

z dnia 17 marca 2026 roku

w sprawie wprowadzenia Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Gminy Jasło

Na podstawie art. 33 ust. 3 i 5 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (tj. Dz. U. z 2025r., poz.1153 z późn. zm.) oraz § 19 rozporządzenia Rady Ministrów z dnia 21 maja 2024r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2024r., poz.773) zarządzam, co następuje:

§1. W celu utrzymania podstawowych atrybutów bezpieczeństwa przetwarzania informacji, w szczególności poufności, dostępności i integralności informacji wprowadza się do stosowania w Urzędzie Gminy Jasło System Zarządzania Bezpieczeństwem Informacji (SZBI) oraz prowadzi związaną z nim dokumentację.

2. Na dokumentację SZBI składają się następujące polityki:

- 1) Polityka Bezpieczeństwa Informacji (PBI) w Urzędzie Gminy Jasło;
- 2) Polityka Ciągłości Działania w Urzędzie Gminy Jasło;
- 3) Polityka Bezpieczeństwa Fizycznego i Środowiskowego w Urzędzie Gminy Jasło;
- 4) Polityka Zarządzania Incydentami w Urzędzie Gminy Jasło;
- 5) Polityka Audytu Wewnętrznego w Urzędzie Gminy Jasło;
- 6) Polityka Bezpieczeństwa w Relacjach z Dostawcami;
- 7) Polityka Zarządzania Podatnościami w Urzędzie Gminy Jasło

stanowiące załączniki do niniejszego zarządzenia.

§3.1. Pracownicy Urzędu Gminy Jasło są zobowiązani do zapoznania się z całością dokumentacji SZBI i potwierdzenia o zapoznaniu się z dokumentacją.

§4. Wykonanie zarządzenia powierza się Sekretarzowi Gminy.

§5. Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT
Wojciech Piękoś

Urząd Gminy Jasło	Polityka Bezpieczeństwa Informacji	Strona	1
		Wydanie	I
		Data wydania	2026.03.16

POLITYKA BEZPIECZEŃSTWA INFORMACJI (PBI) w Urzędzie Gminy Jasło

ZATWIERDZAM

Wojciech Piskos 17.03.2026r
 (Podpis/pieczętka i data)

<i>Urząd Gminy Jasło</i>	<i>Polityka Bezpieczeństwa Informacji</i>	<i>Strona</i>	1
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

**POLITYKA
BEZPIECZEŃSTWA INFORMACJI (PBI)
w Urzędzie Gminy Jasło**

ZATWIERDZAM

(Podpis/pieczątka i data)

<i>Urząd Gminy Jasło</i>	<i>Polityka Bezpieczeństwa Informacji</i>	<i>Strona</i>	3
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

SPIS TREŚCI

Skróty i definicje	4
Rozdział I. Cel i Zakres Polityki Bezpieczeństwa Informacji.....	5
Rozdział II. Role i odpowiedzialności w zakresie Systemu Zarządzania Bezpieczeństwem Informacji.....	6
Rozdział III. Zarządzanie aktywami informacyjnymi	9
Rozdział IV. Kontrola dostępu do informacji	9
Rozdział V. Zarządzanie ryzykiem w bezpieczeństwie informacji	9
Rozdział VI. Bezpieczeństwo teleinformatyczne	10
Rozdział VII. Bezpieczeństwo fizyczne i środowiskowe	10
Rozdział VIII. Bezpieczeństwo zasobów ludzkich	10
Rozdział IX. Zapewnienie ciągłości działania.....	11
Rozdział X. Relacje z podmiotami zewnętrznymi	11
Rozdział XI. Procedura zarządzania projektami.....	12
Rozdział XII. Podstawowe zasady bezpieczeństwa.....	13
Rozdział XIII. Naruszenie bezpieczeństwa informacji.....	15
Rozdział XIV. Zgodność z przepisami prawa i zapisami umownymi	16
Rozdział XV. Deklaracja kierownictwa.....	17

SPIS ZAŁĄCZNIKÓW

Załącznik 1.	SZBI-001-01 Procedura zarządzania aktywami informacyjnymi
Załącznik 2.	SZBI-001-02 Deklaracja stosowania

Urząd Gminy Jasło	Polityka Bezpieczeństwa Informacji	Strona	4
		Wydanie	I
		Data wydania	2026.03.16

SKRÓTY I DEFINICJE

Administrator Danych Osobowych – Urząd Gminy Jasło

Jednostka – Urząd Gminy Jasło ul. Słowackiego 4, 38-200 Jasło

SZBI - System Zarządzania Bezpieczeństwem Informacji

PBI – Polityka Bezpieczeństwa Informacji

Zespół ds. Obsługi Incydentów – zespół osobowy odpowiedzialny za proces zarządzania incydentami – przygotowanie, realizację działań w trakcie wystąpienia incydentu oraz działań likwidujących skutki wystąpienia incydentu.

Informacja poufna – wszelkie informacje, które są chronione przed dostępem osób trzecich oraz przed upublicznieniem. Dane osobowe wchodzą w skład informacji poufnych.

Dane osobowe – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Odbiorca – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Przy czym odbiorcą nie jest organ publiczny, który może otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii Europejskiej lub prawem państw członkowskiego.

Osoba upoważniona – osoba upoważniona przez administratora do przetwarzania danych osobowych, nad którą administrator sprawuje bezpośrednią kontrolę w procesie przetwarzania danych realizowanym przez tę osobę.

Incydent – pojedyncze zdarzenie lub seria niepożądanych zdarzeń związanych z bezpieczeństwem, które stwarzają znaczne prawdopodobieństwo zakłócenia działań lub ujawnienia informacji poufnych. Definiowany jest również jako naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Sytuacja podejrzenia wystąpienia incydentu – pojedyncze zdarzenie lub seria niepożądanych zdarzeń związanych z bezpieczeństwem, które stwarzają znaczne prawdopodobieństwo zakłócenia działań lub ujawnienia informacji poufnych.

Hasło – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;

Usługa kluczowa – usługa, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej.

Przetwarzanie danych osobowych - jakiegokolwiek operacje lub zestaw operacji wykonywanych na danych osobowych.

Audyt - działania mające na celu oceny danej osoby, Jednostki, systemu, procesu, zabezpieczenia mające na celu potwierdzenie spełnienia konkretnych wymagań.

Analiza ryzyka - systematyczne wykorzystanie informacji do zidentyfikowania źródeł i oszacowania ryzyka.

<i>Urząd Gminy Jasło</i>	<i>Polityka Bezpieczeństwa Informacji</i>	<i>Strona</i>	5
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

ROZDZIAŁ I

CEL I ZAKRES POLITYKI BEZPIECZEŃSTWA INFORMACJI

Polityka została wprowadzona w celu zapewnienia właściwego poziomu bezpieczeństwa zasobów informacyjnych jednostki oraz ustanowienie Systemu Zarządzania Bezpieczeństwem Informacji według międzynarodowego standardu PN-EN ISO/IEC 27001:2017 z zachowaniem spójności z normą PN-EN ISO 9001:2015.

Główne cele systemu zarządzania bezpieczeństwem informacji to:

- zapewnienie dostępności do Informacji osobom upoważnionym;
- zabezpieczenie informacji, dokumentów, systemów przetwarzających informacje przed nieautoryzowanym dostępem, modyfikacją lub zniszczeniem;
- minimalizowanie ryzyka utraty informacji;
- zaangażowanie wszystkich pracowników w ochronę informacji;
- zwiększanie świadomości pracowników;
- monitorowanie korzystania z danych osobowych oraz medycznych na wszystkich etapach ich przetwarzania przed nieautoryzowanym dostępem, zmianą, kopiowaniem, zniszczeniem;
- zapewnienie zgodności z prawem obowiązującym na terytorium UE w zakresie ochrony danych osobowych oraz zgodności z umowami.

System Zarządzania Bezpieczeństwem Informacji obejmuje swoim zakresem:

1. Wszystkie realizowane procesy oraz zadania w ramach działania jednostki.
2. Wszystkie informacje przetwarzane przez jednostkę w ramach wykonywania działań wynikających z jej działalności, w tym:
 - a) Informacje przetwarzane w formie tradycyjnej – papierowej;
 - b) Informacje przetwarzane w formie elektronicznej;
 - c) Informacje przetwarzane w formie ustnej – wypowiedane słownie;
 - d) Inne informacje będące własnością Jednostki lub przekazane jej przez kontrahentów w ramach realizacji obowiązujących umów.
3. Wszystkie Zasoby będące własnością Jednostki lub przekazane jej przez kontrahentów w ramach realizacji obowiązujących umów, w tym:
 - a) Personel;
 - b) Budynki i pomieszczenia;
 - c) Sprzęt;
 - d) Systemy, oprogramowanie i technologie pozwalające na przetwarzanie informacji.

<i>Urząd Gminy Jasło</i>	<i>Polityka Bezpieczeństwa Informacji</i>	<i>Strona</i>	6
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

ROZDZIAŁ II

ROLE I ODPOWIEDZIALNOŚCI W ZAKRESIE SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

Zarządzanie Systemem Bezpieczeństwem Informacji w Jednostce zapewnia struktura organizacyjna, w której skład wchodzi:

1. Kierownik Jednostki;
2. Sekretarz Gminy
3. Inspektor Ochrony Danych;
4. Biuro Zarządzania Kryzysowego
5. Referat Funduszy Zewnętrznych i Kontroli
6. Administrator Systemów Informatycznych;
7. Kierujący komórkami organizacyjnymi Jednostki;
8. Pozostały personel Jednostki

KIEROWNIK JEDNOSTKI

- 1) zapewnia zasoby niezbędne do prawidłowego funkcjonowania SZBI;
- 2) podejmuje strategiczne decyzje w procesie zarządzania bezpieczeństwem informacji;
- 3) wyznacza Inspektora Ochrony Danych;
- 4) zatwierdza dokumentację SZBI oraz jej zmiany;
- 5) kieruje i wspiera osoby przyczyniające się do osiągnięcia skuteczności SZBI;
- 6) promuje ciągłe doskonalenie SZBI.

SEKRETARZ GMINY

- 1) odpowiada za zapewnienie zgodności SZBI z właściwymi wymaganiami, w szczególności z wymaganiami norm: PN-EN ISO/IEC 27001 i PN-ISO/IEC 22301;
- 2) inicjuje oraz nadzoruje działania wdrożeniowe, korygujące i zapobiegawcze w zakresie bezpieczeństwa informacji;
- 3) koordynuje proces zarządzania ryzykiem bezpieczeństwa informacji;
- 4) nadzoruje opracowanie, przeglądy i aktualizacje dokumentacji SZBI;
- 5) opracowuje i przeprowadza szkolenia z zakresu SZBI;
- 6) nadzoruje proces zarządzania incydentami bezpieczeństwa;
- 7) nadzoruje lub prowadzi audyty SZBI oraz okresowy przegląd SZBI;
- 8) prowadzi rejestr aktywów;
- 9) wydaje opinie, zalecenia oraz rekomendacje w zakresie związanym z funkcjonowaniem SZBI;
- 10) odpowiada za utrzymywanie kontaktów z grupami zainteresowanych specjalistów lub innymi specjalistycznymi forami oraz stowarzyszeniami zawodowymi z obszaru Bezpieczeństwa informacji;
- 11) podejmuje działania w pozostałych kwestiach związanych z bezpieczeństwem informacji, w zakresie niezastrzeżonym do kompetencji innych osób.

<i>Urząd Gminy Jasło</i>	<i>Polityka Bezpieczeństwa Informacji</i>	<i>Strona</i>	7
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

SAMODZIELNE STANOWISKO DS. ZARZĄDZANIA KRYZYSOWEGO

- 1) odpowiada za wdrożenie oraz utrzymanie zabezpieczeń fizycznych jednostki;
- 2) odpowiada za zapewnienie zgodności z wymaganiami i przyjętymi zabezpieczeniami.

SAMODZIELNE STANOWISKO DS. FUNDUSZY ZEWNĘTRZNYCH I KONTROLI

- 1) prowadzenie klasyfikacji Zasobów jednostki;
- 2) prowadzenie klasyfikacji Zagrożeń jednostki;
- 3) prowadzenie procesu Analizy ryzyka;
- 4) opracowywanie Planu Postępowania z Ryzykiem.

INSPEKTOR OCHRONY DANYCH

- 1) odpowiada za monitorowanie i zapewnienie przestrzegania przepisów o ochronie danych osobowych w Jednostce;
- 2) odpowiada za realizację szkoleń z zakresu ochrony danych osobowych skierowanych do całego personelu Jednostki.

ADMINISTRATOR SYSTEMÓW INFORMATYCZNYCH

- 1) odpowiada za zarządzanie systemem teleinformatycznym Jednostki.
- 2) reprezentuje jednostkę przed organami Krajowego Systemu Cyberbezpieczeństwa;
- 3) zgłasza incydenty do podmiotów KSC.
- 4) identyfikowanie zagrożeń w odniesieniu do systemów informacyjnych Urzędu oraz proponowanie rozwiązań ograniczających ryzyko wynikające z tych zagrożeń;
- 5) analizowanie oprogramowania szkodliwego i określanie jego wpływu na system informacyjny Urzędu;
- 6) wykrywanie przełamania lub ominięcia zabezpieczeń systemu informacyjnego Urzędu, prowadzenie analizy po włamaniowej wraz z określeniem działań niezbędnych do przywrócenia sprawności systemu informacyjnego Urzędu;
- 7) zabezpieczanie informacji potrzebnych do analizy po włamaniowej, pozwalających na określenie wpływu incydentu poważnego na świadczenie usługi kluczowej.

<i>Urząd Gminy Jasło</i>	<i>Polityka Bezpieczeństwa Informacji</i>	<i>Strona</i>	8
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

KIERUJĄCY KOMÓRKAMI ORGANIZACYJNYMI JEDNOSTKI

- 1) nadzorują realizację obowiązków wynikających z SZBI przez podległy im personel;
- 2) identyfikują aktywa oraz dokonują oceny ich krytyczności oraz klasyfikacji;
- 3) dokonują oceny ryzyka bezpieczeństwa informacji w podlegających im obszarach;
- 4) współpracują z Pełnomocnikiem ds. SZBI, Inspektorem Ochrony Danych oraz Administratorem Systemu, w ramach realizowanych przez nich zadań;
- 5) zarządzają ciągłością działania w podlegających im obszarach.

PERSONEL JEDNOSTKI

- 1) realizuje obowiązki wynikające z SZBI w zakresie powierzonych im zadań;
- 2) informuje niezwłocznie o wszystkich zdarzeniach mających wpływ na ryzyko bezpieczeństwa informacji, w tym w szczególności o incydentach bezpieczeństwa;
- 3) współpracuje z Sekretarzem Gminy, Inspektorem Ochrony Danych oraz Administratorem Systemu Informatycznego w ramach realizowanych przez nich zadań;
- 4) odbywa obowiązkowe szkolenia z zakresu SZBI;
- 5) odbywa obowiązkowe szkolenia z zakresu RODO.

<i>Urząd Gminy Jasło</i>	<i>Polityka Bezpieczeństwa Informacji</i>	<i>Strona</i>	9
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

ROZDZIAŁ III

ZARZĄDZANIE AKTYWAMI INFORMACYJNYMI

W celu zapewnienia adekwatnego poziomu bezpieczeństwa aktywów informacyjnych, przedmiotowe aktywa są inwentaryzowane, klasyfikowane i zarządzane zgodnie z obowiązującymi wymaganiami w zakresie ich ochrony. Szczegółowe zasady dotyczące identyfikowania, klasyfikowania, postępowania z aktywami oraz odpowiedzialności za aktywa informacyjne zostały uregulowane w załączniku do niniejszej polityki – załącznik nr 1 - **Procedura zarządzania aktywami informacyjnymi**.

ROZDZIAŁ IV

KONTROLA DOSTĘPU DO INFORMACJI

W ramach zapewnienia ograniczonego dostępu do aktywów informacyjnych Jednostki, w tym do budynków i pomieszczeń, sprzętu i urządzeń oraz systemów informatycznych tylko dla osób i podmiotów uprawnionych, prowadzona jest kontrola dostępu fizycznego i logicznego. Szczegółowe zasady zarządzania dostępem do aktywów informacyjnych Jednostki zostały uregulowane w **SZBI-004 Polityka Bezpieczeństwa Fizycznego i Środowiskowego**.

ROZDZIAŁ V

ZARZĄDZANIE RYZYKIEM W BEZPIECZEŃSTWIE INFORMACJI

Działania związane z zarządzaniem ryzykiem mającym wpływ na bezpieczeństwo informacji obejmują:

- 1) przygotowanie oraz okresową aktualizację dokumentów dot. zarządzania ryzykiem;
- 2) prowadzenie okresowego szacowania ryzyka;
- 3) postępowanie z ryzykiem;
- 4) podejmowanie działań korygujących.

Szczegółowe zasady dot. zarządzania ryzykiem w bezpieczeństwie informacji zostały uregulowane w **SZBI-006 Polityka Zarządzania Ryzykiem**.

<i>Urząd Gminy Jasło</i>	<i>Polityka Bezpieczeństwa Informacji</i>	<i>Strona</i>	10
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

ROZDZIAŁ VI

BEZPIECZEŃSTWO TELEINFORMATYCZNE

W ramach zarządzania bezpieczeństwem teleinformatycznym podejmowane są działania w zakresie szacowania i kontroli ryzyka utraty poufności, integralności, dostępności informacji w związku z korzystaniem z elektronicznej dokumentacji medycznej oraz aplikacji, komputerów i urządzeń mobilnych, sieci komputerowych i transmisji danych. Szczegółowe zasady i wymogi w zakresie bezpieczeństwa teleinformatycznego zostały uregulowane w **SZBI-008 Instrukcja Zarządzania Systemem Informatycznym**.

ROZDZIAŁ VII

BEZPIECZEŃSTWO FIZYCZNE I ŚRODOWISKOWE

W celu zapobieżenia nieuprawnionemu fizycznemu dostępowi, szkodom i zakłóceniom w przetwarzaniu informacji i środkach przetwarzania informacji oraz utracie, zniszczeniu, uszkodzeniu, kradzieży aktywów informacyjnych Jednostki stosowane są mechanizmy ochrony w obszarze bezpieczeństwa fizycznego i środowiskowego. Szczegółowe zasady dot. zarządzania bezpieczeństwem fizycznym i środowiskowym zostały uregulowane w **SZBI-004 Polityka Bezpieczeństwa Fizycznego i Środowiskowego**.

ROZDZIAŁ VIII

BEZPIECZEŃSTWO ZASOBÓW LUDZKICH

Celem ograniczenia ryzyka błędu ludzkiego, kradzieży lub nadużycia oraz zapewnienia, że personel Urzędu, oraz inne osoby lub podmioty wykonujące czynności w imieniu i na rzecz Jednostki lub mające dostęp do aktywów informacyjnych Jednostki są świadomi odpowiedzialności i swoich obowiązków dotyczących bezpieczeństwa informacji oraz wypełniają je w odpowiedni sposób i z uwzględnieniem interesów Jednostki, podejmowane są określone działania w obszarze bezpieczeństwa zasobów ludzkich, w szczególności:

- 1) zapewnienie wykwalifikowanych pracowników lub innych osób oraz podmiotów zewnętrznych do realizacji zadań;
- 2) uwzględnienie odpowiednich zapisów dotyczących odpowiedzialności w zakresie bezpieczeństwa informacji w umowach zawieranych z ww. osobami i podmiotami;
- 3) szkolenie ww. osób i podmiotów w zakresie bezpieczeństwa informacji oraz regularne informowanie o aktualizacji polityk i procedur związanych z ich stanowiskiem pracy.

<i>Urząd Gminy Jasło</i>	<i>Polityka Bezpieczeństwa Informacji</i>	<i>Strona</i>	11
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

ROZDZIAŁ IX

ZAPEWNIENIE CIĄGŁOŚCI DZIAŁANIA

W Jednostce podejmowane są działania w zakresie planowania, weryfikowania, zapewnienia, przeglądu i oceny ciągłości działania i postępowania w przypadku wystąpienia sytuacji kryzysowych. Szczegółowe zasady dot. zarządzania ciągłością działania zostały uregulowane **SZBI-003 Polityka Ciągłości Działania**.

ROZDZIAŁ X

RELACJE Z PODMIOTAMI ZEWNĘTRZNYMI

Celem zapewnienia ochrony aktywów informacyjnych udostępnianych usługodawcom, dostawcom i innym osobom lub podmiotom zewnętrznym wykonującym czynności w imieniu i na rzecz Urzędu lub mającym dostęp do aktywów Urzędu, wprowadza się zasady postępowania w przypadku współpracy związanej z dostępem do aktywów informacyjnych Urzędu i korzystania z usług ww. osób i podmiotów.

W przypadku wykonywania zadań delegowanych lub korzystania z aktywów, w tym przetwarzania informacji powierzonych przez podmioty zewnętrzne w drodze stosownej umowy lub porozumienia, poza wymogami określonymi w obowiązującej w Urzędzie dokumentacji bezpieczeństwa dopuszcza się stosowanie wymogów i zaleceń bezpieczeństwa określonych przez ww. podmioty zewnętrzne, o ile wskazane wymogi i zalecenia zewnętrzne nie obniżają poziomu bezpieczeństwa pozostałych informacji przetwarzanych w Urzędzie. Przedmiotowe zasady i wymogi współpracy zostały uregulowane w **SZBI-009 Polityka bezpieczeństwa w relacjach z dostawcami**.

<i>Urząd Gminy Jasło</i>	<i>Polityka Bezpieczeństwa Informacji</i>	<i>Strona</i>	12
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

ROZDZIAŁ XI

PROCEDURA ZARZĄDZANIA PROJEKTAMI

1. Planowanie projektu

- a) wybór kierownika projektu i zespołu projektowego;
- b) określenie celów projektu i wymagań klienta;
- c) opracowanie planu projektu zawierającego harmonogram, budżet, zasoby oraz ryzyka związane z projektem;
- d) przygotowanie dokumentacji projektowej;
- e) ocena ryzyka związanego z projektem.

2. Realizacja projektu

- a) określenie zasobów niezbędnych do wykonania planu;
- b) monitorowanie postępu prac i harmonogramu;
- c) przydzielenie zadań członkom zespołu;
- d) rozwiązywanie problemów i eliminowanie przeszkód;
- e) zapewnienie, że zespół projektowy pracuje zgodnie z harmonogramem i planem projektu;
- f) dokładna dokumentacja przebiegu projektu.

3. Kontrola projektu

- a) ocenianie postępu prac i harmonogramu;
- b) identyfikacja i zarządzanie ryzykiem;
- c) monitorowanie jakości projektu;
- d) zarządzanie zasobami ludzkimi;
- e) kontrola terminów przygotowania i wykonania projektu;
- f) kontrola zużycia zasobów w trakcie przygotowania i wykonawstwa projektów;
- g) kontrola jakości projektu;
- h) kontrola pracy zespołu projektu;
- i) ocena wyników i reagowanie;
- j) dokładna dokumentacja przebiegu projektu.

4. Zakończenie projektu

- a) rozliczenie projektu;
- b) opracowanie raportu z realizacji projektu;
- c) podjęcie decyzji o zakończeniu;
- d) zakończenie projektu i zwolnienie zespołu projektowego.

<i>Urząd Gminy Jasło</i>	<i>Polityka Bezpieczeństwa Informacji</i>	<i>Strona</i>	13
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

ROZDZIAŁ XII

PODSTAWOWE ZASADY BEZPIECZEŃSTWA

- Skuteczna ochrona zasobów Jednostki wymaga wspólnego działania i zaangażowania wszystkich pracowników.
- W sytuacjach kryzysowych, ujawnienie informacji wrażliwych uznawane jest, jako zagrożenie mniejsze od zniszczenia tych informacji. Nie dotyczy to informacji niejawnych w rozumieniu ustawy o ochronie informacji niejawnych.
- Pracownicy Urzędu zobowiązani są do używania zasobów Jednostki wyłącznie do celów służbowych. W związku z tym wszyscy użytkownicy zasobów podlegają monitoringowi zgodnie z niniejszą Polityką.
- W celu zapewnienia bezpieczeństwa zasobów informacyjnych Jednostki stosuje się następujące ogólne zasady ochrony informacji:
 - Zasada znajomości wymagań polityki bezpieczeństwa informacji**
Każdy pracownik musi zostać zapoznany z aktualnymi procedurami ochrony informacji obowiązujących w Urzędzie;
 - Zasada uprawnionego dostępu**
Każdy pracownik stosuje się do obowiązujących zasad ochrony informacji i spełnia kryteria dopuszczenia do informacji;
 - Zasada przywilejów koniecznych**
Każdy pracownik posiada prawa dostępu do informacji, ograniczone wyłącznie do tych, które są konieczne do wykonywania powierzonych mu zadań;
 - Zasada wiedzy koniecznej**
Każdy pracownik posiada wiedzy o systemie do którego ma dostęp, ograniczoną wyłącznie do zagadnień, które są konieczne do realizacji powierzonych mu zadań;
 - Zasada usług koniecznych**
Systemy informacyjne świadczą tylko takie usługi, które są konieczne do realizacji zadań biznesowych i operacyjnych;
 - Zasada asekuracji**
Każdy mechanizm zabezpieczający musi być ubezpieczony drugim (podobnym). W przypadkach szczególnych może być stosowane dodatkowe (trzecie) niezależne zabezpieczenie. Jako mechanizmy zabezpieczeń dopuszczalne jest stosowanie zabezpieczeń technicznych jak i organizacyjnych;
 - Zasada wyłączności**
Za konfigurowanie systemów bezpieczeństwa informacji nie może być odpowiedzialna osoba, która jednocześnie odpowiedzialna jest za kontrolę ich funkcjonowania;
 - Zasada świadomości zbiorowej**
Wszyscy pracownicy są świadomi konieczności ochrony zasobów informacyjnych i aktywnie uczestniczą w tym procesie;
 - Zasada rozliczalności / indywidualnej odpowiedzialności**
Za bezpieczeństwo poszczególnych elementów odpowiadają- poszczególne osoby;

<i>Urząd Gminy Jasło</i>	<i>Polityka Bezpieczeństwa Informacji</i>	<i>Strona</i>	14
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

- **Zasada obecności koniecznej**
Prawo przebywania w określonych miejscach mają tylko osoby do tego upoważnione;
- **Zasada stałej gotowości**
System jest zabezpieczony na wypadek wystąpienia zagrożeń. Niedopuszczalne jest tymczasowe wyłączanie mechanizmów zabezpieczających;
- **Zasada najłagodniejszego ognia**
Poziom bezpieczeństwa wyznacza najłagodniejszy (najmniej zabezpieczony) element. Elementy takie są wyznaczane w oparciu o wyniki analizy ryzyka;
- **Zasada kompletności**
Skuteczne zabezpieczenie jest tylko wtedy, gdy stosuje się podejście kompleksowe, uwzględniające wszystkie stopnie i ognia ogólnie pojętego procesu przetwarzania informacji;
- **Zasada ewolucji**
Každy system musi ciągle dostosowywać mechanizmy wewnętrzne do zmieniających się warunków zewnętrznych;
- **Zasada odpowiedniości**
Używane mechanizmy muszą być adekwatne do sytuacji;
- **Zasada akceptowanej równowagi**
Podejmowane środki zaradcze nie mogą przekraczać poziomu akceptacji;
- **Zasada świadomej konwersacji**
Nie zawsze i wszędzie trzeba mówić, co się wie, ale zawsze i wszędzie trzeba wiedzieć co, gdzie i do kogo się mówi.

<i>Urząd Gminy Jasło</i>	<i>Polityka Bezpieczeństwa Informacji</i>	<i>Strona</i>	15
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

ROZDZIAŁ XIII NARUSZENIE BEZPIECZEŃSTWA INFORMACJI

1. Podstawową konsekwencją naruszenia bezpieczeństwa informacji jest obniżenie poziomu ochrony przetwarzanych informacji i aktywów wspierających ich przetwarzanie w Jednostce.
2. Każdy, kto posiada dostęp do informacji i aktywów wspierających ich przetwarzanie w Jednostce ma obowiązek informowania podmiotów odpowiedzialnych za bezpieczeństwo przetwarzania informacji w Urzędzie o podejrzeniu lub każdym zidentyfikowanym przypadku naruszenia bezpieczeństwa informacji.
3. Nieprzestrzeganie zasad zawartych w dokumentacji bezpieczeństwa stanowi naruszenie obowiązków pracowniczych i może skutkować pociągnięciem personelu Urzędu do odpowiedzialności dyscyplinarnej.
4. Naruszenie postanowień niniejszej Polityki przez kontrahenta Urzędu lub jego pracowników stanowi podstawę do odstąpienia od umowy i żądania pokrycia powstałej szkody lub zapłaty kary umownej, jeżeli taki obowiązek wynika z zawartej umowy.
5. Z tytułu działań personelu lub kontrahentów Urzędu lub innych osób i podmiotów niezgodnych z przepisami prawa powszechnie obowiązującego (w szczególności dot. przetwarzania danych osobowych), grożą odrębne kary określone w szczególności w:
 - a) kodeksie pracy;
 - b) kodeksie cywilnym;
 - c) kodeksie karnym;
 - d) ustawie o ochronie danych osobowych.
6. W celu uzyskania możliwie pełnej informacji o naruszeniu bądź też podejrzeniu naruszenia bezpieczeństwa informacji w Urzędzie, osoby bądź podmioty niezwiązane z Urzędem mogą zgłaszać przypadki bądź podejrzenie naruszenia bezpieczeństwa aktywów informacyjnych Urzędu na adres: **gmina@gminajaslo.pl**
7. Szczegółowe zasady dot. identyfikowania, zgłaszania, reagowania i obsługi zdarzeń i incydentów związanych z bezpieczeństwem informacji zostały uregulowane w **SZBI-005 Polityka Zarządzania Incydentami**.

