ZARZĄDZENIE NR ON.120.16.2025
STAROSTY SIERPECKIEGO
z dnia 20 marca 2025 r.

w sprawie wprowadzenia Systemu Zarządzania Bezpieczeństwem Informacji

Na podstawie art. 34 ust. 1 ustawy z dnia 5 czerwca 1998 roku o samorządzie powiatowym (Dz. U. z 2024 r. poz. 107 z późn . zm.), 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 2023r. poz. 1206), art. 13 ust. 1 ustawy z dnia 17 lutego 2005r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2023 r. poz. 1557 z późn. zm.) w związku z § 19 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 (Dz. U. z 2024 r. poz. 773), zarządza się, co następuje:

§ **1.1.** W Starostwie Powiatowym w Sierpcu, 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:

1) Deklaracja stosowania załącznik Nr 1,
2) System Zarządzania Bezpieczeństwem Informacji w Starostwie Powiatowym w Sierpcu – dokument wprowadzający – załącznik Nr 2 ,
3) Polityka Bezpieczeństwa Informacji (PBI) załącznik Nr 3,
4) Polityka Bezpieczeństwa Teleinformatycznego (PBTI) załącznik Nr 4,
5) Procedura klasyfikacji informacji i analizy ryzyka załącznik Nr 5.

§ **3.** W Starostwie Powiatowym w Sierpcu 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 i przestrzeganie SZBI w podległych sobie komórkach organizacyjnych.

§ **5.** W związku z wdrożeniem Systemu Zarządzania Bezpieczeństwem Informacji w Starostwie Powiatowym w Sierpcu następuje powołanie następujących ról:

Koordynator Bezpieczeństwa Informacji – Michał Chiczewski – starszy informatyk

Zastępca Koordynatora Bezpieczeństwa Informacji – Hubert Rudowski – pomoc administracyjna.

§ **6.** Traci moc Zarządzenie Nr ON.120.39.2023 Starosty Sierpeckiego z dnia 11 września 2023 r.

§ **7.** Zarządzenie wchodzi w życie z dniem podpisania.

STAROSTA
Przemysław Burzyński

z up. STAROSTY
Magdalena Piotrowska
SEKRETARZ POWIATU

System Zarządzania Bezpieczeństwem Informacji

Starostwo Powiatowe w Sierpcu

Dokument wprowadzający

Wydanie 1.1

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

Historia dokumentu

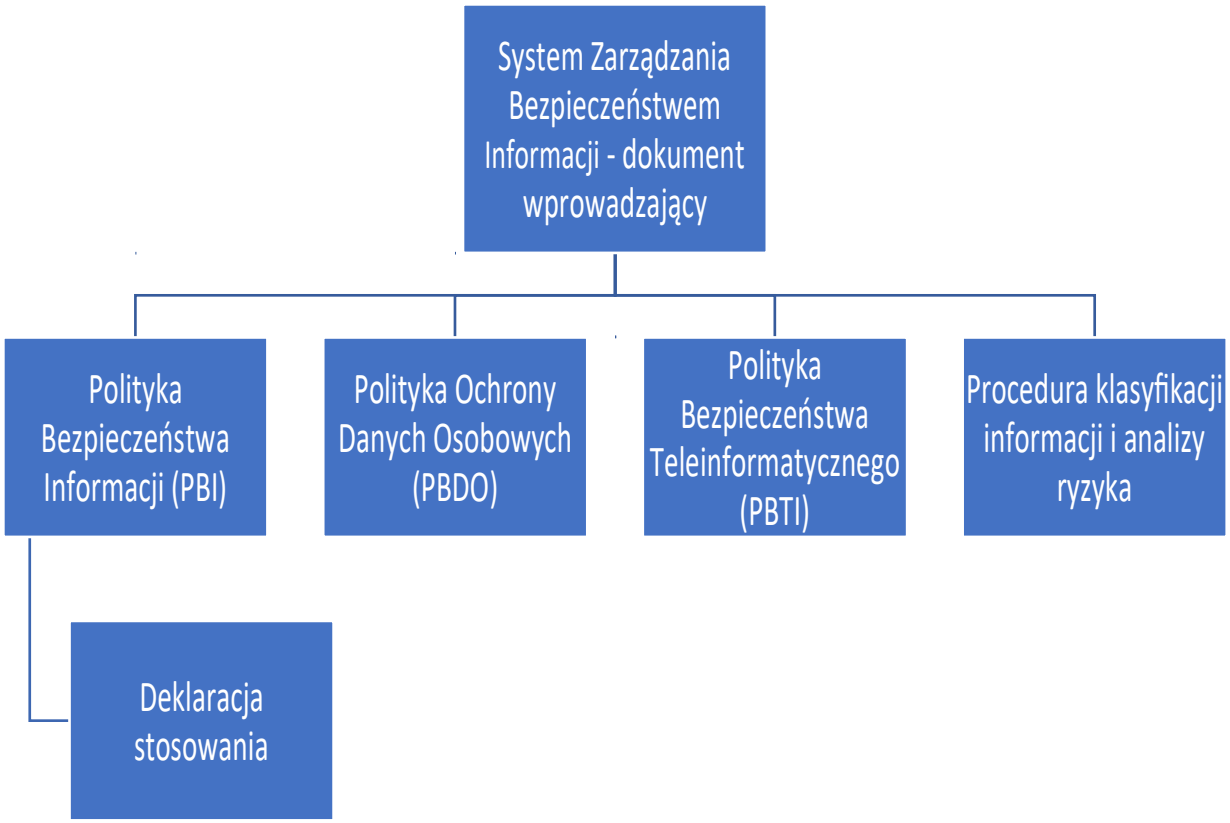
Numer zmiany		Imię i Nazwisko	Zdarzenie	Data zdarzenia
1	Opracował:	Bogusław Kowalski	Utworzenie v.1.0	7.09.2023
	Zatwierdził:	Andrzej Cześnik		11.09.2023
2	Opracował:	Bogusław Kowalski	Aktualizacja v.1.1	13.02.2025
	Zatwierdził:	Przemysław Burzyński		20.03.2025

Spis treści

1. Wprowadzenie

Niniejszy dokument przedstawia główne założenia w obszarze realizacji kluczowych elementów funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w Starostwie Powiatowym w Sierpcu, wraz ze wskazaniem wymagań normy ISO/IEC 27001, a także regulacji zewnętrznych, którym podlega Starostwo:

- 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 Starostwa Powiatowego w Sierpcu 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 Starostwa jest domeną Starosty Sierpeckiego. Podobnie w zakresie bezpieczeństwa informacji, dla najważniejszych zagadnień związanych z artykułowaniem wizji i kierunków rozwoju niezbędne jest wkomponowanie SZBI w struktury zarządzania Starostwem.
W ramach wdrożenia SZBI przyjmuje się, iż Starosta 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 Starostwa,
- Zatwierdzenia dokumentów wchodzących w skład Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).

Koordynator Bezpieczeństwa

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

- Zapewnienie funkcjonowania systemu zarządzania w Starostwie opartego o wymagania normy ISO/IEC 27001,
- Nadzorowanie wspólnych dla wszystkich obszarów Starostwa elementów dokumentacji, zawierającej wymagania dla bezpieczeństwa informacji,
- Realizacja zadań pozwalających na utrzymanie Systemu Zarządzania Bezpieczeństwem Informacji w Starostwie,
- Raportowanie do Starosty 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 Starosty. Do odpowiedzialności Zastępcy Koordynatora należy utrzymanie Systemu Zarządzania Bezpieczeństwem Informacji na terenie Starostwa, w szczególności:

- Zapewnienie funkcjonowania systemu zarządzania w Starostwie opartego o wymagania normy ISO/IEC 27001,
- Wypełnienie wymagań zdefiniowanych we wspólnej dla całego Starostwa 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 Starostwie. 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 Starostwa

Pracownicy Starostwa 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 - Staroście do akceptacji. Zakłada się aktywny udział członków Forum Bezpieczeństwa Informacji w:

- Opiniowaniu treści polityki i innych dokumentów obowiązujących w Starostwie,
- Przygotowaniu materiałów na Przegląd Zarządzania i uczestnictwo w przeglądzie,
- Przygotowaniu zakresu analiz ryzyka oraz opiniowaniu wyników oceny ryzyka przed zatwierdzeniem przez Starostę,
- Definiowaniu działań doskonalących wynikających z audytów, przeglądów, incydentów oraz oceny ryzyka, które mają wpływ na działalność Starostwa. 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 Starostwie. Zespół Zarządzania Incydentami (ZZI) odpowiada między innymi za:

- Klasyfikację zdarzeń identyfikowanych w Starostwie 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:

- Starosta Sierpecki – 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 Starostwie, 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" ma na celu określenie strategicznych kierunków i odpowiedzialności wynikających z wdrożonego SZBI w Starostwie. Wszelkie szczegóły w tym zakresie zostały opisane w dokumentach powiązanych m. in. Polityka Bezpieczeństwa Informacji oraz Polityka Bezpieczeństwa Teleinformatycznego.

Procedura klasyfikacji informacji i analizy ryzyka

Starostwo Powiatowe w Sierpcu

Wydanie 1.1

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

Historia dokumentu

Numer zmiany		Imię i Nazwisko	Zdarzenie	Data zdarzenia
1	Opracował:	Bogusław Kowalski	Utworzenie v.1.0	7.09.2023
	Zatwierdził:	Andrzej Cześnik		11.09.2023
2	Opracował:	Bogusław Kowalski	Aktualizacja v.1.1	13.02.2025
	Zatwierdził:	Przemysław Burzyński		20.03.2025

Spis treści

1. Wprowadzenie

Niniejszy dokument określa metodykę szacowania oraz postępowania z ryzykami związanymi z przetwarzaniem informacji w Starostwie Powiatowym w Sierpcu, zgodnie z normą PN-ISO/IEC 27001:2023., rozdziały 6.1.2, 6.1.3, 8.2 oraz 8.3
Metodyka szacowania i postępowania z ryzykiem w Starostwie Powiatowym w Sierpcu została zaprojektowana oraz wdrożona zgodnie z dobrymi praktykami oraz następującymi regulacjami:

- Norma PN-EN ISO/IEC 27001:2023 (Bezpieczeństwo Informacji, cyberbezpieczeństwo i ochrona prywatności – Systemy zarządzania bezpieczeństwem informacji - Wymagania),
- Norma PN-ISO/IEC 27005 Technika Informatyczna, Techniki bezpieczeństwa, Zarządzanie ryzykiem w bezpieczeństwie informacji,
- Norma PN-ISO 31000 Zarządzanie ryzykiem, Zasady i wytyczne,
- 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;
- Polityka Bezpieczeństwa Teleinformatycznego;
- 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 Starostwie,

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,

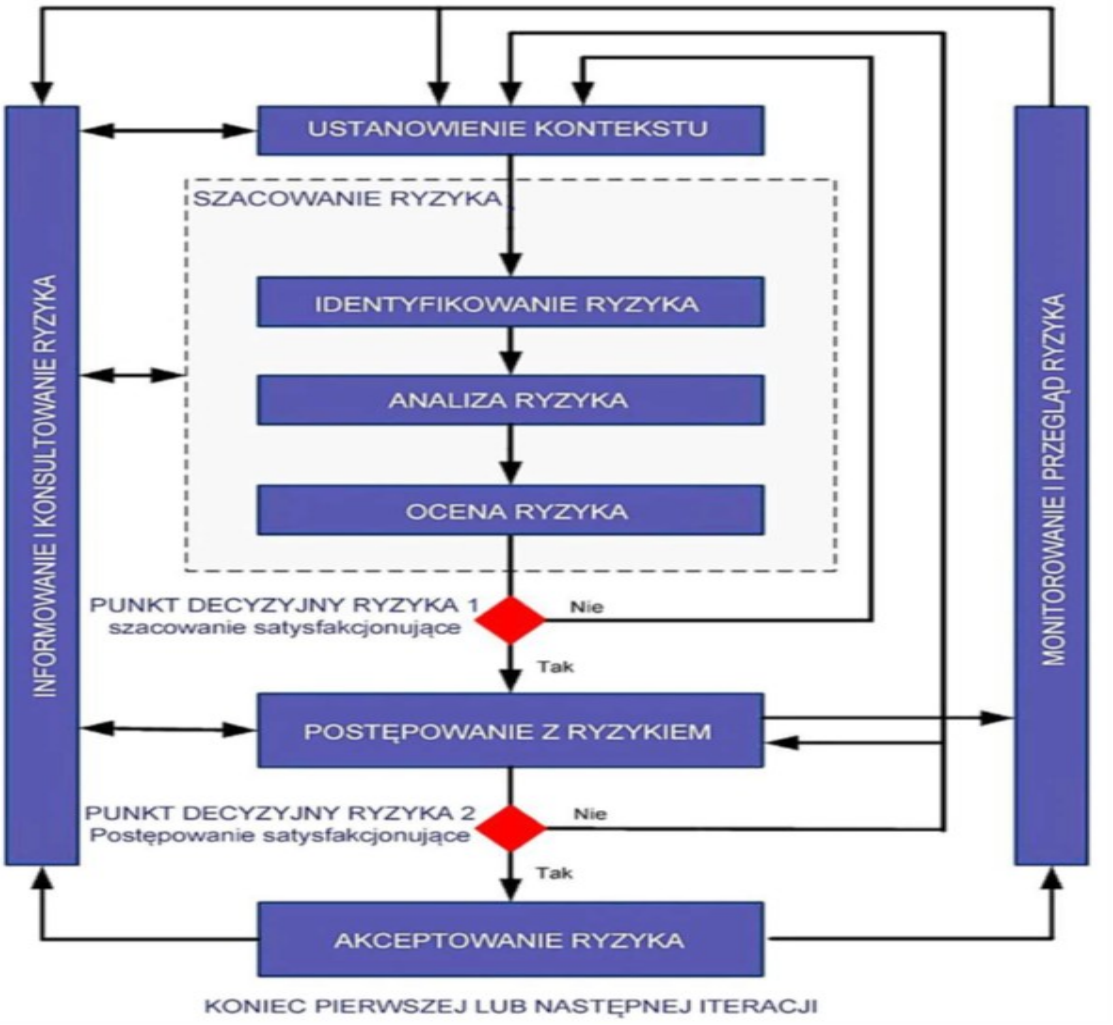
Zarządzanie ryzykiem – skoordynowane działania dotyczące kierowania i nadzorowania organizacji w odniesieniu do ryzyka.

3. Proces zarządzania ryzykiem

Proces zarządzania ryzykiem w bezpieczeństwie informacji w Starostwie Powiatowym w Sierpcu 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

4. Zakres i granice procesu zarządzania ryzykiem

Proces zarządzania ryzykiem w bezpieczeństwie informacji w Starostwie Powiatowym w Sierpcu jest stosowany w całej organizacji i obejmuje wszystkie aktywa informacyjne Starostwa.

Określając zakres i granice zarządzania ryzykiem organizacja wzięła pod uwagę:

- Cele realizowane przez Starostwo,
- 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 Starostwa Powiatowego w Sierpcu, którzy biorą udział w szacowaniu ryzyka oraz postępowaniu z ryzykiem.

5. Cele zarządzania ryzykiem

Celem zarządzania ryzykiem w Starostwie Powiatowym w Sierpcu jest:

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

6. Kontekst zewnętrzny i wewnętrzny Starostwa

Kontekst działalności Starostwa Powiatowego w Sierpcu 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

- Urząd Marszałkowski, Urząd Wojewódzki - sprawna realizacja powierzonych zadań administracyjnych,
- Instytucje publiczne regulujące pracę administracji - sprawna realizacja zadań powierzonych do Starostwa,
- Organizacje pozarządowe na terenie Starostwa - wsparcie dla działalności organizacji, patronat.

Kontekst wewnętrzny

- Starostwa i kadra Kierownicza - bezpieczeństwo zasobów informacyjnych, unikanie i zapobieganie incydentom bezpieczeństwa informacji,
- Pracownicy Starostwa Powiatowego w Sierpcu - 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 Starostwie

- 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 (tj. Dz. U. z 2019 r poz. 1781),
- 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 (tj. Dz. U. z 2022 r. poz. 1634),
- Ustawa z 14 grudnia 218 r o ochronie danych osobowych przetwarzanych w związku ze zwalczaniem przestępczości (Dz. U. z 2019 r poz. 125).

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. Starosta:
    - 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 zdarzyć 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 Starostwa.

Szacując ryzyko Starostwa Powiatowego w Sierpcu:

- 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 podstawą do określenia właściwych opcji postępowania z ryzykiem oraz wyboru adekwatnych zabezpieczeń.

Stosowane przez Starostwo Powiatowe w Sierpcu zabezpieczenia zostały określone w Deklaracji Stosowania.

Dla działań szacowania i postępowania z ryzykiem w Starostwie Powiatowym w Sierpcu stosuje się podejście iteracyjne, polegające na powtarzaniu czynności szacowania ryzyka i postępowania z tym ryzykiem oraz zwiększeniu szczegółowości analizy w każdej iteracji.

