Załącznik nr 1
do Zarządzenia nr 41/2026
z dnia 28.05.2026 r.

POLITYKA BEZPIECZEŃSTWA INFORMACJI

wersja nr 1.0

z dnia 28.05.2026 r.

Właściciel dokumentu:	**Zatwierdzający:**
Sekretarz Gminy	Wójt
Małgorzata Brożyna	**Robert Pluta**
…….	**…….**

Odbiorcy:
Wszyscy pracownicy, klienci oraz kontrahenci Urzędu Gminy Padew Narodowa.

Wymagane potwierdzenie zapoznania się z dokumentem: TAK

Historia zmian dokumentu

Wersja	Data	Treść / Zmiana	Autor
1.0		Ustanowienie dokumentów	

Zawartość

1. O polityce bezpieczeństwa informacji

W celu efektywnej realizacji obowiązków wynikających z Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (tj. Dz.U.2026.20 t.j. z dnia 2026.01.09), Wójt Gminy Padew Narodowa, działając w ramach przysługujących mu kompetencji jako kierownik podmiotu ważnego, ustanawia System Zarządzania Bezpieczeństwem Informacji (SZBI).

Wprowadzenie SZBI ma na celu ograniczenie ryzyk wynikających z rozproszonego zarządzania bezpieczeństwem informacji, zapewnienie jednolitego poziomu zabezpieczeń oraz wsparcie pracowników i kierowników komórek organizacyjnych w realizacji ich obowiązków ustawowych. Dokument ten definiuje ramy dla ochrony usług świadczonych przez Gminę oraz zapewnia odporność infrastruktury teleinformatycznej na współczesne zagrożenia cyfrowe.

2. Kontekst organizacji

Urząd Gminy Padew Narodowa realizuje gminne zadania publiczne oraz zadania z zakresu administracji rządowej wynikające z ustaw oraz porozumień zawartych z innymi jednostkami administracji publicznej. Podstawą prawną funkcjonowania Urzędu jest ustawa o samorządzie gminnym, a sposób realizacji zadań określają wewnętrzne Regulaminy Organizacyjne.

Zróżnicowany charakter realizowanych zadań publicznych, przetwarzanie danych osobowych, informacji prawnie chronionych oraz danych istotnych z punktu widzenia ciągłości działania Urzędu powoduje, że ochrona informacji stanowi element kluczowy dla prawidłowego wykonywania zadań publicznych. System Zarządzania Bezpieczeństwem Informacji stanowi narzędzie zapewniające:

- ujednolicenie zasad zarządzania ryzykiem,
- zapewnienie wysokiego poziomu zabezpieczeń technicznych i organizacyjnych,
- określenie jasnej odpowiedzialności za zasoby informacyjne,
- zagwarantowanie ciągłości świadczenia usług kluczowych dla mieszkańców Gminy.

2.1. Czynniki zewnętrzne

Są to obszary, na które Urząd nie ma bezpośredniego wpływu, ale które kształtują jego obowiązki w zakresie cyberbezpieczeństwa.

W ramach uwarunkowań zewnętrznych, uwzględnia się w szczególności:

Obszar	Specyficzne czynniki dla Gminy Padew Narodowa
Regulacje prawne	Obowiązki podmiotu ważnego wynikające z nowelizacji UoKSC (implementacja dyrektywy NIS2), wymogi Krajowych Ram Interoperacyjności (KRI) oraz RODO.
Zagrożenia cyber	Wzrost ukierunkowanych ataków typu ransomware na infrastrukturę samorządową w Polsce; próby dezinformacji i phishingu wymierzone w pracowników administracji.
Relacje z dostawcami	Zależność od dostawców systemów dziedzinowych (kadry, płace, podatki) oraz operatorów usług chmurowych (np. hosting dla BIP).
Oczekiwania społeczne	Wymóg wysokiej dostępności e-usług dla mieszkańców (portal padewnarodowa.com.pl) oraz gwarancja ochrony danych osobowych przetwarzanych w procesach administracyjnych.
Współpraca instytucjonalna	Relacje z CSIRT GOV, nadzór Wojewody oraz współpraca z innymi jednostkami samorządu terytorialnego (JST) w regionie.

2.2. Czynniki wewnętrzne

Są to elementy specyficzne dla struktury i sposobu działania Urzędu Gminy, które mogą wspierać lub osłabiać bezpieczeństwo informacji.