<i>Urząd Gminy Jasło</i>	<i>Polityka Bezpieczeństwa Informacji</i>	<i>Strona</i>	16
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

ROZDZIAŁ XIV ZGODNOŚĆ Z PRZEPISAMI PRAWA I ZAPISAMI UMOWNYMI

1. W celu uniknięcia naruszenia obowiązujących przepisów prawa, zobowiązań ustawowych, zapisów zawartych umów i porozumień, w Urzędzie prowadzona jest bieżąca kontrola zgodności regulacji wewnętrznych, przyjętych zasad bezpieczeństwa i ich stosowania z ww. przepisami, w tym identyfikowanie, dokumentowanie i aktualizowanie wszystkich istotnych wymagań prawnych, regulacyjnych, umownych oraz podejścia organizacji do ich przestrzegania.
2. Przedmiotowa kontrola dotyczy również zgodności z wymaganiami prawnymi, regulacyjnymi i umownymi, związanymi z prawami własności intelektualnej i użytkowaniem prawnie zastrzeżonego oprogramowania
3. Kierownicy komórek organizacyjnych, w zakresie zadań realizowanych zgodnie z Regulaminem Organizacyjnym prowadzą bieżący nadzór w swoich komórkach w zakresie zgodności z przepisami prawa i zapisami umownymi.
4. Inspektor Ochrony Danych w Urzędzie odpowiedzialny jest za zapewnienia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, w szczególności RODO.
5. Sekretarz Gminy, we współpracy z kierownikami poszczególnych komórek organizacyjnych Urzędu dokonuje okresowych przeglądów regulacji wewnętrznych dotyczących bezpieczeństwa informacji w zakresie ich zgodności z przepisami prawa i zapisami umownymi.
6. Urząd Gminy zapewnia okresowy audyt w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

<i>Urząd Gminy Jasło</i>	<i>Polityka Bezpieczeństwa Informacji</i>	<i>Strona</i>	17
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

ROZDZIAŁ XV DEKLARACJA KIEROWNICTWA

Wójt – kierownik jednostki ma świadomość wagi informacji przetwarzanych w organizacji. Jednostka dokłada wszelkich starań aby zapewnić należyty poziom ochrony informacji.

System Zarządzania Bezpieczeństwem Informacji (SZBI) został oparty na:

- Standardzie PN-EN ISO/IEC 27001:2017;
- Ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych;
- Rozporządzeniu 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;
- Ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;
- Rozporządzeniu Rady Ministrów z dnia 21 maja 2014 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

Niniejszym Jednostka zobowiązuje wszystkich pracowników do przestrzegania zawartych w polityce bezpieczeństwa zasad. Jednocześnie kierownictwo jednostki zobowiązuje się wspierać pracowników w zapewnianiu środków i zasobów koniecznych do utrzymania bezpieczeństwa na wymaganym poziomie.

Kierownictwo jednostki deklaruje zapewnienie niezbędnych środków dla utrzymania i rozwoju Systemu Zarządzania Bezpieczeństwem Informacji.

Szczegółowy opis przyjętych zabezpieczeń został opisany w załączniku do niniejszego dokumentu – załącznik nr 2 - **Deklaracja Stosowania**.

Urząd Gminy Jasło	Procedura zarządzania aktywami informacyjnymi	Strona	1
		Wydanie	I
		Data wydania	2026.03.16

PROCEDURA ZARZĄDZANIA AKTYWAMI INFORMACYJNYMI w Urzędzie Gminy Jasło

ZATWIERDZAM

W O T

Wojciech Pinkoś
(Podpis, pieczęć i data)

<i>Urząd Gminy Jasło</i>	<i>Procedura zarządzania aktywami informacyjnymi</i>	<i>Strona</i>	1
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

PROCEDURA
ZARZĄDZANIA AKTYWAMI
INFORMACYJNYMI
w Urzędzie Gminy Jasło

ZATWIERDZAM

(Podpis/pieczątka i data)

Urząd Gminy Jasło	Procedura zarządzania aktywami informacyjnymi	Strona	3
		Wydanie	I
		Data wydania	2026.03.16

WŁASNOŚĆ AKTYWÓW

1. Za każde z aktywów statystyki publicznej odpowiada kierownictwo Jednostki, poza przypadkami, w których aktywa zostały przypisane wyznaczonym pracownikom komórek organizacyjnych Jednostki. Wyjątek stanowią także aktywa będące składnikami sieci teleinformatycznej Urzędu, za które odpowiedzialny jest Informatyk.
2. W przypadku rozwiązania stosunku pracy z pracownikiem, wszystkie przedmioty wydane pracownikowi takie jak np.: urządzenia teleinformatyczne, klucze, identyfikator osobisty, oprogramowanie, dokumenty i instrukcje muszą być zwrócone przełożonemu lub odpowiedniej komórce organizacyjnej Jednostki najpóźniej w ostatnim dniu świadczenia przez niego pracy na rzecz Urzędu.

ZASADY OCHRONY AKTYWÓW INFORMACYJNYCH

1. Poniższe zasady wprowadzone są w celu ograniczenia ryzyka płynącego z zagrożeń do akceptowalnego poziomu, co oznacza zminimalizowanie możliwości naruszenia bezpieczeństwa aktywów informacyjnych Jednostki, umożliwienie wczesnego wykrycia takiego naruszenia, zminimalizowanie strat związanych z takim naruszeniem oraz sprawne usunięcie jego skutków.
2. Skuteczna ochrona zasobów Jednostki wymaga wspólnego działania, współpracy i zaangażowania wszystkich jej pracowników.
3. W sytuacjach kryzysowych ujawnienie informacji poufnych uznawane jest jako mniejsze zagrożenie od zniszczenia, utraty lub ujawnienia tych informacji. Nie dotyczy to informacji niejawnych w rozumieniu ustawy o ochronie informacji niejawnych.
4. Obowiązek ochrony informacji w przypadku współpracy z kontrahentami i jednostkami zewnętrznymi określany jest w ramach umów zawartych z tymi podmiotami.
5. W celu zapewnienia bezpieczeństwa aktywów informacyjnych w Jednostce stosuje się następujące ogólne zasady:
 - 1) **Zasada przywilejów koniecznych** - każdy pracownik posiada prawa dostępu do zasobów ograniczone wyłącznie do tych, które nie są konieczne do wykonywania powierzonych mu obowiązków;
 - 2) **Zasada wiedzy koniecznej** - pracownikom przekazuje się wiedzę o zasobach ograniczoną wyłącznie do zagadnień, które są konieczne do realizacji powierzonych im zadań.
 - 3) **Zasada asekuracji zabezpieczeń** - ochrona informacji powinna opierać się na co najmniej dwóch mechanizmach zabezpieczenia dla zagrożeń niosących największe ryzyko.
 - 4) **Zasada rozliczalności** – kierownictwo Urzędu dąży do zapewnienia jednoznacznej odpowiedzialności pracowników za powierzone im zasoby oraz za przetwarzane przez nich informacje. Wszyscy użytkownicy zasobów informacyjnych ponoszą odpowiedzialność za:
 - a) realizowane czyny;
 - b) za konsekwencje zaniedbanie swoich obowiązków;

Urząd Gminy Jasło	Procedura zarządzania aktywami informacyjnymi	Strona	4
		Wydanie	I
		Data wydania	2026.03.16

- c) za konsekwencje nieuprawnionego przekazania swoich przywilejów innym osobom;
- d) elektroniczne dokumentowanie tych czynności w rozsądnym zakresie przez korzystanie w tym celu z możliwości systemu teleinformatycznego.

INWENTARYZACJA AKTYWÓW

1. Aktywa związane z informacjami i środkami przetwarzania informacji będące własnością Jednostki lub przez nią wykorzystywane są ewidencjonowane.
2. W spisie aktywów mogą się znaleźć następujące pozycje:
 - 1) Aktywa niematerialne:
 - a) informacje w formie cyfrowej;
 - b) informacje w innej (nie cyfrowej) formie;
 - c) oprogramowanie – kody wynikowe oraz licencje na wykorzystanie programów;
 - d) oprogramowanie – kody źródłowe wraz z licencjami i dokumentacją;
 - e) bazy i zbiory danych;
 - f) wzory dokumentów;
 - g) bazy wiedzy;
 - h) dokumentacje techniczne;
 - i) archiwa.
 - 2) Aktywa niematerialne związane z przetwarzaniem informacji:
 - a) serwery;
 - b) komputery obliczeniowe;
 - c) urządzenia sieciowe;
 - d) stacjonarne komputery osobiste;
 - e) komputery przenośne;
 - f) urządzenia peryferyjne.
 - 3) Zasoby ludzkie
3. Inwentaryzację należy przeprowadzić wykorzystując odpowiednio przygotowane arkusze spisowe:

Urząd Gminy Jasło	Procedura zarządzania aktywami informacyjnymi	Strona	5
		Wydanie	I
		Data wydania	2026.03.16

Numer inwentarzowy:	
Opis:	
Właściciel:	
Zarządzający:	
Użytkownicy:	
Lokalizacja:	
Klasyfikacja:	
Okres ważności:	
Sposób likwidacji:	
Kopia awaryjna (wykonywanie):	
Kopia awaryjna (przechowywanie):	
Wymagania:	
Dostępność:	
Integralność:	
Poufność:	

Sporządził	Dnia:
Zatwierdził:	Dnia:
Jednostka organizacyjna:	
Organizacja:	

<i>Urząd Gminy Jasło</i>	<i>Procedura zarządzania aktywami informacyjnymi</i>	<i>Strona</i>	6
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

KLASYFIKACJA AKTYWÓW

1. Wszystkie aktywa, będące własnością Urzędu lub przez Urząd wykorzystywane, podlegają identyfikacji i klasyfikacji.
2. Klasyfikowanie aktywów określa ich znaczenie dla Urzędu. Identyfikowanie zagrożeń wynikających z naruszenia bezpieczeństwa aktywów odbywa się podczas corocznego szacowania ryzyka w SZBI w formie tworzonego lub aktualizowanego katalogu aktywów.
3. Aktywa dzielimy na dwa rodzaje:
 - 1) Aktywa podstawowe, w skład których wchodzi m.in.:
 - procesy i działania operacyjne, które są realizowane w Urzędzie w celu wypełnienia zadań,
 - informacje – wszelkie aktywa informacyjne potrzebne do realizacji zadań Urzędu, w tym dokumenty w wersji papierowej i elektronicznej, w szczególności: bazy danych i pliki z danymi, kontrakty i umowy, dokumentacja bezpieczeństwa informacji (tzw. systemowa), podręczniki użytkownika, materiały szkoleniowe, dodatkowe (poza systemowe) procedury operacyjne i wspierające, dokumentacja dotycząca ciągłości działania, ślady audytowe, informacje zarchiwizowane.
 - 2) Aktywa wspierające, w skład których wchodzi m.in.:
 - zasoby ludzkie – podzbiór obejmuje wszystkich pracowników zaangażowanych w obsługę systemu informacyjnego, w tym także ich kwalifikacje, umiejętności i doświadczenie,
 - sprzęt – wszystkie fizyczne aktywa wspierające procesy i działania biznesowe, w tym m.in.: sprzęt teleinformatyczny służący do przetwarzania danych oraz nośniki danych,
 - oprogramowanie, obejmuje m.in.: programy, aplikacje, oprogramowanie systemowe i inne uczestniczące w operacjach przetwarzania danych,
 - sieć – obejmuje wszelkie urządzenia telekomunikacyjne i usługi używane do połączenia wielu fizycznie oddalonych komputerów lub elementów systemu informacyjnego, w tym media i usługi wspierające, przekaźniki aktywne i pasywne oraz interfejsy komunikacyjne, w szczególności: Internet, sieć teleinformatyczna, sieć energetyczna, urządzenia sieciowe,
 - siedziba - obejmuje wszystkie lokalizacje Urzędu oraz środki fizyczne potrzebne do ich funkcjonowania, w tym strefy chronione (administracyjne i bezpieczeństwa), podstawowe usługi, łączność, usługi komunalne i techniczne, w szczególności: pomieszczenia biurowe, serwerownie, klimatyzacje, wentylacje, instalacje alarmowe, ogrzewanie i monitoring,
 - organizacja i wartości niematerialne - opisuje strukturę organizacyjną, obejmującą wszystkie struktury ludzkie oraz wartości niematerialne, które mogą mieć na nie wpływ, m.in.: organy władzy, reputacja, wizerunek firmy i kultura organizacyjna.
4. Aktywa są wartościowane według następujących kryteriów:
 - 1) Ważność wysoka – przyznawana jest, gdy utrata lub naruszenie bezpieczeństwa aktywów powoduje przerwanie procesu, należą do nich m.in.:

Urząd Gminy Jasło	Procedura zarządzania aktywami informacyjnymi	<i>Strona</i>	7
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

- informacje nadzorowane, wrażliwe dla Urzędu w szczególności: informacje niejawnie dodatkowo podlegające ochronie w stopniu zgodnym z postanowieniami ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, dane osobowe dodatkowo podlegające ochronie w stopniu zgodnym z postanowieniami RODO, dane statystyczne podlegające ochronie na podstawie ustawy z dnia 29 czerwca 1995 r. o statystyce publicznej, dane finansowo – księgowe, inne informacje, których poufność określają obowiązujące przepisy prawa,
 - zasoby materialne, kluczowe niezbędne do realizowania statutowych celów Urzędu.
- 2) Ważność średnia – przyznawana jest, gdy utrata lub naruszenie bezpieczeństwa aktywów może mieć wpływ na prawidłową realizację procesu, należą do nich m.in.:
- pozostałe informacje nadzorowane, niewrażliwe (np. korespondencja wewnętrzna Urzędu),
 - zasoby materialne wartościowe, które są drogie lub trudno zastępowalne, ale od których nie zależy bezpośrednio funkcjonowanie Jednostki.
- 3) Ważność niska przyznawana jest, gdy utrata lub naruszenie bezpieczeństwa aktywów nie ma wpływu na funkcjonowanie procesu, należą do nich m.in.:
- informacje nienadzorowane i inne informacje publiczne,
 - zasoby materialne zwykłe, które są łatwo odtwarzalne lub zastępowalne i od których nie zależy bezpośrednio funkcjonowanie Jednostki.
5. Właściciel aktywu określa jego wartościowość.
6. Właściciela aktywu określa regulamin organizacyjny Urzędu, w innych przypadkach inne obowiązujące w Jednostce regulacje wewnętrzne lub przepisy prawa powszechnie obowiązującego.

<i>Urząd Gminy Jasło</i>	<i>Procedura zarządzania aktywami informacyjnymi</i>	<i>Strona</i>	8
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

POSTĘPOWANIE Z NOŚNIKAMI INFORMACJI

1. Nośniki informacji zawierające informacje wrażliwe dla Urzędu muszą być przechowywane w sposób uniemożliwiający dostęp do nich osobom nieuprawnionym.
2. Nośniki informacji zawierające kopie bezpieczeństwa i backup'y oraz informacje archiwalne w tym zakresie należy przechowywać w metalowych szafach o podwyższonym bezpieczeństwie przeciwpożarowym lub w sejfach. Pozostałe nośniki należy przechowywać i zabezpieczać zgodnie z wymaganiami obowiązującymi dla informacji na nich zapisanych.
3. Informacje mogą być przechowywane wyłącznie na takich nośnikach informacji, których trwałość zapisu przekracza wymagany przez regulacje wewnętrzne i przepisy prawa powszechnie obowiązującego okres przechowywania danej informacji.
4. Pracownicy do wypełniania obowiązków służbowych mogą korzystać tylko z autoryzowanych nośników informacji. Odstępstwo od tej zasady dopuszczalne jest wyłącznie w przypadku uruchomienia Planu Ciągłości Działania (wyjątek od zasady).
5. Niszczenie nośników informacji zawierających informacje wrażliwe dla Urzędu musi być rejestrowane.
6. W przypadku tymczasowego lub trwałego przekazywania osobom trzecim sprzętu komputerowego wszelkie wymienne nośniki danych powinny być usunięte. Jeśli jest to możliwe, również trwałe nośniki danych muszą być usunięte. Jeśli nie jest to możliwe, usunięte muszą być dane zawarte na trwałych nośnikach. Do ich usunięcia muszą zostać użyte narzędzia zapewniające trwały i bezpieczny charakter tej operacji na przykład wielokrotne zapisanie całego obszaru nośnika losowymi danymi.
7. Za usunięcie wszelkich danych dotyczących Jednostki przed przekazaniem sprzętu komputerowego osobom trzecim odpowiada Informatyk.
8. W przypadku nośników zawierających informacje niejawne należy stosować procedury określające postępowanie z informacjami niejawnymi.
9. Wycofane nośniki informacji, które były wykorzystywane do przetwarzania informacji wrażliwych dla pracodawcy, nie mogą być wynoszone poza siedzibę Jednostki, w której były użytkowane, bez wcześniejszego trwałego usunięcia danych.
10. W przypadku konieczności zniszczenia większych ilości zbędnej dokumentacji niearchiwalnej oraz innych nośników informacji, Kierownik Jednostki może podjąć decyzję o konieczności skorzystania z usług wyspecjalizowanych podmiotów gwarantujących zachowanie poufności danych.

Deklaracja stosowania w Urzędzie Gminy Jasło - wersja 1.0 z dnia 2026.03.16

nr	Cel zabezpieczenia	Zabezpieczenie	Stosuje się T/N	Uzasadnienie wyboru	Sposób spełnienia zabezpieczenia	Status
A.5 Polityki bezpieczeństwa informacji						
A.5.1 Kierunki bezpieczeństwa informacji określone przez kierownictwo Cel: Zapewnienie przez Dyrekcja wytycznych i wsparcia dla działań na rzecz bezpieczeństwa informacji, zgodnie z wymaganiami biznesowymi oraz właściwymi normami prawnymi i regulacjami.						
A.5.1.1	Dokument polityki bezpieczeństwa informacji	Zbiór polityk bezpieczeństwa informacji powinien być opracowany, zatwierdzony przez kierownictwo, opublikowany i zakomunikowany pracownikom i właściwym stronom zewnętrznym.	T	Na podstawie wyników szacowania ryzyka	Zbiór polityk bezpieczeństwa jest opracowany, zatwierdzony przez Kierownika oraz opublikowany i zakomunikowany pracownikom i właściwym stronom zewnętrznym.	Wdrożono skutecznie
A.5.1.2	Przegląd polityki bezpieczeństwa informacji	Polityki bezpieczeństwa informacji należy poddawać przeglądom w zaplanowanych odstępach czasu lub wtedy, gdy wystąpią istotne zmiany, aby zapewnić, że nadal są właściwe, adekwatne i skuteczne.	T	Na podstawie wyników szacowania ryzyka	Polityki bezpieczeństwa informacji są poddawane przeglądowi podczas przeglądu zarządzania lub wtedy, gdy wystąpią istotne zmiany.	Wdrożono skutecznie
A.6 Organizacja bezpieczeństwa informacji						
A.6.1 Organizacja wewnętrzna Cel: Ustanowić strukturę zarządzania w celu zainicjowania oraz nadzorowania wdrażania i eksploatacji bezpieczeństwa informacji w organizacji.						
A.6.1.1	Role i odpowiedzialność za bezpieczeństwo informacji	Odpowiedzialność za bezpieczeństwo informacji powinna być określona i przypisana.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Wszystkie odpowiedzialności związane z bezpieczeństwem informacji zostały określone i przydzielone i są wykonywane zgodnie z decyzją Kierownika.	Wdrożono skutecznie
A.6.1.2	Rozdzielanie obowiązków	Obowiązki i odpowiedzialności pozostające w konflikcie ze sobą należy rozdzielić, celem ograniczenia okazji do nieuprawnionej lub nieumyślnej modyfikacji lub nadużycia aktywów organizacji.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Kolidujące ze sobą obowiązki i obszary odpowiedzialności zostały podzielone w celu zredukowania możliwości nieuprawnionej lub przypadkowej modyfikacji lub nadużycia aktywów organizacji.	Wdrożono skutecznie
A.6.1.3	Kontakty z organami władzy	Należy utrzymywać stosowne kontakty z właściwymi organami władzy.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie zasady zgłaszania incydentów, ustanowione zasady kontaktowania się z odpowiednimi organami władzy.	Wdrożono skutecznie
A.6.1.4	Kontakty z grupami zainteresowanych specjalistów	Należy utrzymywać stosowne kontakty z grupami zainteresowanych specjalistów lub innymi specjalistycznymi forami oraz stowarzyszeniami zawodowymi z obszaru bezpieczeństwa.	N	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Odpowiednie kontakty z grupami specjalnych zainteresowań lub udział w innym seccjalistycznym forum i profesjonalnych stowarzyszeń powinien być utrzymywany.	Wdrożono skutecznie

A.6.1.5	Bezpieczeństwo informacji w zarządzaniu projektami	Bezpieczeństwo informacji należy uwzględnić w zarządzaniu projektami, niezależnie od rodzaju projektu.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Umowy z Wykonawcami którzy mają dostęp do ważnych informacji, baz danych Urzędu zawierają klauzulę o zachowaniu w poufności wszelkich informacji. W każdym realizowanym przez Urząd projekcie zwraca się szczególną uwagę na bezpieczeństwo informacji.	Wdrożono skutecznie
A.6.2 Urządzenia mobilne i telepraca Cel: Cel: Zapewnienie bezpieczeństwa dla telepracy oraz użytkowania urządzeń mobilnych.						
A.6.2.1	Polityka stosowania urządzeń mobilnych	Należy wprowadzić politykę oraz wspierającą ją zabezpieczenia w celu zarządzanie ryzykami, wynikającymi z użytkowania urządzeń mobilnych.	N	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Zabezpieczanie urządzeń mobilnych na podstawie uregulowań wewnętrznych.	Wdrożono skutecznie
A.6.2.2	Telepraca	Należy wdrożyć politykę oraz wspierającą ją zabezpieczenia w celu ochrony informacji pobieranych, przetwarzanych i przechowywanych w miejscach wykonywania telepracy.	N	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Polityka i odpowiednie środki bezpieczeństwa powinny być wdrożone do ochrony dostępu do informacji, przetwarzania lub przechowywania podczas wykonywania pracy na odległość.	Wdrożono skutecznie
A.7 Bezpieczeństwo zasobów ludzkich						
A.7.1 Przed zatrudnieniem Cel: Zapewnienie, że pracownicy, wykonawcy oraz użytkownicy reprezentujący stronę trzecią rozumieją swoje obowiązki, są odpowiedni do wyznaczonych im ról.						
A.7.1.1	Postępowanie sprawdzające	Historię wszystkich kandydatów do pracy należy zweryfikować zgodnie z odpowiednimi przepisami prawnymi, regulacjami i zasadami etycznymi oraz proporcjonalnie do wymagań biznesowych, klasyfikacji informacji, do których będzie potrzebny dostęp oraz dostrzeżonych ryzyk.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Przełożony każdego działu przeprowadza weryfikację wszystkich kandydatów do zatrudnienia zgodnie z procedurą zatrudniania i zwalniania pracowników. W Urzędzie przeprowadzane jest postępowanie sprawdzające.	Wdrożono skutecznie
A.7.1.2	Warunki zatrudnienia	Umowy z pracownikami i kontrahentami powinny określać odpowiedzialność stron w obszarze bezpieczeństwa informacji.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Umowy o pracę, umowy o poufności (jeśli przedmiot umowy tego wymaga) z podwykonawcami, umowy z Klientem, informowanie o PBI i wymaganiach związanych z bezpieczeństwem w Urzędzie. Przeglądy umów przez dział prawny i ich regularna aktualizacja.	Wdrożono skutecznie
A.7.2 Podczas zatrudnienia Cel: Zapewnienie, że pracownicy i kontrahenci są świadomi oraz wypełniają swoje obowiązki związane z bezpieczeństwem informacji.						
A.7.2.1	Odpowiedzialność kierownictwa	Kierownictwo powinno wymagać, aby wszyscy pracownicy i kontrahenci stosowali zasady bezpieczeństwa informacji zgodnie z obowiązującymi w organizacji politykami i procedurami	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Kierownictwo wymaga od wszystkich pracowników i kontrahentów stosowania zasad bezpieczeństwa zgodnie z wprowadzonymi w Urzędzie i politykami i procedurami.	Wdrożono skutecznie

A.7.2.2	Uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji	Wszyscy pracownicy organizacji oraz, w stosownych wypadkach, kontrahenci powinni przejść stosowne kształcenie i szkolenie uświadamiające oraz regularnie otrzymywać aktualizacje polityk i procedur związanych z ich stanowiskiem pracy.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Wszyscy pracownicy Urzędu i, tam, gdzie jest to wskazane, kontrahenci zostali odpowiednio przeszkoleni oraz są regularnie informowani o uaktualnieniach obowiązujących w organizacji polityk i procedur, które są związane z wykonywaną przez nich pracą.	Wdrożono skutecznie
A.7.2.3	Postępowanie dyscyplinarne	Postępowanie dyscyplinarne wobec pracowników naruszających zasady bezpieczeństwa informacji należy prowadzić na podstawie ustalonych i przedstawionych im zasad.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Kierownictwo wspiera proces postępowania dyscyplinarnego stosowanego wobec pracowników, którzy naruszyli bezpieczeństwo informacji.	Wdrożono skutecznie
A.7.3 Zakończenie lub zmiana zatrudnienia Cel: Ochrona interesów organizacji jako część procesu zmiany lub zakończenia zatrudnienia.						
A.7.3.1	Zakończenie zatrudnienia lub zmiana zakresu obowiązków	Należy określić i przedstawić pracownikowi lub kontrahentowi, które odpowiedzialności i obowiązki w zakresie bezpieczeństwa informacji pozostaną aktualne po zakończeniu lub zmianie zatrudnienia, a następnie egzekwować je.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Odpowiedzialności i obowiązki związane z bezpieczeństwem informacji obowiązujące po zakończeniu lub zmianie zatrudnienia, są jasno określone, zakomunikowane pracownikowi lub kontrahentowi i narzucone.	Wdrożono skutecznie
A.8 Zarządzanie aktywami						
A.8.1 Odpowiedzialność za aktywa Cel: Identyfikacja aktywów organizacji oraz określenie odpowiedzialności za ich ochronę.						
A.8.1.1	Inwentaryzacja aktywów	Należy zidentyfikować aktywa związane z informacjami i środkami przetwarzania informacji oraz sporządzić i utrzymywać ewidencję tych aktywów.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie W Urzędzie prowadzi się spisy aktywów.	Wdrożono skutecznie
A.8.1.2	Własność aktywów	Aktywa znajdujące się w ewidencji należy przypisać ich właścicielom.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Wszystkie aktywa w Urzędzie, które zostały zinwentaryzowane posiadają swojego właściciela.	Wdrożono skutecznie
A.8.1.3	Akceptowalne użycie aktywów	Należy zidentyfikować, udokumentować i wdrożyć zasady akceptowalnego użycia informacji oraz aktywów związanych z informacjami i środkami przetwarzania informacji.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Zasady dopuszczalnego korzystania z informacji oraz aktywów związanych z informacją oraz przetwarzaniem informacji zostały określone, udokumentowane i wdrożone.	Wdrożono skutecznie
A.8.1.4	Zwrot aktywów	Wszyscy pracownicy i użytkownicy podmiotów zewnętrznych, w momencie zakończenia zatrudnienia, umowy lub porozumienia, powinni zwrócić wszystkie posiadane aktywa organizacji.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Wszyscy pracownicy oraz użytkownicy podmiotów zewnętrznych są zobowiązani zwrócić wszystkie aktywa należące do organizacji a będące w ich posiadaniu, w momencie ustania zatrudnienia, umowy, porozumienia.	Wdrożono skutecznie

A.8.2 Klasyfikacja informacji Cel: Zapewnienie, że informacje uzyskują ochronę na odpowiednim poziomie, zgodnym z ich znaczeniem dla organizacji.						
A.8.2.1	Klasyfikacja informacji	Informacje powinny być klasyfikowane z uwzględnieniem wymagań prawnych, wartości, krytyczności i wrażliwości na nieuprawnione ujawnienie lub modyfikację.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Informacje w Urzędzie zostały sklasyfikowane z uwzględnieniem wymagań prawnych, ich wartości, krytyczności i wrażliwości na nieupoważnione ujawnienie lub modyfikację.	Wdrożono skutecznie
A.8.2.2	Oznaczanie informacji	Należy opracować i wdrożyć odpowiedni zbiór procedur oznaczania informacji, zgodnych z przyjętym w organizacji schematem klasyfikacji informacji.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie W Urzędzie funkcjonuje procedura oznaczania informacji zgodnie z przyjętym schematem klasyfikacji.	Wdrożono skutecznie
A.8.2.3	Postępowanie z aktywami	Należy opracować i wdrożyć procedury postępowania z aktywami, zgodnie z przyjętym przez organizację schematem klasyfikacji informacji.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Odpowiedni zbiór procedur postępowania z aktywami został opracowany i wdrożony zgodnie z przyjętym w organizacji schematem klasyfikacji.	Wdrożono skutecznie
A.8.3 Obsługa nośników Cel: Zapobiec nieuprawnionemu ujawnieniu, modyfikacji, usunięciu lub zniszczeniu informacji zapisanych na nośnikach.						
A.8.3.1	Zarządzanie nośnikami wymiennymi	Urząd powinien wdrożyć procedury zarządzania nośnikami wymiennymi, zgodne ze schematem klasyfikacji przyjętym w organizacji.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie W Urzędzie funkcjonuje instrukcja regulująca postępowanie z nośnikami wymiennymi zgodnie z przyjętym schematem klasyfikacji. Istnieją też inne dokumenty, które regulują sposób postępowania pracowników tak aby chronić przed nieuprawnionym dostępem do danych.	Wdrożono skutecznie
A.8.3.2	Wycofywanie nośników	Nośniki, które nie będą dłużej wykorzystywane, należy bezpiecznie wycofać, zgodnie z formalnymi procedurami.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Nośniki, które nie będą już dłużej wykorzystywane, są niszczone w sposób bezpieczny, zgodnie z procedurami.	Wdrożono skutecznie
A.8.3.3	Przekazywanie nośników	Nośniki zawierające informacje należy chronić przed nieuprawnionym dostępem, nadużyciem oraz utratą integralności podczas transportu.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Nośniki zawierające informacje są chronione przed nieautoryzowanym dostępem, niewłaściwym użyciem lub uszkodzeniem podczas transferu.	Wdrożono skutecznie
A.9 Kontrola dostępu						
A.9.1 Wymagania biznesowe wobec kontroli dostępu Cel: Ograniczenie dostępu do informacji i środków przetwarzania informacji.						

