeństwa wyników analiz dotyczących Systemu Zarządzania Bezpieczeństwem Informacji i opracowań mających na celu doskonalenie Systemu Zarządzania Bezpieczeństwem Informacji,
- Realizacja zadań wynikających z dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji.

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 Teleinformatycznych

Do obowiązków Administratora Systemów Teleinformatycznych 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 Gminie. 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

Pracownicy Urzędu Gminy 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,
- Aktywny udział we wdrażaniu mechanizmów bezpieczeństwa poprzez opiniowanie możliwości zastosowania określonego rozwiązania przy realizacji zadań danego pracownika.

Działania jakie podejmują pracownicy to:

- Udział w analizie ryzyka i klasyfikacji zasobów,
- Raportowanie incydentów bezpieczeństwa informacji,
- Zgłaszanie wniosków o zmianę w dokumentacji.

Forum bezpieczeństwa informacji

Forum Bezpieczeństwa to ciało doradcze przy Koordynatorze Bezpieczeństwa, które będzie miało wpływ na najważniejsze elementy ciągłego doskonalenia przed przedstawianiem ich najwyższemu kierownictwu - Wójtowi do akceptacji. Zakłada się aktywny udział członków Forum Bezpieczeństwa Informacji w:

- Opiniowaniu treści polityki i innych dokumentów obowiązujących w Gminie,
- Przygotowaniu materiałów na Przegląd Zarządzania i uczestnictwo w przeglądzie,
- Przygotowaniu zakresu analiz ryzyka oraz opiniowaniu wyników oceny ryzyka przed zatwierdzeniem przez Wójta,
- Definiowaniu działań doskonalących wynikających z audytów, przeglądów, incydentów oraz oceny ryzyka, które mają wpływ na działalność Gminy. Rekomenduje się, aby w skład Forum wchodzili: Koordynator, zastępca Koordynatora, Inspektor Ochrony Danych oraz osoby wskazane przez Koordynatora Bezpieczeństwa przed każdym spotkaniem Forum.

Zespół Zarządzania Incydentami

Interdyscyplinarny zespół powoływany przez Koordynatora Bezpieczeństwa, w szczególności odpowiedzialny za przeprowadzenie analizy i dalszą reakcję na występujące incydenty bezpieczeństwa informacji w Gminie. Zespół Zarządzania Incydentami (ZZI) odpowiada między innymi za:

- Klasyfikację zdarzeń identyfikowanych w Gminie 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.

3. Odpowiedzialność za zatwierdzanie dokumentacji

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

- Wójt – Polityki,
- Koordynator Bezpieczeństwa – Procedury, Instrukcje, Zasady.

4. Nadzorowanie dokumentacji

Podstawowym założeniem skutecznego wdrożenia dokumentacji i naturalnego korzystania z niej przez pracowników jest wprowadzenie jednego miejsca w Gminie, 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.

5. Postanowienia końcowe

Wszystkie zagadnienia uwzględnione w dokumencie ,,System Zarządzania Bezpieczeństwem Informacji w Gminie Brudzeń Duży" mają na celu określenie strategicznych kierunków i odpowiedzialności wynikających z wdrożonego SZBI w Urzędzie Gminy. Wszelkie szczegóły w

tym zakresie zostały opisane w dokumentach powiązanych m.in. Polityka Bezpieczeństwa Informacji oraz Polityka Bezpieczeństw Teleinformatycznego.

Polityka Bezpieczeństwa Informacji w Gminie Brudzeń Duży

Wydanie 1.0

Historia dokumentu

Numer zmiany		Imię i Nazwisko	Zdarzenie	Data zdarzenia
1	Opracował:		Utworzenie v.1.0	
	Zatwierdził:			
2				
3				

Spis treści

1. Wprowadzenie

Polityka Bezpieczeństwa Informacji w Gminie 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 Gminy i jest chroniona na każdym szczeblu organizacji.

2. Cele Systemu Zarządzania Bezpieczeństwem Informacji

Głównymi celami Systemu Zarządzania Bezpieczeństwem Informacji w Gminie 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 27001:2017 pkt. 5.2; 6.2; 7.5 wykazuje przywództwo i zaangażowanie w kontekście bezpieczeństwa informacji podczas realizowanych procesów w Gminie 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.

3. Kontekst organizacji

W oparciu o normę PN-EN ISO/IEC 27001:2017 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 interesariuszami 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 oraz dostępności świadczonych usług dla interesariuszy oraz w ramach współpracy z innymi podmiotami i organami nadzoru.

System Zarządzania Bezpieczeństwem Informacji w Gminie 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 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 27001:2017 (Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji - Wymagania),
- Norma PN-EN ISO/IEC 27002:2017 (Technika Informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zabezpieczania 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.

4. 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 Gminę Brudzeń Duży w oparciu o normę PN-ISO/IEC 27001:2017.

Zakres Systemu Zarządzania Bezpieczeństwem Informacji dotyczy zarządzania informacjami, zachowaniu ich poufności, integralności oraz dostępności 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 Gminy, 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.

5. Nadzorowanie dokumentacji

Urząd Gminy 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),
- Polityka Bezpieczeństwa Teleinformatycznego (PBTI),
- Procedura klasyfikacji informacji zewnętrznych i wewnętrznych,
- Metodyka szacowania 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,
- Plany postępowania z ryzykiem.

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

1. Najwyższe kierownictwo:
    - Zatwierdzanie dokumentacji wchodzącej w skład Systemu Zarządzania Bezpieczeństwem Informacji zgodnie z odpowiedzialnością opisaną w dokumentacji wprowadzającej do SZBI,
    - Informowanie koordynatora bezpieczeństwa o konieczności aktualizacji dokumentacji w wyniku zmiany strategicznych kierunków funkcjonowania organizacji.

2. Koordynator bezpieczeństwa:
    - Zatwierdzanie instrukcji i procedur bezpieczeństwa,
    - Nadzór nad opracowywaniem, zatwierdzaniem i dystrybucją dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji,
    - Proponowanie zmian oraz współpraca z innymi komórkami organizacyjnymi w zakresie zapewnienia, że dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji jest zgodna z obowiązującymi przepisami regulacyjnymi,
    - Aktualizacja dokumentacji wraz z zapewnieniem kontroli wersji,
    - Zapewnienie, że aktualne dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji jest udostępniona i zakomunikowana wszystkim pracownikom organizacji.

6. Ocena Systemu Zarządzania Bezpieczeństwem Informacji

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

- Monitorowanie przez Koordynatora Bezpieczeństwa 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 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.

7. Przegląd zarządzania

W celu zapewnienia ciągłego doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji co najmniej raz do roku planuje się i przeprowadza przegląd zarządzania. Koordynator bezpieczeństwa 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, koordynator bezpieczeństwa lub osoba przez niego wskazana przygotowuje sprawozdanie i przekazuje je wszystkim uczestnikom przeglądu. W przypadku, gdy w ramach przeglądu zarządzania zostaną wskazane działania doskonalące, koordynator bezpieczeństwa informuje o tym fakcie osoby odpowiedzialne.

W ramach przeglądu zarządzania:

- Weryfikowana jest efektywność Systemu Zarządzania Bezpieczeństwem Informacji,
- Planowane są działania korekcyjne, korygujące lub zapobiegawcze,
- Omawiany jest Plan Postępowania z Ryzykiem (PPR),
- Planowana jest możliwość ciągłego doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji.

8. 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 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 27001:2017, 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 audytu przedstawiane są przez Koordynatora Bezpieczeństwa do najwyższego kierownictwa.

9. Strategia ciągłości działania

Urząd Gminy 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 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 teleinformatycznych lub podmiot świadczący usługi na rzecz Urzędu Gminy zobowiązany jest do opracowania, aktualizacji oraz testowania planów ciągłości działania.

10. 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, koordynator bezpieczeństwa analizuje zidentyfikowane naruszenia bądź uchybienia, ocenia je pod względem istotności w zakresie

bezpieczeństwa informacji, wyciąga wnioski, a także podejmuje działania naprawcze względem zidentyfikowanych incydentów,

- Koordynator bezpieczeństwa, jeśli uzna to za stosowna, przeprowadza lub zleca przeprowadzenie audytu doraźnego po zidentyfikowaniu i obsłużeniu incydentu bezpieczeństwa,
- Koordynator bezpieczeństwa 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),
- Koordynator bezpieczeństwa 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. W przypadku, gdy incydent dotyczy danych osobowych, koordynator bezpieczeństwa niezwłocznie informuje o tym fakcie Inspektora Ochrony Danych, który zgodnie z Ustawa z dnia 10 maja 2018 o ochronie danych osobowych prowadzi dalsze czynności związane z obsługą incydentu. W sytuacji, gdy incydent bezpieczeństwa związany jest ze świadczeniem usług publicznych, Koordynator bezpieczeństwa po dokonaniu odpowiedniej klasyfikacji dokonuje zgłoszenia incydentu zgodnie z wymaganiami wynikającymi z Ustawy o Krajowym Systemie Cyberbezpieczeństwa z dnia 5 lipca 2018 roku,
- Każdy pracownik jest zobowiązany do zgłoszenia koordynatorowi bezpieczeństwa podejrzenia wystąpienia 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.