9. Identyfikacja aktywów

Starostwo identyfikuje wszystkie zasoby / aktywa związane z procesami funkcjonującymi w Starostwie, czyli wszystkie aktywa, które mogą wpływać na poufność, integralność i dostępność informacji w Starostwie Powiatowym w Sierpcu.

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 Starostwie Powiatowym w Sierpcu klasyfikowane są w następujących grupach:

Informacje publiczne (przeznaczone dla wszystkich):

- Informacje udostępniane na stronach internetowych Starostwa,
- 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 Starostwa,
- 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 Starostwa (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 Starostwo i Jednostki Organizacyjne.

W Starostwie Powiatowym w Sierpcu 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 Starostwa,
- 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 Starostwa. 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 Starostwa. (Wysoka strata finansowa – powyżej 1% budżetu Starostwa)
Poważny	4	Poważny wpływ na realizacje zadania w tym poważne zagrożenie terminu jego realizacji i osiągnięcia celu, poważne konsekwencje prawne, zagrożenie bezpieczeństwa pracowników, poważne straty finansowe, poważny wpływ na wizerunek Starostwa (Poważny skutek finansowy – od 0,5% do 1% budżetu Starostwa)
Średni	3	Średni wpływ na realizację zadań i celów, umiarkowane konsekwencje prawne, średni skutek finansowy, brak wpływu na bezpieczeństwo pracowników, średni wpływ na wizerunek Starostwa. (Średni skutek finansowy – od 0,2% do 5% budżetu Starostwa)
Mały	2	Mały wpływ na realizację celów i zadań, bez skutków prawnych, mały skutek finansowy, brak wpływu na bezpieczeństwo pracowników, niewielki wpływ na wizerunek Starostwa. (Mały skutek finansowy – od 0,1% do 0,2% budżetu Starostwa)
Nieznaczny	1	Znikomy wpływ na realizację zadań i celów, brak skutków prawnych, nieznaczny skutek finansowy, brak wpływu na bezpieczeństwo pracowników, brak wpływu na wizerunek Starostwa. (Nieznaczny skutek finansowy do 0,1 % budżetu Starostwa)

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 Starostwie Powiatowym w Sierpcu 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 Starostwie Powiatowym w Sierpcu 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

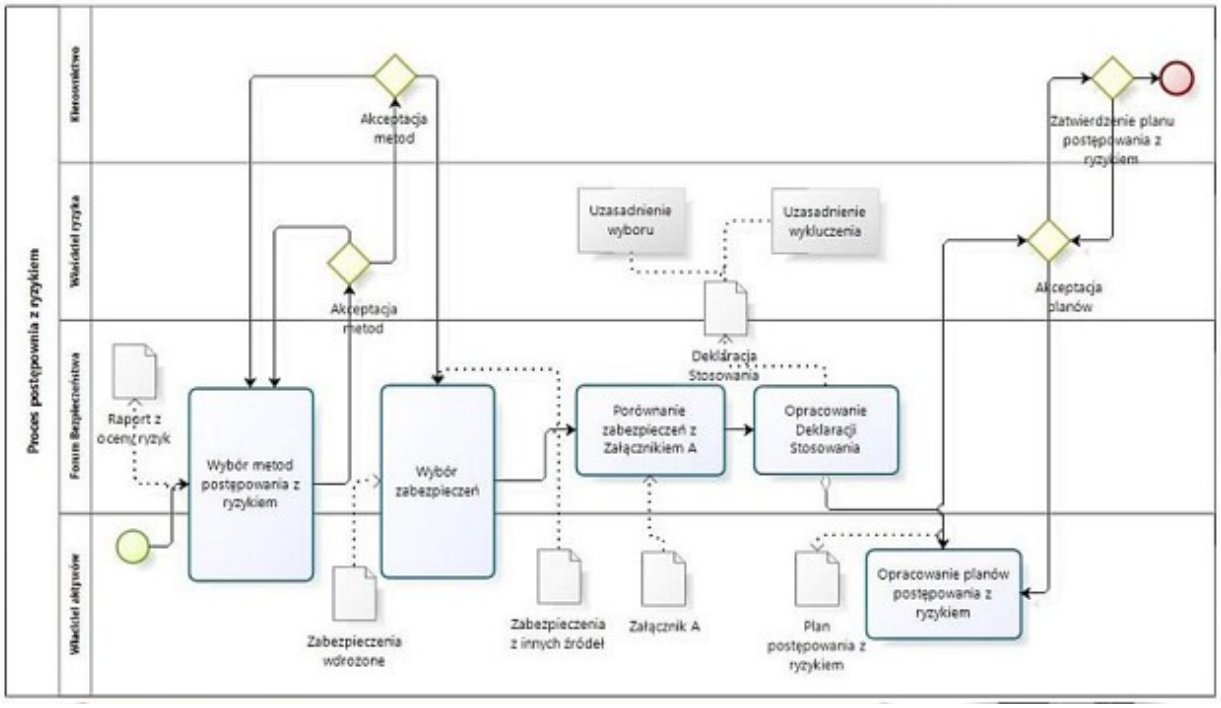
- Ryzykiem akceptowanym jest ryzyko niskie oraz ryzyko umiarkowane. Ryzyko wysokie przekracza akceptowany poziom ryzyka.
- Ryzyko przekraczające akceptowany poziom ryzyka wymaga ustalenia i podjęcia działań ograniczających je do poziomu umiarkowanego lub niskiego poprzez zmniejszenie jego wpływu lub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

Starostwo Powiatowe w Sierpcu 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 Starostwie Powiatowym w Sierpcu.



Dla wszystkich zasobów/działań, których poziom ryzyka będzie wyższy niż dopuszczalny, Starostwo 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 -** podjęcie 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 Starostwie Powiatowym w Sierpcu 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 zarządzania 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)
Załącznik nr 4: Przykłady podatności (wg Normy PN-ISO/IEC 27005)

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 Starostwa Powiatowego w Sierpcu.

.....

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 pogodowe
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 sprzętu (komputery, drukarki, niszczarki, itp.)
	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
	Brak lub niewłaściwe działanie urządzeń podtrzymujących napięcie (np. UPS)
	Brak lub niewystarczająca kontrola i przeglądy klimatyzatora w serwewrowni
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 teleinformatycznego
	Niewystarczające szkolenia personelu Starostwa w zakresie ochrony przeciwpożarowej o ewakuacji.
	Brak lub niewystarczające szkolenia w zakresie obsługi informatycznej
	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
	Niestabilna sieć elektryczna
	Niestabilna sieć informatyczna i telekomunikacyjna
	Brak lub niedostateczny nadzór nad klientami Starostwa przebywającymi w budynku administracyjnym w godzinach jak i po godzinach pracy.
	Brak fizycznej ochrony budynków, drzwi i okien przed włamaniem (np. żaluzje antywłamaniowe)
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

Polityka Bezpieczeństwa Informacji

Starostwo Powiatowe w Sierpcu

Wydanie 1.1

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

Historia dokumentu

Numer zmiany		Imię i Nazwisko	Zdarzenie	Data zdarzenia
1	Opracował:	Bogusław Kowalski	Utworzenie v.1.0	7.09.2023
	Zatwierdził:	Andrzej Cześnik		11.09.2023
2	Opracował:	Bogusław Kowalski	Aktualizacja v.1.1	13.02.2025
	Zatwierdził:	Przemysław Burzyński		20.03.2025

Spis treści

1. Wprowadzenie

Polityka Bezpieczeństwa Informacji w Starostwie Powiatowym w Sierpcu 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 Starostwa i jest chroniona na każdym szczeblu organizacji.

2. Cele Systemu Zarządzania Bezpieczeństwem Informacji

Głównymi celami Systemu Zarządzania Bezpieczeństwem Informacji w Starostwie są:

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

Najwyższe kierownictwo, wdrażając Politykę Bezpieczeństwa Informacji zgodnie z wymaganiami normy PN-EN ISO/IEC 27001:2023 pkt. 5.2; 6.2; 7.5 wykazuje przywództwo i zaangażowanie w kontekście bezpieczeństwa informacji podczas realizowanych procesów w Starostwie 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 27001:2023 pkt 4.3, Organizacja, określając zakres Systemu Zarządzania Bezpieczeństwem Informacji, rozważa jej kontekst wewnętrzny oraz zewnętrzny, identyfikuje strony zainteresowane, a także określa interfejsy i zależności między działaniami wykonywanymi wewnątrz organizacji, a także przez inne organizacje.

System Zarządzania Bezpieczeństwem Informacji obejmuje zakresem całe Starostwo Powiatowe w Sierpcu 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.

Starostwo Powiatowe w Sierpcu zapewnia 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 Starostwie 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 27001:2023 (Bezpieczeństwo Informacji, cyberbezpieczeństwo i ochrona prywatności – Systemy zarządzania bezpieczeństwem informacji - Wymagania),
- 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 Starostwo Powiatowe w Sierpcu w oparciu o normę PN-ISO/ IEC 27001:2023.

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 Starostwa, 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

Starostwo Powiatowe w Sierpcu zobowiązane 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 aktualna 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, Starostwo Powiatowe w Sierpcu 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 Starostwa 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 Starostwo.

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 27001:2023, wymagania prawne, wymagania wewnętrzne oraz zewnętrzne,
- W przypadku pojawienia się niezgodności podejmowane są natychmiastowe działania korygujące,
- Audyt wewnętrzny przeprowadzany jest minimum raz w roku,
- Audytorzy dobierani są w sposób zapewniający zachowanie obiektywności i bezstronności,
- Wyniki audytu przedstawiane są przez Koordynatora Bezpieczeństwa do najwyższego kierownictwa.

9. Strategia ciągłości działania

Starostwo Powiatowe w Sierpcu 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, Starostwo Powiatowe w Sierpcu posiada aktualne plany ciągłości działania systemów, które są własnością Starostwa. W przypadku wykorzystywania usług zewnętrznych obowiązują umowy z zewnętrznymi podmiotami w ramach, których określone są parametry SLA umożliwiające zapewnienie ciągłości działania kluczowych usług Starostwa.

Administrator systemów teleinformatycznych lub podmiot świadczący usługi na rzecz Starostwa Powiatowego w Sierpcu 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 stosowne, 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,
- Obsługa incydentów dotyczących Danych Osobowych została szczegółowo opisana w procedurze zgłaszania incydentów umieszczonej w dokumencie ,,*Polityka Ochrony Danych Osobowych*",
- 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 Starostwie Powiatowym w Sierpcu w całości nadzorowana jest przez Inspektora Ochrony Danych (IOD). W ramach odpowiedzialności Inspektora Ochrony Danych jest przede wszystkim:

- Zapewnienie, że wszystkie zadania realizowane przez Starostwo 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,
- Szczegółowe wytyczne dotyczące ochrony danych osobowych zostały opisane w Polityce Bezpieczeństwa Danych Osobowych (PBDO).

12. Odpowiedzialność pracowników organizacji

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 27001:2023 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 dostosować 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, Starostwo kieruje się w szczególności zasadą ograniczonego celu, ograniczonego przechowywania oraz poufności,
- Starostwo przechowuje dane osobowe osób składających dokumentację aplikacyjną w trybie ogłoszonego do informacji publicznej konkursu przez okres wskazany w jednolitym rzeczowym wykazie akt osobowych,
- Starostwo 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,
- Starostwo zapewnia ochronę przed nieuprawnionym dostępem do tych danych osobowych, a jednocześnie do sprzętu, który służy do przetwarzania takich danych,
- Starostwo 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),
- Starostwo przeprowadza weryfikację czy dane zawarte w dokumentacji aplikacyjnej są zgodne ze stanem faktycznym,
- Starostwo 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 Starostwo do przechowywania powyższych informacji przez określony czas.

Rozwiązanie współpracy z pracownikiem

W przypadku rozwiązania współpracy z pracownikiem Starostwa należy:

- Odebrać wszystkie uprawnienia do systemów teleinformatycznych,
- Odebrać wszystkie uprawnienia umożliwiające dostęp fizyczny do Starostwa,
- 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 Starostwie 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.

Monitorowanie bezpieczeństwa fizycznego

W Starostwie Powiatowym w Sierpcu zgodnie z wymaganiami normy PN-EN ISO/IEC 27001:2023 Załącznik A pkt 7.4 zastosowano monitoring wizyjny w celu kontroli nad nieuprawnionym dostępem fizycznym do pomieszczeń Starostwa.

Dane z monitoringu wizyjnego przechowywane są co najmniej przez okres 30 dni.

16. Bezpieczeństwo informacji w relacjach z Dostawcami

W przypadku dostawców zakres Polityki Bezpieczeństwa Informacji ma zastosowanie do:

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

Poufność informacji pomiędzy Starostwem 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 Starostwa zgodnie z podpisanymi Umowami i służy realizacji celów biznesowych Starostwa.

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

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

17. Bezpieczeństwo informacji w ramach Krajowych Ram Interoperacyjności

W celu zapewnienia Bezpieczeństwa informacji w ramach Krajowych Ram Interoperacyjności Starostwo 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 Starostwo 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.

Starostwo Powiatowe w Sierpcu 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.

Starostwo Powiatowe w Sierpcu 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. Praca zdalna

W celu zapewnienie bezpieczeństwa podczas wykonywania pracy w formie zdalnej organizacja przyjęła następujące zasady:

- Zapewnienie bezpiecznego połączenia z siecią – korzystanie z bezpiecznych, szyfrowanych połączeń VPN,
- Informowanie pracowników Starostwa o konieczności regularnego aktualizowania oprogramowania sprzętu sieciowego (routery) w sieci domowej przez pracowników, których sprzęt stanowi własność,
- Zabrania się wykorzystywania publicznych sieci Wifi,
- Pracownicy zobowiązani są do wykorzystywania tylko i wyłącznie sprzętu służbowego do świadczenia pracy w formie zdalnej,
- Pracownicy podczas opuszczania miejsca pracy (oddalenie się od sprzętu służbowego) zobowiązani są do zablokowania sprzętu uniemożliwiając dostęp osób trzecich,
- Pracownicy zobowiązani są podczas świadczenia pracy w formie zdalnej do uniemożliwienia dostępu osób postronnych do ekranu komputera/telefonu i dokumentów,
- Pracownicy zobowiązani są do unikania rozmów poufnych w miejscach publicznych,
- Pracownicy zobowiązani są po zakończeniu pracy do wyłączenia sprzętu i zabezpieczenia przed dostępem osób trzecich,
- Zabrania się udostępniania sprzętu służbowego do innych celów niż realizacja obowiązków służbowych, a także udostępniania zasobów osobom trzecim.

19. Wykaz załączników

- Załącznik nr 1 – Deklaracja stosowania

Polityka Bezpieczeństwa Teleinformatycznego

Starostwo Powiatowe w Sierpcu

Wydanie 1.1

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
CENTRUM PROJEKTÓW POLSKA CYFROWA

Historia dokumentu

Numer zmiany		Imię i Nazwisko	Zdarzenie	Data zdarzenia
1	Opracował:	Bogusław Kowalski	Utworzenie v.1.0	7.09.2023
	Zatwierdził:	Andrzej Cześnik		11.09.2023
2	Opracował:	Bogusław Kowalski	Aktualizacja v.1.1	13.02.2025
	Zatwierdził:	Przemysław Burzyński		20.03.2025

Spis treści

1. Wprowadzenie

Polityka Bezpieczeństwa Teleinformatycznego w Starostwie Powiatowym w Sierpcu 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 Starostwie Powiatowym w Sierpcu została zaprojektowana oraz wdrożona zgodnie z dobrymi praktykami oraz następującymi regulacjami:

- Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2017 poz. 2247),
- Norma PN-EN ISO/IEC 27001:2023 (Bezpieczeństwo Informacji, cyberbezpieczeństwo i ochrona prywatności – Systemy zarządzania bezpieczeństwem informacji - Wymagania),
- 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 Starostwa i podmiotów zewnętrznych wykonujących prace w infrastrukturze teleinformatycznej Starostwa Powiatowego w Sierpcu.

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:

- Starostwo 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 osobom,
- 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 zabezpieczenia kryptograficzne dostarczane przez producenta urządzenia mobilnego,
- Zabronione jest instalowanie aplikacji, które nie są wykorzystywane do obowiązków służbowych.

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,
- Szczegółowe zasady tworzenia kopii zapasowych danych osobowych przetwarzanych w systemie informatycznym zostały opisane w Polityce Bezpieczeństwa Danych Osobowych ,,*XII Procedura tworzenia kopi zapasowych*".

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 chronić 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 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 Starostwa.