A.9.1.1	Polityka kontroli dostępu	Politykę kontroli dostępu należy ustanowić, udokumentować i poddawać przeglądom zgodnie z wymaganiami biznesowymi i wymaganiami bezpieczeństwa informacji.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie W Urzędzie funkcjonuje Polityka kontroli dostępu i jest poddawana regularnym przeglądom. Dostęp do aktywów w postaci informacji jest uregulowany również poprzez nadanie praw dostępu do poszczególnych aktywów osobom, dla których dostęp do nich jest niezbędny i narzucony przez ich zakres obowiązków.	Wdrożono skutecznie
A.9.1.2	Dostęp do sieci i usług sieciowych	Użytkownicy powinni mieć dostęp wyłącznie do tych sieci i usług sieciowych, do których otrzymali wyraźne uprawnienia.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie W Urzędzie wszyscy użytkownicy posiadają dostęp do sieci i do usług sieciowych tylko w takim zakresie, w jakim zostali autoryzowani. Każdy pracownik jest świadomy, że nie wolno mu podpinać się do sieci wewnętrznej z prywatnym sprzętem zgodnie z wewnętrznymi uregulowaniami.	Wdrożono skutecznie
A.9.2 Zarządzanie dostępem użytkowników Cel: Zapewnienie dostęp uprawnionym użytkownikom i zapobieganie nieuprawnionemu dostępowi do systemów i usług.						
A.9.2.1	Rejestracja i wyrejestrowywanie użytkowników	W celu umożliwienia przydzielania praw dostępu należy wdrożyć formalny proces rejestrowania i wyrejestrowywania użytkowników.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie W Urzędzie przydzielone są uprawnienia dla pracowników do systemów i usług zgodnie z zakresem wykonywanej pracy. Każdy z użytkowników ma obowiązek logować się i wylogowywać każdorazowo kiedy nie pracuje w systemie. Wszyscy pracownicy mając dostęp do systemów operacyjnych na swoich komputerach i wiedzą o polityce czystego ekranu. Narzędzia wymuszają na użytkowniku zmianę hasła w określonym (zgodnie z procedurą) w określonym cyklicznie czasie. Hasła są unikatowe dla danego użytkownika. Istnieje możliwość natychmiastowego odebrania praw dostępu w przypadku kradzieży komputera przenośnego, co chroni przed nieuprawnionym dostępem z zewnątrz.	Wdrożono skutecznie
A.9.2.2	Przydzielanie dostępu użytkownikom	Należy wdrożyć formalny proces przydzielania dostępu użytkownikom w celu nadawania lub odbierania praw dostępu do wszystkich systemów i usług wszystkim kategoriom użytkowników.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie W Urzędzie każdy pracownik z ma zapewniony dostęp do systemów i usług zgodnie ze swoim zakresem obowiązków. Jeżeli pracownik, który nie ma dostępu z uwagi na aktualnie wykonywane zadanie będzie potrzebował tego dostępu, wówczas on sam za zgodą swojego przełożonego lub jego przełożony ma prawo wnioskować o prawo dostępu do odpowiedniego aktywa lub w zakresie systemów i usług do ASI.	Wdrożono skutecznie
A.9.2.3	Zarządzanie prawami uprzywilejowanego dostępu	Przydzielanie i wykorzystanie praw uprzywilejowanego dostępu należy ograniczyć i nadzorować.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie W Urzędzie przyznawanie i korzystanie z uprzywilejowanych praw dostępu jest ograniczone i kontrolowane. Nadzór nad tym należy do ASI.	Wdrożono skutecznie

A.9.2.4	Zarządzanie poufnymi informacjami uwierzytelniającymi użytkowników	Przydzielanie poufnych informacji uwierzytelniających powinno podlegać formalnemu procesowi zarządzania.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie W Urzędzie udzielanie poufnych informacji uwierzytelniających użytkowników nadzorowane jest przez ASI. Rozdział 9.1	Wdrożono skutecznie
A.9.2.5	Przegląd praw dostępu użytkowników	Właściciele aktywów powinni przeglądać prawa dostępu użytkowników w regularnych odstępach czasu.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Właściciel aktywów dokonuje regularnych przeglądów praw dostępu użytkowników.	Wdrożono skutecznie
A.9.2.6	Odbieranie lub dostosowywanie praw dostępu	Przydzielone pracownikom i użytkownikom zewnętrznym prawa dostępu do informacji i środków przetwarzania informacji należy odbierać po zakończeniu zatrudnienia, umowy lub porozumienia lub dostosowywać do zaistniałych zmian.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie W Urzędzie funkcjonuje zasada, że prawa dostępu wszystkich pracowników lub użytkowników podmiotów zewnętrznych do informacji i środków przetwarzania informacji są usuwane w momencie ustania zatrudnienia, umowy, porozumienia lub dostosowane w momencie zaistnienia zmiany.	Wdrożono skutecznie
A.9.3.1	Stosowanie poufnych informacji uwierzytelniających	Użytkownicy powinni mieć obowiązek przestrzegania przyjętych w organizacji zasad stosowania poufnych informacji uwierzytelniających.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie W Urzędzie wszyscy użytkownicy poufnych informacji uwierzytelniających są odpowiedzialni za postępowanie zgodne z praktykami organizacji.	Wdrożono skutecznie
A.9.4 Kontrola dostępu do systemu i aplikacji Cel: Zapobieganie nieuprawnionemu dostępowi do systemów i aplikacji.						
A.9.4.1	Ograniczanie dostępu do informacji	Dostęp do informacji oraz funkcji systemu aplikacyjnego należy ograniczać zgodnie z polityką kontroli dostępu.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie W Urzędzie funkcjonuje Polityka kontroli dostępu do informacji. Każdy ma dostęp do tych informacji, których wymaga jego zakres zobowiązków.	Wdrożono skutecznie
A.9.4.2	Procedury bezpiecznego logowania	Tam, gdzie polityka kontroli dostępu tego wymaga, dostęp do systemów i aplikacji powinien być kontrolowany przez procedurę bezpiecznego logowania.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie W Urzędzie funkcjonują zasady bezpiecznego logowania się. Każdy użytkownik ma niepowtarzalny identyfikator i hasło do systemu.	Wdrożono skutecznie
A.9.4.3	System zarządzania hasłami	Systemy zarządzania hasłami powinny być interaktywne i zapewniać wybór haseł dobrej jakości.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie W Urzędzie systemy zarządzania hasłami oparte są na interaktywnych mechanizmach zapewniających hasła odpowiedniej jakości, zgodnie z wymogiem danego systemu. Każdy pracownik jest świadomy, że nie może nikomu ujawnić swojego hasła osobistego, wie jakie konsekwencje są przewidziane za ujawnienie hasła. Ponadto każdy pracownik wie, że powinien zmienić hasło w trybie natychmiastowym zawsze wtedy kiedy podejrzewa, że w jego posiadanie mogła wejść osoba nieuprawniona	Wdrożono skutecznie

A.9.4.4	Użycie uprzywilejowanych programów narzędziowych	Wykorzystanie programów narzędziowych, umożliwiających obejście zabezpieczeń systemów i aplikacji, powinno podlegać ograniczeniom i ścisłemu nadzorowi.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie W Urzędzie ograniczeniu podlega używanie systemowych programów narzędziowych, które umożliwiają obejście zabezpieczeń systemu lub aplikacji. Każdy pracownik jest informowany o zakazie używania takich programów przy odbiorze sprzętu i podpisaniu protokołu odbioru.	Wdrożono skutecznie
A.9.4.5	Kontrola dostępu do kodów źródłowych programów	Dostęp do kodu źródłowego programów powinien być ograniczony.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie W Urzędzie dostęp do kodów źródłowych mają tylko uprawnieni pracownicy. Kody źródłowe programów i aplikacji znajdują się w bezpiecznym repozytorium do którego dostęp jest tylko za pośrednictwem sieci wewnętrznej i tylko dla uprawnionych osób.	Wdrożono skutecznie
A.10 Kryptografia						
A.10.1 Zabezpieczenia kryptograficzne						
Cel: Zapewnić właściwe i skuteczne wykorzystanie kryptografii do ochrony poufności, autentyczności i/lub integralności informacji.						
A.10.1.1	Polityka stosowania zabezpieczeń kryptograficznych	Należy opracować i wdrożyć politykę stosowania zabezpieczeń kryptograficznych do ochrony informacji.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Stosuje się politykę używania zabezpieczeń kryptograficznych do ochrony informacji.	Wdrożono skutecznie
A.10.1.2	Zarządzanie kluczami	Należy opracować politykę dotyczącą korzystania, ochrony i okresów ważności kluczy kryptograficznych i wdrożyć ją na wszystkich etapach cyklu życia kluczy.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Stosuje się zarządzanie kluczami kryptograficznymi.	Wdrożono skutecznie
A.11 Bezpieczeństwo fizyczne i środowisko						
A.11.1 Obszary bezpieczne						
Cel: Zapewnienie ochrony przed nieautoryzowanym dostępem fizycznym, uszkodzeniami lub zakłóceniami w odniesieniu do informacji należących do organizacji oraz środków przetwarzania informacji.						
A.11.1.1	Fizyczna granica obszaru bezpiecznego	Należy określić granice bezpieczeństwa i wykorzystać je do zabezpieczenia obszarów zawierających wrażliwe lub krytyczne informacje oraz środki przetwarzania informacji.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie W Urzędzie zostały wyznaczone granice obszaru bezpiecznego i mają one swoje zastosowanie do obszarów, w których znajdują się informacje wrażliwe i środki przetwarzania informacji.	Wdrożono skutecznie
A.11.1.2	Fizyczne zabezpieczenie wejść	Bezpieczne strefy należy chronić odpowiednimi zabezpieczeniami wejść zapewniającymi dostęp wyłącznie osobom uprawnionym.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie W Urzędzie obszary bezpieczne są chronione za pomocą fizycznych zabezpieczeń (KONTROLA DOSTĘPU) i tylko uprawnieni użytkownicy mają do nich dostęp.	Wdrożono skutecznie
A.11.1.3	Zabezpieczenie biur, pomieszczeń i obiektów	Należy zaprojektować i stosować fizyczne zabezpieczenia biur, pomieszczeń i obiektów.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie W Urzędzie funkcjonuje ścisła ochrona fizyczna biur, pomieszczeń i urządzeń. Wszystkie pomieszczenia serwerowni zaopatrzone są w SKD.	Wdrożono skutecznie
A.11.1.4	Ochrona przed zagrożeniami zewnętrznymi i środowiskowymi	Należy zaprojektować i stosować fizyczne zabezpieczenia przed katastrofami naturalnymi, wrogim atakiem lub wypadkami.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie W Urzędzie stosowana jest fizyczna ochrona przed katastrofami naturalnymi, złośliwymi atakami lub wypadkami.	Wdrożono skutecznie

A.11.1.5	Praca w obszarach bezpiecznych	Należy zaprojektować i stosować procedury pracy w obszarach bezpiecznych.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie W Urzędzie wszyscy pracownicy oraz strony trzecie stosują się do procedur związanych z przebywaniem w obszarach bezpiecznych.	Wdrożono skutecznie
A.11.1.6	Obszary dostaw i załadunku	Należy sprawować nadzór nad punktami dostępu takimi jak obszary dostaw i załadunku oraz innymi punktami, przez które nieuprawnione osoby mogą wejść do pomieszczeń, i, jeśli to możliwe, odizolować je od środków przetwarzania informacji, aby zapobiec nieuprawnionemu dostępowi.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie W Urzędzie wszystkie punkty dostępu przez które nieuprawnione osoby mogą wejść do budynku, są nadzorowane i odizolowane od środków przetwarzania informacji.	Wdrożono skutecznie
A.11.2 Sprzęt Cel: Zapobiec utracie, uszkodzeniu, kradzieży lub utracie integralności aktywów oraz zakłóceniom w działaniu organizacji.						
A.11.2.1	Lokalizacja i ochrona sprzętu	Sprzęt należy umieścić i chronić w taki sposób, aby zredukować ryzyka wynikające z zagrożeń i niebezpieczeństw środowiskowych oraz okazać do nieuprawnionego dostępu.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Serwery oraz pozostały sprzęt należący do Urzędu jest rozlokowany i chroniony w sposób, który redukuje ryzyka wynikające z zagrożeń i niebezpieczeństw środowiskowych oraz możliwości nieautoryzowanego dostępu.	Wdrożono skutecznie
A.11.2.2	Systemy wspomagające	Sprzęt należy chronić przez awariami zasilania oraz innymi przerwami spowodowanymi awariami systemów wspomagających.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Serwery oraz pozostały sprzęt jest chroniony przed awariami zasilania oraz wszelkimi zakłóceniami spowodowanymi awariami systemów wspomagających.	Wdrożono skutecznie
A.11.2.3	Bezpieczeństwo okablowania	Okablowanie zasilające oraz telekomunikacyjne, przenoszące dane lub wspomagające usługi informacyjne należy chronić przed przechwyceniem, zakłóceniem lub uszkodzeniem.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Okablowanie zasilające i telekomunikacyjne służące do przesyłania danych lub wspomagające usługi informacyjne jest chronione przed przejęciem, zakłóceniami lub uszkodzeniem.	Wdrożono skutecznie
A.11.2.4	Konserwacja sprzętu	Sprzęt należy prawidłowo konserwować w celu zapewnienia jego ciągłej dostępności i integralności.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Cały sprzęt jest prawidłowo konserwowany, co zapewnia jego ciągłą dostępność i integralność.	Wdrożono skutecznie
A.11.2.5	Wynoszenie aktywów	Sprzętu, informacji i programów nie należy wnosić poza siedzibę organizacji bez uzyskania wcześniejszego zezwolenia.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Możliwe jest wyносzenie sprzętu po uzyskaniu pisemnej zgody Kierownika lub bezpośredniego przełożonego.	Wdrożono skutecznie
A.11.2.6	Bezpieczeństwo sprzętu i aktywów poza siedzibą	Aktywa wynoszone poza siedzibę organizacji należy zabezpieczyć przed wystąpieniem różnych ryzyk związanych z pracą poza siedzibą.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Sprzęt pozostający poza siedzibą jest chroniony. Każdy użytkownik jest odpowiedzialny za przekazany mu sprzęt i jest zobowiązany do zapewnienia jego bezpieczeństwa poza siedzibą Urzędu.	Wdrożono skutecznie
A.11.2.7	Bezpieczne zbywanie lub przekazywanie do ponownego użycia	Przed zbyciem lub przekazaniem sprzętu do ponownego użycia należy sprawdzić wszystkie jego składniki zawierające nośniki informacji, dla zapewnienia, że wszystkie wrażliwe dane i licencjonowane programy zostały usunięte lub bezpiecznie nadpisane.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Wszystkie składniki sprzętu zawierające nośniki informacji są sprawdzane przed zbyciem sprzętu, celem upewnienia się, że wszelkie informacje wrażliwe i licencjonowane oprogramowanie zostały usunięte lub bezpiecznie nadpisane.	Wdrożono skutecznie

A.11.2.8	Pozostawienie sprzętu użytkownika bez opieki	Użytkownicy powinni zapewnić odpowiednią ochronę sprzętu pozostawianego bez opieki.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Użytkownicy są zobowiązani do zapewnienia odpowiedniej ochrony sprzętu pozostawionego bez opieki.	Wdrożono skutecznie
A.11.2.9	Polityka czystego biurka i czystego ekranu	Należy wprowadzić politykę czystego biurka dla dokumentów papierowych i przenośnych nośników pamięci oraz politykę czystego ekranu dla środków przetwarzania informacji.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Wszyscy pracownicy Urzędu stosują politykę czystego biurka dla dokumentów papierowych i nośników, a dla środków przetwarzania informacji — politykę czystego ekranu.	Wdrożono skutecznie
A.12 Kontrola dostępu do systemów operacyjnych						
A.12.1 Procedury eksploatacyjne i zakresy odpowiedzialności Cel: Zapewnić poprawną i bezpieczną eksploatację środków przetwarzania informacji.						
A.12.1.1	Dokumentowanie procedur eksploatacyjnych	Procedury eksploatacyjne powinny być udokumentowane i udostępniane wszystkim potrzebującym ich użytkownikom.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Procedury eksploatacyjne są udokumentowane, utrzymywane i dostępne dla wszystkich użytkowników, którzy ich potrzebują.	Wdrożono skutecznie
A.12.1.2	Zarządzanie zmianami	Zmiany w organizacji, procesach biznesowych, środkach przetwarzania informacji i systemach, które mają wpływ na bezpieczeństwo informacji, powinny być nadzorowane.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Wszystkie zmiany w organizacji, procesach biznesowych, środkach przetwarzania informacji i systemach, mających wpływ na bezpieczeństwo informacji, są kontrolowane.	Wdrożono skutecznie
A.12.1.3	Zarządzanie pojemnością	Należy monitorować i dostosowywać wykorzystanie zasobów oraz przewidywać wymaganą pojemność w przyszłości, dla zapewnienia właściwej wydajności systemu.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie W Urzędzie wykorzystanie zasobów jest monitorowane i regulowane oraz przewidywana jest przyszła pojemności systemów, aby zapewnić ich właściwą wydajność.	Wdrożono skutecznie
A.12.1.4	Oddzielanie środowisk rozwojowych, testowych i produkcyjnych	Należy oddzielić środowiska rozwojowe, testowe i produkcyjne celem redukcji ryzyk związanych z nieuprawnionym dostępem lub zmianami w środowisku produkcyjnym.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie W Urzędzie rozdzielamy środowiska rozwojowe, testowe i eksploatacyjne, aby zredukować ryzyko nieupoważnionego dostępu lub zmian w środowisku eksploatacyjnym.	Wdrożono skutecznie
A.12.2 Ochrona przed oprogramowaniem malware Cel: Zapewnić informacjom i środkom przetwarzania informacji ochronę przed szkodliwym oprogramowaniem.						
A.12.2.1	Zabezpieczenia przed szkodliwym oprogramowaniem	Należy wdrożyć zabezpieczenia wykrywające, zapobiegające i odtwarzające, które służą ochronie przed szkodliwym oprogramowaniem, w połączeniu z właściwym uświadamianiem użytkowników.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie W Urzędzie są wdrożone zabezpieczenia chroniące przed oprogramowaniem malware w takim zakresie w jakim jest to wymagane. Wszyscy użytkownicy zostali uświadomieni w zakresie wspomnianego oprogramowania.	Wdrożono skutecznie
A.12.3 Kopie zapasowe Cel: Chronić przed utratą danych.						
A.12.3.1	Zapaszowe kopie informacji	Zapaszowe kopie informacji, oprogramowania i obrazów systemów należy regularnie wykonywać i testować, zgodnie z ustaloną polityką kopii zapasowych.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Kopie zapaszowe informacji i oprogramowania a także obrazy systemów są regularnie tworzone i testowane zgodnie z procedurą.	Wdrożono skutecznie

A.12.4 Rejestrowanie zdarzeń i monitorowanie Cel: Rejestrować zdarzenia i zbierać materiał dowodowy.						
A.12.4.1	Rejestrowanie zdarzeń	Należy tworzyć, przechowywać i systematycznie przeglądać dzienniki zdarzeń rejestrujące działania użytkowników, wyjątki, usterki oraz zdarzenia związane z bezpieczeństwem informacji.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie wszystkie działania użytkowników, błędy oraz zdarzenia związane z bezpieczeństwem informacji są monitorowane przez operatorów i administratorów. Wszystkie zdarzenia mają odzwierciedlenie w logach systemów.	Wdrożono skutecznie
A.12.4.2	Ochrona informacji w dziennikach zdarzeń	Środki służące rejestrowaniu zdarzeń oraz informacje w dziennikach zdarzeń należy chronić przed manipulacją i nieuprawnionym dostępem.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie dostęp do logów jest chroniony w systemach.	Wdrożono skutecznie
A.12.4.3	Rejestrowanie działań administratorów i operatorów	Działania administratorów i operatorów systemów należy rejestrować, a dzienniki chronić i systematycznie przeglądać.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Działania administratora i operatora systemu są rejestrowane a zapisy chronione w systemach.	Wdrożono skutecznie
A.12.4.4	Synchronizacja zegarów	Zegary wszystkich istotnych systemów przetwarzania informacji w organizacji lub domenie bezpieczeństwa należy zsynchronizować z jednym wzorcowym źródłem czasu.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Zegary wszystkich stosownych systemów przetwarzania informacji w organizacji lub domenie bezpieczeństwa są synchronizowane do referencyjnego punktu wzorca czasu.	Wdrożono skutecznie
A.12.5 Zabezpieczenie eksploatowanego oprogramowania Cel: Zapewnić integralność systemów produkcyjnych.						
A.12.5.1	Instalacja oprogramowania w systemach produkcyjnych	Należy wdrożyć procedury nadzoru nad instalacją oprogramowania w systemach produkcyjnych.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie W Urzędzie użytkownik nie jest uprawniony do instalowania oprogramowania.	Wdrożono skutecznie
A.12.6 Zarządzanie podatnościami technicznymi Cel: Zapobieganie wykorzystywaniu podatności technicznych.						
A.12.6.1	Zarządzanie podatnościami technicznym	Informacje o podatnościach technicznych wykorzystywanych systemów informacyjnych należy niezwłocznie pozyskiwać, oceniać stopień narażenia organizacji na te podatności i podejmować odpowiednie środki w celu przeciwdziałania związanemu z nimi ryzyku.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie 1.W Urzędzie zarządza się podatnościami. Pracujący w Urzędzie specjaliści śledzą wszelkie informacje branżowe celem bieżącej informacji o możliwych podatnościach technicznych w systemach i sieciach. Każdą wykrytą podatność, która mogłaby zagrozić bezpieczeństwu informacji w systemach i sieciach działających w Urzędzie zgłaszają do ASI wraz z rekomendacją zabezpieczenia.	Wdrożono skutecznie
A.12.6.2	Ograniczenia w instalowaniu oprogramowania	Należy ustanowić i wdrożyć zasady instalowania oprogramowania przez użytkowników.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Uprawnienia do instalowania oprogramowania ma wyłącznie ASI.	Wdrożono skutecznie
A.12.7 Rozważania dotyczące audytu systemów informacyjnych Cel: Zminimalizować wpływ działań audytu na systemy produkcyjne.						
A.12.7.1	Zabezpieczenia audytu systemów informacyjnych	Należy starannie zaplanować i uzgodnić wymagania audytu oraz działania obejmujące weryfikację systemów produkcyjnych, w celu zminimalizowania zakłóceń w procesach biznesowych.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie W celu minimalizacji ryzyka zakłóceń procesów biznesowych, każdy audyt systemów informacyjnych będzie starannie planowany. Planowane i uzgadniane będą także działania związane ze sprawdzeniem eksploatowanych systemów.	Wdrożono skutecznie

A.13 Bezpieczeństwo komunikacji						
A.13.1 Zarządzanie bezpieczeństwem sieci Cel: Zapewnić ochronę informacji w sieciach oraz wspomagających je środkach przetwarzania informacji.						
A.13.1.1	Zabezpieczenia sieci	Sieci powinny być zarządzane i nadzorowane, w celu ochrony informacji w systemach i aplikacjach.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Sieć jest zarządzana i nadzorowana, aby chronić informacje w systemach i aplikacjach.	Wdrożono skutecznie
A.13.1.2	Bezpieczeństwo usług sieciowych	Umowy dotyczące wszystkich usług sieciowych, świadczonych wewnętrznie lub zleczanych na zewnątrz, powinny zawierać zidentyfikowane mechanizmy zabezpieczeń, poziomy świadczenia usług i wymagania dotyczące zarządzania.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Mechanizmy bezpieczeństwa, poziom usług i wymagania zarządzania wszystkimi usługami sieciowymi będą określone i włączone do umów na dostarczanie tych usług, bez względu na to czy są one realizowane własnymi środkami, czy zleczane na zewnątrz.	Wdrożono skutecznie
A.13.1.3	Rozdzielanie sieci	Grupy usług informacyjnych, użytkowników i systemów informacyjnych powinny być rozdzielone w strukturze sieci.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Grupy usług informacyjnych, użytkowników i systemów informacyjnych są rozdzielone w sieciach.	Wdrożono skutecznie
A.13.2 Przekazywanie informacji Cel: Utrzymać bezpieczeństwo informacji przesyłanych wewnątrz organizacji i wymienianych z podmiotami zewnętrznymi.						
A.13.2.1	Polityki i procedury przesyłania informacji	Należy wdrożyć formalne polityki przesyłania informacji, procedury i zabezpieczenia w celu ochrony wymiany informacji przesyłanych przy użyciu wszystkich rodzajów środków łączności.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie W Urzędzie funkcjonują formalne polityki, procedury i zabezpieczenia w celu ochrony przekazywanej informacji za pomocą wszystkich środków komunikacji.	Wdrożono skutecznie
A.13.2.2	Porozumienia dotyczące przesyłania informacji	Porozumienia powinny uwzględniać bezpieczne przesyłanie informacji biznesowych między organizacją i podmiotami zewnętrznymi.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Umowy o przekazywaniu informacji biznesowych zobowiązują do bezpiecznego przekazywania informacji między organizacją a stronami zewnętrznymi.	Wdrożono skutecznie
A.13.2.3	Wiadomości elektroniczne	Informacje przekazywane w formie wiadomości elektronicznych powinny być odpowiednio chronione.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Informacje zawarte w wiadomościach elektronicznych są odpowiednio zabezpieczone.	Wdrożono skutecznie
A.13.2.4	Umowy o zachowaniu poufności	Należy zidentyfikować, regularnie przeglądać i dokumentować wymagania odnoszące się do umów o zachowaniu poufności lub nieujawnianiu informacji, w sposób odzwierciedlający potrzeby organizacji w zakresie ochrony informacji.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie W Urzędzie okresowo przegląda się i dokumentuje wymagania o zachowaniu poufności lub nieujawnianiu z uwzględnieniem potrzeb organizacji w zakresie ochrony informacji.	Wdrożono skutecznie
A.14 Pozyskiwanie, rozwój i utrzymanie systemów						
A.14.1 Wymagania związane z bezpieczeństwem systemów informacyjnych Cel: Zapewnić, żeby bezpieczeństwo informacji było nieodłączną częścią systemów informacyjnych w całym cyklu życia. Dotyczy to również wymagań wobec systemów informacyjnych dostarczających usług w sieciach publicznych.						
A.14.1.1	Analiza i specyfikacja wymagań bezpieczeństwa informacji	Wymagania dotyczące bezpieczeństwa informacji należy włączyć do wymagań stawianych nowym systemom informacyjnym lub rozbudowie systemów istniejących.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie W Urzędzie analizuje się i specyfikuje wymagania bezpieczeństwa informacji.	Wdrożono skutecznie

A.14.1.2	Zabezpieczanie usług aplikacyjnych w sieciach publicznych	Informacje przesyłane w sieciach publicznych, związane z usługami świadczonymi przez aplikacje, należy chronić przed nieuczciwymi działaniami, sporami dotyczącymi umów oraz nieuprawnionym ujawnieniem i zmianami.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie W Urzędzie zabezpiecza się usługi aplikacyjne w sieciach publicznych.	Wdrożono skutecznie
A.14.1.3	Ochrona transakcji usług aplikacyjnych	Informacje związane z transakcjami dokonywanymi w ramach usług świadczonych przez aplikacje należy chronić, aby zapobiec przerwaniu transmisji, błędom w trasowaniu, nieuprawnionym zmianom wiadomości, nieuprawnionemu ujawnieniu, nieuprawnionemu	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie W Urzędzie chroni się transakcje usług aplikacyjnych.	Wdrożono skutecznie
A.14.2 Bezpieczeństwo w procesach rozwojowych i wsparcia Cel: Zapewnić projektowanie i wdrożenie bezpieczeństwa informacji w ramach cyklu życia systemów infor- macyjnych.						
A.14.2.1	Polityka bezpieczeństwa prac rozwojowych	Należy ustanowić zasady prac nad rozwojem oprogramowania i systemów oraz stosować je w pracach rozwojowych prowadzonych wewnątrz organizacji.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie W Urzędzie na bieżąco wypracowywane są zasady dotyczące rozwoju oprogramowania i systemów. Cały czas trwają prace rozwojowe. Wszystkie zasady są dokumentowane.	Wdrożono skutecznie
A.14.2.2	Procedury kontroli zmian w systemach	Należy nadzorować zmiany w systemach podczas ich cyklu rozwojowego, przy użyciu formalnych procedur kontroli zmian.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Zmiany w systemach w ramach cyklu rozwoju są nadzorowane za pomocą formalnych procedur zarządzania zmianą.	Wdrożono skutecznie
A.14.2.3	Przegląd techniczny aplikacji po zmianach w platformie produkcyjnej	Po dokonaniu zmian w platformach produkcyjnych należy przeprowadzić przegląd krytycznych aplikacji biznesowych oraz przetestować je, aby uzyskać pewność, że zmiany nie miały niekorzystnego wpływu na działalność organizacji lub bezpieczeństwo.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Po dokonaniu zmian w platformach operacyjnych testowane są aplikacje krytyczne, tak aby uzyskać pewność, że zmiany nie miały niekorzystnego wpływu na działalność organizacji lub bezpieczeństwo.	Wdrożono skutecznie
A.14.2.4	Ograniczenia dotyczące zmian w pakietach oprogramowania	Modyfikacji w pakietach oprogramowania należy dokonywać z rozwagą i ograniczać się do zmian niezbędnych, a wszystkie takie zmiany ściśle nadzorować.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Zmiany w oprogramowaniu są minimalne, ograniczone do zmian niezbędnych, a wszelkie zmiany są ściśle nadzorowane.	Wdrożono skutecznie
A.14.2.5	Zasady projektowania bezpiecznych systemów	Należy ustanowić, udokumentować i utrzymywać zasady projektowania bezpiecznych systemów oraz stosować je do wszystkich prac implementacyjnych nad systemami informacyjnymi.		Na podstawie wyników szacowania ryzyka	Zabezpieczenie Zasady budowy bezpiecznych systemów są ustanowione, udokumentowane, utrzymywane i będą stosowane przy wdrażaniu wszystkich systemów informacyjnych.	Wdrożono skutecznie
A.14.2.6	Bezpieczne środowisko rozwojowe	Organizacje powinny ustanowić i odpowiednio chronić bezpieczne środowiska rozwojowe przeznaczone do rozwoju systemów oraz prac integracyjnych obejmujących całość cyklu rozwojowego systemów.		Na podstawie wyników szacowania ryzyka	Zabezpieczenie Urząd tworzy i odpowiednio chroni bezpieczne środowiska do rozwoju i integracji systemu w całym cyklu rozwojowym systemu.	Wdrożono skutecznie
A.14.2.7	Prace rozwojowe zlecane podmiotom zewnętrznym	Organizacja powinna nadzorować i monitorować prace rozwojowe nad systemami zlecone podmiotom zewnętrznym.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Nadzorujemy i monitorujemy prace rozwojowe nad oprogramowaniem, w sytuacji kiedy są one powierzone firmie zewnętrznej.	Wdrożono skutecznie
A.14.2.8	Testowanie bezpieczeństwa systemu	Funkcje bezpieczeństwa należy testować w czasie prac rozwojowych.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Podczas prac rozwojowych w Urzędzie stosowane są opracowania przypadków testowych dla każdej aplikacji.	Wdrożono skutecznie

