Burmistrz Miasta i Gminy Osiek
ul. Rynek 1, 28-221 Osiek

Zarządzenie Nr 126/2025
Burmistrza Miasta i Gminy Osiek
z dnia 08 grudnia 2025 r.

w sprawie wprowadzenia Politykę Bezpieczeństwa Informacji w Urzędzie Miasta i Gminy Osiek

Na podstawie art. 30 ust. 1 w zw. z art. 31 i art. 33 ust. 1 i 3 ustawy z dnia 8 marca 1990 roku o samorządzie gminnym (t.j. Dz. U. z 2025 r. poz. 1153) w zw. z art. 24 ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. 119.1 z 04.05.2016) oraz Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t.j. Dz.U. z 2014, poz. 773) zarządzam, co następuje:

§1

Wprowadzona zostaje Procedura zarządzania incydentami cyberbezpieczeństwa w Urzędzie Miasta i Gminy w Osieku, stanowiąca Załącznik Nr 1 do niniejszego Zarządzenia.

§2

Zobowiązuje się wszystkich pracowników Urzędu Miasta i Gminy w Osieku do stosowania i przestrzegania „Polityki Bezpieczeństwa Informacji", o której mowa w § 1

§3

Wykonanie zarządzenia powierzam Sekretarzowi Miasta i Gminy w Osieku.

§4

Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ
Miasta i Gminy
Magdalena Marynowska

Załącznik nr 1 do Zarządzenia Nr 126/2025
Burmistrza Miasta i Gminy Osiek
z dnia 08 grudnia 2025 r.

POLITYKA BEZPIECZEŃSTWA INFORMACJI

w Urzędzie Miasta i Gminy w Osieku

WSTĘP

Opis objętych systemem referatów i stanowisk pracy

Urząd Miasta i Gminy w Osieku jest jednostką samorządu terytorialnego, którego głównym zadaniem jest realizacja zadań na poziomie gminy. Urząd działa na rzecz mieszkańców miasta i gminy, wykonując zadania własne oraz zlecone przez administrację rządową. W strukturach organizacyjnych Urzędu znajdują się:

- Burmistrz Miasta i Gminy Osiek
- Zastępca Burmistrza Miasta i Gminy Osiek
- Sekretarz Miasta i Gminy w Osieku
- Skarbnik Miasta i Gminy Osiek
- Informatyk
- Referat Finansowo-Księgowy
- Referat Administracyjno-Organizacyjny
- Referat Budownictwa, Inwestycji i Zamówień Publicznych
- Referat Gospodarki Komunalnej, Rolnictwa i Ochrony Środowiska
- Urząd Stanu Cywilnego

§ 1

Postanowienie wstępne

1. **Kompletna oferta**

a) Gospodarka komunalna:
   - Dostarczanie wody, odbiór ścieków,
   - Utrzymanie dróg gminnych, chodników, oświetlenia ulicznego.

b) Planowanie przestrzenne i zagospodarowanie terenu:
   - Uchwalanie miejscowych planów zagospodarowania przestrzennego,
   - Wydawanie decyzji o warunkach zabudowy.

c) Oświata:
   - Prowadzenie przedszkoli, szkół podstawowych, świetlic,
   - Zapewnienie transportu szkolnego i dofinansowań.

d) Pomoc społeczna i wsparcie rodzin:
   - Ośrodek pomocy społecznej.

e) Kultura, sport i rekreacja:
   - Prowadzenie biblioteki, dom kultury, organizowanie imprez lokalnych,
   - Utrzymanie obiektów sportowych i placów zabaw.

f) Ochrona środowiska:
   - Gospodarka odpadami, ochrona zieleni,
   - Edukacja ekologiczna.

g) Bezpieczeństwo publiczne:
   - Współpraca z Policją, Strażą Pożarną,

h) Zadania zlecone (na podstawie ustaw, w imieniu administracji rządowej):
   - Wydawanie dowodów osobistych i prowadzenie ewidencji ludności,
   - Rejestracja urodzeń, małżeństw, zgonów (Urząd Stanu Cywilnego),
   - Przeprowadzanie wyborów i referendów,
   - Wydawanie zezwoleń (np. na alkohol, działalność gospodarczą),

2. Bezpieczeństwo i niezawodność

Bezpieczeństwo informacji zapewnia doświadczony personel wykorzystujący w swej pracy standardowe doskonalone przez lata metody prowadzenia komunikacji wraz z wykorzystaniem nowoczesnych technik a także technologii informatycznych.