W ramach uwarunkowań wewnętrznych, uwzględnia się w szczególności:

Obszar	Specyficzne czynniki dla Gminy Padew Narodowa
Struktura i procesy	Specyfika pracy urzędu gminy wiejskiej – bezpośredni kontakt z interesantem, procesy decyzyjne oparte na statucie gminy i regulaminie organizacyjnym.
Zasoby ludzkie	Świadomość cyberbezpieczeństwa pracowników; ograniczona liczebność kadry IT (częsta w mniejszych gminach), co wymusza precyzyjne definiowanie zastępstw.
Infrastruktura IT	Rozproszenie zasobów: lokalna sieć LAN w urzędzie, urządzenia mobilne pracowników terenowych, dostęp publiczny przez Wi-Fi dla interesantów.
Kultura organizacyjna	Tradycyjne podejście do obiegu dokumentów (hybrydowy model: papierowo-cyfrowy) i wynikające z tego ryzyka (np. ochrona dokumentacji papierowej).
Finanse i priorytety	Budżet gminy ograniczający tempo modernizacji infrastruktury, wymagający optymalizacji nakładów na cyberbezpieczeństwo (zasada proporcjonalności NIS2).
Zasoby informacyjne	Przetwarzanie unikalnych zbiorów danych: rejestry mieszkańców, decyzje podatkowe, dane o planowaniu przestrzennym, bazy portali informacyjnych.

3. Zainteresowane strony

Przyjęte reguły i zasady przetwarzania informacji dotyczą wszystkich pracowników jednostek oraz wykonawców usług i dostaw jak również inne podmioty współpracujące, które w ramach realizacji zawartych umów i na czas ich realizacji jeżeli będą posiadały dostęp do zasobów informacyjnych jednostek. Przyjęte zasady obowiązują niezależnie od formy przetwarzania informacji. Interesariuszami Systemu Zarządzania Bezpieczeństwem Informacji są w szczególności:

a) zainteresowane strony zewnętrzne

Podmiot / Grupa	Potrzeby i oczekiwania	Podstawa prawna / cel
Mieszkańcy i Interesanci	Ciągły dostęp do e-usług i BIP; pewność, że ich dane osobowe (PESEL, dane majątkowe) są bezpieczne i nie wycieką.	RODO, Ustawa o informatyzacji działalności podmiotów publicznych.
CSIRT GOV (ABW)	Terminowe raportowanie incydentów poważnych; utrzymywanie punktu kontaktowego dostępnego 24/7.	Ustawa o Krajowym Systemie Cyberbezpieczeństwa (UoKSC).
Minister Cyfryzacji / NASK	Zgodność ze standardami cyberbezpieczeństwa; raportowanie statystyk i gotowość do audytów.	Dyrektywa NIS2, UoKSC.
Wojewoda Podkarpacki	Sprawozdawczość z zakresu zarządzania kryzysowego i realizacji zadań zleconych.	Ustawa o samorządzie gminnym.
Dostawcy usług IT (np. hosting BIP)	Jasne procedury zgłaszania awarii; precyzyjne zapisy w umowach o odpowiedzialności za bezpieczeństwo danych.	Umowy SLA, ISO 27001 (A.5.19-23).
Banki i Instytucje Finansowe	Bezpieczeństwo transakcji płatniczych (podatki, opłaty lokalne); integralność numerów kont bankowych.	Ustawa o finansach publicznych.

b) zainteresowane strony wewnętrzne

Podmiot / Grupa	Potrzeby i oczekiwania	Podstawa prawna / cel
Wójt Gminy	Minimalizacja ryzyka prawnego i kar finansowych; ochrona wizerunku Gminy jako instytucji zaufania publicznego.	Kierownictwo podmiotu kluczowego (UoKSC).
Pracownicy Urzędu	Czytelne instrukcje bezpiecznej pracy; szkolenia z cyberbezpieczeństwa; sprawne narzędzia IT umożliwiające pracę zdalną/bezpieczną.	KRI (§ 20), Kodeks Pracy.
Referat Organizacyjny / podmiot zewnętrzny świadczący obsługę informatyczną	Jasne kompetencje; budżet na niezbędne zabezpieczenia; wsparcie kierownictwa w egzekwowaniu polityk haseł i dostępu.	ISO 27001 (Rola techniczna).
Inspektor Ochrony Danych (IOD)	Spójność SZBI z wymaganiami RODO; dostęp do rejestrów incydentów naruszenia prywatności.	RODO.
Rada Gminy	Transparentność wydatkowania środków na bezpieczeństwo; zapewnienie ciągłości pracy organów uchwałodawczych.	Ustawa o samorządzie gminnym.