10. Zasady eksploatacji systemów teleinformatycznych

Zasady ogólne:

- Wszelkie zmiany w konfiguracji sprzętu komputerowego wykonują wyznaczeni administratorzy,
- Zasoby teleinformatyczne Starostwa 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,

- Uprawnienia do systemów teleinformatycznych dla firm zewnętrznych możliwe jest tylko i wyłącznie w sytuacji zabezpieczenia prawnego,
- Wszelkie działania firm zewnętrznych w infrastrukturze teleinformatycznej Starostwa muszą 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 Starostwa zobowiązani są do stosowania zasady tzw. ,,czystego biurka",
- Wszyscy pracownicy Starostwa zobowiązani są do stosowania zasady tzw. ,,czystego pulpitu",
- 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 ze Starostwem, pracownik zobowiązany jest do zwrotu wszystkich aktywów powierzonych przez Starostwo,

- 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 Starostwa muszą odbywać się z zapewnieniem ciągłości działania tych środowisk,
- Środowiska teleinformatyczne w Starostwie 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 Starostwa oraz firmy zewnętrzne realizujące przedmiotowe prace na rzecz Starostwa 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 Starostwa 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,
- Wszystkie prace audytowe muszą być realizowane z uwzględnieniem takich samych wymagań jak wymagania dotyczące rozwoju systemów teleinformatycznych tj. wykorzystywanie danych zanonimizowanych, zapewnienie ciągłości działania systemów teleinformatycznych, bieżące monitorowanie systemów teleinformatycznych i skutków oddziaływania prowadzonego audytu.

Użytkownikom systemów teleinformatycznych zabrania się:

- Transferu danych do nieautoryzowanych przez Starostwo lokalizacji sieciowych, przetwarzanie ich w nieautoryzowanej publicznej chmurze obliczeniowej lub przesyłanie na prywatne adresy pocztowe,
- Łączenia zasobów teleinformatycznych Starostwa 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 Starostwa,
- 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 Starostwie, w tym również przygotowywanie wytycznych do postępowań zakupowych realizowanych przez Starostwo 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 Starostwa,
- 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 Starostwie,
- 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 platform: ePUAP oraz e-doręczenia
- 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 oraz platformy e-doręczenia 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 platformach ePUAP oraz e-doręczenia.
- 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 Starostwo Powiatowe w Sierpcu 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 Starostwo Powiatowe w Sierpcu za pośrednictwem systemów teleinformatycznych monitorowane są pod względem zachowania odpowiedniego poziomu dostępności w oparciu o obowiązującą dokumentację eksploatacyjną,
- Zasoby teleinformatyczne Starostwa (sprzęt, oprogramowanie, protokoły komunikacyjne, szyfrujące) projektowane są i wdrażane zgodnie z najlepszymi praktykami w celu odpowiedniego zabezpieczenia przetwarzanych informacji. Podczas projektowania

systemów zarówno pracownicy Starostwa 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 Starostwa,

- 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 Starostwie 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 i 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 do 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 Starostwa 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 Starostwa 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 Starostwa w momencie zidentyfikowania podatności w systemach teleinformatycznych zobowiązany jest do powiadomienia o tym fakcie administratora lub właściciela systemu,
- 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 Starostwa wykorzystujący w ramach obowiązków służbowych systemy teleinformatyczne powinni odbyć szkolenie w zakresie bezpiecznego wykorzystywania systemów i cyberzagrożeń z nimi związanych.

17. Maskowanie danych

W przypadku dostępu do systemów teleinformatycznych przez podmioty zewnętrzne lub osoby, które nie posiadają uprawnień dostępu do danych produkcyjnych organizacja stosuje maskowanie informacji. Maskowanie danych odbywa się zgodnie z poniższymi wytycznymi:

- Analiza wymagań i celów maskowania danych – określenie jakie dane podlegają maskowaniu (np. dane osobowe, dane finansowe) a następnie zdefiniowanie celu maskowania (np. ochrona prywatności, ochrona z regulacjami prawnymi),
- Identyfikacja i klasyfikacja danych – przeprowadzenie inwentaryzacji danych w systemie teleinformatycznym oraz określenie ich klasy poufności,
- Wybór odpowiedniej metody maskowania (np. zastępowanie danych losowymi wartościami, szyfrowanie, anonimizacja),
- Wdrożenie – przeprowadzenie procesu maskowania na wskazanych danych (np. poprzez skrypty automatyzujące),
- Weryfikacja – sprawdzenie czy dane zostały prawidłowo zamaskowane,
- Udokumentowanie procesu maskowania,
- Przeszkolenie personelu z zasad maskowania.

18. Bezpieczeństwo informacji w usługach chmurowych

W przypadku wykorzystywania przez organizację usług umieszczonych w infrastrukturze chmurowej organizacja stosuje następujące podejście:

- Ocena ryzyka (przeprowadzenie analizy ryzyka dla procesów i danych przenoszonych do chmury),
- Wybór Dostawcy usługi chmurowej (sprawdzenie certyfikatów i zgodności z normami bezpieczeństwa ISO 27001, SOC2),
- Weryfikacja lokalizacji centrów przetwarzania danych – rekomendowanymi lokalizacjami jest obszar EOG (Europejskiego Obszaru Gospodarczego),
- Zabezpieczenie dostępu – wdrożenie uwierzytelniania wieloskładnikowego (MFA) dla wszystkich użytkowników oraz stosowanie zasady minimalnych uprawnień w konfiguracji dostępu do zasobów,
- Stosowanie regularnego przeglądu uprawnień,
- Szyfrowanie danych – stosowanie szyfrowania danych (at rest) w spoczynku oraz (in transit) podczas transmisji. Rodzaj stosowanych kluczy szyfrowania (klucze zarządzane przez Dostawcę lub klucze zarządzane przez organizację) uwarunkowany jest od analizy ryzyka,
- Monitorowanie – włączenie monitorowania zdarzeń czynności przeprowadzanych przez użytkowników,
- Szkolenia – przeprowadzenie szkoleń z bezpiecznego wykorzystywania usług chmurowych.

19. Zapobieganie wyciekom informacji

W celu zapewnienia ochrony przed wyciekiem informacji organizacja stosuje:

- Identyfikację i klasyfikację informacji,
- Politykę Bezpieczeństwa Informacji oraz Bezpieczeństwa Teleinformatycznego, które określają zasady bezpiecznego przetwarzania informacji oraz bezpiecznego wykorzystywania systemów teleinformatycznych, w których informacje są umieszczone,
- Stosowanie zasady minimalnych niezbędnych uprawnień do informacji, które są niezbędne do wykonywania obowiązków służbowych,
- Stosowanie szyfrowania danych na podstawie analizy ryzyka,
- Zabezpieczenie dostępu do systemów teleinformatycznych,
- Zabezpieczenie dostępu do pomieszczeń fizycznych,
- Szkolenie pracowników z zakresu bezpiecznego przetwarzania informacji.

POWIAT SIERPECKI
STAROSTWO POWIATOWE W SIERPCU
ul. Świętokrzyska 2a, 09-200 Sierpc, tel. 24 275 91 01, e-mail: starosta@powiat.sierpc.pl

OŚWIADCZENIE
zapoznania się Politykami Systemu Zarządzania Bezpieczeństwem Informacji oraz RODO

Oświadczam, iż zostałam/em zapoznana/y z przepisami dotyczącymi ochrony danych osobowych, w szczególności z przepisami 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 (ogólne rozporządzenie o ochronie danych – RODO, Dz. Urz. UE L Nr 119, str. 1, ze zm.), z przepisami ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r. poz. 730 ze zm.) oraz wydanych na jej podstawie aktów wykonawczych, a także z przepisami wprowadzonej i wdrożonej do stosowania Polityki Bezpieczeństwa Informacji, w tym danych osobowych oraz zobowiązuję się do ich stosowania.

W szczególności, zobowiązuję się do:

- zachowania w tajemnicy danych osobowych, jak również wszelkich innych informacji służbowych, do których mam lub będę miał/a dostęp w związku z wykonywaniem zadań służbowych lub obowiązków pracowniczych,
- niewykorzystywania danych osobowych oraz innych informacji w celach pozasłużbowych, o ile nie są one jawne,
- przestrzegania wdrożonych procedur i regulaminów oraz ustalonego w pracy porządku,
- dbania o dobro zakładu pracy, ochrony jego mienia oraz zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę,
- przestrzegania tajemnicy określonej w odrębnych przepisach, w tym w przepisach szczegółowych,
- przestrzegania zasad współżycia społecznego,
- zachowania w tajemnicy sposobów zabezpieczenia danych osobowych oraz innych informacji, o ile nie są one jawne,
- korzystania ze sprzętu IT oraz oprogramowania wyłącznie w związku z wykonywaniem obowiązków oraz zgodnie z obowiązującymi instrukcjami, procedurami i politykami,
- wykorzystywania jedynie legalnego oprogramowania pochodzącego od Administratora,
- należytej dbałości o sprzęt i oprogramowanie zgodnie z dokumentacją przetwarzania danych osobowych,
- korzystania z komputerów przenośnych zgodnie z obowiązującymi procedurami bezpieczeństwa danych,
- nieudostępniania sprzętu służbowego, w szczególności urządzeń mobilnych, osobom trzecim.
- zapoznania się aktualną Polityką Bezpieczeństwa Informacji oraz jej przestrzegania.
- zapoznanie się z aktualną Polityką Bezpieczeństwa Teleinformatycznego oraz jej przestrzegania.

Oświadczam, iż dnia 18 marca 2025 roku, odbyłem szkolenie z zakresu Polityk Bezpieczeństwa oraz RODO i przyjmuję do stosowania.

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 1 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)

Deklaracja Stosowania

5	Zabezpieczenia organizacyjne	
5.1	Polityki bezpieczeństwa informacji	Polityka Bezpieczeństwa Informacji została zatwierdzona przez najwyższe kierownictwo oraz stosownie ogłoszona pracownikom organizacji oraz właściwym stronom zainteresowanym. Uzasadnienie wyboru zabezpieczenia: zobowiązanie pracowników organizacji oraz stron zainteresowanych do przestrzegania w stosownym zakresie zasad przyjętych w organizacji w ramach przyjętego Systemu Zarządzania Bezpieczeństwem Informacji.
5.2	Role i odpowiedzialność za bezpieczeństwo informacji	Najwyższe kierownictwo wspiera bezpieczeństwo informacji w organizacji określając kierunki działania oraz przejmując, a także rozdzielając odpowiedzialność za bezpieczeństwo informacji w organizacji. Uzasadnienie wyboru zabezpieczenia: ustalenie ról oraz odpowiedzialności za bezpieczeństwo w organizacji w celu swobodnego delegowania zadań w tym zakresie.
5.3	Rozdzielanie obowiązków	Obowiązki i odpowiedzialność rozdzielone są w organizacji zgodnie z regulaminami wewnętrznymi i nie pozostają ze sobą w konflikcie, który mógłby prowadzić do nieuprawnionej lub nieumyślnej modyfikacji lub nadużycia aktywów organizacji. Uzasadnienie wyboru zabezpieczenia: wszystkie osoby pełniące istotną rolę w bezpieczeństwie informacji mają przydzieloną odpowiedzialność oraz skonkretyzowany zakres obowiązków, co pozwala na zapewnienie sprawnie działającego Systemu Zarządzania Bezpieczeństwem Informacji.
5.4	Odpowiedzialność kierownictwa	Kierownictwo wymaga, aby wszyscy pracownicy i kontrahenci stosowali zasady bezpieczeństwa informacji zgodnie z obowiązującymi w organizacji politykami i procedurami poprzez zapewnienie stosownych instrumentów formalnoprawnych. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie informacji przed ich nieuprawnionym przejęciem, zniszczeniem bądź modyfikacją.
5.5	Kontakty z organami władzy	Polityka Bezpieczeństwa Informacji zawiera zapisy w zakresie kontaktu z organami władzy, szczególnie z Prezesem Urzędu Ochrony Danych Osobowych. Uzasadnienie wyboru zabezpieczenia: konieczność dostosowania organizacji do obowiązkowego zgłaszania do organu nadzorczego naruszenia w trybie 72 godzin od momentu jego identyfikacji.
5.6	Kontakty z grupami zainteresowanych specjalistów	Organizacja utrzymuje stosowne kontakty z grupami zainteresowanych specjalistów lub innymi specjalistycznymi forami oraz stowarzyszeniami zawodowymi z obszaru bezpieczeństwa informacji. Uzasadnienie wyboru zabezpieczenia: konieczność zapewnienia procesu ciągłego doskonalenia.
5.7	Rozpoznanie zagrożeń	Polityka Bezpieczeństwa Teleinformatycznego określa zasady dotyczące ochrony przed zagrożeniami spowodowanymi szkodliwym oprogramowaniem. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie informacji przed ich nieuprawnionym przejęciem, zniszczeniem bądź modyfikacją.
5.8	Bezpieczeństwo informacji w zarządzaniu projektami	Organizacja uwzględnia zakres bezpieczeństwa informacji w tworzeniu nowych projektów oraz zarządzania nimi. Uzasadnienie wyboru zabezpieczenia: konieczność uwzględnienia zakresu bezpieczeństwa informacji jeszcze w fazie projektowania.
5.9	Ewidencja informacji i innych powiązanych aktywów	W organizacji utrzymywana jest ewidencja posiadanych aktywów. Uzasadnienie wyboru zabezpieczenia: Zapewnienie kontroli nad posiadanymi aktywami.
5.10	Akceptowalne użycie informacji i innych powiązanych aktywów	Polityka Bezpieczeństwa Informacji oraz Bezpieczeństwa Teleinformatycznego identyfikuje, dokumentuje i wdraża zasady akceptowalnego użycia informacji oraz aktywów związanych z informacjami i środkami przetwarzania informacji. Uzasadnienie wyboru zabezpieczenia: Ustalenie zasad dla pracowników organizacji należytego korzystania z aktywów i informacji organizacji.

5.11	Zwrot aktywów	Polityka Bezpieczeństwa Informacji oraz Bezpieczeństwa Teleinformatycznego określa politykę zwrotu aktywów organizacji przez pracowników kończących zatrudnienie oraz kontrahentów rozwiązujących umowy lub porozumienia. Uzasadnienie wyboru zabezpieczenia: Ochrona posiadanych zasobów przez organizację w zakresie bezpieczeństwa informacji.
5.12	Klasyfikowanie informacji	Kierownictwo zapewnia, że w organizacji informacje są klasyfikowane z uwzględnieniem wymagań prawnych, wartości, krytyczności i wrażliwości na nieuprawnione ujawnienie lub modyfikację oraz wymaga, aby wszyscy pracownicy i kontrahenci stosowali zasady bezpieczeństwa informacji zgodnie z obowiązującymi w organizacji politykami i procedurami. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie danych przed ich nieuprawnionym przejęciem, zniszczeniem bądź modyfikacją.
5.13	Oznaczanie informacji	W organizacji obowiązują regulacje w zakresie oznaczania informacji zgodnie z przyjętym schematem klasyfikacji informacji. Uzasadnienie wyboru zabezpieczenia: systematyczne komunikowanie pracownikom oraz w uzasadnionych przypadkach stronom zainteresowanym zasady, jakie organizacja w ramach bezpieczeństwa informacji przyjęła.
5.14	Przesyłanie informacji	Polityka Bezpieczeństwa Teleinformatycznego określa zasady ochrony wymiany informacji przesyłanych z użyciem wszystkich rodzajów środków łączności. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie przesyłanych danych przed ich nieuprawnionym przejęciem, zniszczeniem bądź modyfikacją.
5.15	Kontrola dostępu	Polityka Bezpieczeństwa Informacji oraz Polityka Bezpieczeństwa Teleinformatycznego określa zasady dostępu do aktywów organizacji. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie danych przed ich nieuprawnionym przejęciem, zniszczeniem bądź modyfikacją.
5.16	Zarządzanie tożsamością	Polityka Bezpieczeństwa Teleinformatycznego określa zasady przydzielania praw dostępu dla pracowników do sieci i usług sieciowych w zakresie nadawania lub odbierania praw dostępu wszystkim kategoriom użytkowników. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie danych przed ich nieuprawnionym przejęciem, zniszczeniem bądź modyfikacją.
5.17	Informacje uwierzytelniające	Organizacja poddaje formalnemu procesowi zarządzania przydzielanie poufnych informacji uwierzytelniających. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie danych poufnych przed ich nieuprawnionym przejęciem, zniszczeniem bądź modyfikacją.
5.18	Prawa dostępu	Polityka Bezpieczeństwa Informacji oraz Bezpieczeństwa Teleinformatycznego określa zasady przydzielania pracownikom i użytkownikom zewnętrznym prawo dostępu do informacji i środków przetwarzania informacji oraz zasady ich odbierania po zakończeniu współpracy. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie danych przed ich nieuprawnionym przejęciem, zniszczeniem bądź modyfikacją.
5.19	Bezpieczeństwo informacji w relacjach z dostawcami	Polityka Bezpieczeństwa Informacji oraz Bezpieczeństwa Teleinformatycznego określa zasady dotyczące współpracy z zewnętrznymi Dostawcami. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie danych przed ich nieuprawnionym przejęciem, zniszczeniem bądź modyfikacją.
5.20	Uwzględnianie bezpieczeństwa informacji w porozumieniach z dostawcami	Polityka Bezpieczeństwa Informacji oraz Bezpieczeństwa Teleinformatycznego określa zasady dotyczące współpracy z zewnętrznymi Dostawcami. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie danych przed ich nieuprawnionym przejęciem, zniszczeniem bądź modyfikacją.
5.21	Zarządzanie bezpieczeństwem informacji w łańcuchu dostaw technologii teleinformatycznych (ICT)	Polityka Bezpieczeństwa Informacji oraz Bezpieczeństwa Teleinformatycznego określa zasady dotyczące współpracy z zewnętrznymi Dostawcami. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie danych przed ich nieuprawnionym przejęciem, zniszczeniem bądź modyfikacją.
5.22	Monitorowanie, przegląd i zarządzanie zmianami w usługach świadczonych przez dostawców	Organizacja regularnie monitoruje, przegląda i audytuje dostarczanie usług zewnętrznych dla organizacji. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie danych przed ich nieuprawnionym przejęciem, zniszczeniem bądź modyfikacją, a także zapewnieniem ciągłości działania usług.