11. Ochrona danych osobowych

Ochrona danych osobowych w Gminie 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 koordynatora bezpieczeństwa oraz najwyższego kierownictwa.

12. Odpowiedzialność pracowników organizacji

W oparciu o normę PN-EN ISO/IEC 27001:2017 Zał. A.6.1, pkt 7.2, odpowiedzialność za bezpieczeństwo informacji w organizacji ponoszą wszyscy pracownicy zgodnie z posiadanymi zakresami obowiązków. Każdy pracownik obowiązany 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,
- 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 Koordynatora Bezpieczeństwa lub 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.

13. Szkolenia w zakresie bezpieczeństwa informacji

Zgodnie z art. 39 ust. 1 lit. b) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. oraz z § 20 ust. 2 pkt 6 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), a także w oparciu o normę PN-EN ISO/IEC 27001:2017 pkt 7.1 – 7.3:

- 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,
- Za politykę szkoleniową odpowiada Koordynator Bezpieczeństwa oraz Inspektor Ochrony Danych,
- 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 przez Inspektora Ochrony Danych oraz Koordynatora Bezpieczeństwa 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.

14. 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 kieruje się w szczególności zasadą ograniczonego celu, ograniczonego przechowywania oraz poufności,
- Urząd Gminy 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 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 zapewnia ochronę przed nieuprawnionym dostępem do tych danych osobowych, a jednocześnie do sprzętu, który służy do przetwarzania takich danych,
- Urząd Gminy 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 przeprowadza weryfikację czy dane zawarte w dokumentacji aplikacyjnej są zgodne ze stanem faktycznym,
- Urząd Gminy 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 do przechowywania powyższych informacji przez określony czas.

Rozwiązanie współpracy z pracownikiem

W przypadku rozwiązania współpracy z pracownikiem Urząd Gminy należy:

- Odebrać wszystkie uprawnienia do systemów teleinformatycznych,
- Odebrać wszystkie uprawnienia umożliwiające dostęp fizyczny do Urzędu Gminy,
- 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.

15. Bezpieczeństwo fizyczne i środowiskowe

Bezpieczeństwo fizyczne w Gminie 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.

16. Bezpieczeństwo informacji w relacjach z Dostawcami

W przypadku dostawców zakres Polityki Bezpieczeństwa Informacji ma zastosowanie do:

- Wszystkich systemów, których Gmina jest dysponentem, dostawcą lub partnerem,
- Informacji będących własnością Gminy,
- 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 Gminie. 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 Gminie ponoszą wszyscy Dostawcy zgodnie z posiadanymi zakresami zawartym w Umowach.

Poufność informacji pomiędzy Gminą 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 Gminy zgodnie z podpisanymi Umowami i służy realizacji celów biznesowych Gminy.

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

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

17. Bezpieczeństwo informacji w ramach Krajowych Ram Interoperacyjności

W celu zapewnienia Bezpieczeństwa informacji w ramach Krajowych Ram Interoperacyjności Urząd Gminy 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 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 na podstawie przepisów § 8 ust. 3 oraz § 10 ust. 5, 6, 11 i 12 Krajowych Ram Interoperacyjności oraz odwołań do rejestrów zawierających dane referencyjne w zakresie niezbędnym do realizacji zadań,
- 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 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.

Urząd Gminy 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.

18. Wykaz załączników

- Załącznik nr 1 – Deklaracja stosowania

Polityka Bezpieczeństwa Teleinformatycznego

w Gminie Brudzeń Duży

Wydanie 1.0

Historia dokumentu

Numer zmiany		Imię i Nazwisko	Zdarzenie	Data zdarzenia
1	Opracował:		Utworzenie v.1.0	
	Zatwierdził:			
2				
3				

Spis treści

1. Wprowadzenie

Polityka Bezpieczeństwa Teleinformatycznego w Gminie 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 Gminie 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 27001:2017 (Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji - Wymagania),
- Norma PN-EN ISO/IEC 27002:2017 (Technika Informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zabezpieczania 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.

2. Zakres stosowania

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

3. 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.
- System teleinformatyczny automatycznie wymusza zmianę hasła nie rzadziej niż co 30 dni,
- W przypadku podejrzenia lub stwierdzenia ujawnienia hasła należy je niezwłocznie zmienić,
- Hasła są przechowywane w postaci zaszyfrowanej,
- Hasło składa się z co najmniej 8 znaków, zawiera małe i wielkie litery oraz cyfry i znaki specjalne,
- 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,
- Wymagany jest brak powtarzalności hasła co najmniej do pięciu wystąpień wstecz.

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.

4. Zarządzanie urządzeniami mobilnymi

W celu zapewnienia ochrony urządzeń mobilnych przyjęto następujące zasady:

- Urząd Gminy 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,
- Każdy pracownik zobowiązany jest do weryfikacji źródła aplikacji, którą planuje zainstalować na urządzeniu mobilnym (dotyczy tylko i wyłącznie aplikacji niezbędnych do realizacji obowiązków służbowych). Rekomendowane jest instalacja aplikacji tylko ze znanych i zweryfikowanych źródeł np. Google Play, AppStore.

5. Kopie zapasowe

Organizacja wprowadziła i stosuje następujące zasady dotyczące kopii zapasowych:

- Dla każdego systemu teleinformatycznego lub grupy systemów opracowywana jest przez administratora tego systemu instrukcja wykonywania kopii bezpieczeństwa, ich testowania oraz odtwarzania. W szczególności instrukcja zawiera metodę, zakres, częstotliwość i harmonogram wykonywania kopii zapasowych, metodę sprawdzania ich poprawności oraz okres ich przechowywania,
- 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,
- Każdy nośnik kopii zapasowej powinien być identyfikowalny przynajmniej przez naniesienie pierwszej daty użycia nośnika, nazwy systemu, z którego wykonano kopię zapasową oraz jednoznacznej identyfikacji wersji kopii zapasowej. Opis może być nanoszony ręcznie lub automatycznie przez urządzenie do wykonywania kopii,
- Nośniki, urządzenia i aplikacje wykorzystywane do wykonywania kopii zapasowych powinny być testowane przez administratorów przynajmniej raz do roku – weryfikowana powinna być możliwość odtworzenia systemu teleinformatycznego,
- Każde testowe odtworzenie danych powinno być odnotowywane w dzienniku administracyjnym systemu teleinformatycznego.

6. 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.

7. 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,
- Osobą odpowiedzialną za aktualność i kompletność dokumentacji jest właściciel zasobu,
- Dokumentacja systemów teleinformatycznych jest udostępniana na zasadzie „wiedzy koniecznej”.

8. 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.

9. Ochrona przed szkodliwym oprogramowaniem

Organizacja wprowadziła i stosuje następujące środki bezpieczeństwa przed szkodliwym oprogramowaniem:

- 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.

10. Zasady eksploatacji systemów teleinformatycznych

Zasady ogólne:

- Wszelkie zmiany w konfiguracji sprzętu komputerowego wykonują wyznaczeni administratorzy,
- Zasoby teleinformatyczne Urzędu Gminy podlegają ewidencjonowaniu i przypisaniu właścicieli tych zasobów, a także ewidencjonowaniu podlega wynoszenie sprzętu poza organizację,
- Uprawnienia do systemów teleinformatycznych przydzielane są zgodnie z zasadą tzw. minimalnych uprawnień, czyli uprawnień niezbędnych do wykonywania obowiązków służbowych na danym stanowisku,
- 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 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 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, pracownik zobowiązany jest do zwrotu wszystkich aktywów powierzonych przez Urząd Gminy,
- 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 muszą odbywać się z zapewnieniem ciągłości działania tych środowisk,
- Środowiska teleinformatyczne w Urzędzie Gminy 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 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 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 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 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,
- Łączenia zasobów teleinformatycznych Urzędu Gminy 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,
- 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, w tym również przygotowywanie wytycznych do postępowań zakupowych realizowanych przez Urząd Gminy 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,

- 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. 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,
- Zarządzanie i nadzorowanie sieci w celu ochrony informacji w podłączonych do sieci systemach teleinformatycznych i aplikacjach,
- Aktualizację planów ciągłości działania oraz procedur odtworzeniowych.