A.14.2.9	Testy akceptacyjne systemów	Dla nowych systemów informacyjnych, ich modernizacji i nowych wersji systemów należy ustanowić programy testów akceptacyjnych i kryteria z nimi związane.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie W Urzędzie stosowane są opracowania przypadków testowych dla każdej aplikacji z osobna.	Wdrożono skutecznie
A.14.3 Dane testowe Cel: Zapewnić ochronę danych stosowanych do testów.						
A.14.3.1	Ochrona danych testowych	Dane testowe należy starannie wybierać, chronić i nadzorować.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Dane testowe są starannie dobrane, chronione i kontrolowane.	Wdrożono skutecznie
A.15 Relacje z dostawcami						
A.15.1 Bezpieczeństwo informacji w relacjach z dostawcami Cel: Zapewnić ochronę aktywów organizacji udostępnianych dostawcom.						
A.15.1.1	Polityka bezpieczeństwa informacji w relacjach z dostawcami	Należy uzgodnić z dostawcą i udokumentować wymagania bezpieczeństwa informacji celem zmniejszenia ryzyk związanych z dostępem dostawcy do aktywów organizacji.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie W Urzędzie odpowiednie zapisy (umowy) ograniczają ryzyko związane z dostępem dostawców do aktywów organizacji.	Wdrożono skutecznie
A.15.1.2	Uwzględnianie bezpieczeństwa w porozumieniach z dostawcami	Należy ustanowić wszystkie istotne wymagania dotyczące bezpieczeństwa informacji i uzgodnić je z każdym dostawcą, który może uzyskać dostęp, przetwarzać, przechowywać, przysyłać lub dostarczać elementy infrastruktury teleinformatycznej dla przetwarzania informacji należących do organizacji.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Wszystkie istotne wymagania bezpieczeństwa informacji są ustanowione i uzgodnione z każdym dostawcą, który może mieć dostęp do informacji organizacji, może ją przetwarzać, przechowywać, przekazywać lub dostarczać komponenty infrastruktury teleinformatycznej.	Wdrożono skutecznie
A.15.1.3	Łańcuch dostaw technologii informacyjnych i telekomunikacyjnych	Porozumienia z dostawcami powinny uwzględniać wymagania odnoszące się do ryzyk w bezpieczeństwie informacji, związanych z usługami technologii informacyjnych i telekomunikacyjnych oraz łańcuchem dostaw produktów.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Umowy z dostawcami internetu zawierają wymagania adresujące ryzyko bezpieczeństwa informacji związane z technicznymi usługami informacyjnymi i komunikacyjnymi i łańcuchem dostaw produktów.	Wdrożono skutecznie
A.15.2 Zarządzanie usługami dostarczonymi przez dostawców Cel: Utrzymanie odpowiedniego poziomu bezpieczeństwa informacji i dostarczanie usług zgodnie z umowami serwisowymi zawartymi z dostawcami.						
A.15.2.1	Monitorowanie i przegląd usług świadczonych przez dostawców	Organizacje powinny regularnie monitorować, przeglądać i audytować dostarczanie usług zewnętrznych.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Urząd regularnie monitoruje, przegląda dostarczanie usług przez dostawców. Jeśli zaszłaby konieczność Urząd przewiduje przeprowadzenie okresowych audytów u dostawcy.	Wdrożono skutecznie

A.15.2.2	Zarządzenie zmianami w usługach świadczonych przez dostawców	Należy zarządzać zmianami w zakresie świadczenia usług przez dostawców, w tym utrzymaniem i doskonaleniem istniejących polityk bezpieczeństwa informacji, procedur i zabezpieczeń, z uwzględnieniem krytyczności informacji, systemów i procesów biznesowych, których dotyczą oraz ponownego szacowania ryzyka.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Zmiany w dostarczaniu usług, łącznie z utrzymaniem i doskonaleniem istniejących polityk bezpieczeństwa, procedur i zabezpieczeń, są zarządzane z uwzględnieniem krytyczności związanych z nimi systemów i procesów biznesowych. Wszystkie zmiany uwzględniane są w regularnych szacowaniach ryzyk. Monitorowanie incydentów pokazuje efektywność w zakresie bezpieczeństwa ze strony świadczonych usług. Każda umowa z dostawcą jasną określa możliwość odstąpienia od umowy w konkretnych przypadkach.	Wdrożono skutecznie
A.16 Zarządzanie incydentami związanymi z bezpieczeństwem informacji						
A.16.1 Zarządzanie incydentami związanymi z bezpieczeństwem informacji oraz udoskonaleniami						
Cel: Zapewnić spójne i skuteczne podejście do zarządzania incydentami związanymi z bezpieczeństwem informacji, z uwzględnieniem informowania o zdarzeniach i słabościach.						
A.16.1.1	Odpowiedzialność i procedury	Należy ustanowić odpowiedzialność kierownictwa oraz procedury zapewniające szybkość, skuteczną i zorganizowaną reakcję na incydenty związane z bezpieczeństwem informacji.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie W Urzędzie funkcjonuje procedura zapewniająca szybką reakcję na incydenty związane z bezpieczeństwem informacji. Kierownictwo jest odpowiedzialne za zapewnienie funkcjonalności odpowiednich procedur w Urzędzie.	Wdrożono skutecznie
A.16.1.2	Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji	Zdarzenia związane z bezpieczeństwem informacji należy zgłaszać odpowiednimi kanałami zarządczymi tak szybko, jak tylko to jest możliwe.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Zdarzenia związane z bezpieczeństwem informacji są w Urzędzie zgłaszane poprzez odpowiednie kanały organizacyjne tak szybko, jak to możliwe, zawsze zgodnie z procedurą.	Wdrożono skutecznie
A.16.1.3	Zgłaszanie słabości związanych z bezpieczeństwem informacji	Należy zobowiązać pracowników oraz kontrahentów korzystających z systemów i usług informacyjnych organizacji do odnotowania i zgłaszania wszelkich zaobserwowanych lub podejrzewanych słabości związanych z bezpieczeństwem informacji w systemach lub usługach.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Pracownicy oraz wykonawcy wykorzystujący systemy informacyjne i usługi organizacji są zobowiązani do zgłaszania zaobserwowanych lub podejrzewanych słabości bezpieczeństwa w systemach i usługach.	Wdrożono skutecznie
A.16.1.4	Ocena i podejmowanie decyzji w sprawie zdarzeń związanych z bezpieczeństwem informacji	Zdarzenia związane z bezpieczeństwem informacji należy ocenić i podjąć decyzję w sprawie zakwalifikowania ich jako incydentów związanych z bezpieczeństwem informacji.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Zdarzenia bezpieczeństwa informacji każdorazowo są oceniane i odpowiednio klasyfikowane, zgodnie z procedurą. Rozdział 16	Wdrożono skutecznie
A.16.1.5	Reagowanie na incydenty związane z bezpieczeństwem informacji	Reakcja na incydenty związane z bezpieczeństwem informacji powinna być zgodna z udokumentowanymi procedurami.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Na incydenty bezpieczeństwa informacji pracownicy reagują zgodnie z udokumentowaną procedurą.	Wdrożono skutecznie
A.16.1.6	Wyciąganie wniosków z incydentów związanych z bezpieczeństwem informacji	Wiedzę zdobytą podczas analizy i rozwiązywania incydentów związanych z bezpieczeństwem informacji należy wykorzystać do zredukowania prawdopodobieństwa wystąpienia lub skutków przyszłych incydentów.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Wiedzę pozyskaną z analizy i rozwiązywania incydentów bezpieczeństwa informacji pracownicy wykorzystują w celu redukcji prawdopodobieństwa wystąpienia lub wpływu przyszłych incydentów.	Wdrożono skutecznie

A.16.1.7	Gromadzenie materiału dowodowego	Organizacja powinna określić i stosować procedury identyfikacji, gromadzenia, pozyskiwania i utrwalania informacji, które mogą stanowić materiał dowodowy. materiał dowodowy w przypadku kiedy będzie konieczność podjęcia czynności prawnych	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie W Urzędzie funkcjonuje procedura służąca identyfikacji, zbieraniu, pozyskiwaniu i utrwalaniu informacji, które mogą posłużyć za materiał dowodowy w przypadku kiedy będzie konieczność podjęcia czynności prawnych.	Wdrożono skutecznie
A.17 Aspekty bezpieczeństwa informacji w Dyrektorzaniu ciągłości działania						
A.17.1 Ciągłość bezpieczeństwa informacji						
Cel: Zaleca się uwzględnienie ciągłości bezpieczeństwa informacji w systemach zarządzania ciągłością działania organizacji.						
A.17.1.1	Planowanie ciągłości bezpieczeństwa informacji	Organizacja powinna określić wymagania dotyczące bezpieczeństwa informacji i ciągłości zarządzania bezpieczeństwem informacji w niekorzystnych sytuacjach np. w czasie kryzysu lub katastrofy.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Urząd ma określone swoje wymagania dla bezpieczeństwa informacji oraz ciągłości zarządzania bezpieczeństwem informacji w niekorzystnych sytuacjach- stosuje się strukturę zastępowalności.	Wdrożono skutecznie
A.17.1.2	Wdrażanie ciągłości bezpieczeństwa informacji	Organizacja powinna ustanowić, udokumentować, wdrożyć i utrzymywać procesy, procedury i zabezpieczenia dla zapewnienia w niekorzystnej sytuacji wymaganego poziomu ciągłości bezpieczeństwa informacji.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Urząd posiada ustanowione, udokumentowane i wdrożone procesy, procedury i zabezpieczenia w celu zapewnienia wymaganego poziomu ciągłości dla bezpieczeństwa informacji w niekorzystnych sytuacjach.	Wdrożono skutecznie
A.17.1.3	Weryfikacja, przegląd i ocena ciągłości bezpieczeństwa informacji	Organizacja powinna weryfikować ustanowione i wdrożone zabezpieczenia ciągłości bezpieczeństwa informacji w regularnych odstępach czasu celem zapewnienia ich aktualności i skuteczności w niekorzystnych sytuacjach. Na bieżącym etapie Urząd zaplanował testowanie planów.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Urząd weryfikuje ustanowione i wdrożone zabezpieczenia ciągłości bezpieczeństwa informacji w regularnych odstępach czasu, w celu zapewnienia, że są właściwe oraz efektywne w niekorzystnych sytuacjach.	Wdrożono skutecznie
A.17.2 Nadmiarowość						
Cel: Zapewnić dostępność środków przetwarzania informacji.						
A.17.2.1	Dostępność środków przetwarzania informacji	Środki przetwarzania informacji należy wdrażać z nadmiarem wystarczającym do spełnienia wymagań dostępności.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Zapewnia się redundancję krytycznych środków przetwarzania informacji, sprzętu i wyposażenia oraz systemów.	Wdrożono skutecznie
A.18 Zgodność						
A.18.1 Zgodność z wymaganiami prawnymi i umownymi						
Cel: Unikać naruszenia zobowiązań prawnych, regulacyjnych lub umownych związanych z bezpieczeństwem informacji oraz innych wymagań dotyczących bezpieczeństwa.						
A.18.1.1	Określenie stosownych wymagań prawnych i umownych	Wszystkie istotne wymagania prawne, regulacyjne, umowne oraz podejście organizacji do ich przestrzegania należy zidentyfikować, udokumentować i aktualizować dla każdego systemu informacyjnego oraz całości organizacji.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Wszelkie wymagania wynikające z ustaw, regulacji wewnętrznych, wytycznych organów nadzoru lub szczególne uwarunkowania są określone i przestrzegane. Kontrolę nad tym sprawuje dział prawny. Każda umowa w Urzędzie jest dodatkowo sprawdzana zarówno od strony wykonalności technicznej jak i prawnej. Nadzór nad aktualizacją przepisów wynikających z ustaw i rozporządzeń w obszarze działalności sprawuje dział prawny.	Wdrożono skutecznie

A.18.1.2	Prawo do własności intelektualnej	Należy wdrożyć odpowiednie procedury zapewniające zgodność z wymaganiami prawnymi, regulacyjnymi i umownymi, związanymi z prawami własności intelektualnej i użytkowaniem prawnie zastrzeżonego oprogramowania.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie W Urzędzie poprzez odpowiednie postępowanie zapewniona jest zgodność z wymaganiami wynikającymi z przepisów prawa, wytycznych organów nadzoru oraz wymagań wynikających z umów, które odnoszą się do praw własności intelektualnej oraz do wykorzystania prawnie zastrzeżonego oprogramowania.	Wdrożono skutecznie
A.18.1.3	Ochrona zapisów	Zapisy należy chronić przed utratą, zniszczeniem, fałszowaniem, nieuprawnionym dostępem i nieuprawnionym opublikowaniem, stosownie do wymagań prawnych, regulacyjnych, umownych i biznesowych.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie W Urzędzie zapewniona jest ochrona zapisów przed utratą, zniszczeniem, fałszerstwem, nieautoryzowanym dostępem oraz nieautoryzowanym ujawnieniem zgodnie z wymaganiami prawnymi, wytycznymi organów nadzoru oraz wymaganiami biznesowymi, a także wynikającymi z umów. W Urzędzie prowadzony jest backup informacji na życzenie Klienta jak i własny.	Wdrożono skutecznie
A.18.1.4	Prywatność i ochrona danych identyfikujących osobę	Należy zapewnić prywatność i ochronę danych identyfikujących osobę stosownie do odpowiednich przepisów prawa i regulacji.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie W Urzędzie prywatność i ochrona danych osobowych jest zapewniona zgodnie z odpowiednimi przepisami prawa i regulacjami.	Wdrożono skutecznie
A.18.1.5	Regulacje dotyczące zabezpieczeń kryptograficznych	Zabezpieczenia kryptograficzne należy stosować zgodnie z odpowiednimi umowami, przepisami i regulacjami.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie W Urzędzie stosuje się odpowiednie zabezpieczenia w celu zgodności z umowami i regulacjami w zakresie zabezpieczeń kryptograficznych.	Wdrożono skutecznie
A.18.2 Przeglądy bezpieczeństwa informacji Cel: Zapewnić zgodne z politykami organizacji i procedurami wdrożenie i stosowanie zasad bezpieczeństwa informacji.						
A.18.2.1	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) należy poddawać niezależnemu przeglądowi w zaplanowanych odstępach czasu lub wtedy, gdy nastąpią istotne zmiany.	T	Na podstawie wyników szacowania ryzyka	Zabezpieczenie Podejście Urzędu do zarządzania bezpieczeństwem informacji oraz jego realizacja (tzn. cele stosowania zabezpieczeń, zabezpieczenia, polityki, procesy i procedury bezpieczeństwa informacji) są poddawane niezależnym przeglądom w zaplanowanych odstępach czasu lub wtedy, gdy nastąpiły znaczące zmiany.	Wdrożono skutecznie
A.18.2.2	Zgodność z politykami bezpieczeństwa i standardami	Kierownicy powinni regularnie dokonywać przeglądu zgodności przetwarzania informacji i procedur z odpowiednimi politykami bezpieczeństwa, standardami i innymi wymaganiami dotyczącymi bezpieczeństwa, w zakresie przydzielonej im odpowiedzialności.	T	Na podstawie wyników szacowania ryzyka	Dokonyje się regularnych przeglądów zgodności przetwarzania informacji i procedur z odpowiednimi politykami bezpieczeństwa, standardami i innymi wymaganiami dotyczącymi bezpieczeństwa, w zakresie przydzielonej im odpowiedzialności.	Wdrożono skutecznie
A.18.2.3	Sprawdzanie zgodności technicznej	Należy regularnie przeglądać systemy informacyjne celem sprawdzenia ich zgodności z politykami bezpieczeństwa informacji i standardami obowiązującymi w organizacji.	T	Na podstawie wyników szacowania ryzyka	Regularnie są przeglądane systemy informacyjne celem sprawdzenia ich zgodności z politykami bezpieczeństwa informacji i standardami obowiązującymi w Urzędzie.	Wdrożono skutecznie

Urząd Gminy Jasło	Polityka Ciągłości Działania	Strona	1
		Wydanie	I
		Data wydania	2026.03.16

POLITYKA CIĄGŁOŚCI DZIAŁANIA w Urzędzie Gminy Jasło

ZATWIERDZAM

WOJCIŚ
 Wojciech Wękoś 17.03.2026r
 (Podpis/pieczątka i data)

<i>Urząd Gminy Jasło</i>	<i>Polityka Ciągłości Działania</i>	<i>Strona</i>	1
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

POLITYKA CIĄGŁOŚCI DZIAŁANIA w Urzędzie Gminy Jasło

ZATWIERDZAM

(Podpis/pieczątka i data)

<i>Urząd Gminy Jasło</i>	<i>Polityka Ciągłości Działania</i>	<i>Strona</i>	3
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

SPIS TREŚCI

Skróty i definicje	4
Rozdział I. Cel i Zakres Systemu Zarządzania Ciągłością Działania	6
Rozdział II. Zapewnienie ciągłości pracy systemów informatycznych	7
Rozdział III. Zapewnienie ciągłości pracy sprzętu informatycznego	8
Rozdział IV. Zapewnienie ciągłości pracy w przypadku braku zasilania elektrycznego	9
Rozdział V. Zapewnienie ciągłości pracy w przypadku braku dostępu do Internetu	10

SPIS ZAŁĄCZNIKÓW

Załącznik 1. SZBI-003-01 Plan Ciągłości Działania

Urząd Gminy Jasło	Polityka Ciągłości Działania	Strona	4
		Wydanie	I
		Data wydania	2026.03.16

SKRÓTY I DEFINICJE

Bezpieczeństwo informacji - zachowanie poufności, integralności i dostępności informacji; dodatkowo, mogą być brane pod uwagę inne własności, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność

Zespół ds. cyberbezpieczeństwa - wewnętrzna struktura odpowiedzialna za cyberbezpieczeństwo w Urzędzie

Ciągłość działania - zdolność Urzędu Gminy do ciągłego świadczenia usług w akceptowalnych ramach czasowych przy zdefiniowanej wcześniej zdolności do działania w czasie zakłócenia

Naruszenie bezpieczeństwa informacji - przypadek, w którym użytkownik lub inna osoba pomija lub niszczy ustanowione zabezpieczenia lub środki ochrony w celu pozyskania nieuprawnionego dostępu do informacji lub do pozostałych zasobów systemu informatycznego

Plan ciągłości działania - udokumentowany zbiór procedur awaryjnych i informacji, które są opracowane, gromadzone i utrzymywane w stanie gotowym do użycia w przypadku wystąpienia incydentu, aby umożliwić Urzędowi kontynuowanie wykonywanych działań krytycznych na możliwym do przyjęcia wcześniej określonym poziomie

Plan odtworzeniowy - dokument zawierający szczegółowy opis postępowania w przypadku wystąpienia określonego zdarzenia (awarii lub katastrofy), mającego na celu usunięcie skutków lub przyczyn awarii lub katastrofy

UKSC – ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa

Zabezpieczenie - środki służące zarządzaniu ryzykiem, łącznie z politykami, procedurami, zaleceniami, praktyką lub strukturami organizacyjnymi, które mogą mieć naturę administracyjną, techniczną, zarządczą lub prawną

Zagrożenie - potencjalna przyczyna niepożądanego incydentu, który powoduje, że ryzyko materializuje się w postaci wymiernej straty poprzez wystawienie danych osobowych na utratę, ujawnienie, zniszczenie lub zmianę

Zagrożenie cyberbezpieczeństwa – potencjalna przyczyna wystąpienia incydentu

Zarządzanie incydemem - obsługa incydentu, wyszukiwanie powiązań między incydentami, usuwanie przyczyn ich wystąpienia oraz opracowywanie wniosków wynikających z obsługi incydentu

Zarządzanie ryzykiem - skoordynowane działania w zakresie zarządzania cyberbezpieczeństwem w odniesieniu do oszacowanego ryzyka; systematyczne stosowanie zasad zarządzania, procedur i praktyk na rzecz działań w zakresie informowania, konsultowania, tworzenia kontekstu oraz identyfikowania, analizy, oceny, postępowania z ryzykiem, monitorowania i przeglądania ryzyka związanego z przetwarzaniem informacji

Zarządzanie ciągłości działania - całościowy proces zarządzania identyfikujący potencjalne zagrożenia i skutki, jakie te zagrożenia mogą wywierać na działalność Urzędu w przypadku ich wystąpienia, który zapewnia kształtowanie odporności Urzędu i umożliwia skuteczną reakcję w celu ochrony interesów kluczowych interesariuszy tj. osób zaangażowanych w działalność Urzędu, reputacji i wizerunku Urzędu

Zarządzanie związane z bezpieczeństwem informacji - stwierdzone wystąpienie stanu systemu, usługi lub sieci, który wskazuje na możliwe naruszenie polityki bezpieczeństwa informacji lub błąd zabezpieczenia, lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem informacji

<i>Urząd Gminy Jasło</i>	<i>Polityka Ciągłości Działania</i>	<i>Strona</i>	5
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

Zespół ds. cyberbezpieczeństwa - zespół osób powołany Zarządzeniem Kierownika Jednostki, realizujący zadania wskazane w art. 8 pkt. 4 i 6, art. 11 ust. 1 pkt. 1-5, art. 12 i art. 13 UKSC

Zespół ds. Zarządzania Ciągłością działania - wewnętrzna struktura odpowiedzialna za zarządzanie ciągłością działania w Urzędzie powołana odrębnym Zarządzeniem Kierownika Jednostki

<i>Urząd Gminy Jasło</i>	<i>Polityka Ciągłości Działania</i>	<i>Strona</i>	6
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

ROZDZIAŁ I

CEL I ZAKRES SYSTEMU ZARZĄDZANIA CIĄGŁOŚCIĄ DZIAŁANIA

Polityka została wprowadzona w celu zapewnienia wszystkim stronom zainteresowanym dostępności krytycznych funkcji biznesowych w przypadku wystąpienia sytuacji kryzysowej oraz System Zarządzania Ciągłości Działania został wprowadzony według międzynarodowego standardu PN-EN ISO 22301:2020.

Główne cele Systemu Zarządzania Ciągłością Działania to:

- Zapobieganie niezaplanowanym przerwom w realizacji procesów i zadań Urzędu;
- Utrzymywanie właściwej i niezawodnej infrastruktury technicznej niezbędnej do ich realizacji;
- Monitorowanie i ograniczanie potencjalnych zagrożeń w środowisku pracy, w tym identyfikację i ocenę niepewnych, które mogą mieć wpływ na realizowane przez Urząd zadania;
- Stałe podnoszenie świadomości pracowników w zakresie utrzymania ciągłości działania i ich roli w przypadku wystąpienia sytuacji kryzysowej.

System Zarządzania Ciągłości Działania obejmuje swoim zakresem:

- 1) Wszystkie realizowane procesy oraz zadania w ramach działania jednostki;
- 2) Wszystkie zasoby będące własnością Urzędu lub przekazane jej przez kontrahentów w ramach realizacji obowiązujących umów, w tym:
 - a) personel;
 - b) budynki i pomieszczenia
 - c) sprzęt;
 - d) systemy, oprogramowanie i technologie pozwalające na przetwarzanie informacji;
 - e) wyznaczeni przez Urząd dostawcy usług, w tym eksperci techniczni.

<i>Urząd Gminy Jasło</i>	<i>Polityka Ciągłości Działania</i>	<i>Strona</i>	7
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

ROZDZIAŁ II

ZAPEWNIENIE CIĄGŁOŚCI PRACY SYSTEMÓW INFORMATYCZNYCH

Procedura zgłaszania awarii systemów informatycznych wykorzystywanych do przetwarzania danych osobowych i informacji w Urzędzie Gminy Jasło.

1. Każdy z użytkowników systemu informatycznego, w sytuacji wystąpienia awarii tego systemu, ma obowiązek niezwłocznego zgłoszenia awarii tego systemu Administratorowi Systemów Informatycznych (ASI).
2. ASI weryfikuje zasadność zgłoszenia, sprawdza czy zgłoszenie dot. zdarzenia spowodowanego awarią systemów informatycznych, ustala źródło awarii (przerwa w zasilaniu prądem, brak połączenia z siecią, wadliwe działanie sprzętu lub aplikacji).
3. ASI podejmuje niezwłoczne działania w celu usunięcia awarii lub zawiadamia niezwłocznie o wystąpieniu awarii osobę obsługującą Jednostkę pod względem informatycznym.
4. Jeżeli awaria jest na tyle skomplikowana, że osoba odpowiedzialna za naprawę nie jest w stanie dokonać naprawy w tym czasie, informuje o szacowanym czasie przywrócenia systemów.
5. ASI powiadamia o tym fakcie Kierownika Jednostki oraz właściwych kierowników
6. Do czasu usunięcia awarii systemu informatycznego, Urząd Gminy Jasło wykorzystuje dokumentację papierową, która po usunięciu awarii systemu informatycznego jest niezwłocznie wprowadzana przez upoważnioną osobę do systemu
7. Wzór dokumentacji papierowej wykorzystywanej alternatywnie w trakcie awarii systemu informatycznego nie musi być ściśle określony. Powinien jednak zawierać elementy niezbędne do kompletnego wprowadzenia danych osobowych do systemu informatycznego. Jeśli dostawca oprogramowania informatycznego przewidział taką sytuację, stosuje się szablony dokumentów papierowych dostarczonych przez dostawcę oprogramowania.
8. Po usunięciu awarii ASI lub dokonuje testu systemu oraz weryfikuje prawidłowość bazy danych, która jest uzupełniana o informacje wytworzone za pomocą zastępczej dokumentacji papierowej.
9. W przypadku uszkodzenia bazy danych należy wykorzystać kopię zapasową w celu przywrócenia poprawności systemu informatycznego.
10. Z czynności mających na celu przywrócenie pracy systemu, ASI sporządza odpowiedni protokół oraz w przypadku konieczności, ocenia z Inspektorem Ochrony Danych, czy incydent należy zgłosić do prezesa Urzędu Ochrony Danych, w tym ocenia skutki dla ochrony danych osobowych w podmiocie.

<i>Urząd Gminy Jasło</i>	<i>Polityka Ciągłości Działania</i>	<i>Strona</i>	8
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

ROZDZIAŁ III

ZAPEWNIENIE CIĄGŁOŚCI PRACY SPRZĘTU INFORMATYCZNEGO

Procedura zgłaszania awarii urządzeń wykorzystywanych do przetwarzania danych osobowych i informacji w Urzędzie Gminy Jasło:

1. Każdy z użytkowników, w sytuacji wystąpienia awarii sprzętu służącego do przetwarzania danych osobowych i informacji ma obowiązek niezwłocznego zgłoszenia awarii tego sprzętu ASI.
2. ASI weryfikuje zasadność zgłoszenia, sprawdza czy zgłoszenie dot. zdarzenia spowodowanego awarią sprzętu, ustala źródło awarii (przerwa w zasilaniu prądem, brak połączenia z siecią, wadliwe działanie sprzętu).
3. ASI podejmuje niezwłoczne działania w celu usunięcia awarii lub zawiadamia niezwłocznie o wystąpieniu awarii osobę obsługującą Urząd Gminy Jasło pod względem informatycznym.
4. Podjęcie diagnostyki w celu eliminacji awarii powinno nastąpić nie później niż w ciągu 2 godzin od zgłoszenia awarii, a sama awaria powinna zostać usunięta w ciągu 24 godzin od daty jej wystąpienia.
5. Do czasu usunięcia awarii Jednostka wykorzystuje dokumentację papierową, która po usunięciu awarii jest niezwłocznie wprowadzana przez upoważnioną osobę do systemu lub wykorzystywany jest inny sprzęt podmiotu.
6. Jeżeli awarii nie da się usunąć w ciągu 24 godzin, ASI zapewnia zapasowe urządzenie spełniające wymogi przepisów prawa i umożliwiające realizowanie świadczeń przez podmiot.
7. ASI powiadamia o tym fakcie Kierownika Jednostki oraz właściwych kierowników.

<i>Urząd Gminy Jasło</i>	<i>Polityka Ciągłości Działania</i>	<i>Strona</i>	9
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

ROZDZIAŁ IV

ZAPEWNIENIE CIĄGŁOŚCI PRACY W PRZYPADKU BRAKU ZASILANIA ELEKTRYCZNEGO

1. Każdy użytkownik systemu ma obowiązek niezwłocznego zgłoszenia braku zasilania sieci energetycznej w Urzędzie Gminy Jasło ASI lub na numer alarmowy, który jest wywieszony na tablicy ogłoszeń.
2. Użytkownik komputera przenośnego, zobowiązany jest do takiej organizacji pracy, aby zapewnić przez cały jej okres maksymalny poziom naładowania baterii, która umożliwi jego pracę bez zasilania, co najmniej przez 2 godziny.
3. Jeżeli użytkownik podejrzewa, że naprawa dostawy prądu może wydłużyć się ponad czas naładowania baterii jest zobowiązany do bezpiecznego przzerwania pracy i wyłączenia sprzętu komputerowego.
4. Do czasu usunięcia awarii prądu, Urząd Gminy Jasło wykorzystuje dokumentację papierową, która po usunięciu awarii systemu informatycznego jest niezwłocznie wprowadzana przez upoważnioną osobę do systemu.
5. Wzór dokumentacji papierowej wykorzystywanej alternatywnie w trakcie awarii systemu informatycznego nie musi być ściśle określony. Powinien jednak zawierać elementy niezbędne do kompletnego wprowadzenia danych osobowych do systemu informatycznego. Jeśli dostawca oprogramowania informatycznego przewidział taką sytuację, stosuje się szablony dokumentów papierowych dostarczonych przez dostawcę oprogramowania.
6. Jeżeli do przetwarzania danych osobowych i informacji użytkowane są komputery stacjonarne wyposażone są one w urządzenia UPS.
7. Jeżeli w Jednostce zlokalizowany jest serwer bazy danych wyposażony jest on w urządzenie UPS.
8. W przypadku braku zasilania użytkownik komputera stacjonarnego ma niezwłoczny obowiązek bezpiecznego zakończenia pracy i wyłączenia stacji roboczej.
9. W przypadku wystąpienia braku zasilania, jeśli serwer bazy danych nie ma takiej opcji, ASI lub upoważniony przez niego pracownik wyłącza serwer bazy danych.
10. W przypadku wyłączenia serwera baz danych w Jednostce, stosuje się zapisy, o których mowa w punktach 4-5 powyżej.