5.23	Bezpieczeństwo informacji dotyczące stosowania usług w chmurze	Polityka Bezpieczeństwa Teleinformatycznego określa zasady dotyczące bezpiecznego wykorzystywania usług chmurowych. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie danych przed ich nieuprawnionym przejęciem, zniszczeniem bądź modyfikacją.
5.24	Planowanie i przygotowanie do zarządzania incydentami związanymi z bezpieczeństwem informacji	Polityka Bezpieczeństwa Informacji określa zasady dotyczące postępowania w przypadku incydentów bezpieczeństwa. Uzasadnienie wyboru zabezpieczenia: systematyczne komunikowanie pracownikom oraz w uzasadnionych przypadkach stronom zainteresowanym zasady, jakie organizacja w ramach bezpieczeństwa informacji przyjęła.
5.25	Ocena i podejmowanie decyzji w sprawie zdarzeń związanych z bezpieczeństwem informacji	Polityka Bezpieczeństwa Informacji określa odpowiedzialność w zakresie decyzji dotyczącej zakwalifikowania zdarzeń ich jako incydentów bezpieczeństwa. Uzasadnienie wyboru zabezpieczenia: prawidłowa obsługa zdarzeń stanowiących incydenty bezpieczeństwa
5.26	Reagowanie na incydenty związane z bezpieczeństwem informacji	Polityka Bezpieczeństwa Informacji określa zasady dotyczące zgłaszania incydentów bezpieczeństwa. Uzasadnienie wyboru zabezpieczenia: określenie sposobu postępowania w przypadku wystąpienia incydentów bezpieczeństwa.
5.27	Wyciąganie wniosków z incydentów związanych z bezpieczeństwem informacji	Wiedza zdobyta podczas analizy i rozwiązywania incydentów związanych z bezpieczeństwem informacji jest wykorzystywana do zredukowania prawdopodobieństwa wystąpienia lub skutków przyszłych incydentów. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie danych przed ich nieuprawnionym przejęciem, zniszczeniem bądź modyfikacją.
5.28	Gromadzenie materiału dowodowego	W przypadku zidentyfikowania zdarzenia stanowiącego incydent bezpieczeństwa, podczas jego obsługi sporządzana jest kompletna dokumentacja zawierająca materiał dowodowy. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie informacji stanowiącej materiał dowodowy ze zidentyfikowanego incydentu bezpieczeństwa.
5.29	Bezpieczeństwo informacji podczas zakłóceń	Organizacja posiada zabezpieczenia przed katastrofami naturalnymi, wrogim atakiem oraz wypadkami. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie danych organizacji przed ich nieuprawnionym przejęciem, zniszczeniem bądź modyfikacją.
5.30	Gotowość ICT do zapewnienia ciągłości działania	Polityka Bezpieczeństwa Informacji określa strategię w zakresie zarządzania ciągłością działania bezpieczeństwa informacji w sytuacjach kryzysowych. Uzasadnienie wyboru zabezpieczenia: zapewnienie ciągłości działania zarządzania bezpieczeństwem informacji.
5.31	Wymagania prawne, regulacyjne i umowne	Wszystkie istotne wymagania prawne, regulacyjne, umowne oraz podejście organizacji do ich przestrzegania jest zidentyfikowane, udokumentowane i aktualizowane dla każdego systemu informacyjnego oraz całości organizacji. Uzasadnienie wyboru zabezpieczenia: systematyczne komunikowanie pracownikom oraz w uzasadnionych przypadkach stronom zainteresowanym zasad, uwarunkowań prawnych jakie organizacja w ramach bezpieczeństwa informacji przyjęła i stosuje.
5.32	Prawa własności intelektualnej	W organizacji przestrzegane są zasady zapewniające zgodność z wymaganiami prawnymi, regulacyjnymi i umownymi, związanymi z prawami własności intelektualnej i użytkowaniem prawnie zastrzeżonego oprogramowania. Uzasadnienie wyboru zabezpieczenia: systematyczne komunikowanie pracownikom oraz w uzasadnionych przypadkach stronom zainteresowanym zasad, unormowań prawnych jakie organizacja w ramach bezpieczeństwa informacji przyjęła i stosuje.
5.33	Ochrona zapisów	W organizacji stosowana jest ochrona zapisów przed utratą, zniszczeniem, fałszowaniem, nieuprawnionym dostępem i nieuprawnionym opublikowaniem, stosownie do wymagań prawnych, regulacyjnych i umownych. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie danych przed ich nieuprawnionym przejęciem, zniszczeniem bądź modyfikacją
5.34	Prywatność i ochrona danych identyfikujących osobę (PII)	Organizacja stosuje zasady mające zapewnić prywatność i ochronę danych identyfikujących osobę stosownie do odpowiednich przepisów prawa i regulacji. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie danych przed ich nieuprawnionym przejęciem, zniszczeniem bądź modyfikacją.

5.35	Niezależny przegląd bezpieczeństwa informacji	Podejście organizacji do zarządzania bezpieczeństwem informacji oraz jego wdrożenie (tzn. cele stosowania zabezpieczeń, zabezpieczenia, polityki, procesy i procedury dotyczące bezpieczeństwa informacji) podlegają przeglądowi w zaplanowanym terminie lub wtedy, gdy nastąpią istotne zmiany. Uzasadnienie wyboru zabezpieczenia: systematyczne komunikowanie pracownikom oraz w uzasadnionych przypadkach stronom zainteresowanym zasad, uwarunkowań prawnych jakie organizacja w ramach bezpieczeństwa informacji przyjęła i stosuje.
5.36	Zgodność z politykami, zasadami i standardami dotyczącymi bezpieczeństwa informacji	Organizacja regularnie dokonuje przeglądu zgodności przetwarzania informacji i procedur z odpowiednimi politykami bezpieczeństwa, standardami i innymi wymaganiami dotyczącymi bezpieczeństwa, w zakresie przydzielonej im odpowiedzialności. Uzasadnienie wyboru zabezpieczenia: weryfikacja zgodności procesów organizacji z przyjętymi regulacjami wewnętrznymi i zewnętrznymi.
5.37	Udokumentowane procedury eksploatacyjne	Organizacja w sposób regularnych dokonuje przeglądów systemów informacyjnych w organizacji celem sprawdzenia ich zgodności z politykami bezpieczeństwa i standardami obowiązującymi w organizacji, a także aktualizacji dokumentacji eksploatacyjnej systemów. Uzasadnienie wyboru zabezpieczenia: weryfikacja zgodności technicznej systemów informacyjnych z przyjętymi regulacjami.
6	**Zabezpieczenia osobowe**	
6.1	Postępowanie sprawdzające	Najwyższe kierownictwo zapewnia procedury weryfikacji kandydatów do pracy zgodnie z odpowiednimi przepisami prawnymi, regulacjami i zasadami etycznymi oraz proporcjonalnie do wymagań biznesowych, klasyfikacji informacji, do których będzie potrzebny dostęp oraz dostrzeżonych ryzyk. Uzasadnienie wyboru zabezpieczenia: zapewnienie odpowiedniej kadry, która wykonując swoje obowiązki będzie miała na względzie zasady prawidłowego przetwarzania informacji.
6.2	Warunki zatrudnienia	Każdy pracownik organizacji, który będzie przetwarzał dane osobowe, którymi organizacja zarządza, podpisuje upoważnienie do przetwarzania danych osobowych. Uzasadnienie wyboru zabezpieczenia: zapewnienie w organizacji procedur, które zmniejszają ryzyko utraty danych osobowych czy udostępnienia osobom nieuprawnionym danych osobowych, którymi organizacja administruje.
6.3	Uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji	Polityka Bezpieczeństwa Informacji określa politykę szkoleniową, jaką organizacja prowadzi względem wszystkich pracowników organizacji oraz w stosownych wypadkach, kontrahentów. Uzasadnienie wyboru zabezpieczenia: systematyczne komunikowanie pracownikom oraz w uzasadnionych przypadkach stronom zainteresowanym zasady, jakie organizacja w ramach bezpieczeństwa informacji przyjęła.
6.4	Postępowanie dyscyplinarne	Polityka Bezpieczeństwa Informacji określa możliwości zastosowania względem pracownika naruszającego zasady bezpieczeństwa informacji organizacji postępowania dyscyplinarnego. Uzasadnienie wyboru zabezpieczenia: uświadomienie pracowników organizacji o konsekwencjach w przypadku naruszenia bezpieczeństwa informacji organizacji.
6.5	Odpowiedzialność po zakończeniu lub zmianie zatrudnienia	Najwyższe kierownictwo lub bezpośredni przełożony komunikuje pracownikom na samym początku zatrudnienia przez jaki okres czasu obowiązuje klauzula poufności względem przetwarzanych danych osobowych w organizacji. Uprawnienia, jakie pracownik miał podczas zatrudnienia na konkretnym stanowisku są cofane przez uprawnione do tego osoby, oddelegowane przez najwyższe kierownictwo. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie danych osobowych przed ich nieuprawnionym przejęciem, zniszczeniem bądź modyfikacją.
6.6	Umowy o zachowaniu poufności lub nieujawnianiu informacji	Organizacja zawiera umowy o zachowaniu poufności z podmiotami zewnętrznymi, a także umowy dotyczące Powierzenia Przetwarzania Danych Osobowych (DPIA). Uzasadnienie wyboru zabezpieczenia: zapewnienie bezpieczeństwa informacji zgodnie z wymaganiami prawnymi.

6.7	Praca zdalna	Polityka Bezpieczeństwa Informacji określa zasady dotyczące pracy zdalnej. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie danych przed ich nieuprawnionym przejęciem, zniszczeniem bądź modyfikacją.
6.8	Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji	Polityka Bezpieczeństwa Informacji określa zasady dotyczące zgłaszania incydentów bezpieczeństwa.Uzasadnienie wyboru zabezpieczenia: określenie sposobu postępowania w przypadku wystąpienia incydentów bezpieczeństwa.
7	**Zabezpieczenia fizyczne**	
7.1	Fizyczne granice obszaru bezpiecznego	Organizacja określiła granice bezpieczeństwa dla obszarów zawierających wrażliwe lub krytyczne informacje oraz środki przetwarzania informacji. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie danych przed ich nieuprawnionym przejęciem, zniszczeniem bądź modyfikacją.
7.2	Wejście fizyczne	Organizacja posiada wyznaczone strefy, do których dostęp posiadają tylko osoby uprawnione. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie danych przed ich nieuprawnionym przejęciem, zniszczeniem bądź modyfikacją.
7.3	Zabezpieczenie biur, pomieszczeń i obiektów	Organizacja posiada fizyczne zabezpieczenia dla biur, pomieszczeń i obiektów, w których dokonywane jest przetwarzanie danych. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie danych przed ich nieuprawnionym przejęciem, zniszczeniem bądź modyfikacją.
7.4	Monitorowanie bezpieczeństwa fizycznego	Polityka Bezpieczeństwa Informacji określa aspekty dotyczące bezpieczeństwa fizycznego i monitorowania. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie danych przed ich nieuprawnionym przejęciem, zniszczeniem bądź modyfikacją.
7.5	Ochrona przed zagrożeniami fizycznymi i środowiskowymi	Organizacja posiada zabezpieczenia przed katastrofami naturalnymi, wrogim atakiem oraz wypadkami. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie danych organizacji przed ich nieuprawnionym przejęciem, zniszczeniem bądź modyfikacją.
7.6	Praca w obszarach bezpiecznych	Organizacja posiada fizyczne zabezpieczenia dla biur, pomieszczeń i obiektów, w których dokonywane jest przetwarzanie danych. Uzasadnienie wyboru zabezpieczenia: Konieczność zabezpieczenia danych w organizacji.
7.7	Czyste biurko i czysty ekran	Polityka Bezpieczeństwa Teleinformatycznego określa wytyczne dotyczące polityki czystego biurka. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie danych organizacji przed ich nieuprawnionym przejęciem, zniszczeniem bądź modyfikacją.
7.8	Lokalizacja i ochrona sprzętu	Organizacja nadzoruje oraz ewidencjonuje sprzęt, który wynoszony jest z organizacji. Uzasadnienie wyboru zabezpieczenia: Konieczność zabezpieczenia danych przetwarzanych w organizacji przez pracowników, którzy dokonują ich przetwarzania poza siedzibą.
7.9	Bezpieczeństwo aktywów poza siedzibą	Organizacja wymaga, aby wszyscy pracownicy i kontrahenci stosowali zasady bezpieczeństwa informacji zgodnie z obowiązującymi w organizacji politykami i procedurami w zakresie użytkowania sprzętu poza siedzibą organizacji. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie aktywów organizacji z danymi organizacji przed nieuprawnionym przejęciem i dostępem do nich.
7.10	Nośniki informacji	W organizacji wdrożone są zasady zarządzania nośnikami wymiennymi. Polityka Bezpieczeństwa Teleinformatycznego określa wytyczne w zakresie postępowania z nośnikami danych w przypadku ich przekazania do użytkowania innym pracownikom lub kontrahentom, a także wycofywanie nośników z użytku. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie danych przed ich nieuprawnionym przejęciem, zniszczeniem bądź modyfikacją.
7.11	Systemy wspomagające	Organizacja zabezpieczyła techniczne środki ochrony sprzętu przed awariami zasilania oraz innymi przerwami spowodowanymi awariami systemów wspomagających. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie danych przed ich nieuprawnionym przejęciem, zniszczeniem bądź modyfikacją.
7.12	Bezpieczeństwo okablowania	Organizacja stosuje fizyczne zabezpieczenia okablowania zasilającego oraz telekomunikacyjnego przenoszącego dane lub wspomagającego usługi informacyjne w organizacji. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie danych przed ich nieuprawnionym przejęciem, zniszczeniem bądź modyfikacją.