11. 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 przekazuje do centralnego repozytorium (prowadzonego w ramach ePUAP przez Ministra właściwego do spraw informatyzacji) oraz udostępnia w Biuletynie Informacji Publicznej wzory dokumentów elektronicznych zgodnie z § 12 ust. 1 rozporządzenia Prezesa Rady Ministrów z dnia 14 września 2011 r. w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych,

- 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.

12. Minimalne wymagania dla systemów teleinformatycznych

- Systemy teleinformatyczne wykorzystywane przez Gminę 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 (sprzęt, oprogramowanie, protokoły komunikacyjne, szyfrujące) projektowane są i wdrażane zgodnie z najlepszymi praktykami w celu odpowiedniego zabezpieczenia przetwarzanych informacji. Podczas projektowania systemów zarówno pracownicy Urzędy Gminy 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 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),
- 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, określonych w załączniku nr 4 do Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności,
- Każdy system teleinformatyczny wraz z wykorzystywanym sprzętem oraz konfiguracją podlega obowiązkowemu ewidencjonowaniu i przypisaniu właściciela,
- 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,
- 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 Gminie 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).

13. 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.

14. 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 przeprowadzają weryfikację korespondencji pod względem potencjalnych zagrożeń bezpieczeństwa.

15. Zasady publikacji informacji na stronie WWW

- Publikacja informacji na stronie WWW może być realizowana tylko i wyłącznie przez pracowników Urzędu Gminy 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 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.

16. 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 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 wykorzystujący w ramach obowiązków służbowych systemy teleinformatyczne powinni odbyć szkolenie w zakresie bezpiecznego wykorzystywania systemów i cyberzagrożeń z nimi związanych.

Polityka Bezpieczeństwa Danych Osobowych Gminy Brudzeń Duży

Wydanie 1.0

Historia dokumentu

Numer zmiany		Imię i Nazwisko	Zdarzenie	Data zdarzenia
1	Opracował:		Utworzenie v.1.0	
	Zatwierdził:			
2				
3				

Spis treści

1. Wprowadzenie

Polityka Bezpieczeństwa Danych Osobowych określa środki techniczne i organizacyjne zastosowane przez Administratora Danych dla zapewnienia ochrony danych osobowych zawartych w systemach informatycznych w wewnętrznej sieci intranetowej oraz zbiorach danych zapisanych w postaci dokumentacji papierowej w Urzędzie Gminy.

Administrator Danych deklaruje podejmowanie wszelkich możliwych działań koniecznych do zapobiegania zagrożeniom, m. in. takich jak:

- sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu, jak np. pożar, zalanie pomieszczeń, katastrofa budowlana, napad, kradzież, włamanie, działania terrorystyczne, niepożądana ingerencja ekipy remontowej,
- niewłaściwe parametry środowiska, zakłócające pracę urządzeń komputerowych (nadmierna wilgotność lub bardzo wysoka temperatura, oddziaływanie pola elektromagnetycznego),
- awarie sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne naruszenia ochrony danych, niewłaściwe działanie serwisantów, w tym pozostawienie serwisantów bez nadzoru, a także przyzwolenie na naprawę sprzętu zawierającego dane poza siedzibą Administratora Danych,
- podejmowanie pracy w systemie z przełamaniem lub zaniechaniem stosowania procedur ochrony danych, np. praca osoby, która nie jest upoważniona do przetwarzania, próby stosowania nie swojego hasła i identyfikatora przez osoby upoważnione,
- celowe lub przypadkowe publikowanie danych w Internecie z ominięciem zabezpieczeń systemu lub wykorzystaniem błędów systemu informatycznego Administratora Danych,
- ataki z sieci Internet,
- naruszenia zasad i procedur określonych w dokumentacji z zakresu ochrony danych osobowych przez osoby upoważnione do przetwarzania danych osobowych, związane z nieprzestrzeganiem procedur ochrony danych, w tym zwłaszcza:

    - niezgodne z procedurami zakończenie pracy lub opuszczenie stanowiska pracy (nieprawidłowe wyłączenie komputera, niezablokowanie wyświetlenia treści na ekranie komputera przed tymczasowym opuszczeniem stanowiska pracy, pozostawienie po zakończeniu pracy nieschowanych, do zamykanych na klucz szaf dokumentów zawierających dane osobowe, niezamknięcie na klucz pokoju po jego opuszczeniu),
    - naruszenie bezpieczeństwa danych przez nieautoryzowane ich przetwarzanie,
    - ujawnienie osobom nieupoważnionym procedur ochrony danych stosowanych u Administratora Danych,

- ujawnienie osobom nieupoważnionym danych przetwarzanych przez Administratora Danych, w tym również nieumyślne ujawnienie danych osobom postronnym przebywającym bez nadzoru lub w niedostatecznie nadzorowanych pomieszczeniach Administratora Danych,
- niewykonywanie stosownych kopii zabezpieczających,
- przetwarzanie danych osobowych w celach prywatnych,
- wprowadzanie zmian do systemu informatycznego Administratora Danych i instalowanie programów bez zgody Administratora Systemu Informatycznego.

2. Definicje

Administrator Danych – Wójt Gminy Brudzeń Duży,

Rozporządzenie RODO - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),

Inspektor Ochrony Danych (IOD) - rozumie się przez to osobę, której Administrator Danych powierzył pełnienie obowiązków Inspektora Ochrony Danych, nadzorującą stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych.

Administrator Systemu Informatycznego (ASI)— rozumie się przez to osobę zarządzającą systemem informatycznym w którym przetwarzane są dane osobowe,

Hasło - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym,

Identyfikator użytkownika - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,

Integralności danych - rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,

Odbiorca danych - rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:

- osoby, której dane dotyczą,
- osoby upoważnionej do przetwarzania danych,

- przedstawiciela, o którym mowa w art. 3 ustawy,
- podmiotu, o którym mowa w art. 31 ustawy,
- organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem,
- osobie upoważnionej do przetwarzania danych osobowych - rozumie się przez to osobę, która upoważniona została do przetwarzania danych osobowych przez Wójta na piśmie.

Pomieszczenia - rozumie się przez to budynki, pomieszczenia lub części pomieszczeń określone przez Administratora Danych, tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego oraz gromadzone w formie dokumentacji papierowej,

Poufności danych - rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom,

Przetwarzanie danych - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,

Przetwarzający - rozumie się przez to podmiot, któremu zostało powierzone przetwarzanie danych osobowych na podstawie umowy zawieranej zgodnie z art. 31 ustawy,

Raport - rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych,

Rozliczalność - rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,

Sieć publiczna - rozumie się przez to sieć telekomunikacyjną niebędącą siecią wewnętrzną, służącą do świadczenia usług telekomunikacyjnych,

Sieć telekomunikacyjna - rozumie się przez to urządzenia telekomunikacyjne i linie telekomunikacyjne, zestawione i połączone w sposób umożliwiający przekaz sygnałów pomiędzy określonymi zakończeniami sieci, za pomocą przewodów, fal radiowych bądź optycznych lub innych środków wykorzystujących energię elektromagnetyczną,

Serwisant — rozumie się przez to firmę lub pracownika firmy zajmującej się sprzedażą, instalacją, naprawą i konserwacją sprzętu komputerowego,

System informatyczny - rozumie się przez to sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów procedur przetwarzania informacji i narzędzi programowych,

Uwierzytelnianie - rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu,

Użytkownik - rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych, której nadano identyfikator i przyznano hasło,

Zbiór danych - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnym według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

3. Cel

Wdrożenie polityki bezpieczeństwa danych osobowych w Urzędzie Gminy Brudzeń Duży ma na celu zabezpieczenie danych osobowych zarówno tych przetwarzanych w systemie informatycznym, jak i poza nim. Realizowane jest to poprzez wykonanie obowiązków wynikających z ustawy i rozporządzenia RODO.

4. Zakres stosowania

Niniejsza polityka bezpieczeństwa danych osobowych (PBDO) dotyczy zarówno danych osobowych przetwarzanych w sposób tradycyjny jak i w systemie informatycznym.
Procedury i zasady określone w niniejszym dokumencie stosuje się do wszystkich osób upoważnionych do przetwarzania danych osobowych, zarówno zatrudnionych, jak i innych, np. wolontariuszy, praktykantów, stażystów.

5. Organizacja przetwarzania danych osobowych

Administrator Danych

Administrator danych realizuje zadania w zakresie ochrony danych osobowych, w tym zwłaszcza:

- podejmuje decyzje o celach i środkach przetwarzania danych osobowych z uwzględnieniem przede wszystkim zmian w obowiązującym prawie, organizacji Administratora Danych oraz technik zabezpieczenia danych osobowych,

- upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnie zakresie, odpowiadającym zakresowi jej obowiązków,
- odwołuje upoważnienia do przetwarzania danych osobowych,
- wyznacza Inspektora Ochrony Danych, Administratora Systemu Informatycznego oraz określa zakres ich zadań i czynności,
- podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur bezpiecznego przetwarzania danych osobowych,
- nadzoruje prowadzenie ewidencji i innej dokumentacji z zakresu ochrony danych osobowych przez Inspektora Ochrony Danych.