<i>Urząd Gminy Jasło</i>	<i>Polityka Ciągłości Działania</i>	<i>Strona</i>	10
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

ROZDZIAŁ V

ZAPEWNIENIE CIĄGŁOŚCI PRACY W PRZYPADKU BRAKU DOSTĘPU DO INTERNETU

1. Jeżeli użytkownik stwierdzi brak dostępu do sieci internetowej należy to zgłosić ASI lub na numer alarmowy, który jest wywieszony na tablicy ogłoszeń.
2. W przypadku konieczności użytkowania sieci i przedłużającej się awarii należy skorzystać z Internetu mobilnego dostępnego w Urzędzie Gminy Jasło jako alternatywne źródło.
3. Za uruchomienie łącza alternatywnego odpowiada ASI lub wskazana przez niego osoba.

Urząd Gminy Jasło	Plan Ciągłości Działania	Strona	1
		Wydanie	I
		Data wydania	2026.03.16

PLAN CIĄGŁOŚCI DZIAŁANIA w Urzędzie Gminy Jasło

ZATWIERDZAM
WÓJT
Wojciech Piękoś
 (Podpis/pieczątka i data)

<i>Urząd Gminy Jasło</i>	<i>Plan Ciągłości Działania</i>	<i>Strona</i>	1
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

PLAN CIĄGŁOŚCI DZIAŁANIA

w Urzędzie Gminy Jasło

ZATWIERDZAM

(Podpis/pieczątka i data)

<i>Urząd Gminy Jasło</i>	<i>Plan Ciągłości Działania</i>	<i>Strona</i>	3
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

CEL PROCEDURY

Celem procedury jest minimalizacja zakłóceń w realizacji działalności statusowej w związku z dysfunkcją systemu informatycznego Urzędu Gminy Jasło.

Aktualizacja formularzy powiązanych z niniejszym dokumentem nie wprowadza zmian do dokumentacji ochrony danych osobowych (SZBI) i nie wymaga ogłoszenia zarządzeniem.

PRZEDMIOT

Przedmiotem procedury jest postępowanie w przypadku zaistnienia zdarzeń mających wpływ (również potencjalny) na bezpieczeństwo informacji oraz ciągłość działania Urzędu Gminy Jasło.

ZAKRES STOSOWANIA

Zdefiniowanie działań koniecznych do podjęcia w przypadku dysfunkcji systemu informatycznego.

ODPOWIEDZIALNOŚĆ I UPRAWNIENIA

- Za opracowanie i utrzymanie niniejszego planu ciągłości działania odpowiedzialny jest ASI
- Za nadzór nad realizacją działań związanych z opracowaniem i utrzymaniem niniejszego planu ciągłości działania odpowiedzialny jest ASI
- Za realizację działań przewidzianych w niniejszym planie ciągłości działania odpowiedzialne są wskazane w nim osoby

OPIS POSTĘPOWANIA

1. Warunki uruchomienia planu

Plan uruchamiany jest w przypadku dysfunkcji systemu informatycznego, mającej wpływ na ciągłość działania Urzędu Gminy Jasło.

2. Osoby oraz zasoby wymagane do realizacji planu

O uruchomieniu planu decyduje Kierownik Jednostki

Urząd Gminy Jasło	Plan Ciągłości Działania	Strona	4
		Wydanie	I
		Data wydania	2026.03.16

DZIAŁANIA ZAPEWNIAJĄCE PRZYWRÓCENIE ZDOLNOŚCI REALIZACJI DZIAŁALNOŚCI STATUTOWEJ

L.p.	Funkcja	Opis działań	Potrzebne zasoby/ odpowiedzialni
1)	Zweryfikować zasadność zgłoszenia od użytkownika	Sprawdzić, czy zgłoszenie dotyczy zdarzenia spowodowanego awarią systemu informatycznego.	Zapewnić: ☐ dostęp do infrastruktury informatycznej na stanowisku, skąd pochodzi zgłoszenie. Odpowiedzialny: ASI
2)	Ustalić źródło awarii	Ustalić, co jest przyczyną awarii: ☐ przerwa w zasilaniu prądem, ☐ brak połączenia z siecią Internet, ☐ wadliwe działanie sprzętu, ☐ wadliwe działanie aplikacji, wadliwe działanie systemu, na którym uruchomiona jest aplikacja.	Zapewnić: ☐ dostęp do serwerowni oraz do sprzętu, który uległ awarii, ☐ kontakt z osobą, która może w porze nocnej pobrać klucze od Urzędu, ☐ w przypadku blokady zamka wezwać konserwatora, ☐ w przypadku awarii zasilania elektrycznego wezwać pogotowie ENERGETYCZNE-24h Odpowiedzialny: ASI
3)	Określić skalę awarii	Ustalić, czy awaria powoduje zatrzymanie pracy: ☐ jednego pomieszczenia pracy lub wydziału (od 1 do 6 osób) ☐ kilku wydziałów (od 7 do 25 osób) ☐ całego budynku urzędu lub wszystkich budynków urzędu	Zapewnić: ☐ kontakt z kluczowymi pracownikami wydziałów, lista z numerami telefonów. Odpowiedzialny: ASI
4)	Ustalić czy wznowianie usługi może odbywać się w dotychczasowej lokalizacji	Działanie ma na celu zweryfikowanie, czy wznowiane usługi uruchamiane będą w dotychczasowej lokalizacji, czy w lokalizacjach alternatywnych.	Zapewnić: ☐ możliwość uruchomienia dowolnych usług w lokalizacji: ☐ infrastrukturę sieciową, zasilanie prądem Odpowiedzialny: ASI

Urząd Gminy Jasło	Plan Ciągłości Działania	Strona	5
		Wydanie	I
		Data wydania	2026.03.16

5)	Zakupić niezbędne elementy wyposażenia, dokonać naprawy (wymiany) urządzeń, uruchomić aplikację	W przypadku braku możliwości zakupu należy znaleźć rozwiązanie alternatywne (np. zdecydować o przeniesieniu aplikacji na stałe na inny serwer).	Zapewnić: ☐ środki na zakup elementów niezbędnych do ponownego uruchomienia systemu. Odpowiedzialny: ASI
6)	Zweryfikować możliwość przeniesienia aplikacji na inny serwer	Sprawdzić, czy aplikacja może być uruchomiona na którymś z działających poprawnie serwerów.	Odpowiedzialny: ASI
7)	Przygotować serwer zastępczy	Jako serwer zastępczy można wykorzystać np. Komputer typu desktop, który należy odpowiednio skonfigurować. Po uruchomieniu aplikacji na serwerze zastępczym należy przetestować jej działanie.	Zapewnić: ☐ maszynę dowolnego typu, która w podstawowym zakresie pozwoli na uruchomienie podstawowych usług. Odpowiedzialny: ASI
8)	Podjąć decyzję o terminie odtworzenia maszyny	W razie konieczności należy skontaktować się z właściwymi kierownikami komórek organizacyjnych.	Zapewnić: ☐ kontakt z kluczowymi pracownikami wydziałów, lista z numerami telefonów. Odpowiedzialny: ASI
9)	Przywrócić funkcjonowanie aplikacji/ systemu	Spróbować usunąć przyczynę nieprawidłowego działania. W razie konieczności należy odtworzyć aplikację korzystając z kopii zapasowych.	Zapewnić: ☐ dostęp do najbardziej aktualnej wersji aplikacji, ☐ dostęp do aktualnej bazy danych. Odpowiedzialny: ASI
10)	Sprawdzenie aplikacji/ systemu	Po przeniesieniu / uruchomieniu należy zweryfikować prawidłowe funkcjonowanie aplikacji / systemów zainstalowanych na serwerze.	Zapewnić: ☐ kontakt z kluczowymi pracownikami wydziałów mogącymi przetestować prawidłowość funkcjonowania systemów i aplikacji. Odpowiedzialny: ASI

Urząd Gminy Jasło	Plan Ciągłości Działania	Strona	6
		Wydanie	I
		Data wydania	2026.03.16

11)	Uruchomienie usługi w systemie informatycznym Urzędu Gminy Jasło	Po uruchomieniu usługi należy powiadomić właściwych kierowników o tym fakcie.	Zapewnić: ☐ kontakt z kluczowymi pracownikami wydziałów, lista z numerami telefonów. Przygotować wykaz zewnętrznych jednostek usługowych realizujących zadania na rzecz Urzędu Gminy Jasło Odpowiedzialny: ASI
-----	--	---	--

TESTOWANIE PLANU

L.p.	Opis testu	Termin realizacji	Oczekiwany wynik	Osoba odpowiedzialna
1)	Symulacja wyłączenie serwera danej aplikacji, brak możliwości wykonywania usług, symulacja na podstawie scenariusza zawartego w protokole.	1 dzień	Wznowienie działania usługi, możliwie na nowej maszynie.	Odpowiedzialny: ASI

SZKOLENIE DLA UCZESTNIKÓW PLANU

Uczestnicy planu są zapoznawani z jego treścią każdorazowo przed przeprowadzeniem jego testowania.

AKTUALIZACJA PLANU

Plan aktualizowany jest każdorazowo w przypadku zmian kadrowych oraz w przypadku niepowodzenia w jego testowaniu.

<i>Urząd Gminy Jasło</i>	<i>Plan Ciągłości Działania</i>	<i>Strona</i>	7
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

Protokół z wykonania testu planu ciągłości działania

Nr protokołu

Jasło, dnia

1. Nazwa planu ciągłości działania:.....

2. Termin testu:

3. Osoba odpowiedzialna:

4. Osoby uczestniczące:

.....

.....

5. Osoba zatwierdzająca wynik testu:

6. Scenariusz testu:

.....

.....

.....

.....

.....

7. Wyniki:

.....

.....

.....

.....

.....

.....

8. Wnioski:

.....

.....

.....

.....

Podpis osoby odpowiedzialnej.....

Urząd Gminy Jasło	Polityka Bezpieczeństwa Fizycznego i Środowiskowego	Strona	1
		Wydanie	I
		Data wydania	2026.03.16

POLITYKA BEZPIECZEŃSTWA FIZYCZNEGO I ŚRODOWISKOWEGO w Urzędzie Gminy Jasło

ZATWIERDZAM

WOJT

Wojciech Kiekoś

(Podpis/pieczętka i data)

<i>Urząd Gminy Jasło</i>	<i>Polityka Bezpieczeństwa Fizycznego i Środowiskowego</i>	<i>Strona</i>	1
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

**POLITYKA
BEZPIECZEŃSTWA
FIZYCZNEGO I ŚRODOWISKOWEGO
w Urzędzie Gminy Jasło**

ZATWIERDZAM

(Podpis/pieczątka i data)

<i>Urząd Gminy Jasło</i>	<i>Polityka Bezpieczeństwa Fizycznego i Środowiskowego</i>	<i>Strona</i>	3
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

SPIS TREŚCI

Skróty i definicje	4
Rozdział I. Cel i Zakres Polityki Bezpieczeństwa Fizycznego i Środowiskowego	6
Rozdział II. Podstawowe zasady bezpieczeństwa fizycznego i środowiskowego	7
Rozdział III. Zapewnianie bezpieczeństwa fizycznego i środowiskowego	8
Rozdział IV. Zarządzanie uprawnieniami w systemie kontroli dostępu	10
Rozdział V. Pomieszczenia i zasoby chronione	10
Rozdział VI. Bezpieczeństwo środowiskowe	11
Rozdział VII. Eksploatacja technicznych systemów zabezpieczeń oraz systemów wspomagających	12
Rozdział VIII. Eksploatacja zabezpieczeń mechanicznych	14
Rozdział IX. Eksploatacja zabezpieczeń techniczno-budowlanych	15
Rozdział X. Eksploatacja elektronicznych systemów zabezpieczeń	16
Rozdział XI. Systemy transmisji sygnałów alarmowych do centrów monitoringu	17
Rozdział XII. Prowadzenie dokumentacji związanej z technicznymi systemami zabezpieczeń	18
Rozdział XIII. Zarządzanie zapisami pochodzącymi z elektronicznych systemów zabezpieczeń	18

SPIS ZAŁĄCZNIKÓW

Załącznik 1. SZBI-004 Rejestr Gości

Urząd Gminy Jasło	Polityka Bezpieczeństwa Fizycznego i Środowiskowego	Strona	4
		Wydanie	I
		Data wydania	2026.03.16

SKRÓTY I DEFINICJE

Administrator Danych Osobowych – Wójt Gminy Jasło

Jednostka – Urząd Gminy Jasło, ul. Słowackiego 4, 38-200 Jasło

SZBI - System Zarządzania Bezpieczeństwem Informacji

PBI – Polityka Bezpieczeństwa Informacji

Informacja poufna – wszelkie informacje, które są chronione przed dostępem osób trzecich oraz przed upublicznieniem. Dane osobowe wchodzi w skład informacji poufnych.

Dane osobowe – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Odbiorca – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Przy czym odbiorcą nie jest organ publiczny, który może otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii Europejskiej lub prawem państw członkowskiego.

Osoba upoważniona – osoba upoważniona przez administratora do przetwarzania danych osobowych, nad którą administrator sprawuje bezpośrednią kontrolę w procesie przetwarzania danych realizowanym przez tę osobę.

Incydent – pojedyncze zdarzenie lub seria niepożądanych zdarzeń związanych z bezpieczeństwem, które stwarzają znaczne prawdopodobieństwo zakłócenia działań lub ujawnienia informacji poufnych. Definiowany jest również jako naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Incydent poważny – incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej.

Sytuacja podejrzenia wystąpienia incydentu – pojedyncze zdarzenie lub seria niepożądanych zdarzeń związanych z bezpieczeństwem, które stwarzają znaczne prawdopodobieństwo zakłócenia działań lub ujawnienia informacji poufnych.

Hasło – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;

Usługa kluczowa – usługa, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej.

Przetwarzanie danych osobowych - jakiegokolwiek operacje lub zestaw operacji wykonywanych na danych osobowych.

Analiza ryzyka - systematyczne wykorzystanie informacji do zidentyfikowania źródeł i oszacowania ryzyka.

SKD – System Kontroli Dostępu

<i>Urząd Gminy Jasło</i>	<i>Polityka Bezpieczeństwa Fizycznego i Środowiskowego</i>	<i>Strona</i>	5
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

Upoważnienie - oświadczenie nadane przez administratora wskazujące z imienia i nazwiska osobę, która ma prawo przetwarzać dane w zakresie wskazanym w tym oświadczeniu, nad którą administrator sprawuje bezpośrednią kontrolę w procesie przetwarzania danych realizowanym przez tę osobę

Zabezpieczenie - środki służące zarządzaniu ryzykiem, łącznie z politykami, procedurami, zaleceniami, praktyką lub strukturami organizacyjnymi, które mogą mieć naturę administracyjną, techniczną, zarządczą lub prawną

Zagrożenie - niepożądane zdarzenie, które powoduje, że ryzyko materializuje się w postaci wymiernej straty poprzez wystawienie danych osobowych na utratę, ujawnienie, zniszczenie lub zmianę

System informatyczny - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych

<i>Urząd Gminy Jasło</i>	<i>Polityka Bezpieczeństwa Fizycznego i Środowiskowego</i>	<i>Strona</i>	6
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

ROZDZIAŁ I

CEL I ZAKRES POLITYKI BEZPIECZEŃSTWA FIZYCZNEGO I ŚRODOWISKOWEGO

Celem Polityki Bezpieczeństwa Fizycznego i Środowiskowego jest zapobiegnięcie nieuprawnionemu fizycznemu dostępowi do zasobów fizycznych Jednostki. Zapobieżenie szkodom i zakłóceniom jakie mogły być skutkiem nieuprawnionego dostępu do budynków i pomieszczeń. Dodatkowo w niniejszej polityce określone zostały zasady wykonywania przeglądów i konserwacji.

Działania opisane w niniejszej polityce obowiązują, we wszystkich oddziałach i komórkach organizacyjnych Urzędu Gminy Jasło. Niniejsza polityka jest elementem Systemu Zarządzania Bezpieczeństwem Informacji.

<i>Urząd Gminy Jasło</i>	<i>Polityka Bezpieczeństwa Fizycznego i Środowiskowego</i>	<i>Strona</i>	7
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

ROZDZIAŁ II

PODSTAWOWE ZASADY BEZPIECZEŃSTWA FIZYCZNEGO I ŚRODOWISKOWEGO

1. Środki bezpieczeństwa fizycznego obejmują:
 - 1) rozmieszczenia i granic stref bezpieczeństwa;
 - 2) konstrukcji budowlanych wyznaczających granice stref bezpieczeństwa;
 - 3) sposobu zabezpieczenia wejścia do obiektu oraz do stref bezpieczeństwa;
 - 4) stosowania bezpośredniej ochrony fizycznej;
 - 5) stosowania systemu sygnalizacji napadu i włamania;
 - 6) stosowania systemu monitoringu wizyjnego;
 - 7) stosowania mechanicznych zabezpieczeń technicznych;
 - 8) dostępu do obszarów bezpiecznych oraz wykonywanie prac w obszarach bezpiecznych.
2. Bezpieczeństwo środowiskowe obejmuje:
 - 1) stosowanie urządzeń ochrony przeciwpożarowej;
 - 2) zabezpieczenie przed zalaniem wodą;
 - 3) zapewnienie właściwych warunków pracy w zakresie temperatury i wilgotności powietrza;
 - 4) stosowanie środków ochrony odgromowej na liniach telekomunikacyjnych;
 - 5) stosowanie zabezpieczeń przeciwprzepięciowych.
3. Zakres stosowania środków bezpieczeństwa fizycznego i środowiskowego wynika z przeprowadzonego i udokumentowanego szacowania ryzyka.
4. Szacowanie ryzyka i określanie wymagań bezpieczeństwa przeprowadza się w oparciu o:
 - 1) charakterystykę obiektu i pełnione przez niego funkcję, w szczególności rodzaj umieszczonych w nim zasobów podlegających ochronie (ludzie, dokumentacja, sprzęt komputerowy, itp.);
 - 2) określenie kategorii potencjalnych zagrożeń;
 - 3) opis topografii, konstrukcji obiektu i architektury, najbliższego otoczenia (zabezpieczenia budowlane i mechaniczne, ogrodzenie, bramy, furty, oświetlenie, miejsca do parkowania, drogi komunikacyjne i ewakuacyjne, inne budowle i elementy towarzyszące);
 - 4) odnotowane w przeszłości czyny przestępcze (rodzaj i typ czynu przestępczego, działania zewnętrzne, wewnętrzne, data, rozmiary, wartość szkody, wynik śledztwa);
 - 5) aktualny stan bezpieczeństwa obiektu;
 - 6) opis i ocenę funkcjonalności i poprawności zainstalowanych technicznych systemów zabezpieczenia, ich poprawności eksploatacji i aktualny stan techniczny (poziom technologiczny, sprawność, dokumentacja, serwisowanie);
 - 7) aktualny stan ochrony fizycznej obiektu;

Urząd Gminy Jasło	Polityka Bezpieczeństwa Fizycznego i Środowiskowego	Strona	8
		Wydanie	I
		Data wydania	2026.03.16

- 8) opis stosowanych procedur i rozwiązań organizacyjnych;
- 9) wnioski co do odpowiedniości (w stosunku do rodzaju i stopnia zagrożeń) kompletności i poprawności zastosowanych zabezpieczeń (mechanicznych, technicznych i proceduralno-organizacyjnych);
- 10) propozycje doskonalenia systemów oraz procedur ochrony obiektu.

ROZDZIAŁ III

ZAPEWNIANIE BEZPIECZEŃSTWA FIZYCZNEGO I ŚRODOWISKOWEGO

1. Kadra kierownicza ustala podział powierzchni biurowych zajmowanych przez komórki i jednostki organizacyjne Jednostki na:
 - 1) strefy administracyjne, do których dostęp posiadają wszyscy pracownicy Urzędu;
 - 2) strefy bezpieczeństwa, do których dostęp jest ograniczony do osób posiadających specjalne prawa dostępu;
 - 3) strefy ogólnodostępnej, do której dostęp posiadają goście i inni interesanci.
2. Ochrona stref administracyjnych i stref bezpieczeństwa sprawowana jest na zasadach określonych w:
 - 1) przepisach o ochronie osób i mienia;
 - 2) planie ochrony obiektu (jeżeli został opracowany);
 - 3) niniejszej polityce.
3. Strefa bezpieczeństwa powinna być ustalona na obszarze wydzielonym solidnymi konstrukcjami budowlanymi. Za solidne konstrukcje budowlane uznaje się takie, których ściany zewnętrzne i stropy budynków, w których zlokalizowane są strefy bezpieczeństwa, posiadają klasę odporności włamaniowej równoważnej murowi o grubości 25 cm wykonanemu z pełnej cegły. Natomiast pomieszczenia stref bezpieczeństwa powinny mieć ściany o odporności włamaniowej równoważnej murowi o grubości 12,5 cm.
4. Wszystkie drzwi z kontrolą dostępu muszą być zaopatrzone w urządzenia samozamykające.
5. Pomieszczenia biurowe w strefie administracyjnej posiadają zamki klasy 0. Pomieszczenia w strefach bezpieczeństwa powinny posiadać zamki klasy C lub klasy 7 zabezpieczenia (wg normy PN-EN 12209:2005) oraz drzwi antywłamaniowe klasy C (wg normy PN-EN 1627:2011), z odpornością ogniową co najmniej 60 minut.
6. Wejście oraz wyjście ze stref bezpieczeństwa jest rejestrowane. Rejestruje się tożsamość osób, cel pobytu oraz czas ich wejścia i wyjścia. Wzór rejestru stanowi **załącznik SZBI-004-01 Rejestr gości – strefa bezpieczeństwa** do niniejszego dokumentu.

<i>Urząd Gminy Jasło</i>	<i>Polityka Bezpieczeństwa Fizycznego i Środowiskowego</i>	<i>Strona</i>	9
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

ROZDZIAŁ IV ZARZĄDZANIE UPRAWNIENIAMI W SYSTEMIE KONTROLI DOSTĘPU

1. W przypadku zastosowania systemu kontroli dostępu uprawnienia są jednoznacznie powiązane z urządzeniami aktywującymi przejście, które pełnią także rolę identyfikatorów.
2. Wstęp do poszczególnych stref jest ograniczony tylko do tych osób, które uzyskały stosowne uprawnienia.
3. Uprawnienia przyznawane są zgodnie z profilem dostępu (zakresem odpowiedzialności i uprawnień) na danym stanowisku pracy. Uprawnienia dostępu są nadawane wyłącznie w zakresie wynikającym z zajmowanego stanowiska i potrzebą wykonywania obowiązków służbowych na danym stanowisku pracy. Bezzasadne nadawanie uprawnień do pomieszczeń będzie kwalifikowane jako incydent związany z naruszeniem bezpieczeństwa informacji.
4. Za przyznawanie, zmianę oraz odbieranie uprawnień dostępu do stref bezpieczeństwa odpowiedzialny jest Kierownik Jednostki

ROZDZIAŁ V POMIESZCZENIA I ZASOBY CHRONIONE

1. Wnoszenie i wynoszenie do i ze stref bezpieczeństwa komputerowych nośników danych może mieć miejsce tylko w przypadkach wynikających z procedur eksploatacji zainstalowanego tam sprzętu teleinformatycznego.
2. Strefy bezpieczeństwa powinny być chronione systemem sygnalizacji włamania i napadu.
3. W uzasadnionych przypadkach, zarówno strefy administracyjne jak i strefy bezpieczeństwa, powinny być poddane monitoringowi wizyjnemu.
4. Strefy bezpieczeństwa nie posiadają oznakowania wewnątrz lub na zewnątrz, które wskazywałyby na to, że znajdują się w nich szczególnie chronione zasoby.
5. W strefach bezpieczeństwa dopuszcza się przebywanie osób bez uprawnień dostępu do tych stref tylko w wyjątkowych sytuacjach i za zezwoleniem dyrektora komórki organizacyjnej, któremu podlega dane pomieszczenie.
6. Serwery, aktywne i pasywne urządzenia sieci teleinformatycznej, centrale telefoniczne i archiwa muszą być umieszczone w strefach bezpieczeństwa.
7. Zasoby, którym nadano status zasobu kluczowego podlegają szczególnej ochronie i są dodatkowo zabezpieczane przed pożarem i zalaniem.

<i>Urząd Gminy Jasło</i>	<i>Polityka Bezpieczeństwa Fizycznego i Środowiskowego</i>	<i>Strona</i>	10
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

ROZDZIAŁ VI

BEZPIECZEŃSTWO ŚRODOWISKOWE

1. Przy planowaniu zabezpieczeń technicznych i organizacyjnych, ich rodzaju i siły, bierze się pod uwagę ryzyka związane z występującymi lokalnie zagrożeniami, takimi jak pożar, zalanie, trzęsienie ziemi, wybuch, wyładowania atmosferyczne, niepokoje społeczne i inne formy naturalnych lub spowodowanych przez działania umyślne bądź błędy człowieka katastrof. Ponadto analizie jest poddawany wpływ sąsiedztwa innych obiektów lub lokalnych instalacji i dróg (np. pożar w sąsiednim budynku, woda przeciekająca przez dach, powódź, bliska katastrofa komunikacyjna, eksplozja, zamieszki uliczne).
2. Pomieszczenia, w których zlokalizowane są zasoby kluczowe, wyposaża się w:
 - 1) system sygnalizujący wystąpienie pożaru;
 - 2) system klimatyzacji w serwerowniach.
3. Nie prowadzi się instalacji wodnych przez pomieszczenia, w których zlokalizowane są zasoby kluczowe do przetwarzania informacji (serwery, centra danych).
4. Urządzenia zapewniające bezpieczeństwo środowiskowe poddawane są regularnej kontroli zgodnie z obowiązującymi przepisami prawa, normami oraz zaleceniami producentów.
5. Na wypadek zagrożenia pożarem dla każdej z lokalizacji jednostek organizacyjnych Urzędu opracowuje się instrukcje przeciwpożarowe. Ciągi komunikacyjne obiektów muszą być zaopatrzone w tabliczki informujące o kierunku ewakuacji i w miarę potrzeby wyposażone w oświetlenie awaryjne.
6. Parametry środowiska, w którym pracuje sprzęt systemu teleinformatycznego zaliczany jest do zasobów kluczowych, tj. temperatura, jest monitorowana w celu natychmiastowego wykrycia odchyleń, które mogłyby mieć negatywne skutki dla tego sprzętu.
7. Budynek, w którym znajdują się systemy teleinformatyczne wskazane w ust. 6 powinien być wyposażony, zgodnie z przepisami ppoż., w samoczynnie załączające się oświetlenie awaryjne (bezpieczeństwa i ewakuacyjne).

<i>Urząd Gminy Jasło</i>	<i>Polityka Bezpieczeństwa Fizycznego i Środowiskowego</i>	<i>Strona</i>	11
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

ROZDZIAŁ VII

EKSPLOATACJA TECHNICZNYCH SYSTEMÓW ZABEZPIECZEŃ ORAZ SYSTEMÓW WSPOMAGAJĄCYCH

1. Systemy zabezpieczenia technicznego Urzędu muszą spełniać następujące funkcje:
 - 1) zabezpieczenia budowlane i zabezpieczenia mechaniczne muszą zagwarantować uniemożliwienie dostępu osobom niepowołanym do chronionych pomieszczeń i urzędów oraz zabezpieczyć osoby i mienie przed potencjalnymi zagrożeniami;
 - 2) system monitorowania w przypadku wystąpienia alarmu musi zapewnić podjęcie odpowiednich działań stosownych do zaistniałego zdarzenia;
 - 3) system monitoringu musi zapewnić, poprzez rozmieszczone kamery, rozpoznanie rodzaju zagrożenia i śledzenie rozwoju sytuacji, prowadzenie obserwacji obrazu z kilku kamer oraz automatyczną jednoczesną rejestrację tych obrazów;
 - 4) SKD musi zabezpieczyć chronione pomieszczenie (grupę pomieszczeń) lub wydzieloną strefę przed dostępem do nich osób nieuprawnionych.
2. Wszystkie systemy zabezpieczeń podlegają regularnym przeglądom dokonywanym przez osoby posiadające odpowiednie uprawnienia. Przegląd polega na sprawdzeniu poprawności działania danego systemu zgodnie z dokumentacją techniczno-eksploatacyjną systemu.
3. Przeglądy systemów zabezpieczeń poza ustalonym harmonogramem przeprowadzane są każdorazowo w przypadku wystąpienia incydentów zagrażających lub mogących powodować zagrożenie dla bezpieczeństwa osób i mienia (np. katastrofa budowlana w sąsiedztwie obiektu, tąpnięcie, kolizja drogowa powodująca szczególne zagrożenie w pobliżu budynku, pożar, roboty budowlane w sąsiednich budynkach, ewakuacja osób i mienia z budynku, interwencja służb ratunkowych mająca wpływ na stan techniczny obiektu, wystąpienie anomalii pogodowych, itp.).
4. Przeprowadzenie przeglądu odnotowuje się w dzienniku przeglądów prowadzonych dla każdego z funkcjonujących w Urzędzie systemów zabezpieczeń. Dziennik przeglądu zawiera następujące informacje:
 - 1) datę i czas przeglądu;
 - 2) dane personalne wykonującego przegląd;
 - 3) wynik przeglądu;
 - 4) dane personalne osoby nadzorującej/kontrolującej;
 - 5) uwagi z przeglądu.
5. Administrator Obiektu nadzoruje i dokumentuje bieżące prace konserwacyjne, w tym wymianę lub prostą naprawę elementów każdego z systemów zabezpieczeń, które nie wymagają posiadania stosownych uprawnień specjalistycznych. Pozostałe prace konserwacyjne wykonują pracownicy podmiotów zewnętrznych posiadający stosowne uprawnienia. Prace konserwacyjne polegają na wykonaniu niezbędnych czynności

Urząd Gminy Jasło	Polityka Bezpieczeństwa Fizycznego i Środowiskowego	Strona	12
		Wydanie	I
		Data wydania	2026.03.16

mających na celu utrzymanie systemu w sprawności techniczno-użytkowej zgodnie z dokumentacją techniczno-eksploatacyjną systemu. Prace konserwacyjne dla wszystkich systemów zabezpieczenia przeprowadzane są nie rzadziej niż raz na 12 miesięcy.

6. Wymiany lub naprawy o wysokim poziomie technologicznym dokonuje podmiot zewnętrzny posiadający stosowne uprawnienia producenta, dystrybutora wyrobu lub specjalistyczne urządzenia do naprawy lub wymiany.
7. Dla każdego systemu alarmowego oraz dla każdego innego systemu technicznego zabezpieczeń funkcjonującego w Urzędzie jest założony dziennik lub system rejestrowania zawierający:
 - 1) rejestr wyposażenia;
 - 2) rejestr zdarzeń;
 - 3) rejestr prac konserwacyjnych;
 - 4) rejestr prac serwisowych.