7.13	Konserwacja sprzętu	Organizacja zapewnia ciągłą konserwację sprzętu w celu zapewnienia jego niezawodności oraz dostępności. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie danych organizacji przed ich nieuprawnionym przejęciem, zniszczeniem bądź modyfikacją.
7.14	Bezpieczne zbywanie lub przekazywanie do ponownego użycia	Polityka Bezpieczeństwa Teleinformatycznego określa zasady dotyczące przekazania sprzętu do ponownego użycia. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie danych organizacji przed ich nieuprawnionym przejęciem, zniszczeniem bądź modyfikacją i zapewnienie, że wszystkie wrażliwe dane i licencjonowane programy zostały usunięte lub bezpiecznie nadpisane.
8	**Zabezpieczenia technologiczne**	
8.1	Urządzenia końcowe użytkownika	Polityka Bezpieczeństwa Teleinformatycznego określa zasady dotyczące użytkowania sprzętu przez pracowników. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie danych przed ich nieuprawnionym przejęciem, zniszczeniem bądź modyfikacją.
8.2	Prawa uprzywilejowanego dostępu	Polityka Bezpieczeństwa Teleinformatycznego określa zasady przydzielania praw dostępu dla pracowników do sieci i usług sieciowych w zakresie uprzywilejowanego dostępu. Przydzielanie tych uprawnień jest ograniczane i szczególnie nadzorowane. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie danych przed ich nieuprawnionym przejęciem, zniszczeniem bądź modyfikacją.
8.3	Ograniczanie dostępu do informacji	Polityka Bezpieczeństwa Informacji oraz Bezpieczeństwa Teleinformatycznego określa zasady nadzoru i kontroli dostępu do informacji. Uzasadnienie wyboru zabezpieczenia: uświadomienie pracowników organizacji o konsekwencjach w przypadku naruszenia bezpieczeństwa informacji organizacji.
8.4	Dostęp do kodu źródłowego	Organizacja ograniczyła dostęp do kodów źródłowych programów dla wyznaczonych pracowników. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie danych przed ich nieuprawnionym przejęciem, zniszczeniem bądź modyfikacją.
8.5	Bezpieczne uwierzytelnianie	Polityka Bezpieczeństwa Teleinformatycznego określa zasady dotyczące bezpiecznego uwierzytelniania oraz zarządzania hasłami. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie danych przed ich nieuprawnionym przejęciem, zniszczeniem bądź modyfikacją.
8.6	Zarządzanie pojemnością	Organizacja monitoruje wykorzystywanie zasobów w celu zapewnienia właściwej wydajności systemów, a także planuje wymagania w zakresie odpowiedniego zarządzania pojemnością. Uzasadnienie wyboru zabezpieczenia: Zapewnienie odpowiedniej wydajności systemów.
8.7	Ochrona przed szkodliwym oprogramowaniem	Organizacja wdrożyła zabezpieczenia wykrywające, zapobiegające i odtwarzające, które służą ochronie przed szkodliwym oprogramowaniem. Zasady ich stosowania, aktualizacji zostały określone w Polityce Bezpieczeństwa Teleinformatycznego. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie danych przed ich nieuprawnionym przejęciem, zniszczeniem bądź modyfikacją.
8.8	Zarządzanie podatnościami technicznymi	Polityka Bezpieczeństwa Teleinformatycznego określa zasady dotyczące zarządzania podatnościami w systemach teleinformatycznych. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie systemów przed zagrożeniami wynikającymi z podatności systemowych.
8.9	Zarządzanie konfiguracją	Kierownictwo organizacji określiło zasady zmian w organizacji, procesach biznesowych, środkach przetwarzania informacji i systemach, które mają wpływ na bezpieczeństwo informacji poprzez wydanie wewnętrznych aktów prawnych. Akty te są wszystkim pracownikom zakomunikowane. Ustalone zostały w nich również zasady odpowiedzialności użytkowników za poszczególne obszary organizacji. Polityka Bezpieczeństwa Teleinformatycznego określa również zasady eksploatacji. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie danych przed ich nieuprawnionym przejęciem, zniszczeniem bądź modyfikacją oraz ustalenie zakresu odpowiedzialności w organizacji.
8.10	Usuwanie informacji	Polityka Bezpieczeństwa Teleinformatycznego określa w dziale poświęconym obsługom nośników informacje dotyczące bezpiecznego usuwania informacji. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie informacji przed nieuprawnionym dostępem.

8.11	Maskowanie danych	Polityka Bezpieczeństwa Teleinformatycznego określa zasady dotyczące maskowania danych. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie danych przed ich nieuprawnionym przejęciem, zniszczeniem bądź modyfikacją.
8.12	Zapobieganie wyciekom danych	Polityka Bezpieczeństwa Teleinformatycznego określa zasady dotyczące ochrony przed wyciekiem danych. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie danych przed ich nieuprawnionym przejęciem, zniszczeniem bądź modyfikacją.
8.13	Zapasowe kopie informacji	Polityka Bezpieczeństwa Teleinformatycznego określa zasady dotyczące kopii zapasowych. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie danych przed ich nieuprawnionym przejęciem, zniszczeniem bądź modyfikacją.
8.14	Nadmiarowość środków przetwarzania informacji	Środki przetwarzania informacji wdrożono z odpowiednim nadmiarem wystarczającym do spełnienia wymagań dostępności. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie danych przed ich nieuprawnionym przejęciem, zniszczeniem bądź modyfikacją, a także zapewnienie ciągłości działania usług.
8.15	Rejestrowanie	Polityka Bezpieczeństwa Teleinformatycznego określa zasady dotyczące rejestrowania zdarzeń użytkowników w systemach teleinformatycznych. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie danych przed ich nieuprawnionym przejęciem, zniszczeniem bądź modyfikacją.
8.16	Działania monitorujące	Polityka Bezpieczeństwa Teleinformatycznego określa zasady dotyczące rejestrowania zdarzeń użytkowników w systemach teleinformatycznych. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie danych przed ich nieuprawnionym przejęciem, zniszczeniem bądź modyfikacją.
8.17	Synchronizacja zegarów	Polityka Bezpieczeństwa Teleinformatycznego określa zasady dotyczące synchronizacji zegarów w systemach teleinformatycznych. Uzasadnienie wyboru zabezpieczenia: prowadzenie ciągłego nadzoru nad systemami oraz operatorami tych systemów.
8.18	Użycie uprzywilejowanych programów narzędziowych	Organizacja określiła w Polityce Bezpieczeństwa Teleinformatycznego wytyczne dotyczące wykorzystywania oprogramowania. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie danych przed ich nieuprawnionym przejęciem, zniszczeniem bądź modyfikacją
8.19	Instalacja oprogramowania w systemach produkcyjnych	Polityka Bezpieczeństwa Teleinformatycznego określa zasady dotyczące instalacji oprogramowania w systemach produkcyjnych. Uzasadnienie wyboru zabezpieczenia: nadzór nad oprogramowaniem wykorzystywanym w organizacji.
8.20	Bezpieczeństwo sieci	Polityka Bezpieczeństwa Teleinformatycznego określa zasady dotyczące zabezpieczania sieci teleinformatycznych, usług sieciowych z nimi związanych a także separacji fizycznej i logicznej. Uzasadnienie wyboru zabezpieczenia: nadzór i kontrola infrastruktury sieciowej organizacji
8.21	Bezpieczeństwo usług sieciowych	Polityka Bezpieczeństwa Teleinformatycznego określa zasady dotyczące zabezpieczania sieci teleinformatycznych, usług sieciowych z nimi związanych a także separacji fizycznej i logicznej. Uzasadnienie wyboru zabezpieczenia: nadzór i kontrola infrastruktury sieciowej organizacji
8.22	Rozdzielanie sieci	Polityka Bezpieczeństwa Teleinformatycznego określa zasady dotyczące zabezpieczania sieci teleinformatycznych, usług sieciowych z nimi związanych a także separacji fizycznej i logicznej. Uzasadnienie wyboru zabezpieczenia: nadzór i kontrola infrastruktury sieciowej organizacji
8.23	Filtrowanie treści internetowych	Polityka Bezpieczeństwa Teleinformatycznego określa zasady dotyczące identyfikowania i zapobiegania użyciu stron internetowych o szkodliwym działaniu. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie danych przed ich nieuprawnionym przejęciem, zniszczeniem bądź modyfikacją.
8.24	Użycie kryptografii	Polityka Bezpieczeństwa Teleinformatycznego określa zasady stosowania zabezpieczeń kryptograficznych w systemach organizacji w celu ochrony poufności, autentyczności i integralności informacji. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie danych przed ich nieuprawnionym przejęciem, zniszczeniem bądź modyfikacją.

8.25	Bezpieczne wytwarzanie oprogramowania	Polityka Bezpieczeństwa Teleinformatycznego określa zasady projektowania, wdrażania i rozwoju systemów w organizacji oraz ich bezpiecznej eksploatacji. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie danych przed ich nieuprawnionym przejęciem, zniszczeniem bądź modyfikacją w wyniku budowy lub rozbudowy systemu informacyjnych.
8.26	Wymagania bezpieczeństwa aplikacji	Polityka Bezpieczeństwa Teleinformatycznego określa wymagania dla systemów teleinformatycznych. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie danych przed ich nieuprawnionym przejęciem, zniszczeniem bądź modyfikacją w wyniku budowy lub rozbudowy systemó informacyjnych.
8.27	Zasady bezpiecznej architektury systemu i jej projektowania	Polityka Bezpieczeństwa Teleinformatycznego określa zasady projektowania, wdrażania i rozwoju systemów w organizacji oraz ich bezpiecznej eksploatacji. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie danych przed ich nieuprawnionym przejęciem, zniszczeniem bądź modyfikacją w wyniku budowy lub rozbudowy systemów informacyjnych.
8.28	Bezpieczne kodowanie	Polityka Bezpieczeństwa Teleinformatycznego określa zasady projektowania, wdrażania i rozwoju systemów w organizacji oraz ich bezpiecznej eksploatacji. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie danych przed ich nieuprawnionym przejęciem, zniszczeniem bądź modyfikacją w wyniku budowy lub rozbudowy systemów informacyjnych.
8.29	Testowanie bezpieczeństwa podczas wytwarzania i akceptowania	Polityka Bezpieczeństwa Teleinformatycznego określa zasady projektowania, wdrażania i rozwoju systemów w organizacji oraz ich bezpiecznej eksploatacji. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie danych przed ich nieuprawnionym przejęciem, zniszczeniem bądź modyfikacją w wyniku budowy lub rozbudowy systemu informacyjnych.
8.30	Wytwarzanie zlecane podmiotom zewnętrznym	Polityka Bezpieczeństwa Teleinformatycznego określa zasady projektowania, wdrażania i rozwoju systemów w organizacji oraz ich bezpiecznej eksploatacji. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie danych przed ich nieuprawnionym przejęciem, zniszczeniem bądź modyfikacją w wyniku budowy lub rozbudowy systemu informacyjnych.
8.31	Oddzielanie środowisk rozwojowych, testowych i produkcyjnych	Polityka Bezpieczeństwa Teleinformatycznego określa zasady dotyczące separacji środowisk. Uzasadnienie wyboru zabezpieczenia: Redukcja ryzyk związanych z nieuprawnionym dostępem lub zmianami w środowisku produkcyjnym.
8.32	Zarządzanie zmianami	Kierownictwo organizacji określiło zasady zmian w organizacji, procesach biznesowych, środkach przetwarzania informacji i systemach, które mają wpływ na bezpieczeństwo informacji poprzez wydanie wewnętrznych aktów prawnych. Akty te są wszystkim pracownikom zakomunikowane. Ustalone zostały w nich również zasady odpowiedzialności użytkowników za poszczególne obszary organizacji. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie danych przed ich nieuprawnionym przejęciem, zniszczeniem bądź modyfikacją oraz ustalenie zakresu odpowiedzialności w organizacji.
8.33	Informacje testowe	Polityka Bezpieczeństwa Teleinformatycznego określa zasady postępowania z danymi testowymi podczas prac rozwoju oprogramowania. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie danych przed ich nieuprawnionym przejęciem, zniszczeniem bądź modyfikacją w wyniku budowy lub rozbudowy systemu informacyjnych.
8.34	Ochrona systemów informacyjnych podczas testów audytowych	Polityka Bezpieczeństwa Teleinformatycznego określa zasady dotyczące ochrony systemów informacyjnych podczas testów audytowych. Uzasadnienie wyboru zabezpieczenia: zabezpieczenie danych przed ich nieuprawnionym przejęciem, zniszczeniem bądź modyfikacją w wyniku budowy lub rozbudowy systemów informacyjnych, a także zapewnienie ciągłości działania.

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*
1.	Proces wydawania dowodów osobistych, aktów ślubu, aktów urodzenia	Ryzyko zniekształcenia danych - wydania obywatelowi błędnego dokumentu	1.Awaria sprzętu,niewłaściwe funkcjonowanie urządzeń 2.Błąd użytkownika	Błąd użytkownika, błąd systemu teleinformatycznego, brak kopii zapasowych	Wydanie dokumentu zawierającego błędy, utrata wizerunku, koszty finansowe	3	2	6	Stosowanie właściwych procedur
		Ryzyko utraty /modyfikacji danych wrażliwych	Kradzież dokumentów, nieautoryzowany dostęp do pomieszczeń	Niezabezpieczone pomieszczenie, pozostawienie dokumentów w drukarce, Brak lub niejasno określone zasady zachowania poufności informacji gromadzonych i przetwarzanych przez pracowników,Brak lub nieregularne archiwizowanie informacji	Ujawnienie danych wrażliwych, utrata wizerunku, kary finansowe	3	3	9	Stosowanie właściwych procedur
2.	Procesy meldunkowe	Ryzyko zniekształcenia danych - wydania obywatelowi błędnego dokumentu	1.Awaria sprzętu,niewłaściwe funkcjonowanie urządzeń 2.Błąd użytkownika	Błąd użytkownika, błąd systemu teleinformatycznego, brak kopii zapasowych	Utrata wizerunku	3	2	6	Stosowanie właściwych procedur
3.	Ewidencja ludności	Ryzyko błędnej ewidencji	1.Awaria sprzętu,niewłaściwe funkcjonowanie urządzeń 2.Błąd użytkownika	Błąd użytkownika, błąd systemu teleinformatycznego, brak kopii zapasowych	Utrata wizerunku	3	2	6	Stosowanie właściwych procedur
4.	SIO - System Informacji Oświatowej	Ryzyko utraty /modyfikacji danych wrażliwych	Kradzież dokumentów, nieautoryzowany dostęp do pomieszczeń	Niezabezpieczone pomieszczenie, pozostawienie dokumentów w drukarce, Brak lub niejasno określone zasady zachowania poufności informacji gromadzonych i przetwarzanych przez pracowników,Brak lub nieregularne archiwizowanie informacji	Ujawnienie danych wrażliwych, utrata wizerunku, kary finansowe	3	3	9	Stosowanie właściwych procedur
5.	Rejestry: PESEL, rejestr mieszkańców, rejestr Dowodów Osobistych, aktów urodzenia, aktów stanu cywilnego	Ryzyko ujawnienia danych wrażliwych	Kradzież dokumentów, nieautoryzowany dostęp do pomieszczeń	Niezabezpieczone pomieszczenie, pozostawienie dokumentów w drukarce, Brak lub niejasno określone zasady zachowania poufności informacji gromadzonych i przetwarzanych przez pracowników	Ujawnienie danych wrażliwych, utrata wizerunku, kary finansowe	4	3	12	Przechowywanie dokumentów w szafach zamykanych na klucz. Niszczenie dokumentów w niszczarkach
	Zasoby								
	Sprzęt - urządzenia przetwarzania danych, urządzenia przenośne,urządzenia stacjonarne, urządzenia peryferyjne, nośniki danych	Ryzyko dla zasobów zgodne z ryzykiem w Arkuszu zasobów							
	Oprogramowanie - system operacyjny, aplikacje biznesowe	Ryzyko dla zasobów zgodne z ryzykiem w Arkuszu zasobów							
	Sieć	Ryzyko dla zasobów zgodne z ryzykiem w Arkuszu zasobów							

	Personel	Ryzyko dla zasobów zgodne z ryzykiem w Arkuszu zasobów							
	Siedziba - budynki, biura, łączność, usługi komunalne i techniczne (woda, śmieci)	Ryzyko dla zasobów zgodne z ryzykiem w Arkuszu zasobów							
	Organizacja -organy nadzorcze	Ryzyko dla zasobów zgodne z ryzykiem w Arkuszu zasobów							
	Dostawcy zewnętrzni	Ryzyko dla zasobów zgodne z ryzykiem w Arkuszu zasobów							