Inspektor ochrony Danych (IOD)

Inspektor Ochrony Danych realizuje zadania w zakresie nadzoru nad przestrzeganiem zasad ochrony danych osobowych, w tym zwłaszcza:

- informowanie administratora oraz pracowników o obowiązkach spoczywających na nich na mocy Rozporządzenia RODO o ochronie danych osobowych oraz innych przepisów,
- monitorowanie przestrzegania Rozporządzenia RODO oraz innych przepisów Unii i państw członkowskich oraz polityk administratora lub procesora,
- szkolenie personelu uczestniczącego w operacjach przetwarzania,
- przeprowadzania systematycznych audytów w organizacji, w której został powołany,
- udzielania wskazówek administratorowi w przedmiocie wdrożenia odpowiednich skutecznych środków technicznych jak również organizacyjnych mających zabezpieczyć dane osobowe oraz informacje w jaki sposób zminimalizować dane ryzyko,
- udzielania na żądanie zaleceń co do oceny skutków oraz monitorowanie ich wykonania w przypadku, gdy administrator danych przed rozpoczęciem przetwarzania zobowiązany jest do przeprowadzenia oceny skutków planowanych operacji przetwarzania dla ochrony danych.

Administrator Systemu Informatycznego (ASI)

Administrator Systemu Informatycznego realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym Administratora Danych, w tym zwłaszcza:

- zarządza systemem informatycznym, w którym przetwarzane są dane osobowe,
- przeciwdziała dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe,
- przydziela każdemu użytkownikowi identyfikator oraz hasło do systemu informatycznego oraz dokonuje ewentualnych modyfikacji uprawnień, a także usuwa lub wyłącza konta użytkowników zgodnie z zasadami określonymi w Polityce Bezpieczeństwa Teleinformatycznego,

- nadzoruje działanie mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych,
- podejmuje działania w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego,
- w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego informuje IOD o naruszeniu i współdziała z nim przy usuwaniu skutków naruszenia,
- sprawuje nadzór nad wykonywaniem napraw, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe,
- sprawuje nadzór nad wykonywaniem kopii zabezpieczających, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego,
- prowadzi rejestr wykonywanych kopii zabezpieczających oraz dziennik systemu informatycznego,
- podejmuje działania służące zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji.

Osoba upoważniona do przetwarzania danych osobowych (personel)

Osoba upoważniona do przetwarzania danych osobowych jest zobowiązana przestrzegać następujących zasad:

- przetwarza dane osobowe wyłącznie w zakresie ustalonym indywidualnie przez Administratora Danych w upoważnieniu i tylko w celu wykonywania nałożonych na nią obowiązków. Zakres dostępu do danych przypisany jest do niepowtarzalnego identyfikatora użytkownika, niezbędnego do rozpoczęcia pracy w systemie. Rozwiązanie stosunku pracy lub odwołanie z pełnionej funkcji powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych,
- pracownik musi zachować tajemnicę danych osobowych oraz przestrzegać procedur ich bezpiecznego przetwarzania. Przestrzeganie tajemnicy danych osobowych obowiązuje przez cały okres zatrudnienia u Administratora Danych, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji,
- stosuje określone przez Administratora Danych oraz Inspektora Ochrony Danych procedury oraz wytyczne mające na celu zgodne z prawem, w tym zwłaszcza adekwatne, przetwarzanie danych,
- korzysta z systemu informatycznego w sposób zgodny ze wskazówkami Inspektora Ochrony Danych oraz Administratora Systemu Informatycznego,
- zabezpiecza dane przed ich udostępnianiem osobom nieupoważnionym.

Wzór Upoważnienia do przetwarzania danych osobowych stanowi Załącznik nr 1 do niniejszej Polityki Bezpieczeństwa Danych Osobowych.

Rejestr czynności przetwarzania

Administrator Danych wykonuje i prowadzi na bieżąco rejestr czynności przetwarzania zgodnie z RODO, który zawiera:

- imię i nazwisko lub nazwę administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie - przedstawiciela administratora oraz Inspektora Ochrony Danych,
- cele przetwarzania,
- opis kategorii osób, których dane dotyczą oraz kategorii danych osobowych,
- kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych,
- gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacji odpowiednich zabezpieczeń,
- jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1,
- jeżeli jest to możliwe planowane terminy usunięcia danych.

W przypadku działania jako podmiot, któremu inny administrator powierzył przetwarzanie w trybie art. 28 RODO, prowadzony jest rejestr wszystkich kategorii czynności przetwarzania dokonywanych na rzecz każdego z administratorów.
Wzór rejestru czynność przetwarzania stanowi Załącznik nr 2 do niniejszej Polityki Bezpieczeństwa Danych Osobowych.

Szacowanie ryzyka i wybór zabezpieczeń

Administrator Danych przeprowadza ogólne szacowanie ryzyka, które polega na przyporządkowaniu potencjalnych zagrożeń dla bezpieczeństwa danych osobowych wraz z zapisem i uzasadnieniem decyzji o konkretnych działaniach związanych z zabezpieczeniem tych danych.

Administrator Danych zobowiązany jest do uwzględnienia możliwości nieuprawnionego lub przypadkowego:

- zniszczenia,
- utraty,
- zmodyfikowania,
- ujawnienia,
- dostępu.

Szacowanie ryzyka przeprowadzane jest z perspektywy potencjalnych negatywnych skutków dla osób, których dane osobowe są przetwarzane w ramach prowadzonej działalności.

Realizowanie obowiązków informacyjnych

Administrator Danych przekazuje każdej osobie, której dane są przetwarzane informacje, o zakresie przetwarzania danych i jego czasie, chyba że przepis ustawy przewiduje zwolnienie z tego obowiązku.
Administrator Danych zapewnia możliwość dostępu do treści przetwarzanych danych osobowych w formie udostępnienia bezpłatnej kopii danych osobowych (w formie elektronicznej lub papierowej), chyba że przepis ustawy zwalnia z tego obowiązku lub żądanie osoby, której dane są przetwarzane jest ewidentnie nieuzasadnione lub nadmiarowe.
W przypadku uznania żądania za ewidentnie nieuzasadnione lub nadmiarowe należy uzasadnić odmowę realizacji żądania wskazując powody przemawiające za przyjęciem takiej kwalifikacji i w formie pisemnej przekazać uzasadnienie osobie wnoszącej żądanie informując, o możliwości wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.
W przypadku tych informacji, które są przetwarzane przy użyciu środków elektronicznych na podstawie zgody lub umowy, Administrator Danych przetwarza je w formie pozwalającej na przekazanie i odczyt przez innego administratora - jeżeli osoba, której dane dotyczą skorzysta z uprawnienia do przeniesienia dostarczonych przez nią danych.

Wzór Klauzuli informacyjnej stanowi Załącznik nr 3 do niniejszej Polityki Bezpieczeństwa Danych Osobowych.

Powierzanie przetwarzania danych osobowych

W przypadku konieczności przekazania danych osobowych - zarówno w formie papierowej, jak i elektronicznej do podmiotu, który ma realizować cele wskazane przez Administratora Danych, uprzednio zawiera się umowę powierzenia przetwarzania. Administrator Danych prowadzi ewidencję zawartych umów powierzenia przetwarzania.

Wzór ewidencji podmiotów z którymi zawarto umowę przetwarzania danych osobowych stanowi Załącznik nr 4 do niniejszej Polityki Bezpieczeństwa Danych Osobowych.

Sposób przepływu danych w systemie informatycznym Administratora Danych

Przepływ danych w systemie informatycznym odbywa się na zasadzie łączenia się aplikacji klienckich do baz danych zainstalowanych na serwerze. Wszelkie przepływy danych pomiędzy poszczególnymi bazami odbywają się za pośrednictwem aplikacji klienckich. Autoryzacja do baz danych odbywa się za pomocą wydzielonego użytkownika i hasła.

Bezpieczeństwo osobowe

- kandydaci na pracowników są dobierani z uwzględnieniem ich kompetencji merytorycznych, a także kwalifikacji moralnych. Zwraca się uwagę na takie cechy kandydata, jak uczciwość, odpowiedzialność oraz przewidywalność zachowań,
- ryzyko utraty bezpieczeństwa danych przetwarzanych przez Administratora Danych pojawiające się ze strony osób trzecich, które mają dostęp do danych osobowych (np. serwisanci), jest minimalizowane przez podpisanie umów powierzenia przetwarzania danych osobowych,
- ryzyko ze strony osób, które potencjalnie mogą w łatwiejszy sposób uzyskać dostęp do danych osobowych (np. osoby sprzątające pomieszczenia Administratora Danych), jest minimalizowane przez zobowiązywanie ich do zachowania tajemnicy na podstawie pisemnych oświadczeń.