4. Cele bezpieczeństwa informacji

Nadrzędnym celem Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w Urzędzie Gminy Padew Narodowa jest zapewnienie ciągłego i bezpiecznego świadczenia usług publicznych oraz ochrona zasobów informacyjnych przed wszelkimi zagrożeniami wewnętrznymi i zewnętrznymi, świadomymi lub przypadkowymi.

Urząd realizuje następujące cele strategiczne:

- **Zgodność prawna i regulacyjna:** Zapewnienie pełnej zgodności z ustawą o krajowym systemie cyberbezpieczeństwa (jako podmiot kluczowy), rozporządzeniem KRI oraz RODO.
- **Ciągłość działania:** Zagwarantowanie dostępności usług kluczowych i systemów informatycznych, w tym Biuletynu Informacji Publicznej (biuletyn.net) oraz portalu gminnego.
- **Ochrona aktywów:** Zapewnienie poufności, integralności i dostępności danych przetwarzanych w systemach dziedzinowych Urzędu.
- **Budowanie świadomości:** Systematyczne podnoszenie kompetencji pracowników w zakresie cyberbezpieczeństwa.

Operacjonalizacja celów:

- Cele bezpieczeństwa informacji są ustanawiane dla odpowiednich funkcji i poziomów w strukturze Urzędu Gminy.
- Cele muszą być mierzalne (o ile to możliwe), uwzględniać wymagania bezpieczeństwa informacji oraz wyniki oceny ryzyka i postępowania z ryzykiem.
- Cele są monitorowane, komunikowane pracownikom oraz aktualizowane w miarę potrzeb (np. po wystąpieniu istotnego incydentu lub zmiany w infrastrukturze).

Ustanawianie i dokumentowanie celów:

Wszelkie cele szczegółowe na dany okres rozliczeniowy (rok kalendarzowy) oraz plany ich osiągnięcia są dokumentowane i zatwierdzane przez Wójta Gminy. Proces ustanawiania, monitorowania oraz rozliczania celów realizowany jest za pomocą formularza „Karta celów SZBI" o numerze F 00-1.

5. Podstawy prawne

Podstawą do opracowania i wdrożenia niniejszej polityki są w szczególności:

- Rozporządzenie Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (ogólne rozporządzenie o ochronie danych RODO),
- Dyrektywa Parlamentu Europejskiego i Rady (UE) w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii (NIS2)
- Ustawa o krajowym systemie cyberbezpieczeństwa,
- Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne
- Rozporządzenie Rady Ministrów w sprawie w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych
- Krajowe Normy: PN-EN ISO/IEC-27001:2023-08.

6. Ciągłe doskonalenie systemu

Wdrożony i utrzymywany w jednostkach System Zarządzania Bezpieczeństwem Informacji:

- podlega cyklicznym (nie rzadziej niż raz do roku) przeglądom,
- poddawany jest cyklicznym audytom wewnętrznym i zewnętrznym wskazującym potencjalne niezgodności i inicjującym działania korygujące,
- oparty jest na ciągłym procesie zarządzania ryzykiem w ramach którego oceniana jest efektywność istniejących zabezpieczeń oraz podejmowane są decyzje dotyczące wdrażania działań mających na celu wyeliminowanie lub ograniczenie zidentyfikowanych ryzyk.