Właściciel ryzyka	Nazwa aktywu/ proces biznesowy	Ryzyko	Zagrożenie	Podatności / Przyczyna (Czynniki ryzyka)	Skutek ryzyka	Skutek /wpływ zagrożenia na P,I,D	Prawdopodobieństwo wystąpienia zagrożenia	Miara Ryzyka (istotność)	Postępowanie z ryzykiem	Reakcja na ryzyko	Zabezpieczenie
Informatyk	SPRZĘT							0			
	Sprzęt - urządzenia przetwarzania danych	Ryzyko nieautoryzowanego działania	1. Kradzież urządzenia 2. Nieuprawniony dostęp 3. Złamanie haseł	Niewłaściwa ochrona fizyczna budynku, pomieszczeń, drzwi, okien, urządzenie pozostawione bez blokady ekranu, nieprawidłowe uprawnienia,instalacja przez użytkownika szkodliwego oprogramowania,Włamanie do sieci wewnętrznej. Nieprzestrzeganie zasad czystego biurka i pulpitu. Nieprzestrzeganie polityki tworzenia haseł.	Możliwość wykorzystania danych przez osoby niepowołane, utrata wizerunku	5	4	20	Wybranie i wdrożenie zabezpieczenia	Przeciwdziałanie: 1.Zdefiniowanie osób odpowiedzialnych za bezpieczną eksploatację systemów teleinformatycznych 2.Szkolenia pracowników 3.Przestrzeganie przez użytkowników procedur SZBI 4.Sporządzenie dokumentacji technicznej wymaganej przez KSC	1) A.11.2.8 2) A.9.3.1, A.9.4.1, A.9.4.2, A.11.2.1, A.11.1.1, A.11.1.2,A.12.2.1. 3) A.7.2, A.9.4.3
	Sprzęt - urządzenia przetwarzania danych	Ryzyko awarii technicznej	1.Awaria sprzętu,niewłaściwe funkcjonowanie urządzeń 2.Błąd użytkownika	Stary sprzęt -brak planów okresowej wymiany sprzętu, nieumiejętne użytkowanie,brak kompetencji użytkowników, utrata zasilania, brak zasilania awaryjnego, brak wsparcia serwisowego	Zakłócenia w realizacji procesów, ograniczony dostęp do danych, nieterminowe wykonywanie zadań	5	4	20	Wybranie i wdrożenie zabezpieczenia	Przeciwdziałanie: sporządzenie dokumentacji wymaganej przez KSC	Cykliczna wymiana sprzętu,umowy serwisowe, szkolenie użytkowników, dokumentacja A.7.2, A.11.2.4, A11.2.2,A 12.1.1, A. 12.6.1
	Strona WWW Urzędu	Ryzyko ataku hakerskiego na stronę www	Atak hakerski umożliwiający przejęcie kontroli nad serwisem	Słabe zabezpieczenia techniczne	Utrata reputacji i dobrego wizerunku	5	3	15	Wybranie i wdrożenie zabezpieczenia	Wdrożenie protokołu https , aktualizacja certyfikatu X.509, upgrade wersji TLS	
	Serwer pocztowy	Ryzyko przejęcia danych wrażliwych	Atak phishingowy, ransomware	Słabe zabezpieczenia techniczne, błąd użytkownika	Utrata danych, utrata reputacji, możliwe zaszyfrowanie plików	4	3	12	Akceptacja ryzyka	Monitorowanie ryzyka	A.13.2.3, A.15.2.1, A.15.2.2
	Sprzęt - przenośne urządzenia przetwarzania danych	Ryzyko utraty danych wrażliwych	1.Kradzież, utrata urządzenia. 2.Nieuprawniony dostęp	Niezabezpieczenie urządzenia przez użytkownika,brak zasad zwrotu i rozliczania mienia powierzonego pracownikom	Utrata danych, utrata reputacji, utrata aktywu	4	3	12	Akceptacja ryzyka	Monitorowanie ryzyka	A.6.2.1 Polityka w zakresie urządzeń mobilnych, Szkolenia użytkowników
Informatyk	APLIKACJE							0			
	Aplikacje	Nieuprawniony dostęp do informacji w aplikacjach	Wykorzystanie aplikacji w sposób nieautoryzowany	Brak odpowiedniego nadzoru nad oprogramowaniem, nieumiejętne korzystanie z oprogramowania, brak aktualizacji oprogramowania, niewłaściwie przypisane prawa dostępu,opuszczenie stanowiska pracy bez wylogowania się z aplikacji, brak lub niewłaściwa ochrona przed nieautoryzowanym dostępem do systemów operacyjnych	Możliwość utraty danych, modyfikacji danych	4	3	12	Akceptacja ryzyka	Monitorowanie ryzyka	Instrukcja korzystania z oprogramowania, właściwie przydzielone prawa dost epu, stosowanie się użytkownika do PBT
	Aplikacje	Ryzyko naruszenia praw autorskich	Nielegalne przetwarzanie danych	Brak licencji, prawa administratora nadane użytkownikom - możliwość instalacji nieautoryzowanych aplikacji	Możliwość utraty danych,możliwość poniesienia kosztów finansowych związanych z brakiem licencji	3	2	6	Akceptacja ryzyka	Monitorowanie ryzyka	A.12.6.2 Przestrzeganie zasad instalacji oprogramowania
	Aplikacje	Ryzyko przerwania działania kluczowych aplikacji	Brak dostępu do aplikacji	Nieaktualizowane oprogramowanie, nieskuteczna ochrona antywirusowa, brak lub niewłaściwa ochrona przed nieuprawnionym dostępem do aplikacji, luki w systemach	Brak realizacji zadań, możliwe kary - koszty finansowe	3	3	9	Akceptacja ryzyka	Monitorowanie ryzyka	A.12.2.1 Aktualizacja oprogramowania, stosowanie procedur dostępu, uświadamianie pracowników
Informatyk	Sieć										
	Lokalna sieć teleinformatyczna	Ryzyko utraty danych lub zniekształcenia danych	Atak phishingowy	Brak zabezpieczeń technicznych i proceduralnych sieci, urządzeń brzegowych	Utrata danych, utrata wizerunku firmy, koszty finansowe	5	4	20	Wybranie i wdrożenie zabezpieczenia	Wdrożenie procedur i mechanizmów segmentacji sieci,izolacji końcowych użytkowników, mechanizmów monitorujących sieć wewnątrz, wdrozenie aplikacji i sprzetu zabezpieczającego	A.13.1.1, A.13.1.2, A.13.1.3
Informatyk	Pliki: - konfiguracyjne (aplikacje, bazy danych, systemy, sieci), poczty elektronicznej										
	Pliki: - konfiguracyjne (aplikacje, bazy danych, systemy, sieci), poczty elektronicznej	Ryzyko utraty danych lub zniekształcenia danych	Nieautoryzowany dostęp do informacji, zużycie nośników informacji, złamanie haseł	Brak lub niewłaściwa ochrona bezpieczeństwa plików systemowych, w tym kodów źródłowych	Naruszenie ochrony danych osobowych, naruszenie poufności, utrata niezapisanych danych, kary dla Urzędu	4	3	12	Akceptacja ryzyka	Stosowanie procedur, szkolenie pracowników	Stosowanie procedur SZBI
Informatyk	Kopie zapasowe										

	Kopie zapasowe	Ryzyko utraty lub zniekształcenia danych	Utrata danych, zniekształcenie danych	Brak lub nieregularne tworzenie kopii zapasowych informacji przetwarzanych w systemach teleinformatycznych	Brak aktualnych danych, możliwa nieterminowa realizacja zadań, możliwe kary finansowe	5	4	20	Wybranie i wdrożenie zabezpieczenia	Stosowanie procedur kopii zapasowych	A.12.3.1Proces tworzenia i okresowego odtwarzania kopi zapasowych, kopiowane istotnych danych na dyski zewnętrzne
Informatyk	NOŚNIKI DANYCH							0			
	Nośniki danych	Ryzyko ujawnienia, modyfikacji, utraty danych z nośników informacji	Zagubienie, kradzież, niszczenie nośników informacji	Brak stosownych procedur postępowania z nośnikami, niekontrolowane kopiowanie, brak staranności przy pozbywaniu się nośników	Naruszenie ochrony danych osobowych, naruszenie poufności, utrata niezapisanych danych, kary dla Urzędu	4	3	12	Akceptacja ryzyka	Stosowanie procedur, szkolenie pracowników	A.8.3.1 , A.8.3.2, A.8.3.3
Sekretarz	SIEDZIBA							0			
	Siedziba - budynki	Brak dostaw mediów (prąd, woda, internet)	Uszkodzenie infrastruktury	Awaria po stronie dostawcy, ograniczenie dostaw, awaria infrastruktury budynku	Brak możliwości wykorzystania sprzętu elektronicznego, brak możliwości zapewnienia właściwych warunków pracy	3	3	9	Transfer ryzyka - Ubezpieczenie	Monitorowanie ryzyka	A.11.2.2. A.11.2.3
	Siedziba - budynki	Utrata aktywów	Nieuprawniony dostęp lub włamanie, nieautoryzowane wejście do obszarów chronionych	Brak fizycznej ochrony budynków, drzwi i okien, brak stosowania Polityki kluczy,	Utrata danych w wersji papierowej, utrata plików lub aplikacji,kradzież sprzętu i nośników danych, instalacja nieautoryzowanych urządzeń	4	3	12	Akceptacja ryzyka	Stosowanie procedur bezpieczeństwa fizycznego i środowiskowego	A.11.1., A11.2.8, A.11.2.9
	Siedziba - budynki	Uszkodzenie lub zniszczenie dokumentów archiwalnych i dokumentacji	Wichura, pożar, zalanie z rur,	Nagłe zjawiska pogodowe	Utrata danych , możliwa nieterminowa realizacja zadań, możliwe kary finansowe , utrata wizerunku	3	4	12	Transfer ryzyka - Ubezpieczenie	Monitorowanie ryzyka	A.11.1.4
Sekretarz	PERSONEL							0			
	Personel	Ryzyko nieautoryzowanego działania	Nieuprawnione kopiowanie oprogramowania, zniekształcenie danych, nielegalne przetwarzanie danych	Nieaktualne prawa dostępu użytkowników, brak stosowania ochrony poufnych informacji uwierzytelniających, brak świadomości pracowników	Wyciek informacji, brak realizacji zadań statusowych Gminy, utrata wizerunku	4	3	12	Akceptacja ryzyka	Monitorowanie ryzyka	A.7, A.9.2, A 9.3
	Personel	Ryzyko nieautoryzowanego działania	Błąd ludzki, celowe szkodliwe działanie pracownika	Nieprawidłowa weryfikacja personelu podczas zatrudnienia, nieprawidłowe uprawnienia, błąd użytkownika, brak zastępowalności	Wyciek informacji, brak realizacji zadań statusowych Gminy, utrata wizerunku	4	3	12	Akceptacja ryzyka	Monitorowanie ryzyka	A.7.1 Weryfikacja pracowników przed zatrudnieniem
	Personel – użytkownik systemu	Ryzyko nieautoryzowanego działania	Kradzież danych	Mała świadomość zagrożeń teleinformatycznych, brak lub niejasno określone zasady zachowania poufności informacji gromadzonych i przetwarzanych przez pracowników	utrata reputacji Gminy , skutki prawne	4	3	12	Akceptacja ryzyka	Monitorowanie ryzyka	A.7.2.2, A,7.2.3
Prawnik	UMOWY Z DOSTAWCAMI							0			
	Umowy z dostawcami	Ryzyko utraty danych z aktywów udostępnianych dostawcom	Nielegalne pozyskanie danych	Brak zapisów dotyczących zapewnienia bezpieczeństwa informacji w umowach z dostawcami, brak lub niejasne zasady udzielania informacji podmiotom zewnętrznym	Wyciek informacji, utrata reputacji	4	3	12	Akceptacja ryzyka	Stosowanie stosownych zapisów w umowach z dostawcami	A.15

							Wartość aktywa		Wartości przed wdrożeniem postępowania			
nr ryzyka	**Właściciel ryzyka**	**Nazwa aktywu/ proces biznesowy**	**Ryzyko**	**Zagrożenie**	**Podatności / Przyczyna (Czynniki ryzyka)**	**Skutek ryzyka**	**Skutek /wpływ zagrożenia na P,I,D**	**Prawdopodobieństwo wystąpienia zagrożenia**	**Miara Ryzyka (istotność)**	**Postępowanie z ryzykiem**	**Reakcja na ryzyko**	**Zabezpieczenie**
	Wójt	* Procesy, których utrata lub pogorszenie uniemożliwia wypełnienie misji organizacji										
1.		Proces ciągłości działania Urzędu Gminy	Ryzyko przerwania ciągłości działania Urzędu	1.Utrata dostaw prądu 2.Awaria urządzenia telekomunikacyjnego 3.Niewystarczająca obsada stanowisk 4.Awaria kluczowego sprzętu,niewłaściwe funkcjonowanie urządzeń	1. Brak zasilania awaryjnego/ możliwy krótki okres niestabilności sieci w wyniku przełączenia zasilania UPS na agregat prądotwórczy 2. Pojedynczy punkt uszkodzenia 3.Nieobecność personelu 4.Brak planów ciągłości działania lub odstąpienie od ich aktualizacji	Przerwa w działaniu Urzędu, brak możliwości realizacji czynności, niedotrzymanie terminów ustawowych, opóźnienia krytycznych płatności,kary administracyjne, utrata wizerunku	5	4	20	Wybranie i wdrożenie zabezpieczenia	Przeprowadzenie testów PCD	A 5.30 A 5.29
	Skarbnik Gminy / Główny Księgowy	* Procesy, których utrata lub pogorszenie uniemożliwia wypełnienie misji organizacji										
1.		Proces Kadry/ Płace Urzędu i podległych jednostek budżetowych	Ryzyko utraty danych wrażliwych	Nieautoryzowany dostęp do aktywów, nieakceptowalne użycie aktywów	Brak świadomości pracownika, pozostawienie danych bez zabezpieczeń fizycznych (szafka zamykana na klucz)	Utrata danych, koszty finansowe, straty wizerunkowe	4	3	12	Akceptacja ryzyka	Monitorowanie ryzyka	Stosowanie procedur
		Proces Kadry/ Płace Urzędu i podległych jednostek budżetowych	Ryzyko nieterminowej realizacji zadań	Awaria urządzenia, niewłaściwe funkcjonowanie urządzenia, błąd aplikacji	Stary sprzęt -brak planów okresowej wymiany sprzętu, nieumiejętne użytkowanie,brak kompetencji użytkowników, utrata zasilania, brak zasilania awaryjnego, brak wsparcia serwisowego	Brak realizacji zadań w wyznaczonym terminie, koszty finansowe, koszty wizerunkowe	4	3	12	Akceptacja ryzyka	Monitorowanie ryzyka	Stosowanie procedur
2.		Procesy finansowo-księgowe Urzędu i jednostek budżetowych	Ryzyko utraty danych wrażliwych	Nieautoryzowany dostęp do aktywów, nieakceptowalne użycie aktywów	Brak świadomości pracownika, pozostawienie danych bez zabezpieczeń fizycznych (szafka zamykana na klucz)	Utrata danych, koszty finansowe, straty wizerunkowe	4	3	12	Akceptacja ryzyka	Monitorowanie ryzyka	Stosowanie procedur
3.		Procesy bankowe	Ryzyko utraty danych wrażliwych	Nieautoryzowany dostęp do aktywów, nieakceptowalne użycie aktywów	Brak świadomości pracownika, pozostawienie danych bez zabezpieczeń fizycznych (szafka zamykana na klucz)	Utrata danych, koszty finansowe, straty wizerunkowe	4	3	12	Akceptacja ryzyka	Monitorowanie ryzyka	Stosowanie procedur
4.		Procesy ubezpieczeniowe	Ryzyko utraty danych wrażliwych	Nieautoryzowany dostęp do aktywów, nieakceptowalne użycie aktywów	Brak świadomości pracownika, pozostawienie danych bez zabezpieczeń fizycznych (szafka zamykana na klucz)	Utrata danych, koszty finansowe, straty wizerunkowe	4	3	12	Akceptacja ryzyka	Monitorowanie ryzyka	Stosowanie procedur
5.		Zarządzanie aktywami Urzędu i jednostek podległych	Ryzyko braku zdefiniowanej odpowiedzialności za aktywa	Nieautoryzowany dostęp do aktywów, nieakceptowalne użycie aktywów	Brak świadomości pracownika, pozostawienie danych bez zabezpieczeń fizycznych (szafka zamykana na klucz)	Utrata danych, koszty finansowe, straty wizerunkowe	4	3	12	Akceptacja ryzyka	Monitorowanie ryzyka	A. 5.36, Stosowanie procedur
		Informacje wrażliwe							0			
6.		Dane osobowe pracowników Gminy oraz jednostek budżetowych	Ryzyko utraty danych wrażliwych	Wyciek informacji, kradzież informacji	Błąd pracownika, atak hakerski,Brak lub niewłaściwa ochrona przed nieautoryzowanym dostępem do systemów operacyjnych	Utrata danych w wersji papierowej, utrata plików lub aplikacji,straty wizerunkowe	4	3	12	Akceptacja ryzyka	Monitorowanie ryzyka	Stosowanie procedur
7.		Dokumenty finansowo - księgowe Urzędu, jednostek budżetowych, placówek oświatowych (Akcyza, Stypendia, Kadry i Płace, Podatki i opłaty lokalne))	Ryzyko utraty danych wraąliwych	Wyciek informacji, kradzież informacji	Błąd pracownika, atak hakerski,Brak lub niewłaściwa ochrona przed nieautoryzowanym dostępem do systemów operacyjnych	Utrata danych w wersji papierowej, utrata plików lub aplikacji,straty wizerunkowe	4	3	12	Akceptacja ryzyka	Monitorowanie ryzyka	Stosowanie procedur
8.		Faktury sprzedażowe / zakupowe	Ryzyko utraty danych wrażliwych	Wyciek informacji, kradzież informacji	Błąd pracownika, atak hakerski,Brak lub niewłaściwa ochrona przed nieautoryzowanym dostępem do systemów operacyjnych	Utrata danych w wersji papierowej, utrata plików lub aplikacji,straty wizerunkowe	4	3	12	Akceptacja ryzyka	Monitorowanie ryzyka	Stosowanie procedur
9.		Dokumenty bankowe	Ryzyko utraty danych wrażliwych	Wyciek informacji, kradzież informacji	Błąd pracownika, atak hakerski,Brak lub niewłaściwa ochrona przed nieautoryzowanym dostępem do systemów operacyjnych	Utrata danych w wersji papierowej, utrata plików lub aplikacji,straty wizerunkowe	4	3	12	Akceptacja ryzyka	Monitorowanie ryzyka	Stosowanie procedur
	Sekretarz Gminy	* Procesy, których utrata lub pogorszenie uniemożliwia wypełnienie misji organizacji							0			
1.		Wybory samorządowe, ogólnopolskie, referenda	Ryzyko utraty/ modyfikacji danych	Nieuprawniony dostęp lub włamanie, nieautoryzowane wejście do obszarów chronionych	Brak fizycznej ochrony budynków, drzwi i okien, brak stosowania Polityki kluczy, polityki uprawnień	Utrata danych w wersji papierowej, utrata plików lub aplikacji,straty wizerunkowe	4	3	12	Akceptacja ryzyka	Monitorowanie ryzyka	Stosowanie właściwych procedur
2.		Proces dostarczania wody mieszkańcom	Ryzyko utraty/ modyfikacji danych	Nieuprawniony dostęp lub włamanie, nieautoryzowane wejście do obszarów chronionych	Brak fizycznej ochrony budynków, drzwi i okien, brak stosowania Polityki kluczy, polityki uprawnień	Utrata danych w wersji papierowej, utrata plików lub aplikacji,straty wizerunkowe	4	3	12	Akceptacja ryzyka	Monitorowanie ryzyka	Stosowanie właściwych procedur
3.		Proces Obrony Cywilnej	Ryzyko utraty/ modyfikacji danych	Nieuprawniony dostęp lub włamanie, nieautoryzowane wejście do obszarów chronionych	Brak fizycznej ochrony budynków, drzwi i okien, brak stosowania Polityki kluczy, polityki uprawnień	Utrata danych w wersji papierowej, utrata plików lub aplikacji,straty wizerunkowe	4	3	12	Akceptacja ryzyka	Monitorowanie ryzyka	Stosowanie właściwych procedur
4.		SIO - System Informacji Oświatowej	Ryzyko utraty/ modyfikacji danych	Nieuprawniony dostęp lub włamanie, nieautoryzowane wejście do obszarów chronionych	Brak fizycznej ochrony budynków, drzwi i okien, brak stosowania Polityki kluczy, polityki uprawnień	Utrata danych w wersji papierowej, utrata plików lub aplikacji,straty wizerunkowe	4	3	12	Akceptacja ryzyka	Monitorowanie ryzyka	Stosowanie właściwych procedur
		Informacje wrażliwe							0			