Szkolenia w zakresie ochrony danych osobowych

Inspektor Ochrony Danych uwzględnia następujący plan szkoleń:

- szkoli się każdą osobę, która ma zostać upoważniona do przetwarzania danych osobowych. Szkolenia wewnętrzne wszystkich osób upoważnionych do przetwarzania danych osobowych przeprowadzane są w przypadku każdej zmiany zasad lub procedur ochrony danych osobowych, przeprowadza się szkolenia dla osób innych niż upoważnione do przetwarzania danych, jeśli pełnione przez nie funkcje wiążą się z zabezpieczeniem danych osobowych.

Zabezpieczenie sprzętu przetwarzającego dane osobowe

Serwery zlokalizowane są w zabezpieczonych antywłamaniowo pomieszczeniach, do których wejście ma jedynie Administrator Systemu Informatycznego. Dostęp do serwerów zabezpieczony jest poprzez hasło logowania.
Administrator Systemu Informatycznego wskazuje użytkownikom, jak postępować, aby zapewnić prawidłową eksploatację systemu informatycznego.
Okablowanie sieciowe zostało zaprojektowane w ten sposób, że dostęp do linii teletransmisyjnych jest możliwy tylko z pomieszczeń zamykanych na klucz. Ponadto kable sieciowe nie krzyżują się z okablowaniem zasilającym, co zapobiega interferencjom.

Serwis sprzętu przetwarzającego dane osobowe

Bieżąca konserwacja sprzętu wykorzystywanego do przetwarzania danych osobowych prowadzona jest tylko przez Administratora Systemu Informatycznego. Natomiast poważne naprawy wykonywane przez personel zewnętrzny realizowane są w siedzibie Urzędu po zawarciu z podmiotem wykonującym naprawę umowy o powierzenie przetwarzania danych osobowych, określającej kary umowne za naruszenie bezpieczeństwa danych.
Administrator Systemu Informatycznego dopuszcza konserwowanie i naprawę sprzętu poza siedzibą Administratora Danych jedynie po trwałym usunięciu danych. Zużyty sprzęt służący do przetwarzania danych osobowych może być zbywany dopiero po trwałym usunięciu danych.
Wszystkie awarie, działania konserwacyjne i naprawy systemu informatycznego są opisywane w stosownych protokołach, podpisywanych przez osoby w tych działaniach uczestniczące.
W uzasadnionych przypadkach możliwy jest dostęp za pośrednictwem sieci VPN dla osób, które nie są pracownikami Urzędu Gminy, ale świadczą na rzecz Urzędu Gminy usługi.

Zabezpieczenia po stronie personelu

Osoby upoważnione do przetwarzania danych osobowych powinny:

- zapewnić ustawienie ekranów komputerowych tak, by uniemożliwić osobom nieuprawnionym oglądanie ich zawartości,
- nie pozostawiać bez kontroli dokumentów, nośników danych i sprzętu w miejscach publicznych oraz w samochodach,
- odpowiednio zabezpieczyć akta, pamięci przenośne i komputery,
- nie stosować do powtórnego użytku dokumentów zadrukowanych jednostronnie,
- nie dokonywać zapisywania haseł wymaganych do uwierzytelnienia się w systemie na papierze lub innym nośniku,
- przetwarzać pliki z danymi, które są niezbędne do wykonywania obowiązków służbowych,
- przechowywać nośniki z danymi w zamkniętych na klucz szafach,
- nośniki wycofane z eksploatacji przekazać do Administratora Systemu Informatycznego w celu trwałego skasowania danych zgodnie z obowiązującymi regulacjami wewnętrznymi,
- szyfrować dane osobowe, które będą przekazywane za pośrednictwem poczty elektronicznej,
- zabezpieczyć dokumenty zawierające dane osobowe w odpowiednich szafach przed opuszczeniem pomieszczenia,
- zapewnić bezpieczeństwo fizyczne dla dokumentów i sprzętu (ochrona przed zalaniem, pożarem, zewnętrznymi czynnikami atmosferycznymi),
- odpowiednio zabezpieczyć pomieszczenia przed nieuprawnionym dostępem.

Postępowanie z nośnikami przenośnymi zawierającymi dane osobowe

- dane z nośników przenośnych, które nie są kopiami zabezpieczającymi, po wprowadzeniu do systemu informatycznego Administratora Danych powinny być trwale usuwane z tych nośników przez fizyczne zniszczenie (np. płyty CD-ROM) lub usunięcie danych powinno odbywać się za pomocą oprogramowania trwale usuwającego pliki. Za wykonanie tych czynności odpowiada Administrator Systemu Informatycznego,
- uszkodzone nośniki przed ich wyrzuceniem należy zniszczyć fizycznie w niszczarce służącej do niszczenia nośników lub certyfikowanym urządzeniu,
- wydruki zawierające dane osobowe, które nie będą dalej eksploatowane należy codziennie przed zakończeniem pracy zniszczyć w niszczarce.

Odpowiedzialność osób upoważnionych do przetwarzania danych osobowych

Niezastosowanie się do prowadzonej przez Administratora Danych polityki bezpieczeństwa przetwarzania danych osobowych, której założenia określa niniejszy dokument, i naruszenie procedur ochrony danych przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52 Kodeksu Pracy. Niezależnie od rozwiązania stosunku pracy osoby popełniające przestępstwo będą pociągane do odpowiedzialności karnej zwłaszcza na podstawie art. 51-52 ustawy oraz art. 266 Kodeksu Karnego.

Przykładowo przestępstwo można popełnić wskutek:

- stworzenia możliwości dostępu do danych osobowych osobom nieupoważnionym,
- niezabezpieczenia nośnika lub komputera przenośnego,
- zapoznania się z hasłem innego pracownika wskutek wykonania nieuprawnionych operacji w systemie informatycznym Administratora Danych.

Przeglądy polityki bezpieczeństwa danych osobowych

Polityka bezpieczeństwa danych osobowych powinna być poddawana przeglądowi przynajmniej raz na rok. W razie istotnych zmian dotyczących przetwarzania danych osobowych Inspektor Ochrony Danych może zarządzić jej przegląd stosownie do potrzeb.

Inspektor Ochrony Danych analizuje, czy polityka bezpieczeństwa danych osobowych i pozostała dokumentacja z zakresu ochrony danych osobowych jest adekwatna do:

- zmian w budowie systemu informatycznego,
- zmian organizacyjnych Administratora Danych, w tym również zmian statusu osób upoważnionych do przetwarzania danych osobowych,
- zmian w obowiązującym prawie.

Inspektor Ochrony Danych po uzgodnieniu z Wójtem może, stosownie do potrzeb, przeprowadzić wewnętrzny audyt zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych. Przeprowadzenie audytu wymaga uzgodnienia jego zakresu z Administratorem Systemu Informatycznego. Zakres, przebieg i rezultaty audytu dokumentowane są na piśmie w protokole podpisywanym zarówno przez Inspektora Ochrony Danych, jak i Administratora Systemu Informatycznego.

Postępowanie w przypadku naruszenia ochrony danych osobowych

Każdy pracownik Administratora Danych, w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych, jest obowiązany do niezwłocznego poinformowania o tym bezpośredniego przełożonego, Administratora Systemu Informatycznego lub/oraz Inspektora Ochrony Danych.

Inspektor Ochrony Danych, który stwierdził lub uzyskał informację wskazującą na naruszenie ochrony danych osobowych jest obowiązany niezwłocznie zapisać wszelkie informacje i okoliczności związane z danym zdarzeniem, a w szczególności dokładny czas uzyskania informacji oraz jej treść o naruszeniu ochrony danych osobowych lub samodzielnego wykrycia tego faktu oraz podjąć decyzję czy naruszenie powinno zostać zgłoszone do Prezesa Urzędu Ochrony Danych Osobowych.