7. Zakres systemu

Zakres ustanowionego Systemu Zarządzania Bezpieczeństwem Informacji obejmuje lokalizację Urzędu Gminy Padew Narodowa:

1. Informacje przetwarzane w ramach wszelkich realizowanych w jednostkach procesów, czynności przetwarzania i zadań, zarówno w formie tradycyjnej (m.in. informacje wydrukowane lub zapisane na papierze) jak i elektronicznej.
2. Aktywa wspierające przetwarzanie informacji w ramach ww. procesów oraz realizowanych zadań, w tym:
    a. personel (wszyscy pracownicy bez względu na formę zatrudnienia, praktykanci, stażyści, wolontariusze oraz inne osoby i podmioty zewnętrzne wykonujące czynności w imieniu i na rzecz jednostek i/lub mające dostęp do aktywów informacyjnych jednostek),
    b. budynki i pomieszczenia, w których są przetwarzane informacje,
    c. sprzęt, w tym sprzęt komputerowy, urządzenia mobilne oraz inne nośniki danych, na których znajdują się informacje podlegające ochronie, oprogramowanie, infrastruktura sieciowa i serwerowa
    d. systemy aplikacyjne, systemy operacyjne i oprogramowanie narzędziowe stanowiące składowe systemów teleinformatycznych wykorzystywanych do przetwarzania informacji.

Polityka i opisane w niej zasady nie dotyczą informacji przetwarzanych na podstawie ustawy o ochronie informacji niejawnych.

8. Podstawowe zasady bezpieczeństwa informacji

1. **Zasada ograniczenia celu** – dane osobowe oraz inne przetwarzane informacje muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami. Cel ten musi być określony w momencie ich pozyskiwania. (art. 5 ust.1 lit. b RODO).
2. **Zasada zgodności z prawem, rzetelności i przejrzystości** – dane osobowe oraz inne przetwarzane informacje muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dotyczą. Wszelkie informacje i komunikaty związane z przetwarzaniem muszą być łatwo dostępne i zrozumiałe oraz sformułowane jasnym i prostym językiem (art. 5 ust. 1 lit. a i motyw 39 RODO).
3. **Zasada minimalizacji danych** - pozyskiwane mogą być jedynie dane adekwatne i niezbędne dla osiągnięcia celów konkretnych, uzasadnionych i określonych w momencie zbierania danych. Nie można zbierać informacji, które nie mają związku z celem przetwarzania, są nadmiarowe lub już nieprzydatne (np. ze względu na ich nieaktualność) (art. 5 ust. 1 lit. c i motyw 39 RODO).
4. **Zasada prawidłowości danych** - dane osobowe oraz inne przetwarzane informacje muszą być prawidłowe i w razie potrzeby uaktualniane. Należy podejmować wszelkie rozsądne działania, aby informacje, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane (art. 5 ust. 1 lit. d RODO).

5. **Zasada ograniczenia czasowego** - dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, dla których dane te są przetwarzane. Przechowywanie danych zgromadzonych np. w celu realizacji umowy powinno być zakończone w momencie przedawnienia roszczeń czy innych praw i obowiązków wynikających z przepisów prawa (art. 5 ust. 1 lit. e RODO).
6. **Zasada integralności i poufności** -dane osobowe oraz inne informacje muszą być przetwarzane w sposób zapewniający im odpowiednie bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych (art. 5 ust. 1 lit. f RODO).
7. **Zasada ograniczonego przetwarzania -** podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie administratora, przez co rozumie się przetwarzanie na podstawie i w zakresie udzielonego upoważnienia lub zawartej umowy powierzenia przetwarzania danych osobowych. (art. 29 RODO)**.**
8. **Zasada rozliczalności –** decyzje związane z przetwarzaniem informacji ze szczególnym uwzględnieniem zabezpieczeń muszą być dokumentowane. Wszelkie działania związane z przetwarzaniem danych (w szczególności decyzje dotyczące dostępu do informacji lub zasobów służących do jej przetwarzania) muszą być dokumentowane lub powodować tworzenie zapisów pozwalających na ocenę zgodności podejmowanych działań z przyjętymi zasadami.
9. **Zasada odpowiedzialności** – odpowiedzialność za czynności przetwarzania, podejmowanie decyzji o dostępie do informacji, dokumentację, procesy i środki przetwarzania musi być jednoznacznie przypisana do pracowników lub komórek organizacyjnych.
10. **Zasada wiedzy koniecznej** – możliwość uzyskania dostępu do informacji wyłącznie w zakresie niezbędnym dla realizacji obowiązków służbowych lub zapisów umowy.
11. **Zasada identyfikowalności** – osoby, procesy, urządzenia uzyskujące dostęp do informacji lub zasobów służących do jej przetwarzania muszą być w sposób jednoznaczny identyfikowalne.
12. **Zasada uwierzytelnienia** – mechanizmy kontroli dostępu osoby, procesu, urządzenia do informacji lub zasobów służących do jej przetwarzania muszą wykorzystywać właściwe środki uwierzytelniające oraz zapewniać bezpieczeństwo informacji uwierzytelniających.
13. **Rozdzielenie obowiązków** – rozdzielenie obowiązków związanych z podejmowaniem decyzji związanych z dostępem do informacji oraz zasobów wykorzystywanych do jej przetwarzania od obowiązków związanych z techniczną ich realizacją.
14. **Zasada uwzględnienia ochrony danych w fazie projektowania** – wdrożenie nowej czynności przetwarzania, procesu (w szczególności z wykorzystaniem narzędzi informatycznych) musi być poprzedzone fazą planowania obejmującą analizę związanych z nią ryzyk oraz uwzględnienie odpowiednich zabezpieczeń.