5.		Zbiory dokumentów: delegacje, zwolnienia lekarskie, urlopy , pełnomocnictwa, upoważnienia	Ryzyko utraty / modyfikacji aktywów	Nieuprawniony dostęp lub włamanie, nieautoryzowane wejście do obszarów chronionych	Brak fizycznej ochrony budynków, drzwi i okien, brak stosowania Polityki kluczy,	Utrata danych w wersji papierowej, utrata plików lub aplikacji, straty wizerunkowe	3	3	9	Akceptacja ryzyka	Monitorowanie ryzyka	Stosowanie właściwych procedur
6.		Decyzje ws. wycinki drzew	Ryzyko utraty / modyfikacji aktywów	Nieuprawniony dostęp lub włamanie, nieautoryzowane wejście do obszarów chronionych	Brak fizycznej ochrony budynków, drzwi i okien, brak stosowania Polityki kluczy,	Utrata danych w wersji papierowej, utrata plików lub aplikacji, straty wizerunkowe	3	3	9	Akceptacja ryzyka	Monitorowanie ryzyka	Stosowanie właściwych procedur
7.		Decyzje o warunkach zabudowy	Ryzyko utraty / modyfikacji aktywów	Nieuprawniony dostęp lub włamanie, nieautoryzowane wejście do obszarów chronionych	Brak fizycznej ochrony budynków, drzwi i okien, brak stosowania Polityki kluczy,	Utrata danych w wersji papierowej, utrata plików lub aplikacji, straty wizerunkowe	3	3	9	Akceptacja ryzyka	Monitorowanie ryzyka	Stosowanie właściwych procedur
8.		Zbiory dokumentów dotyczące interesantów Gminy	Ryzyko ujawnienia danych wrażliwych	Kradzież dokumentów, nieautoryzowany dostęp do pomieszczeń	Niezabezpieczone pomieszczenie, pozostawienie dokumentów w drukarce, Brak lub niejasno określone zasady zachowania poufności informacji gromadzonych i przetwarzanych przez pracowników,Brak lub nieregularne archiwizowanie informacji	Ujawnienie danych wrażliwych, utrata wizerunku, kary finansowe	3	3	9	Akceptacja ryzyka	Monitorowanie ryzyka	Stosowanie właściwych procedur
9.		Zbiory dokumentów dotyczące pracowników Gminy	Ryzyko ujawnienia danych wrażliwych	Kradzież dokumentów, nieautoryzowany dostęp do pomieszczeń	Niezabezpieczone pomieszczenie, pozostawienie dokumentów w drukarce, Brak lub niejasno określone zasady zachowania poufności informacji gromadzonych i przetwarzanych przez pracowników,Brak lub nieregularne archiwizowanie informacji	Ujawnienie danych wrażliwych, utrata wizerunku, kary finansowe	3	3	9	Akceptacja ryzyka	Monitorowanie ryzyka	Stosowanie właściwych procedur
10.		Elektroniczne Zarządzanie Dokumentacją,	Ryzyko ujawnienia danych wrażliwych	Błąd użytkownika	Brak lub niejasno określone zasady obiegu dokumentacji wewnątrz organizacji	Ujawnienie danych wrażliwych, utrata wizerunku, kary finansowe	3	3	9	Akceptacja ryzyka	Monitorowanie ryzyka	Stosowanie właściwych procedur
11.		Akcja Kurierska - system doręczania kart powołania	Ryzyko niedostarczenia karty w wymaganym czasie	1.Awaria sprzętu,niewłaściwe funkcjonowanie urządzeń 2. Błąd użytkownika	Błąd systemu teleinformatycznego,	Brak realizacji zadań	3	2	6	Akceptacja ryzyka	Monitorowanie ryzyka	Stosowanie właściwych procedur
	Kierownik USC	Procesy, których utrata lub pogorszenie uniemożliwia wypełnienie misji organizacji										
1.		Proces wydawania dowodów osobistych, aktów ślubu, aktów urodzenia	Ryzyko wydania obywatelowi błędnego dokumentu	1.Awaria sprzętu,niewłaściwe funkcjonowanie urządzeń 2. Błąd użytkownika	Błąd użytkownika, błąd systemu teleinformatycznego,brak kopii zapasowych	Wydanie dokumentu zawierającego błędy, utrata wizerunku, koszty finansowe	3	2	6	Akceptacja ryzyka	Monitorowanie ryzyka	Stosowanie właściwych procedur
2.		Proces wydawania dowodów osobistych, aktów ślubu, aktów urodzenia	Ryzyko utraty danych wrażliwych	Kradzież dokumentów, nieautoryzowany dostęp do pomieszczeń	Niezabezpieczone pomieszczenie, pozostawienie dokumentów w drukarce, Brak lub niejasno określone zasady zachowania poufności informacji gromadzonych i przetwarzanych przez pracowników,Brak lub nieregularne archiwizowanie informacji	Ujawnienie danych wrażliwych, utrata wizerunku, kary finansowe	3	3	9	Akceptacja ryzyka	Monitorowanie ryzyka	Stosowanie właściwych procedur
3.		Procesy meldunkowe	Ryzyko ujawnienia danych wrażliwych	Kradzież dokumentów, nieautoryzowany dostęp do pomieszczeń	Niezabezpieczone pomieszczenie, pozostawienie dokumentów w drukarce, Brak lub niejasno określone zasady zachowania poufności informacji gromadzonych i przetwarzanych przez pracowników	Ujawnienie danych wrażliwych, utrata wizerunku, kary finansowe	3	3	9	Akceptacja ryzyka	Monitorowanie ryzyka	Stosowanie właściwych procedur
4.		Ewidencja ludności	Ryzyko ujawnienia danych wrażliwych	Kradzież dokumentów, nieautoryzowany dostęp do pomieszczeń	Niezabezpieczone pomieszczenie, pozostawienie dokumentów w drukarce, Brak lub niejasno określone zasady zachowania poufności informacji gromadzonych i przetwarzanych przez pracowników	Ujawnienie danych wrażliwych, utrata wizerunku, kary finansowe	3	3	9	Akceptacja ryzyka	Monitorowanie ryzyka	Stosowanie właściwych procedur
5.		SIO - System Informacji Oświatowej	Ryzyko ujawnienia danych wrażliwych	Kradzież dokumentów, nieautoryzowany dostęp do pomieszczeń	Niezabezpieczone pomieszczenie, pozostawienie dokumentów w drukarce, Brak lub niejasno określone zasady zachowania poufności informacji gromadzonych i przetwarzanych przez pracowników	Ujawnienie danych wrażliwych, utrata wizerunku, kary finansowe	3	3	9	Akceptacja ryzyka	Monitorowanie ryzyka	Stosowanie właściwych procedur
		Informacje wrażliwe							0			
6.		Rejestry: PESEL, rejestr mieszkańców, rejestr Dowodów Osobistych, aktów urodzenia, aktów stanu cywilnego	Ryzyko ujawnienia danych wrażliwych	Kradzież dokumentów, nieautoryzowany dostęp do pomieszczeń	Niezabezpieczone pomieszczenie, pozostawienie dokumentów w drukarce, Brak lub niejasno określone zasady zachowania poufności informacji gromadzonych i przetwarzanych przez pracowników	Ujawnienie danych wrażliwych, utrata wizerunku, kary finansowe	4	3	12	Akceptacja ryzyka	Monitorowanie ryzyka	Przechowywanie dokumentów w szafach zamykanych na klucz. Niszczenie dokumentów w niszczarkach
	ASI	*Procesy, których utrata lub pogorszenie uniemożliwia wypełnienie misji organizacji										
1.		Utrzymanie ciągłości działania infrastruktury i sprzętu teleinformatycznego	Ryzyko braku ciągłości działania infrastruktury teleinformatycznej	Przerwanie procesów biznesowych Urzędu	Brak właściwych zabezpieczeń technicznych, brak aktualizacji dokumentacji / procedur wraz ze zmianami w otoczeniu	Brak realizacji zadań statutowych Urzędu, kary finansowe	4	4	16	Wybranie i wdrożenie zabezpieczenia	Wdrożenie procesu zarządzania incydentem,	Proces zarządzania Incydentem,Prowadzenie okresowych analiz ryzyka w zakresie bezpieczeństwa,Audyty wewnętrzne z zakresu bezpieczeństwa informacji
	Inspektor Ochrony Danych Osobowych	*Procesy, których utrata lub pogorszenie uniemożliwia wypełnienie misji organizacji							0			
1.		Proces identyfikacji zbiorów danych osobowych będących w posiadaniu Urzędu	Ryzyko ujawnienia danych wrażliwych	Wyciek danych osobowych	Brak identyfikacji wszystkich zbiorów danych wrażliwych	Możliwość wykorzystania danych przez osoby niepowołane, utrata wizerunku	3	3	9	Akceptacja ryzyka	Monitorowanie ryzyka	Stosowanie procedur
	Informatyk	SPRZĘT							0			

1.		Sprzęt - urządzenia przetwarzania danych	Ryzyko nieautoryzowanego działania	1. Kradzież urządzenia 2. Nieuprawniony dostęp 3. Złamanie haseł	Niewłaściwa ochrona fizyczna budynku, pomieszczeń, drzwi, okien, urządzenie pozostawione bez blokady ekranu, nieprawidłowe uprawnienia,instalacja przez użytkownika szkodliwego oprogramowania,Włamanie do sieci wewnętrznej,Nieprzestrzeganie zasad czystego biurka i pulpitu. Nieprzestrzeganie polityki tworzenia haseł.	Możliwość wykorzystania danych przez osoby niepowołane, utrata wizerunku	5	4	20	Wybranie i wdrożenie zabezpieczenia	Przeciwdziałanie: 1.Zdefiniowanie osób odpowiedzialnych za bezpieczną eksploatację systemów teleinformatycznych 2.Szkolenia pracowników 3.Przestrzeganie przez użytkowników procedur SZBI 4.Sporządzenie dokumentacji technicznej wymaganej przez KSC	A 5.36, A 5.15, A 5.16, A 5.17. A 5.18, A 7.3, A 7.8
2.		Sprzęt - urządzenia przetwarzania danych	Ryzyko awarii technicznej	1.Awaria sprzętu,niewłaściwe funkcjonowanie urządzeń 2. Błąd użytkownika	Stary sprzęt -brak planów okresowej wymiany sprzętu, nieumiejętne użytkowanie,brak kompetencji użytkowników, utrata zasilania, brak zasilania awaryjnego, brak wsparcia serwisowego	Zakłócenia w realizacji procesów, ograniczony dostęp do danych, nieterminowe wykonywanie zadań	5	4	20	Wybranie i wdrożenie zabezpieczenia	Przeciwdziałanie: sporządzenie dokumentacji wymaganej przez KSC	Cykliczna wymiana sprzętu,umowy serwisowe, szkolenie użytkowników, dokumentacja A 8.6, A 8.9, A 7.13
3.		Strona WWW Urzędu	Ryzyko ataku hakerskiego na stronę www	Atak hakerski umożliwiający przejęcie kontroli nad serwisem	Słabe zabezpieczenia techniczne	Utrata reputacji i dobrego wizerunku	5	3	15	Wybranie i wdrożenie zabezpieczenia	Wdrożenie protokołu https , aktualizacja certyfikatu X.509, upgrade wersji TLS	
4.		Serwer pocztowy	Ryzyko przejęcia danych wrażliwych	Atak phishingowy, ransomware	Słabe zabezpieczenia techniczne, błąd użytkownika	Utrata danych, utrata reputacji, możliwe zaszyfrowanie plików	4	3	12	Akceptacja ryzyka	Monitorowanie ryzyka	A 8.6, A 8.9, A 7.13
5.		Sprzęt - przenośne urządzenia przetwarzania danych	Ryzyko utraty danych wrażliwych	1. Kradzież, utrata urządzenia. 2.Nieuprawniony dostęp	Niezabezpieczenie urządzenia przez użytkownika,Brak zasad zwrotu i rozliczania mienia powierzonego pracownikom	Utrata danych, utrata reputacji, utrata aktywu	4	3	12	Akceptacja ryzyka	Monitorowanie ryzyka	Polityka w zakresie urządzeń mobilnych, Szkolenia użytkowników
	Informatyk	APLIKACJE							0			
1.		Aplikacje	Nieuprawniony dostęp do informacji w aplikacjach	Wykorzystanie aplikacji w sposób nieautoryzowany	Brak odpowiedniego nadzoru nad oprogramowaniem, nieumiejętne korzystanie z oprogramowania, brak aktualizacji oprogramowania, niewłaściwie przypisane prawa dostępu,opuszczenie stanowiska pracy bez wylogowania się z aplikacji,Brak lub niewłaściwa ochrona przed nieautoryzowanym dostępem do systemów operacyjnych	Możliwość utraty danych, modyfikacji danych	4	3	12	Akceptacja ryzyka	Monitorowanie ryzyka	Instrukcja korzystania z oprogramowania, właściwie przydzielone prawa dost epu, stosowanie się użytkownika do PBT
2.		Aplikacje	Ryzyko naruszenia praw autorskich	Nielegalne przetwarzanie danych	Brak licencji -Prawa administratora nadane użytkownikom- możliwość instalacji nieautoryzowanych aplikacji	Możliwość utraty danych,możliwość poniesienia kosztów finansowych związanych z brakiem licencji	3	2	6	Akceptacja ryzyka	Monitorowanie ryzyka	A 8.9 Przestrzeganie zasad instalacji oprogramowania
3.		Aplikacje	Ryzyko przerwania działania kluczowych aplikacji	Brak dostępu do aplikacji	Nieaktualizowane oprogramowanie, nieskuteczna ochrona antywirusowa,Brak lub niewłaściwa ochrona przed nieuprawnionym dostępem do aplikacji, luki w systemach	Brak realizacji zadań, możliwe kary - koszty finansowe	3	3	9	Akceptacja ryzyka	Monitorowanie ryzyka	A 8.9 Aktualizacja oprogramowania, stosowanie procedur dostępu, uświadamianie pracowników
	Informatyk	Sieć										
1.		Lokalna sieć teleinformatyczna	Ryzyko utraty danych lub zniekształcenia danych	Atak phishingowy	Brak zabezpieczeń technicznych i proceduralnych sieci, urządzeń brzegowych	Utrata danych, utrata wizerunku firmy, koszty finansowe	5	4	20	Wybranie i wdrożenie zabezpieczenia	Wdrożenie procedur i mechanizmów segmentacji sieci,izolacji końcowych użytkowników, mechanizmów monitorujących sieć wewnątrz, wdrożenie aplikacji i sprzętu zabezpieczającego	A 8.20, A 8.22
	Informatyk	Pliki: - konfiguracyjne (aplikacje, bazy danych, systemy, sieci), poczty elektronicznej										
1.		Pliki: - konfiguracyjne (aplikacje, bazy danych, systemy, sieci), poczty elektronicznej	Ryzyko utraty danych lub zniekształcenia danych	Nieautoryzowany dostęp do informacji,Zużycie nośników informacji, złamanie haseł	Brak lub niewłaściwa ochrona bezpieczeństwa plików systemowych, w tym kodów źródłowych	Naruszenie ochrony danych osobowych, naruszenie poufności, utrata niezapisanych danych, kary dla Urzędu	4	3	12	Akceptacja ryzyka	Stosowanie procedur, szkolenie pracowników	Stosowanie procedur SZBI
		Kopie zapasowe										
1.		Kopie zapasowe	Ryzyko utraty lub zniekształcenia danych	Utrata danych, zniekształcenie danych	Brak lub nieregularne tworzenie kopii zapasowych informacji przetwarzanych w systemach teleinformatycznych	Brak aktualnych danych, możliwa nieterminowa realizacja zadań, możliwe kary finansowe	5	4	20	Wybranie i wdrożenie zabezpieczenia	Stosowanie procedur kopii zapasowych	A 8.13Proces tworzenia i okresowego odtwarzania kopi zapasowych, kopiowane istotnych danych na dyski zewnętrzne
	Informatyk	NOŚNIKI DANYCH							0			