Administrator Systemu Informatycznego, który stwierdził fakt lub uzyskał informację o naruszeniu bezpieczeństwa danych osobowych w systemie informatycznym jest obowiązany niezwłocznie:

- wygenerować i wydrukować wszystkie dokumenty i raporty, które mogą pomóc w ustaleniu wszelkich okoliczności zdarzenia, opatrzyć je datą i godziną oraz podpisać,
- przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, w tym określić skalę zniszczeń, metody dostępu osoby nieuprawnionej do danych osobowych w systemie informatycznym służącym do przetwarzania danych osobowych,
- podjąć odpowiednie kroki w celu powstrzymania lub ograniczenia dostępu osoby nieuprawnionej do danych osobowych, zminimalizować szkody i zabezpieczyć przed usunięciem śladów naruszenia ochrony, w szczególności poprzez:
    - fizyczne odłączenie urządzeń i segmentów sieci, które mogły umożliwić dostęp do danych osobowych osobie nieuprawnionej,

- wylogowanie użytkownika podejrzanego o naruszenie bezpieczeństwa danych osobowych,
- zmianę hasła użytkownika, przez konto którego uzyskano nielegalny dostęp do danych osobowych w celu uniknięcia ponownej próby uzyskania takiego dostępu,

- dokonać szczegółowej analizy stanu systemu informatycznego w celu potwierdzenia lub wykluczenia faktu naruszenia bezpieczeństwa danych osobowych,
- przywrócić prawidłowe działanie systemu informatycznego służącego przetwarzaniu danych osobowych.

Po przywróceniu prawidłowego stanu, należy przeprowadzić szczegółową analizę, w celu określenia przyczyn naruszenia ochrony danych osobowych lub podejrzenia takiego naruszenia, oraz podjąć kroki, mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.
Jeżeli przyczyną zdarzenia był błąd użytkownika, należy przeprowadzić szkolenie wszystkich osób biorących udział w procesie przetwarzania danych osobowych w Urzędzie Gminy.
Jeżeli przyczyną zdarzenia była infekcja wirusem lub innym szkodliwym oprogramowaniem, należy ustalić źródło jego pochodzenia i utworzyć zabezpieczenia antywirusowe oraz organizacyjne, wykluczające podobne zdarzenia w przyszłości.
Jeżeli przyczyną zdarzenia było zaniedbanie ze strony użytkownika należy wyciągnąć wobec niego konsekwencje wynikające z przepisów prawa pracy oraz wewnętrznych uregulowań Urzędu Gminy.
W przypadku, kiedy użytkownik nie jest pracownikiem Administratora Danych, konsekwencje wynikające z umowy, na podstawie której osoba ta posiada uprawnienia do przetwarzania danych osobowych.
Inspektor Ochrony Danych przygotowuje szczegółowy raport o przyczynach, przebiegu i wnioskach ze zdarzenia naruszenia bezpieczeństwa danych osobowych i przekazuje go Administratorowi Danych. Jeżeli zdarzenie dotyczyło naruszenia zabezpieczeń systemu informatycznego służącego przetwarzaniu danych osobowych to Inspektor Ochrony Danych w przygotowaniu raportu współpracuje z Administratorem Systemu Informatycznego.
Naruszenie bezpieczeństwa danych wpisuje się do odpowiedniego rejestru prowadzonego przez Administratora Danych
Wzór rejestru naruszeń stanowi Załącznik nr 5 do niniejszej Polityki Bezpieczeństwa Danych Osobowych.

Postępowanie w wypadku klęski żywiołowej

Klęska żywiołowa jest katastrofą, spowodowaną działaniem sił przyrody takich jak ogień, huragan, woda lub ich przejawami.
W przypadku wystąpienia zagrożenia powodującego konieczność przeprowadzenia ewakuacji osób lub mienia z pomieszczeń, w których przetwarzane są dane osobowe, mają zastosowanie przepisy niniejszego rozdziału oraz innych przepisów szczegółowych.

Osoby biorące udział w akcji ratunkowej mają prawo wejść do pomieszczeń, w których przetwarzane są dane osobowe.
W przypadku ogłoszenia alarmu ewakuacyjnego użytkownicy przebywający w pomieszczeniach, w których są dane osobowe, obowiązani są do przerwania pracy i w miarę możliwości przed opuszczeniem tych pomieszczeń do:

- zamknięcia systemu informatycznego,
- zabezpieczenia danych osobowych gromadzonych w kartotekach.

W czasie trwania akcji ratunkowej i po jej zakończeniu Inspektor Ochrony Danych oraz obecni użytkownicy powinni, w miarę możliwości, zabezpieczyć dane osobowe przed nieuprawnionym do nich dostępem.
Obowiązek ten ciąży w równym stopniu na innych pracownikach Administratora Danych, obecnych przy akcji ratunkowej.

Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych

Kopie zapasowe przechowywane są na serwerze oraz dodatkowo na osobnym serwerze plików przeznaczonym do przechowywania kopii zapasowych. Serwer i serwer plików zlokalizowane są w jednym budynku. Dostęp do serwerowni i serwera plików mają: Administrator, Administrator Systemów Informatycznych oraz Zastępca Wójta. Przebywanie osób nieuprawnionych do przetwarzania danych osobowych w pomieszczeniu serwerowni dopuszczalne jest za zgodą Administratora i/lub w obecności Administratora Systemów Informatycznych.
Kopie zapasowe przechowywane są przez okres 28 dni w przypadku baz danych aplikacji dziedzinowych oraz przez okres roku w przypadku systemu operacyjnego (dotyczy serwera). Administrator Systemów Informatycznych sprawdza okresowo kopie zapasowe i ocenia ich przydatność do odtworzenia zasobów systemu w wypadku jego awarii. Kopie baz danych aplikacji dziedzinowych są automatycznie kasowane po 28 dniach od dnia ich wykonania.
Nośniki zawierające kopie zapasowe baz z danymi osobowymi, po ustaniu ich użyteczności lub w przypadku ich uszkodzenia podlegają likwidacji. Urząd zleca niszczenie nośników (jeżeli ulegną awarii) kopii zapasowych specjalistycznej firmie zewnętrznej.

Postanowienia końcowe

Polityka bezpieczeństwa danych osobowych jest dokumentem wewnętrznym Urzędu Gminy Brudzeń Duży. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się przed dopuszczeniem do przetwarzania danych z niniejszym dokumentem oraz złożyć stosowne oświadczenie, potwierdzające znajomość jego treści.

Załącznik nr 1 – Wzór upoważnienia do przetwarzania danych osobowych

UPOWAŻNIENIE

do przetwarzania danych osobowych

Z dniem ..... upoważniam Panią/Pana .

.....

do przetwarzania danych osobowych, administrowanych lub/i powierzonych do przetwarzania w Urzędzie Gminy Brudzeń Duży, w postaci papierowej oraz w ramach nadanych dostępów do systemów informatycznych, zgodnie z zajmowanym stanowiskiem.

Jednocześnie, wraz z nadanym upoważnieniem, zobowiązuję Panią/Pana do przestrzegania przepisów dotyczących ochrony danych osobowych oraz wprowadzonej i wdrożonej do stosowania przez Administratora „Polityki Bezpieczeństwa Danych Osobowych".

Niniejsze upoważnienie traci moc:

najpóźniej z dniem odwołania albo rozwiązania lub wygaśnięcia umowy o pracę, umowy zlecenia, umowy o dzieło lub innej umowy cywilnoprawnej łączącej Pana/Panią z Administratorem.

....

Miejscowość, data (z upoważnienia Administratora)

OŚWIADCZENIE

o zapoznaniu się z Polityką Bezpieczeństwa Danych Osobowych

Oświadczam, iż zostałam/em zapoznana/y z przepisami dotyczącymi ochrony danych osobowych, w szczególności ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000), wydanych na jej podstawie aktów wykonawczych oraz 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, a także wprowadzonego i wdrożonego do stosowania przez Administratora „Polityki Bezpieczeństwa Danych Osobowych".

Zobowiązuję się do:

1) zachowania w tajemnicy danych osobowych jak również innych informacji stanowiących tajemnicę przedsiębiorcy w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (tj. Dz.U. z 1993 r. nr 47 poz. 211), do których mam lub będę miał/a dostęp w związku z wykonywaniem zadań służbowych lub obowiązków pracowniczych,
2) niewykorzystywania danych osobowych oraz innych informacji w celach pozasłużbowych o ile nie są one jawne,
3) zachowania w tajemnicy sposobów zabezpieczenia danych osobowych oraz innych informacji o ile nie są one jawne,
4) korzystania ze sprzętu IT oraz oprogramowania wyłącznie w związku z wykonywaniem obowiązków,
5) wykorzystywania jedynie legalnego oprogramowania pochodzącego od Administratora,
6) należytej dbałości o sprzęt i oprogramowanie zgodnie z dokumentacją przetwarzania danych osobowych,
7) korzystania z komputerów przenośnych zgodnie z dokumentacją przetwarzania danych osobowych,
8) nieudostępniania sprzętu służbowego, w szczególności urządzeń mobilnych, osobom trzecim.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami, może być uznane przez Pracodawcę za ciężkie naruszenie obowiązków pracowniczych w rozumieniu art. 52 § 1 pkt I Kodeksu Pracy lub za naruszenie przepisów karnych ww. ustawy o ochronie danych osobowych lub ciężkie naruszenie obowiązków umownych w przypadku umowy cywilnoprawnej.