<i>Urząd Gminy Jasło</i>	<i>Polityka Bezpieczeństwa Fizycznego i Środowiskowego</i>	<i>Strona</i>	13
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

ROZDZIAŁ VIII

EKSPLOATACJA ZABEZPIECZEŃ MECHANICZNYCH

1. Do zabezpieczeń mechanicznych zalicza się: kraty, żaluzje, okiennice, folie antywłamaniowe, zamki w drzwiach (w szczególności te, do których bezpośredni dostęp mają osoby postronne), inne zabezpieczenia otworów okiennych, włazów, kanałów wentylacyjnych, rygle, klódki, zamki, zasuw z blokadą mechaniczną.
2. Zabezpieczenia mechaniczne muszą być zamontowane przez uprawniony podmiot zgodnie z warunkami technicznymi wynikającymi z certyfikatu lub aprobaty technicznej.
3. Zabezpieczenia mechaniczne podlegają przeglądom przeprowadzanym przez Administratora Obiektu, zgodnie z harmonogramem - dotyczy tylko tych zabezpieczeń, które są dostępne dla osób postronnych i nie ma możliwości realizacji nadzoru przez inne systemy zabezpieczeń.
4. Przeglądy polegają na sprawdzeniu stanu technicznego elementów zabezpieczenia mechanicznego, przeprowadzanych w następujący sposób:
 - 1) w przypadku krat, żaluzji, okiennic i innych zabezpieczeń otworów okiennych, włazów, kanałów wentylacyjnych:
 - a) sprawdzenie mocowań do murów (np. poprzez poruszenie elementów zabezpieczenia w pionie i poziomie i obserwacji reakcji elementów mocujących);
 - b) sprawdzenie istnienia odkształceń mechanicznych na poszczególnych elementach, przy zastosowaniu metody porównawczej z opisem w dokumentacji technicznej;
 - c) sprawdzenie występowania śladów po próbach penetracji lub usunięcia zabezpieczenia np. w postaci opiłków, śladów tynku, rysach na elementach zabezpieczeń, itp.;
 - d) sprawdzić stan powłok lakierniczych i zabezpieczeń antykorozyjnych elementów narażonych na bezpośrednie działanie czynników atmosferycznych lub innych szkodliwych czynników dla mechanizmów klódek, zamków, rygli (szczególnie kurz, pył);
 - 2) w przypadku klódek i zamków - sprawdzenie działania kluczy zapasowych oraz mechanizmu ryglującego przez otwarcie i zamknięcie klódek i zamków, przegród mechanicznych i budowlanych;
 - 3) w przypadku rygli i zasuw z blokadą mechaniczną - porównanie położenia elementów ruchomych z opisem w dokumentacji technicznej.
5. Wycofane z użycia elementy zabezpieczeń mechanicznych zawierające informacje o kodzie zamków (klucze, wkładki, karty elektroniczne) niszczone są mechanicznie.

<i>Urząd Gminy Jasło</i>	<i>Polityka Bezpieczeństwa Fizycznego i Środowiskowego</i>	<i>Strona</i>	14
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

ROZDZIAŁ IX

EKSPLOATACJA ZABEZPIECZEŃ TECHNICZNO-BUDOWLANYCH

1. Do zabezpieczeń techniczno-budowlanych zalicza się drzwi, śluzy, ściany, stropy, ogrodzenia (wykonane z różnych materiałów), furtki, bramy, zapory, szlabany, kołowroty (w szczególności te, do których bezpośrednio dostęp mają osoby postronne).
2. Zabezpieczenia techniczno-budowlane podlegają przeglądom przeprowadzanym przez Administratora Obiektu, zgodnie z harmonogramem - dotyczy tylko tych zabezpieczeń, które są dostępne dla osób postronnych i nie ma możliwości realizacji nadzoru przez inne systemy zabezpieczeń.
3. Przeglądy polegają na sprawdzeniu stanu technicznego elementów zabezpieczenia mechanicznego, przeprowadzanych w następujący sposób:
 - 1) sprawdzenie mocowań elementów ruchomych i elementów umocowanych na stałe do podłoża (np. poprzez poruszenie elementów konstrukcji zabezpieczenia i obserwacji reakcji elementów mocujących);
 - 2) sprawdzenie istnienia odkształceń mechanicznych na poszczególnych elementach, przy zastosowaniu metody porównawczej z opisem w dokumentacji technicznej;
 - 3) sprawdzenie występowania śladów po próbach penetracji lub usunięcia zabezpieczenia np. w postaci opiłków, śladów tynku, rysach na elementach zabezpieczeń, rdzy, itp.;
 - 4) sprawdzenie mechanizmów ryglowych (zamków, rygli, itp.);
 - 5) porównanie położenia elementów ruchomych z opisem w dokumentacji technicznej.
4. Wymiana/naprawa zabezpieczeń dokonywana jest pod nadzorem Administratora Obiektu.

<i>Urząd Gminy Jasło</i>	<i>Polityka Bezpieczeństwa Fizycznego i Środowiskowego</i>	<i>Strona</i>	15
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

ROZDZIAŁ X

EKSPLOATACJA ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZEŃ

1. Do elektronicznych systemów zabezpieczeń zalicza się Systemy Sygnalizacji Włamania i Napadu, Systemy Kontroli Dostępu oraz inne systemy współdziałające z elektronicznymi systemami zabezpieczeniowymi, np. system oświetlenia podczerwienią.
2. Elektroniczne systemy zabezpieczeniowe i systemy współdziałające podlegają przeglądom przeprowadzanym przez Administratora Obiektu zgodnie z harmonogramem i zakresem konserwacji systemu przeprowadzanej przez pracownika podmiotu zewnętrznego, posiadającego licencję pracownika zabezpieczenia technicznego.
4. Czynności konserwacyjne dokonywane przez pracownika podmiotu zewnętrznego są przeprowadzane nie rzadziej niż raz na 12 miesięcy i obejmują:
 - 1) sprawdzenie prawidłowości funkcjonowania systemu sygnalizacji włamania i napadu w zakresie określonym w dokumentacji technicznej;
 - 2) sprawdzenie ciągłości działania zasilania podstawowego i sprawności zasilania awaryjnego;
 - 3) sprawdzenie poprawności działania akustycznych lub optycznych sygnalizatorów alarmowych;
 - 4) sprawdzenie czujników systemu;
 - 5) sprawdzenie mocowania czujek do podłoża (uchwytów, ścian).
5. Przeglądy SKD są przeprowadzane przez Administratora Obiektu i obejmują, w zależności od zastosowanego rozwiązania technicznego, sprawdzenie:
 - 1) trybu pracy urządzeń wg wskazań paneli sterujących bądź aplikacji zarządzającej, poprzez porównanie z dokumentacją systemu;
 - 2) działania przycisków otwierających wyjścia z czytnikami działającymi jednostronnie, w tym działania przycisków ewakuacyjnych w przypadku, gdy SKD nie współpracuje z systemem ppoż.;
 - 3) działania czytników systemu z odpowiednią kartą dostępu;
 - 4) mocowania czytników, samozamykaczy, zamków elektromagnetycznych drzwi i przejść;
 - 5) ilości i rozmieszczenia czytników zgodnie z danymi w dzienniku systemu;
 - 6) limitu użytkowników systemu.
6. Czynności konserwacyjne dokonywane przez pracownika podmiotu zewnętrznego są przeprowadzane nie rzadziej niż raz na 12 miesięcy i obejmują sprawdzenie:
 - 1) prawidłowości funkcjonowania systemu SKD w zakresie określonym w dokumentacji technicznej;
 - 2) ciągłości działania zasilania podstawowego i sprawności zasilania awaryjnego, w tym wymiana akumulatorów zgodnie z harmonogramem załączonym do dokumentacji technicznej systemu;

Urząd Gminy Jasło	Polityka Bezpieczeństwa Fizycznego i Środowiskowego	Strona	16
		Wydanie	I
		Data wydania	2026.03.16

- 3) działania części elektromechanicznych (elektrozaczepów, trzymaczy elektromagnetycznych, śluz, tripodów itp.).

ROZDZIAŁ XI

SYSTEMY TRANSMISJI SYGNAŁÓW ALARMOWYCH DO CENTRUM MONITORINGU

1. Przeglądy systemu transmisji sygnałów alarmowych do centrów monitoringu są przeprowadzane przez podmiot zewnętrzny zgodnie z harmonogramem i obejmują sprawdzenie trybu pracy urządzenia wg wskazań paneli sterujących poprzez porównanie z dokumentacją systemu.
2. Czynności konserwacyjne dokonywane przez pracownika podmiotu zewnętrznego są przeprowadzane nie rzadziej niż raz na 12 miesięcy i obejmują:
 - 1) sprawdzenie ciągłości działania zasilania podstawowego i sprawności zasilania awaryjnego;
 - 2) sprawdzenie systemu anten, masztów, stanu uziemienia;
 - 3) sprawdzenie/potwierdzenie prawidłowego działania systemu/systemów w centrum monitoringu.

<i>Urząd Gminy Jasło</i>	<i>Polityka Bezpieczeństwa Fizycznego i Środowiskowego</i>	<i>Strona</i>	17
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

ROZDZIAŁ XII

PROWADZENIE DOKUMENTACJI ZWIĄZANEJ Z TECHNICZNYMI SYSTEMAMI ZABEZPIECZEŃ

1. Administrator Obiektu jest odpowiedzialny za prowadzenie wszelkich ewidencji, wykazów uprawnień, rejestrów, w tym rejestrów elektronicznych systemów zabezpieczeń.
2. Wszelka dokumentacja wskazana w ust. 1 jest klasyfikowana jako informacja wrażliwa.
3. Administrator Obiektu jest odpowiedzialny za aktualność i kompletność dokumentacji technicznych własnych systemów zabezpieczeń (tzn. dokumentacji powykonawczej, zmian w tej dokumentacji, aktualnych plików konfiguracyjnych systemów i urządzeń).

ROZDZIAŁ XIII

ZARZĄDZANIE ZAPISAMI POCHODZĄCYMI Z ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZEŃ

1. Administrator Obiektu jest odpowiedzialny za utrzymanie rejestrów elektronicznych własnych systemów zabezpieczeń. Okres przechowywania zapisów pochodzących z elektronicznych systemów zabezpieczeń powinien wynosić co najmniej 14 dni.
2. W przypadku powierzenia utrzymania rejestrów systemów kontroli dostępu, sygnalizacji napadu i włamania umowa z usługodawcą musi zapewniać Jednostce skuteczną kontrolę nad zapisami przez umieszczenie w niej:
 - 1) warunków i czasu przechowywania rejestrów (14 dni);
 - 2) wymagań bezpieczeństwa w odniesieniu do rejestrów;
 - 3) zasad dostępu Urzędu do przechowywanych zapisów, w tym uzyskania kopii stanowiących materiał dowodowy, jeśli zachodzi taka potrzeba;
 - 4) sposobów komunikowania się Jednostki z usługodawcą, w tym potwierdzenia dostarczenia kopii rejestrów w trybie awaryjnym;
 - 5) zakres odpowiedzialności usługodawcy za utratę lub uszkodzenie rejestrów.
3. W przypadku stwierdzenia incydentu naruszenia bezpieczeństwa informacji Administrator Obiektu wykonuje kopie rejestrów elektronicznych systemów zabezpieczeń dla celów dowodowych.

Urząd Gminy Jasło	Polityka Zarządzania Incydentami	Strona	1
		Wydanie	I
		Data wydania	2026.03.16

POLITYKA ZARZĄDZANIA INCYDENTAMI w Urzędzie Gminy Jasło

ZATWIERDZAM

Wojciech Pukos
 (Podpis/pieczątka i data)

<i>Urząd Gminy Jasło</i>	<i>Polityka Zarządzania Incydentami</i>	<i>Strona</i>	1
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

POLITYKA ZARZĄDZANIA INCYDENTAMI w Urzędzie Gminy Jasło

ZATWIERDZAM

(Podpis/pieczątka i data)

<i>Urząd Gminy Jasło</i>	<i>Polityka Zarządzania Incydentami</i>	<i>Strona</i>	3
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

SPIS TREŚCI

Skróty i definicje	4
Rozdział I. Cel i Zakres Polityki Zarządzania Incydentami.....	5
Rozdział II. Odpowiedzialność	5
Rozdział III. Przykłady sytuacji wystąpienia incydentu oraz podejrzenia wystąpienia incydentu	6
Rozdział IV. Zgłaszanie incydentu	7
Rozdział V. Obsługa incydentu	8

SPIS ZAŁĄCZNIKÓW

- Załącznik 1. SZBI-005-01 Formularz zgłoszenia incydentu
- Załącznik 2. SZBI-005-02 Rejestr incydentów

<i>Urząd Gminy Jasło</i>	<i>Polityka Zarządzania Incydentami</i>	<i>Strona</i>	4
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

SKRÓTY I DEFINICJE

Zespół ds. Cyberbezpieczeństwa – Zarządzania incydentami – zespół osobowy odpowiedzialny za proces zarządzania incydentami – przygotowanie, realizację działań w trakcie wystąpienia incydentu oraz działań likwidujących skutki wystąpienia incydentu.

Informacja poufna – wszelkie informacje, które są chronione przed dostępem osób trzecich oraz przed upublicznieniem. Dane osobowe wchodzą w skład informacji poufnych.

Dane osobowe – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Odbiorca – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Przy czym odbiorcą nie jest organ publiczny, który może otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii Europejskiej lub prawem państw członkowskiego.

Osoba upoważniona – osoba upoważniona przez administratora do przetwarzania danych osobowych, nad którą administrator sprawuje bezpośrednią kontrolę w procesie przetwarzania danych realizowanym przez tę osobę.

Incydent – pojedyncze zdarzenie lub seria niepożądanych zdarzeń związanych z bezpieczeństwem, które stwarzają znaczne prawdopodobieństwo zakłócenia działań lub ujawnienia informacji poufnych. Definiowany jest również jako naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Incydent poważny – incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej.

Sytuacja podejrzenia wystąpienia incydentu – pojedyncze zdarzenie lub seria niepożądanych zdarzeń związanych z bezpieczeństwem, które stwarzają znaczne prawdopodobieństwo zakłócenia działań lub ujawnienia informacji poufnych.

Hasło – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;

Usługa kluczowa – usługa, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, wymieniona w Rozporządzeniu Rady Ministrów z 11.09.2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych

<i>Urząd Gminy Jasło</i>	<i>Polityka Zarządzania Incydentami</i>	<i>Strona</i>	5
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

ROZDZIAŁ I

CEL I ZAKRES STOSOWANIA POLITYKI ZARZĄDZANIA INCYDENTAMI

Celem polityki zarządzania incydentami jest zapewnienie, że zdarzenia związane z bezpieczeństwem informacji oraz słabości systemów informacyjnych, są zgłaszane w sposób umożliwiający szybkie i możliwie najbardziej efektywne podjęcie działań korygujących przez określone osoby odpowiedzialne.

Działania opisane w niniejszej polityce obowiązują, we wszystkich oddziałach i komórkach organizacyjnych w Urzędzie Gminy Jasło. Niniejsza polityka jest elementem Systemu Zarządzania Bezpieczeństwem Informacji ustanowionego w Urzędzie Gminy Jasło.

ROZDZIAŁ II

ODPOWIEDZIALNOŚĆ

Odpowiedzialność za prawidłowe zgłoszenie incydentów dotyczących bezpieczeństwa spoczywa na wszystkich pracownikach Urzędu Gminy Jasło.

Odpowiedzialnymi za zapobieganie, rozwiązywanie oraz naprawę skutków wystąpienia incydentów bezpieczeństwa jest Zespół ds. Cyberbezpieczeństwa – Zarządzania incydentami, zwanym dalej Zespołem. W skład Zespołu wchodzi:

1. Administrator Systemów Informatycznych,
2. Inspektor Ochrony Danych Osobowych,
3. Biuro Zarządzania Kryzysowego

Zakres obowiązków Zespołu ds. Cyberbezpieczeństwa – Zarządzania incydentami w obszarze zarządzania incydentami:

1. Niezwłoczne reagowanie na incydenty bezpieczeństwa informacji w określony i z góry ustalony sposób.
2. Ocenę istniejących i potencjalnych zagrożeń w zakresie bezpieczeństwa informacji.
3. Ocenę przyczyn i skutków incydentów naruszenia bezpieczeństwa informacji w tym gromadzenie materiału dowodowego.
4. Przygotowywanie propozycji działań korygujących i naprawczych oraz nadzór nad ich wprowadzaniem.
5. Prowadzenie działań zmierzających do wzrostu świadomości w zakresie zapewnienia bezpieczeństwa informacji w Jednostce.
6. Współpracę z Rządowym Zespołem Reagowania na Incydenty Komputerowe CERT.

Urząd Gminy Jasło	Polityka Zarządzania Incydentami	Strona	6
		Wydanie	I
		Data wydania	2026.03.16

ROZDZIAŁ III

PRZYKŁADY SYTUACJI WYSTĄPIENIA INCYDENTU ORAZ PODEJRZENIA WYSTĄPIENIA INCYDENTU

1. Osoba nieuprawniona korzystająca z urządzenia, konta, profilu osoby uprawnionej.
2. Ujawnienia hasła dostępu osobie nieuprawnionej.
3. Znalezienie hasła dostępu zapisanego na papierze.
4. Wejście osoby nieuprawnionej do strefy chronionej.
5. Samodzielne instalowanie oprogramowania.
6. Awaria sprzętu lub oprogramowania, które wyraźnie wskazują naумыślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie systemu, a w tym sam fakt pozostawienia serwisantów bez nadzoru.
7. Jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie.
8. Stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji).
9. Nastąpiła niedopuszczalna manipulacja danymi w systemie.
10. Ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą elementy systemu zabezpieczeń (informacja poufna).
11. Praca w systemie lub w sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie np. sygnał o uporczywym nieautoryzowanym logowaniu, itp.
12. Ujawniono istnienie nie autoryzowanych kont dostępu do danych lub tzw. "bocznej furtki".
13. Podmieniono lub zniszczono nośniki z danymi bez odpowiedniego upoważnienia lub w niedozwolony sposób skasowano lub kopiowano dane osobowe.
14. Rażąco naruszono dyscyplinę pracy w zakresie przestrzegania Polityki Bezpieczeństwa Informacji (nie wylogowanie się, pozostawienie włączonego komputera po zakończeniu pracy, nie zamknięcie pokoju z komputerem, nie wykonywanie w ustalonych terminach kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.).
15. Stwierdzenie nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych, w tym także osobowych (otwarte szafy, regały, biurka).
16. Sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na infrastrukturę teleinformatyczną jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.
17. Niewłaściwe parametry środowiska jak zbyt wysoka temperatura lub nadmierna wilgotność (w szczególności dotyczy to serwerowni).

<i>Urząd Gminy Jasło</i>	<i>Polityka Zarządzania Incydentami</i>	<i>Strona</i>	7
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

ROZDZIAŁ IV ZGŁASZANIE INCYDENTÓW

Wszyscy pracownicy Urzędu Gminy Jasło są zobowiązani do zgłaszania zauważonych przez siebie incydentów, błędów oraz sytuacji podejrzanych jako incydenty. Zgłoszenie może nastąpić jedną z poniższych metod poprzez wypełnienie i przekazanie formularza zgłoszenia wystąpienia/ podejrzenia wystąpienia incyduentu dostępnego na stronie wewnętrznej Jednostki:

- kontakt elektroniczny z Działem Informatyki, e-mail: informatyk@urząd.gminajaslo.pl
- kontakt bezpośredni z Działem Informatyki Urzędu: tel. +48 134436636

Obsługa incydentów przez pracowników Urzędu Gminy Jasło została ograniczona jedynie do identyfikacji wystąpienia zdarzenia lub jego podejrzenia oraz jego zgłoszenia. Pełną obsługą incydentów zajmuje się Zespół ds. Cyberbezpieczeństwa – Zarządzania incydentami.

Zgłoszenie powinno obejmować:

1. Imię i nazwisko zgłaszającego;
2. Stanowisko zgłaszającego;
3. Numer telefonu zgłaszającego;
4. Adres e-mail zgłaszającego;
5. Data wystąpienia incyduentu;
6. Data wykrycia incyduentu;
7. Usługa lub obszar na który incydent ma wpływ;
8. Kategoria zdarzenia;
9. Opis incyduentu.

W celu ułatwienia procesu zgłaszania incydentów wprowadzono **Formularz zgłoszenia incyduentu** stanowiący załącznik 1 do niniejszej polityki.

<i>Urząd Gminy Jasło</i>	<i>Polityka Zarządzania Incydentami</i>	<i>Strona</i>	8
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

ROZDZIAŁ V OBSŁUGA INCYDENTÓW

Obsługa incydentów obejmuje działania podejmowane w przypadku wystąpienia zdarzenia oraz działań zapobiegawczych, przygotowawczych oraz działań po wystąpieniu incydentu. Proces obsługi incydentów przez zwykłych użytkowników została ograniczona jedynie do udziału w szkoleniach z zakresu bezpieczeństwa oraz identyfikacji i zgłaszania zdarzeń niepożądanych – incydentów. Proces pełnej obsługi incydentów został powierzony Zespołowi ds. Cyberbezpieczeństwa – Zarządzania incydentami.

Działania podejmowane przez Zespół:

1. Przygotowanie;
2. Identyfikacja incydentów;
3. Ograniczenie skutków incydentu;
4. Wdrożenie środków naprawczych;
5. Odzyskiwanie – przywracanie działania;
6. Wyciąganie wniosków.

Ad. 1. Przygotowanie

Przygotowanie jest fazą poprzedzającą wystąpienie incydentów. Jej głównym elementem jest wdrożenie, ustanowienie oraz zakomunikowanie podstawowych zasad bezpieczeństwa.

- 1) Szkolenie pracowników
Pracownicy wskazani przez Zespół i zatwierdzeni przez Kierownika Jednostki przynajmniej raz w roku odbywają szkolenie z zakresu cyberbezpieczeństwa. Przeprowadzenie szkolenia dokumentowane jest listą obecności. Szkolenia dla użytkowników obowiązkowo obejmują tematykę: identyfikacji zagrożeń; sposobów zgłaszania incydentów; podstawowych zasad bezpieczeństwa.
- 2) Identyfikacja znanych podatności
Ponadto Zespół ma obowiązek rozpoznawania znanych podatności. Proces realizuje poprzez utrzymywanie aktualnej wiedzy, pozyskiwania nowych informacji z zakresu cyberzagrożeń m.in. z portali: sekurak.pl; opensecurity.pl; zaufanatrzeciastrona.pl
- 3) Skanowanie podatności
Dodatkowo raz na 2 lata w Jednostce realizowany jest audyt bezpieczeństwa zawierający skanowanie podatności. Audyt realizowany jest przez jednostkę zewnętrzną. Wymaganiem stawianym jednostce zewnętrznej jest przygotowanie szeregu zaleceń po audytowych, których celem jest poprawa stanu bezpieczeństwa.
- 4) Usuwanie znanych podatności
W przypadku wykrycia lub otrzymania informacji o istnieniu podatności należy podjąć kroki w celu jej usunięcia. Odpowiedzialnym za usunięcie podatności w systemie informatycznym jest Administrator Systemów Informatycznych.

Urząd Gminy Jasło	Polityka Zarządzania Incydentami	Strona	9
		Wydanie	I
		Data wydania	2026.03.16

Ad. 2. Identyfikacja incydentów

Identyfikacja to właściwy początek obsługi incydu, w momencie spostrzeżenia przez użytkownika nieprawidłowości w systemie lub sieci oraz stwierdzeniu, iż atak ma miejsce należy dokonać wstępnej analizy incydu, określić jego źródła, a w szczególności zdarzenia na bezpieczeństwo danych. W tym momencie pracę rozpoczyna zespół reagowania na incydy.

W fazie identyfikacji incydu, Zespół podejmuje działania:

- 1) Jednoznacznie potwierdza zaistnienie incydu na podstawie wstępnych danych.
- 2) Klasyfikuje incydent zgodnie z przyjętą klasyfikacją, określa kategorię incydu (tabela 1 – Klasyfikacja incydentów) oraz jego istotność (tabela 2 – Istotność incydentów).
- 3) Określa zasoby, których dotyczy incydent (jakie systemy, które usługi, które dane są „dotknięte” incydem).

Tabela 1. Klasyfikacja incydentów (wg The European CSIRT Network)

1	Obrażliwe i nielegalne treści	spam, dyskredytacja, obrażanie, pornografia dziecięca, przemoc
2	Złośliwe oprogramowanie	wirus, robak sieciowy, koń trojański, oprogramowanie szpiegowskie, dialer
3	Gromadzenie informacji	skanowanie, podsłuch, inżynieria społeczna
4	Próby włamań	wykorzystanie znanych luk systemowych, próby nieuprawnionego logowania, wykorzystanie nieznanych luk systemowych
5	Włamania	włamanie na konta uprzywilejowane, włamanie na konto zwykłe, włamanie do aplikacji
6	Dostępność zasobów	atak blokujący serwis (DOS), rozproszony atak blokujący serwis (DDoS), sabotaż komputerowy
7	Bezpieczeństwo informacji	nieuprawniony dostęp do informacji, nieuprawniona zmiana informacji
8	Oszustwa komputerowe	nieuprawnione wykorzystanie zasobów, naruszenie praw autorskich, kradzież tożsamości, podszywanie się
9	Inne incydy	inne

Waga występujących incydentów określana jest na podstawie Tabela.2., gdzie najważniejszym elementem jest dostępność usługi.

Tabela 2. Istotności incydentów

Istotność incydu	Skutki finansowe	Skutki prawne	Skutki reputacyjne	Skutki technologiczne (niedostępność usługi kluczowej)
R0 – krytyczna	powyżej 500tys.	niezgodność z wymaganiami prawa	negatywne opinie w skali kraju	powyżej 24 godzin
R1 – wysoka	do 500 tys.	niezgodność z wymaganiami prawa	negatywne opinie w skali kraju	do 24 godzin
R2 – średnia	do 100 tys.	-	negatywne opinie w skali kraju	-
R3 – niska	do 5 tys.	-	negatywne opinie w skali lokalnej	-

Urząd Gminy Jasło	Polityka Zarządzania Incydentami	Strona	10
		Wydanie	I
		Data wydania	2026.03.16

Incydenty klasy R3 mogą być realizowane przez Informatyka oraz Inspektora Ochrony Danych Osobowych Urzędu Gminy Jasło.

Incydenty klasy R2 – R0 muszą być realizowane w pełnym Zespole ds. Cyberbezpieczeństwa – Zarządzania incydentów. Dodatkowo w przeciągu godziny od wykrycia incyduentu musi zostać poinformowany Kierownik Jednostki.

Wszystkie występujące incydenty podlegają ewidencji w załączniku do niniejszej polityki – załącznik 2 - **SZBI-005-02 Rejestr incydentów**. Odpowiedzialnym za uzupełnianie rejestru jest Administrator Systemów Informatycznych.

Incydent poważny

Jest to incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowe. Wszystkie incydenty poważne otrzymują klasę R0.

Jako incydenty poważne określany jest jako:

- 1) Incydent, który doprowadził do braku dostępności usługi kluczowej powyżej 24 godzin.
- 2) Incydent, który spowodował co najmniej jedną z poniżej wymienionych okoliczności:
 - śmierć człowieka,
 - ciężki uszczerbek na zdrowiu,
 - inny niż ciężki uszczerbek na zdrowiu więcej niż jednej osoby,
 - brak poufności danych przetwarzanych w usłudze,
 - brak integralności danych przetwarzanych w usłudze.

Incydenty poważne poza wpisaniem do rejestru oraz reakcją na nie, podlegają dodatkowo zgłoszeniu do CSIRT NASK. Czas na zgłoszenie incyduentu wynosi 24 godziny.

Odpowiedzialnym za dokonywanie zgłoszeń jest Administrator Systemów Informatycznych.

Zgłoszenie powinno zawierać:

- 1) Dane podmiotu zgłaszającego, w tym numer we właściwym rejestrze, siedzibę i adres
- 2) Imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby dokonującej zgłoszenia
- 3) Imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby uprawnionej do składania wyjaśnień dotyczących zgłaszanych informacji
- 4) Opis wpływu incyduentu poważnego na świadczenie usługi kluczowej, w tym:
 - usługi kluczowe zgłaszającego, na które incydent poważny miał wpływ,
 - liczbę użytkowników usługi kluczowej, na których incydent poważny miał wpływ,
 - moment wystąpienia i wykrycia incyduentu poważnego oraz czas jego trwania,
 - zasięg geograficzny obszaru, którego dotyczy incydent poważny,
 - wpływ incyduentu poważnego na świadczenie usługi kluczowej przez innych operatorów usług kluczowych i dostawców usług cyfrowych,
 - przyczynę zaistnienia incyduentu poważnego i sposób jego przebiegu oraz skutki jego oddziaływania na systemy informacyjne lub świadczone usługi kluczowe.
- 5) Informacje umożliwiające CSIRT NASK określenie, czy incydent dotyczy dwóch lub większej liczby państw członkowskich Unii Europejskiej

Urząd Gminy Jasło	Polityka Zarządzania Incydentami	Strona	11
		Wydanie	I
		Data wydania	2026.03.16

- 6) W przypadku incydentu, który mógł mieć wpływ na świadczenie usługi kluczowej, opis przyczyn tego incydentu, sposób jego przebiegu oraz prawdopodobne skutki oddziaływania na systemy informacyjne
- 7) Informacje o podjętych działaniach zapobiegawczych
- 8) Informacje o podjętych działaniach naprawczych
- 9) Inne istotne informacje

Wszystkie incydenty poważne muszą być zgłaszane do CSIRT, zgłaszanie pozostałych incydentów jest nieobowiązkowe.

W celu zgłaszania incydentów wykorzystywana jest platforma: *incydent.cert.pl*

Ad. 3. Ograniczanie skutków incydentów

Po dokonaniu analizy incydentu i zaangażowaniu odpowiednich stron należy podjąć kroki mające na celu zminimalizowanie skutków ataku, ograniczenie jego rozmiarów oraz zapobieganie dalszym szkodom.

- 1) Jeśli to możliwe należy jak najszybciej zapobiec rozprzestrzenianiu się ataku do innych systemów/sieci odłączając zainfekowany obszar oraz źródło ataku
- 2) Nie należy korzystać z zainfekowanego systemu, gdyż pliki, w których zostały zapisane dowody potwierdzające szkodliwą działalność hakera, mogą ulec modyfikacjom
- 3) Należy znaleźć wszystkie pliki używane przez atakującego i ocenić skalę zagrożenia
- 4) Jeśli atak został zatrzymany można przejść do zwalczania jego skutków

Ad. 4. Wdrożenie środków naprawczych

W zależności od rodzaju incydentu należy usunąć wszelkie złośliwe oprogramowanie oraz podejrzane pliki, zlikwidować w systemie luki wykorzystane przez atakującego. Jeżeli atak miał źródło wewnątrz organizacji, należy ograniczyć dostęp do kont osobom zaangażowanym w incydent, wyciągnąć konsekwencje wobec tych osób. Ponadto należy zabezpieczyć dowody, zlikwidować skutki szkodliwej działalności i jeśli to konieczne powiadomić organy ścigania.