9. Odstępstwa

Podejmowanie jakichkolwiek działań mogących naruszać przyjęte w niniejszej Polityce zasady wymaga pisemnej zgody Wójta.
Odstępstwa od zasad wyrażonych w innych wymienionych w załączniku 1 dokumentów SZBI wymagają akceptacji osoby zatwierdzającej dokument, którego odstępstwo dotyczy.

10. Odpowiedzialność

1. W stosunku do osób naruszających zasady przyjęte w niniejszej Polityce oraz innych przygotowanych na jej podstawie dokumentach stanowiących składowe Systemu Zarządzania Bezpieczeństwem Informacji wszczynane będzie postępowanie dyscyplinarne zgodnie z obowiązującym w danej jednostce organizacyjnej regulaminem pracy.
2. Postępowanie sprzeczne z obowiązującymi zasadami może być uznane przez Pracodawcę za ciężkie naruszenie obowiązków pracowniczych w rozumieniu art. 52 § 1 pkt 1 Kodeksu Pracy.
3. Wszczęcie postępowania dyscyplinarnego nie wyklucza odpowiedzialności karnej za przestępstwa popełnione przeciwko bezpieczeństwu informacji.

11. Deklaracja najwyższego kierownictwa

Jako Wójt Gminy Padew Narodowa, deklaruję pełne zaangażowanie w rozwój i doskonalenie Systemu Zarządzania Bezpieczeństwem Informacji. Moim celem jest zapewnienie, aby przetwarzanie informacji w Urzędzie odbywało się w sposób gwarantujący ich poufność, integralność i dostępność.

Bezpieczeństwo cyfrowe mieszkańców oraz ciągłość działania administracji lokalnej są priorytetami, które realizujemy poprzez systematyczne zarządzanie ryzykiem, szkolenia personelu oraz inwestycje w bezpieczne technologie. Niniejsza Polityka jest fundamentem budowania zaufania obywateli do Gminy jako nowoczesnego i bezpiecznego urzędu.

11. Wykaz polityk Systemu Zarządzania Bezpieczeństwem Informacji

00. Polityka Bezpieczeństwa Informacji wersja: 1.0
01. Role i odpowiedzialności wersja: 1.0
02. Polityka nadzoru nad dokumentami wersja: 1.0
03. Klasyfikacja informacji wersja: 1.0
04. Procedura audytów wewnętrznych Systemu Zarządzania Bezpieczeństwem Informacji wersja: 1.0
05. Polityka bezpieczeństwa osobowego wersja: 1.0
06. Polityka zarządzania ciągłością działania w zakresie systemów informatycznych wersja: 1.0
07. Polityka zarządzania kopiami bezpieczeństwa wersja: 1.0
08. Procedura monitorowania systemów informatycznych wersja: 1.0
09. Polityka zarządzania zasobami wersja: 1.0
10. Polityka zarządzania dostępem do usług teleinformatycznych wersja: 1.0
11. Polityka wykorzystania technologii kryptograficznych wersja: 1.0
12. Regulamin korzystania z urządzeń i usług teleinformatycznych wersja: 1.0
13. Polityka bezpieczeństwa fizycznego wersja: 1.0

14. Procedura zgłaszania i obsługi incydentów bezpieczeństwa informacji wersja: 1.0
15. Polityka nadzoru nad dostawcami wersja: 1.0
16. Polityka zarządzania ryzykiem wersja: 1.0
17. Polityka ochrony danych osobowych wersja: 1.0