_____

(podpis osoby upoważnionej)

Załącznik nr 2 – Wzór rejestru czynności przetwarzania danych osobowych

Nazwa stanowiska ……..

Nazwa zbioru:	
Jednostka wykonująca / komórka:	
Wykorzystywane oprogramowanie [dostawca oprogramowania] a. postać papierowa:	
Podstawa prawna:	
Cel przetwarzania:	
Kategorie osób, których dane dotyczą:	
Sposób zbierania danych:	
Pola informacyjne:	
Informacja o udostępnianiu danych:	
Informacja o powierzeniu przetwarzania:	
Informacja o odbiorcach danych:	
Informacja dot. transferu do kraju trzeciego lub org. międzynarodowej:	
Adnotacje dotyczące zmian (wpis/modyfikacja/wykreślenie):	

Załącznik nr 3 – Klauzula informacyjna

Klauzula informacyjna

Zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016 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 (dalej RODO) (Dz. Urz. UE L 119, s. I), informujemy, że:

I. Administratorem Pani/Pana danych osobowych jest Urząd Gminy Brudzeń Duży z siedzibą ul. Toruńska 2, 09-414 Brudzeń Duży.
2. Kontakt z Administratorem Danych osobowych jest możliwy pod adresem e-mail: iod@instytut.info.pl
3. Inspektorem Ochrony Danych w Urzędzie Gminy Brudzeń Duży jest Pani Edyta Wasilewska.
4. Podstawą prawną przetwarzania Pani/Pana danych osobowych jest:
    a. art. 6 ust. I lit b RODO, tj. przetwarzanie jest konieczne do realizacji łączącej nas umowy;
    b. art. 6 ust. I lit. c RODO lub art. 9 ust. 2 lit. b, tj. przetwarzanie jest niezbędne do realizacji obowiązków na nas ciążących;
    c. art. 6 ust. I lit. f RODO, tj. przetwarzanie jest niezbędne dla realizacji celów wynikających z prawnie uzasadnionych interesów Administratora, np. ewentualna konieczność odpierania lub realizacji roszczeń cywilnoprawnych.
    d. art. 6 ust. 1 lit. a RODO tj. przetwarzanie odbywa się na podstawie udzielonej zgody (wyjątkowe sytuacje np. przetwarzanie wizerunku).
5. Celem przetwarzania danych osobowych przez Urząd Gminy Brudzeń Duży jest realizacja zadań publicznych Administratora, świadczenie przez niego usług, a także wykonywanie obowiązków prawnych i dochodzenie ewentualnych roszczeń, wynikających z przepisów prawa cywilnego oraz obrony przed roszczeniami, jeśli takowe się pojawią. Dane osobowe przetwarzane są w celu prawidłowej realizacji tych zadań, wykonania obowiązków prawnych, jakie ciążą na administratorze.
6. Podanie przez Państwa danych osobowych jest dobrowolne, jednak niezbędne do zrealizowania zadania/umowy/świadczenia.
7. Mają Państwo prawo dostępu do swoich danych osobowych, do ich sprostowania, żądania ich usunięcia lub wniesienia sprzeciwu, jak również prawo do żądania od Administratora ograniczenia przetwarzania Państwa danych, a także do ich przenoszenia. W przypadku wyrażenia zgody na przetwarzanie danych mają Państwo prawo jej wycofania w każdym momencie bez wpływu na zgodność z prawem przetwarzania, jakiego dokonano przed wycofaniem tej zgody.
8. Administrator informuje, że Pani/Pana dane osobowe będą przetwarzane przez okres wymagany prawem, w przypadku umów cywilnych maksymalnie przez okres uwzględniający okres przedawnienia możliwych roszczeń, a w przypadku przetwarzania na podstawie zgody — do momentu jej wycofania.

9. Jeżeli Pan/Pani uzna, że dane osobowe będą przetwarzane niezgodnie z wymogami prawa ma Pan/Pani prawo wnieść skargę do organu nadzorczego — Prezesa Urzędu Ochrony Danych Osobowych.
10. Odbiorcą Pani/Pana danych osobowych mogą być współpracujące z nami firmy, w tym informatyczne, kurierskie itp. a także uprawnione do tego jednostki administracyjne i urzędy.
11. Państwa dane nie będą podlegały profilowaniu i nie będą przekazywane do państw trzecich.

Załącznik nr 4 – Wzór ewidencji podmiotów, z którymi zawarto umowy powierzenia przetwarzania danych osobowych

Lp.	**Nazwa podmiotu, z którym zawarto umowę powierzenia** *(konkretne dane identyfikujące podmiot, z którym zawarto umowę powierzenia)*	**Data powierzenia**	**Cel powierzenia** *(np. realizowanie wsparcia technicznego w zakresie prawidłowego działania systemu informatycznego użytkowanego przez spółkę)*	**Zakres powierzonych danych** *(wskazać lub opisać, do jakich konkretnie danych procesor może mieć dostęp na podstawie umowy powierzenia – wszelkie informacje, które przetwarzane są w formie elektronicznej, w zakresie niezbędnym do dokonania konkretnej czynności wynikającej z umowy)*
1.				
2.				
3.				

Załącznik nr 5 – Wzór rejestru naruszeń ochrony danych osobowych

L.p.	**Ogólny opis zdarzenia, okoliczności i data** *Np. zaginięcie nośnika z danymi, zainfekowanie skrzynki mailowej, zniszczenie danych w postaci papierowego wydruku, zaginięcie segregatora z danymi*	**Skutki**	**Podjęte działania zaradcze**	**Osoba zgłaszająca naruszenie**	**Klasyfikacja naruszenia** *(do wyboru jedno z poniższych) -po zbadaniu stwierdzono brak naruszenia ochrony danych - stwierdzono naruszenie, które nie zostało zgłoszone do organu nadzorczego -stwierdzono naruszenie, które zostało zgłoszone do organu nadzorczego (data zgłoszenia) -stwierdzono naruszenie, które zgłoszono do organu nadzorczego oraz o którym poinformowano osoby, których danych naruszenie dotyczyło*
1.					
2.					
3.					

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

Wydanie 1.0

Historia dokumentu

Numer zmiany		Imię i Nazwisko	Zdarzenie	Data zdarzenia
1	Opracował:		Utworzenie v.1.0	
	Zatwierdził:			
2				
3				

Spis treści

1. 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 27001:2017-06., 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 27001:2017-06 Technika Informatyczna, Techniki bezpieczeństwa, 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,
- 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 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 Gminy Brudzeń Duży
- Deklaracja Stosowania

2. 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,

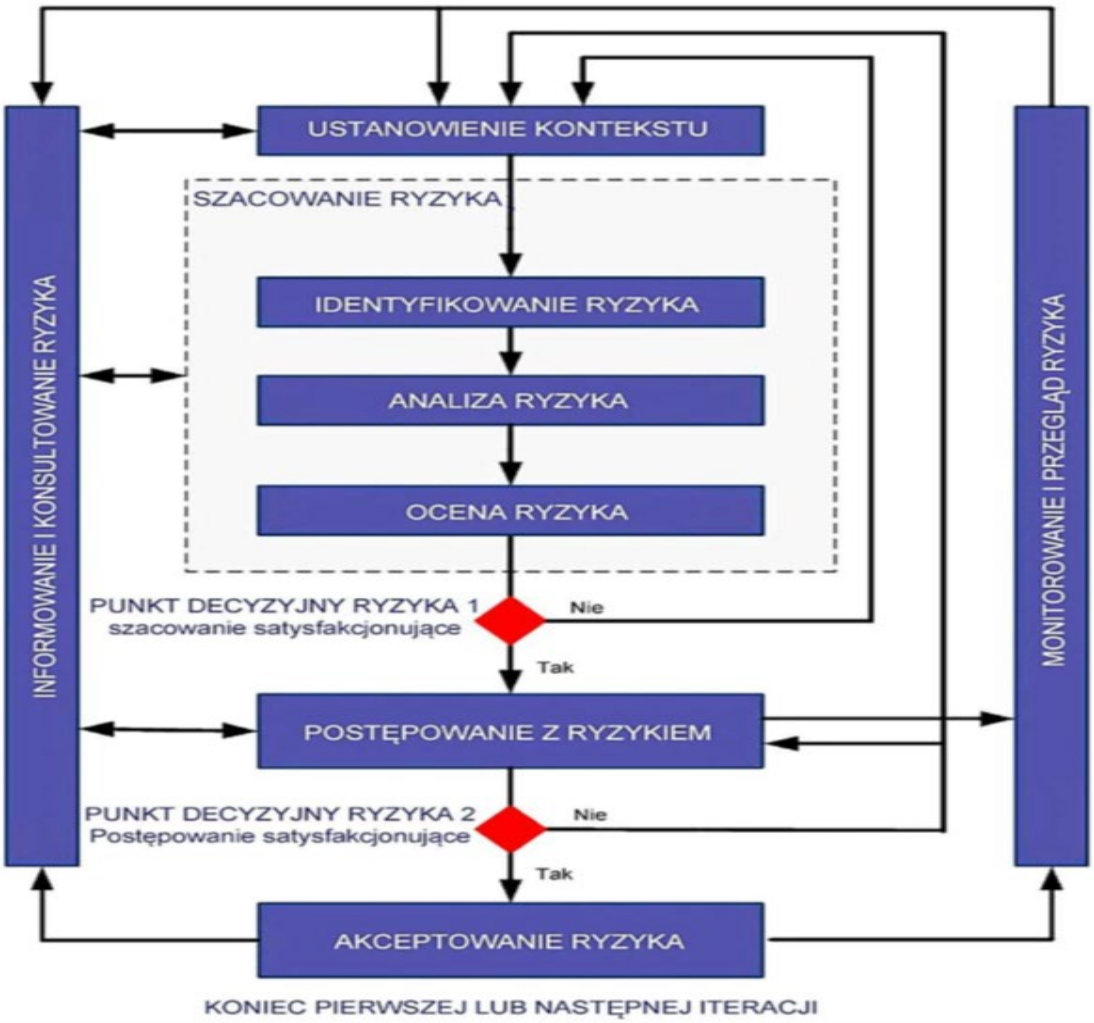
Zarządzanie ryzykiem – skoordynowane działania dotyczące kierowania i nadzorowania organizacji w odniesieniu do ryzyka.