Ad. 5. Odzyskiwanie – przywracanie działania

Jeżeli poprzednie kroki zostały wykonane poprawnie, atak został zatrzymany, jego źródło odłączone, a szkodliwa działalność oraz jej skutki zostały usunięte, można przejść do przywracania stanu sprzed ataku.

- 1) Wznowić ponownie ruch sieciowy oraz podłączyć do sieci zainfekowany obszar (o ile był odłączony)
- 2) Jeśli zachodzi prawdopodobieństwo, że którekolwiek z haseł użytkowników mogło zostać złamane, należy zmienić wszystkie hasła w danym systemie
- 3) W przypadku, gdy uszkodzeniu lub zainfekowaniu uległ system, najlepszym rozwiązaniem jest jego ponowna instalacja z kopii zapasowej utworzonej przed atakiem lub z oryginalnego nośnika

<i>Urząd Gminy Jasło</i>	<i>Polityka Zarządzania Incydentami</i>	<i>Strona</i>	12
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

Ad. 6. Wyciąganie wniosków

Ostatnim etapem jest udokumentowanie szczegółów incydentu oraz wyciągnięcie wniosków na podstawie sporządzonego raportu.

Raport powinien zawierać następujące elementy:

1. Przyczynę incydentu;
2. Opis wszystkich podejmowanych działań i procesów;
3. Skutki ataku;
4. Wnioski.

Urząd Gminy Jasło	Formularz zgłoszenia incydentu	Strona	1
		Wydanie	I
		Data wydania	2026.03.16

Zgłaszający incydent		
Imię i nazwisko*:		
Stanowisko:		
E-mail:		
Tel.:		
Opis incydentu		
Data wystąpienia incydentu:		
Data wykrycia incydentu*:		
Usługa lub obszar na które incydent miał wpływ:		
Kategoria zdarzenia:	☐	Podjęta wiadomość e-mail podejrzone załączniki, phishing, szantaż;
	☐	Złośliwe oprogramowanie trojan, banker, spyware, ransomware, zagrożenia mobilne;
	☐	Oszustwa internetowe fałszywa działalność w sieci, kradzież tożsamości;
	☐	Włamania serwer, aplikacja, konto, system, itp
	☐	Utrata dostępności usługi DoS, DDoS, sabotaż, awaria, zaniedbanie, prace techniczne;
	☐	Naruszenia bezpieczeństwa informacji nieuprawniony dostęp do informacji, nieuprawniona zmiana informacji lub jej skasowanie;
	☐	Podatności błędy w oprogramowaniu lub aplikacjach
	☐	Nielegalne treści;
	☐	Inne.
Opis incydentu*:		

*pola obowiązkowe

<i>Urząd Gminy Jasło</i>	<i>Rejestr incydentów</i>	<i>Strona</i>	1
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

**REJESTR INCYDENTÓW CYBERBEZPIECZEŃSTWA
w Urzędzie Gminy Jasło**

L.p.	Data zgłoszenia	Zadanie publiczne, którego dotyczy zgłoszenie	Opis zdarzenia	Kategoria incydentu	Podjęte działania zapobiegawcze	Podjęte działania naprawcze

Kategorie incydentu:

A – Podejrzana wiadomość e-mail

B – Próba oszustwa

C – Podatności

D – Złośliwe oprogramowanie

E – Nielegalne treści

F – Inny incydent

Urząd Gminy Jasło	Polityka Audytu Wewnętrznego	Strona	1
		Wydanie	I
		Data wydania	2026.03.16

POLITYKA AUDYTU WEWNĘTRZNEGO w Urzędzie Gminy Jasło

ZATWIERDZAM

Wojciech Piękoś

(Podpis/pieczątka i data)

<i>Urząd Gminy Jasło</i>	<i>Polityka Audytu Wewnętrznego</i>	<i>Strona</i>	1
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

POLITYKA AUDYTU WEWNĘTRZNEGO w Urzędzie Gminy Jasło

ZATWIERDZAM

(Podpis/pieczątka i data)

<i>Urząd Gminy Jasło</i>	<i>Polityka Audytu Wewnętrznego</i>	<i>Strona</i>	3
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

SPIS TREŚCI

Skróty i definicje	4
Rozdział I. Cel i Zakres Polityki Audytu Wewnętrznego	6
Rozdział II. Planowanie audytów	7
Rozdział III. Wybór audytorów	7
Rozdział IV. Przeprowadzanie audytu wewnętrznego	8

SPIS ZAŁĄCZNIKÓW

- Załącznik 1. SZBI-006-01 Harmonogram audytów
- Załącznik 2. SZBI-006-02 Raport z audytu wewnętrznego
- Załącznik 3. SZBI-00-03 Lista kontrolna audytu wewnętrznego

Urząd Gminy Jasło	Polityka Audytu Wewnętrznego	Strona	4
		Wydanie	I
		Data wydania	2026.03.16

SKRÓTY I DEFINICJE

Administrator Danych Osobowych – Urząd Gminy Jasło, ul. Słowackiego 4, 38-200 Jasło

SZBI - System Zarządzania Bezpieczeństwem Informacji

PBI – Polityka Bezpieczeństwa Informacji

Zespół ds. Obsługi Incydentów – zespół osobowy odpowiedzialny za proces zarządzania incydentami – przygotowanie, realizację działań w trakcie wystąpienia incyduentu oraz działań likwidujących skutki wystąpienia incyduentu.

Informacja poufna – wszelkie informacje, które są chronione przed dostępem osób trzecich oraz przed upublicznieniem. Dane osobowe wchodzą w skład informacji poufnych.

Dane osobowe – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Odbiorca – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Przy czym odbiorcą nie jest organ publiczny, który może otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii Europejskiej lub prawem państw członkowskiego.

Osoba upoważniona – osoba upoważniona przez administratora do przetwarzania danych osobowych, nad którą administrator sprawuje bezpośrednią kontrolę w procesie przetwarzania danych realizowanym przez tę osobę.

Incydent – pojedyncze zdarzenie lub seria niepożądanych zdarzeń związanych z bezpieczeństwem, które stwarzają znaczne prawdopodobieństwo zakłócenia działań lub ujawnienia informacji poufnych. Definiowany jest również jako naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Incydent poważny – incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej.

Sytuacja podejrzenia wystąpienia incyduentu – pojedyncze zdarzenie lub seria niepożądanych zdarzeń związanych z bezpieczeństwem, które stwarzają znaczne prawdopodobieństwo zakłócenia działań lub ujawnienia informacji poufnych.

Hasło – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;

Usługa kluczowa – usługa, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej.

Przetwarzanie danych osobowych - jakiekolwiek operacje lub zestaw operacji wykonywanych na danych osobowych.

Audyt - działania mające na celu oceny danej osoby, Jednostki, systemu, procesu, zabezpieczenia mające na celu potwierdzenie spełnienia konkretnych wymagań.

Analiza ryzyka - systematyczne wykorzystanie informacji do zidentyfikowania źródeł i oszacowania ryzyka.

Wewnętrzny audyt - audyt przeprowadzany dla potrzeb własnych Urzędu, zazwyczaj przez swoich pracowników lub osoby powołane z zewnątrz przez Pełnomocnika.

<i>Urząd Gminy Jasło</i>	<i>Polityka Audytu Wewnętrznego</i>	<i>Strona</i>	5
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

Wewnętrzny audyt planowy – audyt ujęty w rocznym programie audytów wewnętrznych.

Wewnętrzny audyt pozaplanowy - audyt nieujęty w rocznym programie audytów przeprowadzany ze względu na pogorszenie się jakości, wzrost ilości reklamacji, zmiany organizacyjne, zmiany w przepisach, uwagi w protokołach pokontrolnych instytucji administracji państwowej lub innych nadrzędnych.

Audyt – osoba posiadająca kompetencje do przeprowadzania audytu.

Wymagania stawiane audytorowi:

- wykształcenie wyższe lub średnie
- znajomość organizacji i Systemu Zarządzania Jakością,
- świadectwo ukończenia kursu na audytora organizowanego przez uznane jednostki w zakresie systemów zarządzania jakością.

Audyt wyznaczony do kierowania audytem określany jest audytorem wiodącym

Audytor – organizacja/ komórka, która jest organizowana.

Niezgodność – niespełnienie wymagania.

Działanie korygujące – działania podejmowane w celu wyeliminowania przyczyny wykrytej niezgodności lub innej niepożądaney sytuacji.

<i>Urząd Gminy Jasło</i>	<i>Polityka Audytu Wewnętrznego</i>	<i>Strona</i>	6
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

ROZDZIAŁ I

CELE I ZAKRES POLITYKI AUDYTU WEWNĘTRZNEGO

Celem polityki jest określenie:

1. Czy działania w zakresie zarządzania jakością są zgodne z:
 - a) zaplanowanymi ustaleniami;
 - b) wymaganiami norm ISO 9001:2015;
 - c) obowiązującymi przepisami;
 - d) standardami akredytacyjnymi.
2. Czy System Zarządzania Jakością spełnia wymagania ustanowione przez Urząd Gminy Jasło oraz czy jest skutecznie wdrożony i utrzymywany?

Polityka obejmuje swoim zakresem:

1. Wszystkie realizowane procesy oraz zadania w ramach działania jednostki.
2. Wszystkie informacje przetwarzane przez jednostkę w ramach wykonywania działań wynikających z jej działalności, w tym:
 - a) informacje przetwarzane w formie tradycyjnej – papierowej;
 - b) informacje przetwarzane w formie elektronicznej;
 - c) informacje przetwarzane w formie ustnej – wypowiedziane słownie;
 - d) inne informacje będące własnością Jednostki lub przekazane jej przez kontrahentów w ramach realizacji obowiązujących umów.
3. Wszystkie Zasoby będące własnością Jednostki lub przekazane jej przez kontrahentów w ramach realizacji obowiązujących umów, w tym:
 - a) personel;
 - b) budynki i pomieszczenia;
 - c) sprzęt;
 - d) systemy, oprogramowanie i technologie pozwalające na przetwarzanie informacji.

<i>Urząd Gminy Jasło</i>	<i>Polityka Audytu Wewnętrznego</i>	<i>Strona</i>	7
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

ROZDZIAŁ II

PLANOWANIE AUDYTÓW

Kierownik Jednostki zatwierdza roczny harmonogram audytów wewnętrznych określony w **załączniku SZBI-006-01 Harmonogram audytów**.

W ciągu jednego roku należy przeprowadzić jeden lub więcej audytów wewnętrznych, tak aby pokryć swoim zakresem całość zakresu Systemu Zarządzania bezpieczeństwem Informacji. Audyty wewnętrzne planuje się w oparciu o szacowanie ryzyka oraz o wyniki poprzednich audytów.

Roczny program audytu wewnętrznego SZBI musi zawierać następujące informacje dotyczące każdego audytu wewnętrznego:

- okres audytu (dokładne daty lub miesiąc, w którym planowany jest audyt)
- zakres audytu (działy, procesy, rozdziały normy itp.)
- kryteria audytu (normy, prawo i przepisy, dokumentacja wewnętrzna, standardy korporacyjne i/lub zobowiązania umowne)
- metody audytowania (przegląd dokumentacji, wywiady z pracownikami, przegląd rejestrów, przegląd systemów informacyjnych itd.)
- kto będzie przeprowadzać audyt (jeśli będzie to więcej niż jeden audytor, należy podać, kto jest kierownikiem zespołu audytującego)

Przeprowadzone audyty muszą być odnotowane w harmonogramie audytów wewnętrznych.

ROZDZIAŁ III

WYBÓR AUDYTORÓW

Kierownik Jednostki wyznaczy audytorów wewnętrznych. Audytorem wewnętrznym może być ktoś z wewnątrz lub z zewnątrz organizacji. Kryteria wyboru osób na funkcję audytora wewnętrznego są następujące:

- znajomość ISO/IEC 27001
- znajomość wymagań prawnych i regulacyjnych
- znajomość technik audytu systemów zarządzania bezpieczeństwem informacji
- wiedza dotycząca funkcjonowania technologii informacyjnych i komunikacyjnych wystarczająca do zrozumienia celów działania audytowanych systemów, jak również wpływu tych technologii na bezpieczeństwo

Audytorzy wewnętrzni muszą być wybierani w sposób zapewniający ich obiektywność i niezależność tj. z zapewnieniem unikania konfliktów interesów – audytorzy nie mogą bowiem oceniać wyników swojej własnej pracy. Zaleca się, aby audytorzy wewnętrzni ukończyli szkolenie dla audytorów wewnętrznych wg. norm ISO/IEC 27001.

<i>Urząd Gminy Jasło</i>	<i>Polityka Audytu Wewnętrznego</i>	<i>Strona</i>	8
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

ROZDZIAŁ IV

PRZEPROWADZANIE AUDYTU WEWNĘTRZNEGO

Osoby odpowiedzialne za audyty wewnętrzne wskazane są w rocznym planie audytu wewnętrznego - **SZBI-006-01 Harmonogram audytów**. Jeśli audyt przeprowadzany jest przez zespół składający się z kilku audytorów, osoba odpowiedzialna za dany audyt wskazana jest jako Audytor wiodący. Audytor wiodący odpowiada za przeprowadzenie i udokumentowanie wyników audytu w raporcie z audytu. Podczas audytu wewnętrznego należy wziąć pod uwagę:

- kryteria określone w **SZBI-006-01 Harmonogram audytów**
- wyniki poprzednich audytów wewnętrznych lub zewnętrznych
- wyniki szacowania ryzyka, wdrożenie zabezpieczeń, analizę wpływu na działalność itd.
- listę kontrolną audytu wewnętrznego – załącznik 3 - **SZBI-006-03 Lista kontrolna audytu wewnętrznego**

Po wykonaniu audytu wewnętrznego audytorzy opracowują i zachowują następujące dokumenty:

- raport z audytu wewnętrznego – załącznik 2 - **SZBI-006-02 Raport z audytu wewnętrznego**
- proponowane działania korygujące w przypadku wystąpienia niezgodności

Raport z audytu wewnętrznego jest przekazany do Kierownika Jednostki oraz kierownictwa audytowanych obszarów. W przypadku wystąpienia niezgodności niezwłocznie podejmuje się działania korygujące. Wyniki audytów wewnętrznych są daną wejściową do okresowych przeglądów zarządzania.

Urząd Gminy Jasło	Raport z audytu wewnętrznego	Strona	1
		Wydanie	I
		Data wydania	2026.03.16

Raport z audytu wewnętrznego

Raport z Audytu Wewnętrznego w Urzędzie Gminy Jasło	Termin przeprowadzenia audytu.....	Nr audytu:.....
<u>Cel audytu:</u>		
<u>Zakres audytu:</u>		
<u>Kryteria audytu:</u>		
<u>Zespół audytorów:</u>		
<u>Audytowane obszary/zabezpieczenia:</u>		
<u>Zestawienie niezgodności:</u> (proszę wskazać punkt normy dla każdej niezgodności)		
<u>Zestawienie uwag/ obserwacji do doskonalenia:</u>		
<u>Ustalenia i wnioski:</u>		
<u>Podsumowanie/uwagi:</u> (rozbieżne stanowiska, sprawy sporne, napotkane przeszkody)		

Podpis audytora wiodącego

.....

Zatwierdził raport

.....

Urząd Gminy Jasło	Lista kontrolna audytu wewnętrznego	Strona	1
		Wydanie	I
		Data wydania	2026.03.16

Lista kontrolna audytu wewnętrznego

Pkt. wymagań	Wymaganie normy ISO/IEC 27001	Zgodność Tak/Nie	Dowody
4.2	Czy organizacja określiła zainteresowane strony?		
4.2	Czy istnieje lista wszystkich zainteresowanych stron?		
4.3	Czy zakres jest udokumentowany, włącznie z jasno określonymi granicami i interfejsami?		
5.1	Czy ogólne cele SZBI są zgodne ze strategicznymi kierunkami działania?		
5.1	Czy kierownictwo zapewnia realizację celów SZBI?		
5.2	Czy istnieje Polityka bezpieczeństwa informacji z określonymi celami lub założeniami służącymi do określenia celów?		
5.2	Czy w organizacji komunikuje się Politykę bezpieczeństwa informacji?		
5.3	Czy określone są i komunikowane role i odpowiedzialność w zakresie bezpieczeństwa informacji?		
6.1.2	Czy udokumentowany jest proces szacowania ryzyka, włącznie z kryteriami akceptacji ryzyka i kryteriami szacowania ryzyka?		
6.1.2, 8.2	Czy zidentyfikowano ryzyka, ich właścicieli, prawdopodobieństwo, skutki oraz poziom ryzyka; czy informacje te są udokumentowane?		
6.1.3	Czy udokumentowano proces postępowania z ryzykiem, włącznie z opcjami postępowania z ryzykiem?		
6.1.3, 8.3	Czy wszystkie ryzyka nieakceptowalne są przedmiotem postępowania zgodnego z opcjami i zabezpieczeniami z Załącznika A; czy jest to udokumentowane?		
6.1.3	Czy Deklaracja stosowania została opracowana, wraz uzasadnieniem i stanem wdrożenia dla każdego zabezpieczenia?		
6.1.3, 8.3	Czy istnieje Plan postępowania z ryzykiem, zatwierdzony przez właścicieli ryzyk?		
6.2	Czy Plan postępowania z ryzykiem określa, kto jest odpowiedzialny za wdrożenie wymienionych zabezpieczeń, z użyciem jakich zasobów, w jakich terminach i jaki jest sposób oceny wdrożenia?		
7.1	Czy zapewniono zasoby wystarczające dla wszystkich elementów SZBI?		
7.2	Czy określono wymagane kompetencje, przeprowadzono właściwe szkolenia i utrzymywane są rejestry uzyskanych kompetencji?		
7.3	Czy pracownicy są uświadomieni w zakresie treści Polityki bezpieczeństwa informacji, ich ról oraz konsekwencji nie przestrzegania zasad?		

Urząd Gminy Jasło	Lista kontrolna audytu wewnętrznego	Strona	2
		Wydanie	I
		Data wydania	2026.03.16

7.4	Czy istnieje proces komunikacji związanej z bezpieczeństwem informacji, włącznie z określoną odpowiedzialnością i wskazaniem treści komunikacji?		
7.5	Czy istnieje proces zarządzania dokumentami i rejestrami, włącznie z określeniem, kto dokonuje przeglądów i zatwierdzania dokumentów, gdzie i jak są one publikowane, przechowywane i chronione?		
7.5	Czy kontroluje się dokumenty pochodzenia zewnętrznego?		
8.1	Czy określone zostały i czy kontroluje się procesy outsourcingowe?		
9.1	Czy określone jest, co ma być mierzone, jaką metodą, kto jest odpowiedzialny i kto będzie analizować i oceniać wyniki pomiarów?		
9.1	Czy wyniki pomiarów są udokumentowane i raportowane do osób odpowiedzialnych?		
9.2	Czy istnieje plan audytu uwzględniający okresy audytu, odpowiedzialność, raportowanie, zakres i kryteria audytów?		
9.2	Czy audyty wewnętrzne przeprowadzane są zgodnie z planem audytów, wyniki audytów są rejestrowane poprzez Raporty z audytu wewnętrznego, a odnośne działania korygujące są inicjowane?		
9.3	Czy przeprowadza się regularnie przeglądy dokonywane przez kierownictwo, a ich wyniki są dokumentowane w protokołach z posiedzeń kierownictwa?		
9.3	Czy kierownictwo podjęło decyzję o wszystkich elementach SZBI kluczowych dla sukcesu wdrożenia SZBI?		
10.1	Czy organizacja reaguje na każdą niezgodność?		
10.1	Czy organizacja rozważa eliminację przyczyn niezgodności i tam gdzie jest to niezbędne podjęcie działań korygujących?		
10.1	Czy rejestruje się wszystkie niezgodności oraz dotyczące ich działania korygujące?		
A.5.1.1	Czy wszystkie niezbędne polityki bezpieczeństwa są zatwierdzane przez kierownictwo i publikowane?		
A.5.1.2	Czy wszystkie polityki bezpieczeństwa podlegają przeglądom i są aktualizowane?		
A.6.1.1	Czy odpowiedzialności i obowiązki związane z bezpieczeństwem informacji są jasno określone poprzez jeden lub więcej dokumentów?		
A.6.1.2	Czy obowiązki i odpowiedzialność są określone tak, aby unikać konfliktu interesów, szczególnie dla tych systemów informacyjnych, gdzie występują duże ryzyka?		
A.6.1.3	Czy jest jasno określone, kto odpowiada za kontakty z organami władzy?		
A.6.1.4	Czy jest jasno określone, kto odpowiada za kontakty ze stowarzyszeniami i grupami zainteresowań?		
A.6.1.5	Czy w każdym projekcie uwzględnia się zasady bezpieczeństwa informacji?		

Urząd Gminy Jasło	Lista kontrolna audytu wewnętrznego	Strona	3
		Wydanie	I
		Data wydania	2026.03.16

A.6.2.1	Czy istnieją zasady bezpiecznego posługiwania się urządzeniami mobilnymi?		
A.6.2.2	Czy istnieją zasady określające sposób ochrony informacji służbowych w miejscach, z których wykonywana jest telepraca?		
A.7.1.1	Czy przeprowadza się procedurę sprawdzającą kandydatów na pracowników lub podwykonawców?		
A.7.1.2	Czy umowy z pracownikami i podwykonawcami określają odpowiedzialność za bezpieczeństwo informacji?		
A.7.2.1	Czy kierownictwo aktywnie wymaga od wszystkich pracowników i podwykonawców postępowania zgodnego z zasadami bezpieczeństwa informacji?		
A.7.2.2	Czy istnieje program uświadamiania dla pracowników i podwykonawców i czy są oni szkoleni w zakresie swoich obowiązków związanych z bezpieczeństwem informacji?		
A.7.2.3	Czy wszyscy pracownicy łamiący zasady bezpieczeństwa informacji podlegali formalnym procedurom dyscyplinarnym?		
A.7.3.1	Czy odpowiedzialność za bezpieczeństwo informacji nie wygasa wraz z zakończeniem zatrudnienia??		
A.8.1.1	Czy stworzono Rejestr aktywów?		
A.8.1.2	Czy dla każdego aktywu w Rejestrze określono właściciela?		
A.8.1.3	Czy udokumentowano zasady odpowiedniego posługiwania się informacjami i aktywami?		
A.8.1.4	Czy wszyscy pracownicy i podwykonawcy zwrócili wszystkie aktywa po zakończeniu ich umów?		
A.8.2.1	Czy informacje są klasyfikowane według zdefiniowanych kryteriów?		
A.8.2.2	Czy informacja klasyfikowana jest oznaczana zgodnie z procedurą?		
A.8.2.3	Czy istnieją procedury posługiwania się informacją klasyfikowaną?		
A.8.3.1	Czy istnieją procedury określające sposób posługiwania się nośnikami wymiennymi zgodnie z zasadami klasyfikacji?		
A.8.3.2	Czy istnieje formalna procedura pozbywania się nośników?		
A.8.3.3	Czy nośniki zawierające informacje wrażliwe są chronione podczas transportu?		
A.9.1.1	Czy istnieje Polityka kontroli dostępu, określająca wymagania biznesowe i wymagania bezpieczeństwa dla kontroli dostępu?		
A.9.1.2	Czy użytkownicy mają dostęp tylko do tych sieci i usług, do których użytkowania są uprawnieni?		
A.9.2.1	Czy prawa dostępu są przydzielane w oparciu o formalny proces rejestracji?		
A.9.2.2	Czy funkcjonuje system kontroli dostępu regulujący dostęp do systemów informacyjnych?		

Urząd Gminy Jasło	Lista kontrolna audytu wewnętrznego	Strona	4
		Wydanie	I
		Data wydania	2026.03.16

A.9.2.3	Czy uprzywilejowanymi uprawnieniami zarządza się ze szczególną ostrożnością?		
A.9.2.4	Czy hasła startowe i inne poufne informacje uwierzytelniające są dostarczane w bezpieczny sposób?		
A.9.2.5	Czy właściciele aktywów sprawdzają okresowo wszystkie uprawnienia?		
A.9.2.6	Czy usuwa się wszystkie uprawnienia dla pracowników i podwykonawców wraz z zakończeniem ich umów?		
A.9.3.1	Czy istnieją jasno określone zasady obowiązujące użytkowników w zakresie ochrony haseł oraz innych informacji uwierzytelniających?		
A.9.4.1	Czy dostęp do aplikacji i baz danych jest ograniczony zgodnie z Polityką kontroli dostępu?		
A.9.4.2	Czy wymuszane jest bezpieczne logowanie się do systemów, zgodnie z Polityką kontroli dostępu?		
A.9.4.3	Czy systemy zarządzania hasłami są interaktywne i umożliwiają użytkownikom tworzenie bezpiecznych haseł?		
A.9.4.4	Czy użytkowanie oprogramowania narzędziowego umożliwiającego obchodzenie zabezpieczeń jest ściśle kontrolowane i ograniczone do wąskiego grona pracowników?		
A.9.4.5	Czy dostęp do kodu źródłowego jest ograniczony do uprawnionych osób?		
A.10.1.1	Czy istnieje polityka określająca zasady posługiwania się szyfrowaniem i innymi zabezpieczeniami kryptograficznymi?		
A.10.1.2	Czy odpowiednio chroni się klucze kryptograficzne?		
A.11.1.1	Czy istnieją obszary bezpieczne służące do ochrony informacji wrażliwych?		
A.11.1.2	Czy wejście do obszarów bezpiecznych jest chronione poprzez zabezpieczenia umożliwiające wejście tylko autoryzowanym osobom?		
A.11.1.3	Czy obszary bezpieczne zlokalizowane są tak, aby były niewidoczne i trudno dostępne dla osób z zewnątrz?		
A.11.1.4	Czy zainstalowano systemy alarmowe, przeciwpożarowe i inne tego typu systemy?		
A.11.1.5	Czy określone są i przestrzegane procedury pracy w obszarach bezpiecznych?		
A.11.1.6	Czy obszary dostaw i załadunku są kontrolowane w sposób uniemożliwiający osobom zewnętrznym wejście do siedziby?		
A.11.2.1	Czy wyposażenie umieszczone jest tak, że chronione jest przed nieautoryzowanym dostępem oraz przed zagrożeniami środowiskowymi?		
A.11.2.2	Czy wyposażenie podłączone jest do zasilaczy UPS?		
A.11.2.3	Czy kable zasilające i telekomunikacyjne są odpowiednio chronione?		

Urząd Gminy Jasło	Lista kontrolna audytu wewnętrznego	Strona	5
		Wydanie	I
		Data wydania	2026.03.16

A.11.2.4	Czy sprzęt serwisuje się regularnie, zgodnie ze specyfikacją producenta i dobrymi praktykami?		
A.11.2.5	Czy każdorazowo przy wynoszeniu aktywów poza siedzibę autoryzuje się fakt wyniesienia danego aktywu?		
A.11.2.6	Czy aktywa są odpowiednio chronione, gdy nie znajdują się w siedzibie?		
A.11.2.7	Czy wszystkie informacje i licencjonowane oprogramowanie są usuwane z nośników lub sprzętu przed pozbyciem się nośnika lub sprzętu?		
A.11.2.8	Czy użytkownicy chronią sprzęt, gdy pozostaje on poza ich kontrolą?		
A.11.2.9	Czy istnieje polityka wymuszająca na użytkownikach usuwanie dokumentów papierowych oraz nośników i blokowanie ekranu, gdy nie są oni przy swoich miejscach pracy?		
A.12.1.1	Czy udokumentowane są procedury operacyjne dla systemów informatycznych?		
A.12.1.2	Czy ściśle kontroluje się wszystkie zmiany w systemach informatycznych oraz w innych procesach, które mogą wpływać na bezpieczeństwo informacji?		
A.12.1.3	Czy monitoruje się użycie zasobów i planuje się ich pojemność/przepustowość?		
A.12.1.4	Czy ściśle odseparowane od siebie są środowiska rozwojowe, testowania i produkcyjne?		
A.12.2.1	Czy zainstalowane jest i aktualizowane oprogramowanie antywirusowe i inne zabezpieczające przed złośliwym kodem?		
A.12.3.1	Czy istnieje polityka dotycząca kopii zapasowych i czy kopie zapasowe wykonywane są zgodnie z tą polityką?		
A.12.4.1	Czy działania użytkowników, błędy i inne zdarzenia z systemów IT są rejestrowane i czy ktoś przegląda i analizuje te rejestry?		
A.12.4.2	Czy dzienniki zdarzeń są chronione przed nieuprawnionymi modyfikacjami?		
A.12.4.3	Czy dzienniki działań administratorów są chronione przed dostępem administratorów (zmianą, skasowaniem); czy są one regularnie sprawdzane?		
A.12.4.4	Czy zegary wszystkich systemów IT są zsynchronizowane z jednym źródłem prawidłowego czasu?		
A.12.5.1	Czy ściśle kontroluje się instalację oprogramowania; czy istnieją odnośne procedury?		
A.12.6.1	Czy jest osoba wyznaczona do zbierania informacji o podatnościach i czy podatności te są szybko usuwane?		
A.12.6.2	Czy istnieją reguły określające restrykcje dotyczące instalacji oprogramowania przez użytkowników?		