1.		Nośniki danych	Ryzyko ujawnienia, modyfikacji, utraty danych z nośników informacji	1. Zagubienie 2. Kradzież 2. Zniszczenie nośników informacji.	1.Brak stosownych procedur postępowania z nośnikami Niekontrolowane kopiowanie, brak staranności przy pozbywaniu się nośników	Naruszenie ochrony danych osobowych, naruszenie poufności, utrata niezapisanych danych, kary dla Urzędu	4	3	12	Akceptacja ryzyka	Stosowanie procedur, szkolenie pracowników	A. 7.10
	Sekretarz	SIEDZIBA							0			
1.		Siedziba - budynki	Brak dostaw mediów (prąd, woda, internet)	Uszkodzenie infrastruktury	Awaria po stronie dostawcy, ograniczenie dostaw, awaria infrastruktury budynku	Brak możliwości wykorzystania sprzętu elektronicznego, brak możliwości zapewnienia właściwych warunków pracy	3	3	9	Transfer ryzyka - Ubezpieczenie	Monitorowanie ryzyka	A 7.1
2.		Siedziba - budynki	Utrata aktywów	Nieuprawniony dostęp lub włamanie, nieautoryzowane wejście do obszarów chronionych	Brak fizycznej ochrony budynków, drzwi i okien, brak stosowania Polityki kluczy,	Utrata danych w wersji papierowej, utrata plików lub aplikacji,kradzież sprzętu i nośników danych, instalacja nieautoryzowanych urządzeń	4	3	12	Akceptacja ryzyka	Stosowanie procedur bezpieczeństwa fizycznego i środowiskowego	A 7.1, A 7.2, A 7.3
3.		Siedziba - Archiwum	Uszkodzenie lub zniszczenie dokumentów archiwalnych i dokumentacji	1. Wichura, pożar, zalanie z rur	1. Nagłe zjawiska pogodowe	Utrata danych , możliwa nieterminowa realizacja zadań, możliwe kary finansowe, utrata wizerunku	3	4	12	Transfer ryzyka - Ubezpieczenie	Monitorowanie ryzyka	A 7.1, A 7.2, A 7.3
	Sekretarz	PERSONEL							0			
1.		Personel	Ryzyko nieautoryzowanego działania	Nieuprawnione kopiowanie oprogramowania, zniekształcenie danych, nielegalne przetwarzanie danych	Nieaktualne prawa dostępu użytkowników, brak stosowania ochrony poufnych informacji uwierzytelniających, brak świadomości pracowników	Wyciek informacji, brak realizacji zadań statusowych Gminy, utrata wizerunku	4	3	12	Akceptacja ryzyka	Monitorowanie ryzyka	A 6.3, A 6.8
2.		Personel	Ryzyko nieautoryzowanego działania	Błąd ludzki, celowe szkodliwe działanie pracownika	Nieprawidłowa weryfikacja personelu podczas zatrudnienia, nieprawidłowe uprawnienia, błąd użytkownika, brak zastępowalności	Wyciek informacji, brak realizacji zadań statusowych Gminy, utrata wizerunku	4	3	12	Akceptacja ryzyka	Monitorowanie ryzyka	A 6.1 Weryfikacja pracowników przed zatrudnieniem
3.		Personel – użytkownik systemu	Ryzyko nieautoryzowanego działania	Kradzież danych	Mała świadomość zagrożeń teleinformatycznych,Brak lub niejasno określone zasady zachowania poufności informacji gromadzonych i przetwarzanych przez pracowników	utrata reputacji Gminy , skutki prawne	4	3	12	Akceptacja ryzyka	Monitorowanie ryzyka	A 6.3, A 6.8
		UMOWY Z DOSTAWCAMI							0			
1.		Umowy z dostawcami	Ryzyko utraty danych z aktywów udostępnianych dostawcom	Nielegalne pozyskanie danych	Brak zapisów dotyczących zapewnienia bezpieczeństwa informacji w umowach z dostawcami,Brak lub niejasne zasady udzielania informacji podmiotom zewnętrznym	Wyciek informacji, utrata reputacji	4	3	12	Akceptacja ryzyka	Stosowanie stosownych zapisów w umowach z dostawcami	A 5.19

Wpływ	Odpowiednik punktowy	Przesłanki
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 Powiatu. (Wysoka strata finansowa – powyżej 1% budżetu -Powiatu)
Poważny	4	Poważny wpływ na realizacje zadania w tym poważne zagrożenie terminu jego realizacji, jaki i osiągniecie celu, poważne konsekwencje prawne, zagrożenie bezpieczeństwa pracowników, poważne straty finansowe, poważny wpływ na wizerunek Powiatu (Poważny skutek finansowy – od 0,5% do 1% budżetu Powiatu)
Średni	3	Średni wpływ na realizację zadań i celów, umiarkowane konsekwencje prawne, średni skutek finansowy, brak wpływu na bezpieczeństwo pracowników, średni wpływ na wizerunek Powiatu. (Średni skutek finansowy – od 0,2% do 5% budżetu Powiatu)
Mały	2	Mały wpływ na realizację celów i zadań, bez skutków prawnych, mały skutek finansowy, brak wpływu na bezpieczeństwo pracowników, niewielki wpływ na wizerunek Powiatu. (Mały skutek finansowy – od 0,1% do 0,2% budżetu Powiatu)
Nieznaczny	1	Znikomy wpływ na realizację zadań i celów, brak skutków prawnych, nieznaczny skutek finansowy, brak wpływu na bezpieczeństwo pracowników, brak wpływu na wizerunek Powiatu. (Nieznaczny skutek finansowy do 0,1 % budżetu Powiatu)

Waga prawdopodobieństwa	Prawdopodobieństwo wystąpienia	Zasady oceny prawdopodobieństwa ryzyka
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

Ocena ryzyka - matryca tolerancji

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

Istotność zagrożenia					
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 wystąpienia zagrożenia				

Wybranie i wdrożenie zabezpieczenia

Transfer ryzyka umowa z dostawcą

Unikanie ryzyka

dopuszczalne Akceptacja ryzyka monitorowanie

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 lektromagnetyczne
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

Rodzaj	Przykłady podatności	Przykłady zagrożeń
Sprzęt	Niewystarczające utrzymanie / błędna instalacja nośników pamięci	Naruszenie zdolności utrzymania systemu informacyjnego
	Brak planów okresowej wymiany	Zniszczenie urządzeń lub nośników
	Wrażliwość na wilgoć, pył, zanieczyszczenie	Pył, korozja, wychłodzenie
	Wrażliwość na promieniowanie elektromagnetyczne	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

Zabezpieczenia zgodnie z Załącznikiem A normy ISO/IEC 27001

5.1	Polityki bezpieczeństwa informacji
5.2	Role i odpowiedzialność za bezpieczeństwo informacji
5.3	Rozdzielanie obowiązków
5.4	Odpowiedzialność kierownictwa
5.5	Kontakty z organami władzy
5.6	Kontakty z grupami zainteresowanych specjalistów
5.7	Rozpoznanie zagrożeń
5.8	Bezpieczeństwo informacji w zarządzaniu projektami
5.9	Ewidencja informacji i innych powiązanych aktywów
5.10	Akceptowalne użycie informacji i innych powiązanych aktywów
5.11	Zwrot aktywów
5.12	Klasyfikowanie informacji
5.13	Oznaczanie informacji
5.14	Przesyłanie informacji
5.15	Kontrola dostępu
5.16	Zarządzanie tożsamością
5.17	Informacje uwierzytelniające
5.18	Prawa dostępu
5.19	Bezpieczeństwo informacji w relacjach z dostawcami
5.20	Uwzględnianie bezpieczeństwa informacji w porozumieniach z dostawcami
5.21	Zarządzanie bezpieczeństwem informacji w łańcuchu dostaw technologii teleinformatycznych (ICT)
5.22	Monitorowanie, przegląd i zarządzanie zmianami w usługach świadczonych przez dostawców
5.23	Bezpieczeństwo informacji dotyczące stosowania usług w chmurze
5.24	Planowanie i przygotowanie do zarządzania incydentami związanymi z bezpieczeństwem informacji
5.25	Ocena i podejmowanie decyzji w sprawie zdarzeń związanych z bezpieczeństwem informacji
5.26	Reagowanie na incydenty związane z bezpieczeństwem informacji
5.27	Wyciąganie wniosków z incydentów związanych z bezpieczeństwem informacji
5.28	Gromadzenie materiału dowodowego
5.29	Bezpieczeństwo informacji podczas zakłóceń
5.30	Gotowość ICT do zapewnienia ciągłości działania
5.31	Wymagania prawne, regulacyjne i umowne
5.32	Prawa własności intelektualnej
5.33	Ochrona zapisów
5.34	Prywatność i ochrona danych identyfikujących osobę (PII)
5.35	Niezależny przegląd bezpieczeństwa informacji
5.36	Zgodność z politykami, zasadami i standardami dotyczącymi bezpieczeństwa informacji
5.37	Udokumentowane procedury eksploatacyjne
6.1	Postępowanie sprawdzające
6.2	Warunki zatrudnienia
6.3	Uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji
6.4	Postępowanie dyscyplinarne
6.5	Odpowiedzialność po zakończeniu lub zmianie zatrudnienia
6.6	Umowy o zachowaniu poufności lub nieujawnianiu informacji
6.7	Praca zdalna
6.8	Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji
6.1	Postępowanie sprawdzające
6.2	Warunki zatrudnienia

6.3	Uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji
6.4	Postępowanie dyscyplinarne
6.5	Odpowiedzialność po zakończeniu lub zmianie zatrudnienia
6.6	Umowy o zachowaniu poufności lub nieujawnianiu informacji
6.7	Praca zdalna
6.8	Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji
6.1	Postępowanie sprawdzające
6.2	Warunki zatrudnienia
6.3	Uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji
6.4	Postępowanie dyscyplinarne
6.5	Odpowiedzialność po zakończeniu lub zmianie zatrudnienia
6.6	Umowy o zachowaniu poufności lub nieujawnianiu informacji
6.7	Praca zdalna
6.8	Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji
6.1	Postępowanie sprawdzające
6.2	Warunki zatrudnienia
6.3	Uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji
6.4	Postępowanie dyscyplinarne
6.5	Odpowiedzialność po zakończeniu lub zmianie zatrudnienia
6.6	Umowy o zachowaniu poufności lub nieujawnianiu informacji
6.7	Praca zdalna
6.8	Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji
6.1	Postępowanie sprawdzające
6.2	Warunki zatrudnienia
6.3	Uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji
6.4	Postępowanie dyscyplinarne
6.5	Odpowiedzialność po zakończeniu lub zmianie zatrudnienia
6.6	Umowy o zachowaniu poufności lub nieujawnianiu informacji
6.7	Praca zdalna
6.8	Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji
6.1	Postępowanie sprawdzające
6.2	Warunki zatrudnienia
6.3	Uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji
6.4	Postępowanie dyscyplinarne
6.5	Odpowiedzialność po zakończeniu lub zmianie zatrudnienia
6.6	Umowy o zachowaniu poufności lub nieujawnianiu informacji
6.7	Praca zdalna
6.8	Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji
6.1	Postępowanie sprawdzające
6.2	Warunki zatrudnienia
6.3	Uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji
6.4	Postępowanie dyscyplinarne
6.5	Odpowiedzialność po zakończeniu lub zmianie zatrudnienia
6.6	Umowy o zachowaniu poufności lub nieujawnianiu informacji
6.7	Praca zdalna
6.8	Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji
6.1	Postępowanie sprawdzające
6.2	Warunki zatrudnienia
6.3	Uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji
6.4	Postępowanie dyscyplinarne
6.5	Odpowiedzialność po zakończeniu lub zmianie zatrudnienia
6.6	Umowy o zachowaniu poufności lub nieujawnianiu informacji
6.7	Praca zdalna
6.8	Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji

7.1	Fizyczne granice obszaru bezpiecznego
7.2	Wejście fizyczne
7.3	Zabezpieczenie biur, pomieszczeń i obiektów
7.4	Monitorowanie bezpieczeństwa fizycznego
7.5	Ochrona przed zagrożeniami fizycznymi i środowiskowymi
7.6	Praca w obszarach bezpiecznych
7.7	Czyste biurko i czysty ekran
7.8	Lokalizacja i ochrona sprzętu
7.9	Bezpieczeństwo aktywów poza siedzibą
7.10	Nośniki informacji
7.11	Systemy wspomagające
7.12	Bezpieczeństwo okablowania
7.13	Konserwacja sprzętu
7.14	Bezpieczne zbywanie lub przekazywanie do ponownego użycia
8.1	Urządzenia końcowe użytkownika
8.2	Prawa uprzywilejowanego dostępu
8.3	Ograniczanie dostępu do informacji
8.4	Dostęp do kodu źródłowego
8.5	Bezpieczne uwierzytelnianie
8.6	Zarządzanie pojemnością
8.7	Ochrona przed szkodliwym oprogramowaniem
8.8	Zarządzanie podatnościami technicznymi
8.9	Zarządzanie konfiguracją
8.10	Usuwanie informacji
8.11	Maskowanie danych
8.12	Zapobieganie wyciekom danych
8.13	Zapasowe kopie informacji
8.14	Nadmiarowość środków przetwarzania informacji
8.15	Rejestrowanie
8.16	Działania monitorujące
8.17	Synchronizacja zegarów
8.18	Użycie uprzywilejowanych programów narzędziowych
8.19	Instalacja oprogramowania w systemach produkcyjnych
8.20	Bezpieczeństwo sieci
8.21	Bezpieczeństwo usług sieciowych
8.22	Rozdzielanie sieci
8.23	Filtrowanie treści internetowych
8.24	Użycie kryptografii
8.25	Bezpieczne wytwarzanie oprogramowania
8.26	Wymagania bezpieczeństwa aplikacji
8.27	Zasady bezpiecznej architektury systemu i jej projektowania
8.28	Bezpieczne kodowanie
8.29	Testowanie bezpieczeństwa podczas wytwarzania i akceptowania
8.30	Wytwarzanie zlecane podmiotom zewnętrznym
8.31	Oddzielanie środowisk rozwojowych, testowych i produkcyjnych
8.32	Zarządzanie zmianami
8.33	Informacje testowe
8.34	Ochrona systemów informacyjnych podczas testów audytowych

komórki organizacyjne:
Starosta
Wicestarosta
Sekretarz Powiatu
Skarbnik Powiatu
Biuro Rady i Zarządu Powiatu
Wydział Organizacji i Nadzoru
Wydział Finansowy
Wydział Komunikacji i Transportu
Wydział Architektury i Budownictwa
Wydział Rolnictwa i Środowiska
Wydział Geodezji i Gospodarki Nieruchomościami
Wydział Oświaty i Zdrowia
Referat Zarządzania Kryzysowego i Obrony Cywilnej
Pełnomocnik ds. Ochrony Informacji Niejawnych
Samodzielne stanowiska ds. kadr i płac
Samodzielne stanowiska ds. promocji powiatu i komunikacji z Mieszkańcami
Samodzielne stanowiska ds. rozwoju powiatu i zamówień publicznych
Powiatowy Rzecznik Konsumentów

~~Akcyza~~
~~KAP System Rejestrów Państwowych – bezpieczeństwo, funkcjonowanie i użyteczność55~~
~~Stypendia~~
~~Kadry i Płace~~
~~Podatki i opłaty lokalne~~
~~Auta~~
~~Woda~~
~~System Informacji Oświatowej~~
~~Umowy na dostarczanie wody i odprowadzanie ścieków~~
~~Umowy najmu lokali mieszkalnych i użytkowych~~
~~Ewidencja ludności~~
~~USC win~~
~~System rejestru wyborców~~
~~AP USC 3- sprawozdawczość~~
~~System wydawania dpwodów osobistych~~
~~Decyzje o warunkach zabudowy~~
~~Akcja Kurierska~~
~~Decyzje w sprawie wycinki drzew i krzewów~~

1 Wybranie i wdrożenie zabezpieczenia	Zapobieganie
2 Transfer ryzyka	
3 Unikanie ryzyka	
4 Akceptacja ryzyka	