3. 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

4. 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 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.

5. 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,
- Uzyskanie bezpieczeństwa informacji, w tym danych osobowych;
- Minimalizacja skutków wpływy incydentów na działalność Urzędu.

6. Kontekst zewnętrzny i wewnętrzny Urzędu

Kontekst działalności Urzędu Miasta i Gminy 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 Miasta i Gminy - oczekiwanie sprawnego działania urzędu, racjonalne kosztowo realizowanie zadań administracji publicznej,
- Starostwo Powiatowe – 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 Miasta i Gminy - realizacja zadań Urzędu wynikających ze statutu oraz uchwał Rady, nadzorowanie pracy Burmistrza oraz podległych mu jednostek organizacyjnych,
- Burmistrz i kadra Kierownicza Urzędu Miasta i Gminy - bezpieczeństwo zasobów informacyjnych, unikanie i zapobieganie incydentom bezpieczeństwa informacji,
- Pracownicy Urzędu Miasta i Gminy - 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.)

7. 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. Burmistrz Miasta i Gminy:
    - 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.

8. 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.

Szacując ryzyko Urząd Miasta i Gminy:

- 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 Urząd Miasta i Gminy 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.

9. Identyfikacja aktywów

Gmina 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.

10. Klasyfikacja informacji

Informacje przetwarzane w Urzędzie Miasta i Gminy klasyfikowane są w następujących grupach:

Informacje publiczne (przeznaczone dla wszystkich):

- Informacje udostępniane na stronach internetowych Urzędu,
- 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,
- 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 (faktury, dane przetwarzane w dziale księgowości, dane kadrowe, osobowe, dane związane z utrzymaniem systemów teleinformatycznych).

11. Identyfikacja zagrożeń

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

W Urzędzie Miasta i Gminy 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,
- 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 Miasta i Gminy. 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 Miasta i Gminy 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

12. 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

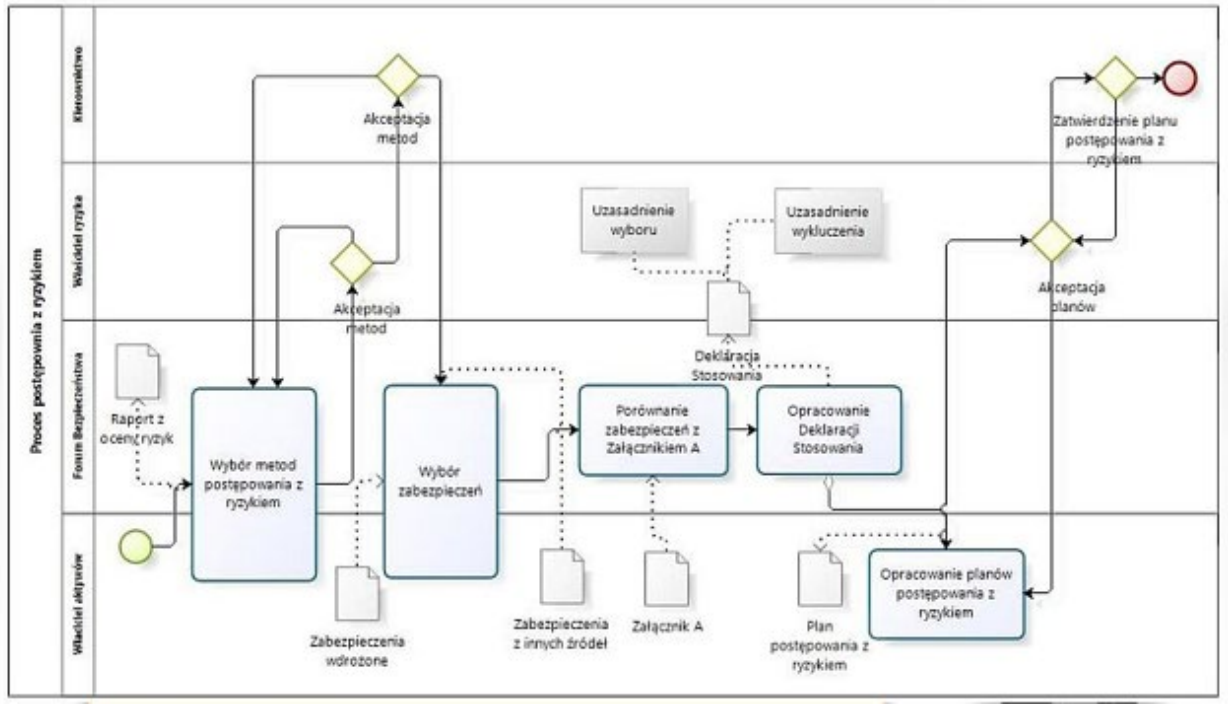
- Ryzykiem akceptowanym jest ryzyko niskie oraz ryzyko umiarkowane. Ryzyko wysokie przekracza akceptowany poziom ryzyka.
- Ryzyko przekraczające akceptowany poziom ryzyka wymaga ustalenia i podjęcia działań ograniczających je do poziomu umiarkowanego lub niskiego poprzez zmniejszenie jego wpływu lub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

Urząd Miasta i Gminy 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.

13. Postępowanie z ryzykiem

Schemat procesu postępowania z ryzykiem w Urzędzie Miasta i Gminy w Sannikach.



Dla wszystkich zasobów/działań, których poziom ryzyka będzie wyższy niż dopuszczalny, Urząd Gminy 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.

14. 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.

15. Wykaz załączników

Załącznik nr 1: Arkusz Identyfikacji, oceny oraz określenia metody przeciwdziałania ryzyku
Załącznik nr 2: Zbiorczy rejestr ryzyk na rok……
Załącznik nr 3: Lista typowych zagrożeń wraz z identyfikacją typów źródeł (wg Normy PN-ISO/IEC 27005:2017-06), Załącznik C
Załącznik nr 4: Przykłady podatności (wg Normy PN-ISO/IEC 27005:2017-06), Załącznik D

Załącznik nr 1:
Arkusz Identyfikacji, oceny oraz określenia metody przeciwdziałania ryzyku

Arkusz Identyfikacji, oceny oraz określenia metody przeciwdziałania ryzyku

L. P.	Aktywo / Zasób	Ryzyko	Zagrożenie	Podatność /Przyczyna	Skutek *	Wpływ zagrożenia na P,I,D	Prawdopodobieństwo**	Istotność ryzyka (kol. 6xkol.7)***	Metoda przeciwdziałania ryzyku
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*

*Wpływ zgodny z Tabelą nr 1
**Prawdopodobieństwo zgodne z Tabelą nr 2
*** Istotność ryzyka zgodna z Tabelą nr 3

.....
podpis

Załącznik nr 2
Zbiorczy rejestr ryzyk na rok...

Zbiorczy rejestr ryzyk na rok…….

L.P.	Aktywo / zasób	Ryzyko *	Właściciel ryzyka	Reakcja na ryzyko
1	*2*	*3*	*4*	*5*
1.				
2.				
3.				

*Skala ryzyka: poważne

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

.....
Podpis

Załącznik Nr.3

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 4: 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