Urząd Gminy Jasło	Lista kontrolna audytu wewnętrznego	Strona	6
		Wydanie	I
		Data wydania	2026.03.16

A.12.7.1	Czy audyty systemów informatycznych planowane i wykonywane są w sposób minimalizujący ryzyko zakłóceń pracy?		
A.13.1.1	Czy sieci kontroluje się w sposób zapewniający ochronę informacji w systemach i aplikacjach?		
A.13.1.2	Czy określono wymagania bezpieczeństwa dla wewnętrznych i zewnętrznych usług sieciowych, czy są one włączane do umów?		
A.13.1.3	Czy odpowiednio dla różnych sieci segreguje się grupy użytkowników, usług i systemów?		
A.13.2.1	Czy sposoby ochrony transferu informacji są określone w formalnych politykach i procedurach?		
A.13.2.2	Czy istnieją umowy ze stronami trzecimi regulujące bezpieczeństwo transferu informacji?		
A.13.2.3	Czy wiadomości wymieniane przez sieci są odpowiednio chronione?		
A.13.2.4	Czy istnieje dokument zawierający zapisy dotyczące poufności, które mają być włączane do umów ze stronami trzecimi?		
A.14.1.1	Czy określa się wymagania bezpieczeństwa dla nowych systemów informacyjnych lub dla zmian w tych systemach?		
A.14.1.2	Czy informacje w aplikacjach korzystających z sieci publicznych są odpowiednio chronione?		
A.14.1.3	Czy informacje dotyczące transakcji dokonywanych z użyciem sieci publicznych są odpowiednio chronione?		
A.14.2.1	Czy określono zasady bezpiecznego projektowania i rozwoju oprogramowania i systemów?		
A.14.2.2	Czy istnieją formalne procedury zarządzania zmianami w systemach?		
A.14.2.3	Czy krytyczne aplikacje są testowane po zmianach lub aktualizacjach w systemach operacyjnych?		
A.14.2.4	Czy w systemach informacyjnych wprowadza się tylko konieczne zmiany?		
A.14.2.5	Czy zasady tworzenia bezpiecznych systemów są udokumentowane i stosowane?		
A.14.2.6	Czy środowisko rozwoju jest odpowiednio chronione przed nieuprawnionym dostępem i zmianami?		
A.14.2.7	Czy monitoruje się rozwój systemów wykonywany przez partnerów outsourcingowych?		
A.14.2.8	Czy w pracach rozwojowych uwzględnia się testowanie prawidłowości wdrożenia wymagań bezpieczeństwa?		
A.14.2.9	Czy określono kryteria akceptacji systemów?		
A.14.3.1	Czy dane testowe wybiera się uważnie i czy są one chronione?		
A.15.1.1	Czy udokumentowano politykę postępowania z ryzykami związanymi z dostawcami i partnerami?		

Urząd Gminy Jasło	Lista kontrolna audytu wewnętrznego	Strona	7
		Wydanie	I
		Data wydania	2026.03.16

A.15.1.2	Czy wszystkie odnośne wymagania bezpieczeństwa są włączane do umów z partnerami i dostawcami?		
A.15.1.3	Czy umowy z dostawcami usług chmurowych zawierają wymagania bezpieczeństwa i niezawodności?		
A.15.2.1	Czy regularnie monitoruje się dostawców – oraz audytuje tam, gdzie jest to wskazane - na zgodność z wymaganiami bezpieczeństwa?		
A.15.2.2	Czy uwzględnia się ryzyka i istniejące procesy przy wprowadzaniu zmian do ustaleń i umów z dostawcami i partnerami?		
A.16.1.1	Czy jasno określono procedury i odpowiedzialność w zakresie zarządzania incydentami?		
A.16.1.2	Czy wszystkie zdarzenia związane z bezpieczeństwem informacji są sprawnie i terminowo raportowane?		
A.16.1.3	Czy pracownicy i podwykonawcy zgłaszają słabe punkty w systemie bezpieczeństwa?		
A.16.1.4	Czy wszystkie zdarzenia związane z bezpieczeństwem są oceniane i klasyfikowane?		
A.16.1.5	Czy udokumentowane są procedury reagowania na incydenty?		
A.16.1.6	Czy analizuje się incydenty, aby pozyskać wiedzę, jak ich unikać?		
A.16.1.7	Czy istnieją procedury określające sposoby zbierania dowodów, które będą akceptowalne w procesach sądowych?		
A.17.1.1	Czy określono wymagania ciągłości bezpieczeństwa informacji?		
A.17.1.2	Czy istnieją procedury zapewniające ciągłość bezpieczeństwa informacji podczas sytuacji kryzysowej lub katastrofy?		
A.17.1.3	Czy przeprowadza się ćwiczenia i testy w celu zapewnienia skutecznego reagowania?		
A.17.2.1	Czy infrastruktura IT posiada redundancję (np. ośrodek zapasowy) aby spełniać swoje zadania podczas katastrofy?		
A.18.1.1	Czy określono i udokumentowano wszystkie wymagania prawne, branżowe, umowne i inne?		
A.18.1.2	Czy istnieją procedury wymuszające respektowanie praw własności intelektualnej, w szczególności użytkowania licencjonowanego oprogramowania?		
A.18.1.3	Czy wszystkie rejestry chronione są zgodnie z określonymi wymaganiami prawnymi, umownymi i innymi?		
A.18.1.4	Czy dane osobowe są chronione zgodnie z prawem i określonymi zasadami?		
A.18.1.5	Czy zabezpieczenia kryptograficzne są stosowane zgodnie z prawem i określonymi zasadami?		

Urząd Gminy Jasło	Lista kontrolna audytu wewnętrznego	<i>Strona</i>	8
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

A.18.2.1	Czy bezpieczeństwo informacji podlega regularnym przeglądom niezależnych audytorów?		
A.18.2.2	Czy kierownicy regularnie sprawdzają, jak realizowane są w ich obszarach kompetencji polityki i procedury bezpieczeństwa?		
A.18.2.3	Czy systemy informacyjne są regularnie kontrolowane na zgodność z politykami i standardami bezpieczeństwa informacji?		

Urząd Gminy Jasło	Polityka Bezpieczeństwa w relacjach z dostawcami	Strona	1
		Wydanie	I
		Data wydania	2026.03.16

POLITYKA BEZPIECZEŃSTWA W RELACJACH Z DOSTAWCAMI

ZATWIERDZAM

Wójt
Wojciech Mękoś

(Podpis/pieczętka i data)

<i>Urząd Gminy Jasło</i>	<i>Polityka Bezpieczeństwa w relacjach z dostawcami</i>	<i>Strona</i>	1
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

POLITYKA BEZPIECZEŃSTWA W RELACJACH Z DOSTAWCAMI

ZATWIERDZAM

(Podpis/pieczętka i data)

<i>Urząd Gminy Jasło</i>	<i>Polityka Bezpieczeństwa w relacjach z dostawcami</i>	<i>Strona</i>	3
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

SPIS TREŚCI

Skróty i definicje	4
Rozdział I. Cel i Zakres Polityki Bezpieczeństwa w relacjach z dostawcami.....	6
Rozdział II. Dostęp podmiotów zewnętrznych do aktywów Urzędu.....	6

SPIS ZAŁĄCZNIKÓW

Załącznik 1. SZBI-007-01 Ankieta oceny procesora

Urząd Gminy Jasło	Polityka Bezpieczeństwa w relacjach z dostawcami	Strona	4
		Wydanie	I
		Data wydania	2026.03.16

SKRÓTY I DEFINICJE

Administrator Danych Osobowych – Wójt Gminy Jasło, ul. Słowackiego 4 38-200

Jednostka – Urząd Gminy Jasło

SZBI - System Zarządzania Bezpieczeństwem Informacji

PBI – Polityka Bezpieczeństwa Informacji

Zespół ds. Obsługi Incydentów – zespół osobowy odpowiedzialny za proces zarządzania incydentami – przygotowanie, realizację działań w trakcie wystąpienia incyduentu oraz działań likwidujących skutki wystąpienia incyduentu.

Informacja poufna – wszelkie informacje, które są chronione przed dostępem osób trzecich oraz przed upublicznieniem. Dane osobowe wchodzą w skład informacji poufnych.

Dane osobowe – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Odbiorca – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Przy czym odbiorcą nie jest organ publiczny, który może otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii Europejskiej lub prawem państw członkowskiego.

Osoba upoważniona – osoba upoważniona przez administratora do przetwarzania danych osobowych, nad którą administrator sprawuje bezpośrednią kontrolę w procesie przetwarzania danych realizowanym przez tę osobę.

Incydent – pojedyncze zdarzenie lub seria niepożądanych zdarzeń związanych z bezpieczeństwem, które stwarzają znaczne prawdopodobieństwo zakłócenia działań lub ujawnienia informacji poufnych. Definiowany jest również jako naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Incydent poważny – incyduentu, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej.

Sytuacja podejrzenia wystąpienia incyduentu – pojedyncze zdarzenie lub seria niepożądanych zdarzeń związanych z bezpieczeństwem, które stwarzają znaczne prawdopodobieństwo zakłócenia działań lub ujawnienia informacji poufnych.

Hasło – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;

Usługa kluczowa – usługa, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej.

Przetwarzanie danych osobowych - jakiegokolwiek operacje lub zestaw operacji wykonywanych na danych osobowych.

Audyt - działania mające na celu oceny danej osoby, Zakładu, systemu, procesu, zabezpieczenia mające na celu potwierdzenie spełnienia konkretnych wymagań.

<i>Urząd Gminy Jasło</i>	<i>Polityka Bezpieczeństwa w relacjach z dostawcami</i>	<i>Strona</i>	5
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

Analiza ryzyka - systematyczne wykorzystanie informacji do zidentyfikowania źródeł i oszacowania ryzyka.

Podmiot zewnętrzny - wszyscy pracownicy m.in. wykonawców i kontrahentów, dostawców produktów, materiałów i usług, wykonujących czynności w imieniu i na rzecz Urzędu Gminy Jasło lub mających dostęp do aktywów Jednostki w związku z realizacją zawartej umowy lub porozumienia.

<i>Urząd Gminy Jasło</i>	<i>Polityka Bezpieczeństwa w relacjach z dostawcami</i>	<i>Strona</i>	6
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

ROZDZIAŁ I

CEL I ZAKRES POLITYKI BEZPIECZEŃSTWA W RELACJACH Z DOSTAWCAMI

Celem polityki jest zapewnienie ochrony aktywów informacyjnych udostępnianych usługodawcom, dostawcom i innym osobom oraz podmiotom zewnętrznym wykonującym czynności w imieniu i na rzecz. Polityka reguluje zasady współpracy między Jednostką, a podmiotami zewnętrznymi współpracującymi z Urzędem.

Polityka Bezpieczeństwa w relacjach z dostawcami swoim zakresem obejmuje:

1. Wszystkie realizowane procesy oraz zadania w ramach działania jednostki;
2. Wszystkie zasoby będące własnością Urzędu lub przekazane jej przez kontrahentów w ramach realizacji obowiązujących umów, w tym:
 - a) personel;
 - b) budynki i pomieszczenia;
 - c) sprzęt;
 - d) systemy, oprogramowanie i technologie pozwalające na przetwarzanie informacji;
 - e) wyznaczeni przez Urząd dostawcy usług, w tym eksperci techniczni.

ROZDZIAŁ II

DOSTĘP PODMIOTÓW ZEWNĘTRZNYCH DO AKTYWÓW URZĘDU

Pracownicy podmiotów zewnętrznych, realizujący określone zadania na podstawie zawartej umowy lub porozumienia mogą otrzymać dostęp do aktywów informacyjnych Urzędu, w tym do:

1. Informacji sklasyfikowanych w poszczególnych grupach:
 - a) dane osobowe;
 - b) tajemnice prawnie chronione;
 - c) tajemnice Urzędu;
 - d) informacje jawne.
2. Aktywów wspierających przetwarzanie ww. informacji:
 - a) sprzęt (w tym komputery, nośniki informacji);
 - b) oprogramowanie;
 - c) sieć;
 - d) personel Urzędu;
 - e) siedziba, Urząd;

<i>Urząd Gminy Jasło</i>	<i>Polityka Bezpieczeństwa w relacjach z dostawcami</i>	<i>Strona</i>	7
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

- f) organizacja (w tym procedury wewnętrzne określające zasady i tryb funkcjonowania poszczególnych struktur organizacyjnych Urzędu), w ograniczonym zakresie, niezbędnym do realizacji zleconych prac.

Przyznawanie, zmiana i odbieranie ww. dostępu do aktywów informacyjnych odbywa się zgodnie z obowiązującymi przepisami prawa, na formalny wniosek właściwego kierownika komórki organizacyjnej, odpowiedzialnego za przygotowanie lub realizację umowy lub porozumienia. Przyznawanie rozszerzonych uprawnień lub dodatkowych przywilejów możliwe jest po przedłożeniu stosownego uzasadnienia przez ww. kierownika i po formalnym odnotowaniu przedmiotowej zmiany.

Zasady dostępu fizycznego do budynków i pomieszczeń Urzędu dla pracowników podmiotów zewnętrznych:

1. Pracownicy podmiotów zewnętrznych mają swobodny dostęp do ogólnodostępnej strefy bezpieczeństwa obejmującej wejścia do budynków Urzędu: hole, korytarze oraz wybrane pomieszczenia niestanowiące pomieszczeń ograniczonego dostępu i/lub podwyższonego poziomu bezpieczeństwa.
2. Pracownicy podmiotów zewnętrznych mogą uzyskać dostęp do strefy administracyjnej lub strefy ograniczonego dostępu, w tym pomieszczeń biurowych, w zakresie wynikającym z realizacji zadań określonych w treści zawartych umów lub porozumień i na formalny wniosek właściwego kierownika.
3. W strefie o podwyższonym poziomie bezpieczeństwa obejmującej m.in. serwerownię, pracownicy podmiotów zewnętrznych mogą przebywać tylko pod ścisłym nadzorem wybranych pracowników Działu Informatyki. Dostęp do strefy o podwyższonym poziomie bezpieczeństwa jest na bieżąco rejestrowany.

WERYFIKACJA PROCESORA PRZETWARZANIA DANYCH OSOBOWYCH

Nr	TREŚĆ PYTANIA	ODPOWIEDZI	
		TAK/NIE/ND	UWAGI/KOMENTARZE
1.	Czy dostawca prowadzi rejestr naruszeń?	<i>Rejestr naruszeń jest dokumentem, w którym powinny być ewidencjonowane wszelkie incydenty naruszenia ochrony danych osobowych. W rejestrze opisuje się zdarzenie, które miało miejsce, skutki naruszenia oraz podjęte działania zaradcze, mające na celu usunięcie skutków naruszenia oraz zminimalizowanie prawdopodobieństwa powtórzenia się naruszenia w przyszłości.</i>	
2.	Czy pracownicy / współpracownicy dostawcy są upoważnieni do przetwarzania danych osobowych?	<i>Każda osoba mająca dostęp do danych osobowych powinna zostać upoważniona do ich przetwarzania przez administratora lub podmiot przetwarzający. Pytanie ma na celu zweryfikowanie czy dostawca udzielił swoim pracownikom / współpracownikom ww. upoważnień.</i>	
3.	Czy osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub podlegają odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy?	<i>Wymóg zobowiązania do zachowania tajemnicy przez osoby przetwarzające dane z upoważnienia podmiotu przetwarzającego wynika z art. 28 RODO. Konieczne jest zatem, aby osoby upoważnione do przetwarzania danych podpisały zobowiązanie do zachowania poufności (może być to odrębny dokument lub takie zobowiązanie może być częścią umowy zawartej pomiędzy dostawcą a jego pracownikiem / współpracownikiem).</i>	
4.	Jeżeli dostawca dokonuje transferów danych do państw poza EOG, to czy zapewniony jest mechanizm legalizujący taki transfer?	<i>W przypadku transferów danych poza EOG (EOG obejmuje kraje UE oraz Islandię, Norwegię oraz Liechtenstein) należy zapewnić aby taki transfer był legalny (przykładem mechanizmu legalizującego transfer jest zawarcie umowy z kontrahentem w brzmieniu zgodnym ze standardowymi klauzulami umownymi przyjętymi przez Komisję Europejską). Przykładem, gdy dochodzi do transferu jest sytuacja, gdy zawarta jest umowa na świadczenie usług hostingowych z usługodawcą, którego serwery znajdują się w USA.</i>	

Kryteria dodatkowe - ocena wiedzy fachowej oraz wiarygodności dostawcy (w przypadku niespełnienia co najmniej jednego z wymogów określonych w pytaniach nr 5-13, należy ankietę przekazać do oceny Inspektora Ochrony Danych (IOD))

5.	Czy został powołany Inspektor Ochrony Danych (IOD) lub została wyznaczona osoba do wykonywania zadań związanych z zapewnieniem zgodności przetwarzania danych osobowych u dostawcy z obowiązującym prawem?	<i>IOD jest powoływany w przypadkach określonych w art. 37 RODO, a także gdy dany podmiot zdecyduje się na jego wyznaczenie w sytuacji, gdy przepisy nie narzucają takiego obowiązku. Jeżeli nie ma formalnie powołanego IOD, wówczas należy wskazać, czy została wyznaczona inna osoba, która jest odpowiedzialna za wykonywanie zadań w zakresie ochrony danych osobowych u dostawcy.</i>		
6.	Czy IOD lub inna osoba wyznaczona do wykonywania zadań związanych z ochroną danych osobowych posiada odpowiednie kwalifikacje, dające gwarancję zgodności przetwarzania danych osobowych zgodnie z przepisami prawa?	<i>Za osobę spełniającą wskazany wymóg uważa się w szczególności: osobę, która posiada co najmniej 2-letnie doświadczenie w pełnieniu funkcji administratora bezpieczeństwa informacji, osobę, która ukończyła studia podyplomowe w dziedzinie ochrony danych osobowych lub bezpieczeństwa informacji na uczelni wyższej, radcę prawnego lub adwokata z co najmniej 2-letnim doświadczeniem w dziedzinie ochrony danych osobowych.</i>		
7.	Czy dostawca posiada wdrożone mechanizmy identyfikacji oraz oceny i notyfikacji naruszeń ochrony danych osobowych?	<i>Celem tego pytania jest zweryfikowanie, czy dostawca posiada dostateczną wiedzę i kompetencje, aby być w stanie zidentyfikować oraz ocenić naruszenia ochrony danych osobowych w jego organizacji.</i>		
8.	Czy dostawca posiada certyfikaty w zakresie bezpieczeństwa informacji lub wdrożył system zarządzania bezpieczeństwem informacji?	<i>Chodzi o certyfikaty takie jak np.: certyfikat bezpieczeństwa informacji 27001, certyfikat CISA (Certified Information Systems Auditor), certyfikat CISSP (Certified Information Systems Security Professional) itp.</i>		
9.	Czy dostawca posiada doświadczenie w świadczeniu usług związanych z powierzeniem przetwarzania danych? Jeśli tak, to jak długie? Prosimy o udokumentowanie świadczenia przedmiotowych usług.	<i>Udokumentowaniem współpracy mogą być przede wszystkim stosowne rekomendacje pisemne udzielone przez innych Zleceniodawców. Rekomendacje powinny w miarę możliwości zawierać dane kontaktowe umożliwiające ich weryfikację</i>		
10.	Czy osoby po stronie dostawcy dedykowane do obsługi administratora danych zostały przeszkolone i zapoznane z przepisami o ochronie danych? Czy jest to udokumentowane?	<i>Administrator może prosić o udokumentowanie faktu przeprowadzenia szkoleń dla wskazanych osób</i>		
11.	Czy dostawca opracował i wdrożył politykę ochrony danych lub podobną procedurę?	<i>Chodzi o spełnienie obowiązku wynikającego z art. 24 RODO w szczególności art. 24 ust. 2 RODO</i>		

12.	Czy dostawca dobrał zabezpieczenia zapewniające bezpieczeństwo przetwarzanych danych osobowych w odniesieniu do oceny skutków ich przetwarzania dla praw i wolności osób, których dane dotyczą? (na podstawie szacowania ryzyka pod kątem ochrony prywatności - Privacy Impact Assessment)?	Odniesienie do Art. 24, 25, 32 RODO		
13.	Czy dostawca wdrożył odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku związanemu z ich przetwarzaniem, w tym: - pseudonimizację i szyfrowanie danych; - zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania; - zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.	Odniesienie do Art. 32 ust. 1 lit a)-c) RODO. Prosimy o wskazanie jakie konkretnie środki organizacyjne i techniczne służą realizacji poszczególnych, wskazanych celów		

Urząd Gminy Jasło	Polityka Zarządzania Podatnościami	Strona	1
		Wydanie	I
		Data wydania	2026.03.16

POLITYKA ZARZĄDZANIA PODATNOŚCIAMI w Urzędzie Gminy Jasło

Tytuł dokumentu
System
Zastosowanie
Status

ZATWIERDZAM
WOJT
Wojciech Rakos
 (Podpis/pieczętka i data)

<i>Urząd Gminy Jasło</i>	<i>Polityka Zarządzania Podatnościami</i>	<i>Strona</i>	1
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

**POLITYKA
ZARZĄDZANIA
PODATNOŚCIAMI
w Urzędzie Gminy Jasło**

ZATWIERDZAM

(Podpis/pieczątka i data)

<i>Urząd Gminy Jasło</i>	<i>Polityka Zarządzania Podatnościami</i>	<i>Strona</i>	3
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

SPIS TREŚCI

Rozdział I.	Odpowiedzialność	4
Rozdział II.	Wykrywanie podatności	5
Rozdział III.	Priorytetyzacja podatności	6
Rozdział IV.	Ocena podatności.....	7
Rozdział V.	Raport.....	8
Rozdział VI.	Naprawa	9
Rozdział VII.	Weryfikacja	9

SPIS ZAŁĄCZNIKÓW

- Załącznik 1. SZBI-008-01 Harmonogram skanowania podatności
- Załącznik 2. SZBI-008-02 Rejestr podatności

<i>Urząd Gminy Jasło</i>	<i>Polityka Zarządzania Podatnościami</i>	<i>Strona</i>	4
		<i>Wydanie</i>	I
		<i>Data wydania</i>	2026.03.16

ROZDZIAŁ I ODPOWIEDZIALNOŚĆ

Odpowiedzialnym za realizację procesu zarządzania podatnościami jest Zespół ds. Obsługi Incydentów zwanym dalej Zespołem, na czele z Administratorem Systemów Informatycznych. W skład Zespołu wchodzi:

1. Administrator Systemów Informatycznych
2. Inspektor Ochrony Danych Osobowych

Do zadań Zespołu należy:

1. Wykrywanie podatności
2. Klasyfikacja i priorytetyzacji podatności
3. Ocena podatności
4. Raportowanie podatności do kierownika jednostki(ocena, skutek, plan postępowania)
5. Wdrożenie działań podjętych przez kierownika jednostki (naprawa, mitygacja, brak działań)
6. Weryfikacja podatności
7. Umieszczenie podatności w Rejestrze podatności

Organem decyzyjnym, przyjmującym lub odrzucającym proponowane działania zaradcze jest Kierownik Jednostki.

Urząd Gminy Jasło	Polityka Zarządzania Podatnościami	Strona	5
		Wydanie	I
		Data wydania	2026.03.16

ROZDZIAŁ II

WYKRYWANIE PODATNOŚCI

Wykrywanie podatności w organizacji jest realizowane na podstawie:

1. Informacji/ zgłoszeń otrzymanych od CERT Polska

Osobami do kontaktu (min. 2 osoby) wyznaczonymi oraz zgłoszonymi w jednostce są:

I.	Imię i Nazwisko	
	Tel.	
	Mail.	
II.	Imię i Nazwisko	
	Tel.	
	Mail.	

W tym przypadku poszczególne potencjalne podatności są poddawane sprawdzeniu ręcznemu przez działu ds. Obsługi Incydentów. Każda informacja o możliwej podatności jest uwzględniana w – załącznik 2 - **SZBI-008-02 Rejestr podatności**. W przypadku braku odniesienia/ powiązania zgłoszenia podatności do obecnie wykorzystywanego systemu informatycznego, fakt przyjęcia informacji jest również notowany w rejestrze i oznaczany w kolumnie *status* jako – *nie dotyczy*.

2. Cyklicznie realizowanych skanów podatności

Skan podatności realizowany jest cyklicznie zgodnie z przyjętym – załącznik 1 - **SZBI-008-01 Harmonogram skanowania podatności**. Skany dodatkowo są realizowane po każdej znacznej zmianie w infrastrukturze informatycznej jednostki.

Urząd Gminy Jasło	Polityka Zarządzania Podatnościami	Strona	6
		Wydanie	I
		Data wydania	2026.03.16

ROZDZIAŁ III

PRIORYTETYZACJA PODATNOŚCI

Priorytet podatności jest zależny od zasobu którego bezpośrednio dotyczy. Nadawana jest na podstawie **SZBI-005-03 Analiza Ryzyka** dla danego zasobu. Czynnikiem determinującym nadanie priorytetu jest zagrożenie materializacji ryzyka na zasobie stanowiącym podatność.

Priorytet niski	1-4
Priorytet średni	5-8
Priorytet wysoki	9-15
Priorytet krytyczny	16-25

- priorytet krytyczny – działania muszą być podjęte w przeciągu tygodnia;
- priorytet wysoki – działania muszą być podjęte w przeciągu miesiąca;
- priorytet średni – działania powinny być podjęte w przeciągu 6 miesięcy;
- priorytet niski – działania powinny być podjęte w przeciągu 1 roku.

Urząd Gminy Jasło	Polityka Zarządzania Podatnościami	Strona	7
		Wydanie	I
		Data wydania	2026.03.16

ROZDZIAŁ IV

OCENA PODATNOŚCI

Podatności są oceniane zgodnie z modelem *Common Vulnerability Scoring System* (CVSS), w tym celu wykorzystywana jest poniższy formularz. Na podstawie uzyskanego wyniku przyznaje się ocenę.

Wynik	Ocena	Interpretacja
0.1 - 3.9	Niski	Wykorzystanie takich podatności wymaga zazwyczaj lokalnego lub fizycznego dostępu do systemu.
4.0 - 6.9	Średni	- Podatności, które wymagają od atakującego manipulowania ofiarami za pomocą taktyk socjotechnicznych. - Podatności na ataki typu Denial of Service, które są trudne do skonfigurowania. - Exploity, które wymagają, aby atakujący znajdował się w tej samej sieci lokalnej co ofiara. - Luki, których wykorzystanie zapewnia jedynie bardzo ograniczony dostęp. - Luki, które do skutecznego wykorzystania wymagają uprawnień użytkownika.
7.0 - 8.9	Wysoki	- Luka jest trudna do wykorzystania. - Wykorzystanie jej może prowadzić do zwiększenia poziomu uprawnień. - Wykorzystanie luki może spowodować znaczną stratę danych lub przestój w pracy.
9.0 - 10.0	Krytyczna	- Wykorzystanie luki prawdopodobnie doprowadzi do przejęcia kontroli nad serwerami lub urządzeniami infrastruktury na poziomie użytkownika. - Wykorzystanie jest zazwyczaj proste, w tym sensie, że atakujący nie potrzebuje żadnych specjalnych danych uwierzytelniających ani wiedzy o poszczególnych ofiarach, nie musi też przekonywać docelowego użytkownika, na przykład za pomocą socjotechniki, do wykonania jakiejś specjalnej funkcji. - W przypadku krytycznych luk, zaleca się jak najszybsze ich załatwienie lub aktualizację, chyba że istnieją inne środki zaradcze. Na przykład, czynnikiem łagodzącym może być fakt, że instalacja nie jest dostępna z Internetu

Urząd Gminy Jasło	Polityka Zarządzania Podatnościami	Strona	8
		Wydanie	I
		Data wydania	2026.03.16

ROZDZIAŁ V

RAPORT

Raport zawiera szczegółowe informacje ilościowe oraz jakościowe na temat wykrytych podatności i określa ich priorytety. Taki raport zawiera również rekomendacje, a także porusza kwestię mitygacji zagrożenia – umieszczone są w nim działania, które należy przedsięwziąć w celu rozwiązania problemu.

Raport musi uwzględniać elementy takie jak:

- 1) data wykrycia podatności;
- 2) sposób wykrycia podatności;
- 3) priorytet wykrytej podatności;
- 4) ocena podatności;
- 5) opis wykrytej podatności;
- 6) proponowane dalsze działania naprawcze/ mitygacyjne lub brak działania (w tym wskazanie wszelkich niezbędnych środków do podjęcia działań):
 - a) **Naprawa** – całkowite zapobieganie wykorzystaniu podatności. Możliwe jest to dzięki poprawce udostępnionej przez producenta oprogramowania.
 - b) **Mitygacja** – polega na zmniejszeniu prawdopodobieństwa wykorzystania podatności bądź też na zmniejszeniu jej wpływu. Należy mieć na uwadze, iż jest to rozwiązanie tymczasowe, z którego warto skorzystać do momentu wydania oficjalnej poprawki, która umożliwi usunięcie podatności.
 - c) **Brak działania** – sprowadza się do zaakceptowania istnienia podatności. Organizacje decydują się na ten krok w przypadku, gdy koszty naprawy znacznie przewyższają konsekwencje wykorzystania podatności.

Raport przygotowywany jest przez Administratora Systemów Informatycznych, przy wsparciu zespołu ds. Cyberbezpieczeństwa – Zarządzania incydentami. Raport przedstawiany jest kierownikowi jednostki w czasie nie krótszym niż 2 dni robocze od momentu wykrycia podatności.

Kierownik jednostki podejmuje decyzję o podjęciu dalszych działań. Podjęta decyzja jest dokumentowana na raporcie. Decyzja musi obejmować datę wydania decyzji oraz przyjęcie jednego z zaproponowanych sposobów postępowania (propozycje naprawy, mitygacji lub brak działań).

Urząd Gminy Jasło	Polityka Zarządzania Podatnościami	Strona	9
		Wydanie	I
		Data wydania	2026.03.16

ROZDZIAŁ VI NAPRAWA

Naprawa jest obszarem działania polegającym na wdrożeniu w życie podjętych przez kierownictwo środków zaradczych. Podjęcie działań zaradczych lub ich zaniechanie jest dokumentowane w – załącznik 2 - **SZBI-008-02 Rejestr podatności**.

Czas naprawy/ kolejność naprawy poszczególnych podatności jest realizowany zgodnie nadanym jej priorytetem.

ROZDZIAŁ VII WERYFIKACJA

W ramach weryfikacji realizowane jest sprawdzenie, czy dane, wykryte zagrożenie zostało wyeliminowane. Każda podatność, która była poddana procesowi naprawy i mitygacji musi przejść proces weryfikacji, który jest oznaczany w – załącznik 2 - **SZBI-008-02 Rejestr podatności** datą zakończenia weryfikacji oraz osobą odpowiedzialną za jej weryfikację. Podatności naprawione mogą zostać oznaczone statusem *zamknięte* w – załącznik 2 - **SZBI-008-02 Rejestr podatności**. Podatności poddane mitygacji oraz pozostawione bez dalszych działań muszą cały czas posiadać status podatności *otwartych*.

Urząd Gminy Jasło	Harmonogram skanowania podatności	<i>Strona</i>	1
		<i>Wydanie</i>	I
		<i>Data wydania</i>	

[illegible]

Urząd Gminy Jasło	Rejestr podatności	Strona	1
		Wydanie	I
		Data wydania	

Rejestr podatności w Urzędzie Gminy Jasło na rok

[illegible]