3. Definicja bezpieczeństwa i zakresu systemu

Celem zarządzającego bezpieczeństwem informacji jest zapewnienie bezpieczeństwa informacjom chronionym, zarówno własnym jak i powierzonym przez klientów, w tym danych osobowych, poprzez zapewnienie informacjom cech poufności, integralności oraz dostępności.

4. Zakres Systemu Bezpieczeństwa Informacji

Zakres Systemu Bezpieczeństwa Informacji określony przez Politykę Bezpieczeństwa Informacji mają zastosowanie do całego systemu informacyjnego Urzędu Miasta i Gminy, a w szczególności do:

a) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których są przetwarzane informacje podlegające ochronie,
b) informacji będących własnością Urzędu Miasta i Gminy,

c) informacji będących własnością interesantów Urzędu Miasta i Gminy,

d) wszystkich lokalizacji Urzędu Miasta i Gminy w Osieku, czyli budynków i pomieszczeń, sposobów ich zabezpieczenia, których są lub będą przetwarzane dane podlegające ochronie,

e) wszystkich pracowników w rozumieniu Kodeksu Pracy, stażystów, wolontariuszy i innych osób mających dostęp do informacji podlegających ochronie.

5. Słownik pojęć:

Autentyczność – właściwość polegająca na tym, że pochodzenie lub zawartość danych opisujących obiekt są takie jak deklarowane;

Dostępność – właściwość określająca, że zasób systemu teleinformatycznego jest możliwy do wykorzystania na żądanie w założonym czasie, przez podmiot uprawniony do pracy w systemie teleinformatycznym;

Integralność – właściwość polegająca na tym, że zasób systemu teleinformatycznego nie został zmodyfikowany w sposób nieuprawniony;

Poufność – właściwość zapewniająca, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom fizycznym;

Autoryzacja – proces, w którym sprawdzane jest czy dany podmiot ma prawo dostępu do zasobów o które prosi. Autoryzacja jest poprzedzona uwierzytelnieniem podmiotu;

Aktywa informacyjne – dane różnego rodzaju oprogramowanie i dokumentacja związana z opracowaniem wdrożeniem, a następnie eksploatacją danego systemu IT;

Analiza ryzyka – proces systematycznej identyfikacji ryzyk, określenia ich wielkości identyfikowania obszarów wymagających zabezpieczeń;

Dane osobowe – informacje o osobach fizycznych chronione zgodnie z ustawą o ochronie danych osobowych;

Incydent związany z bezpieczeństwem informacji – pojedyncze zdarzenia lub seria niepożądanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań i zagrażają bezpieczeństwu informacji;

Urząd, UMiG – oznacza Urząd Miasta i Gminy w Osieku;

Kopia zapasowa - kopia danych lub oprogramowania. Celem jej wykonania jest odtworzenie systemu po awarii;

Ocena ryzyka – proces porównywania oszacowanego ryzyka z określonymi kryteriami w celu określenia znaczenia ryzyka;

Postępowanie z ryzykiem – proces wyboru wdrażania środków w celu zmniejszenia ryzyka do akceptowanego poziomu;

Pracownik – osoba fizyczna, która zawarła z UMiG umowę o pracę;

Ryzyko – iloczyn prawdopodobieństwa skutku, że określone zagrożenie wykorzysta podatność zasobu lub grupy zasobów albo spowodować szkody straty lub zniszczenie zasobów;

Serwer – komputer świadczący usługi wchodzący w skład systemu informatycznego;

Stacja robocza – komputer, na którym w strukturach Urzędu pracują osoby obsługujące aplikacje informatycznego;

System IT/ system – synonim systemu informatycznego. Każdy system teleinformatyczny ma przypisane imienne, co najmniej 1 osobę będącą jego administratorem (najczęściej administrator systemu oraz administrator merytoryczny);

Szacowanie ryzyka – całościowy proces analizy oceny ryzyka odbywający się na zasadach określonych w odrębnej procedurze dotyczącej zarządzania ryzykiem wewnętrznym w Urzędzie;

Uwierzytelnienie – proces polegający na zweryfikowaniu zadeklarowanej tożsamości osoby, urządzenia lub usługi biorącej udział w wymianie danych;

Użytkownik systemu – pracownik lub współpracownik, który w ramach swoich zadań wykonuje zadania związane z używaniem aplikacji informatycznych;

Właściciel aktywów – pracownik lub współpracownik UMiG który w ramach swoich kompetencji podejmuje decyzje odnośnie osoby wykorzystania aktywów, do których ma uprawnienia. W szczególności poprzez decyzje o sposobie wykorzystania rozumie się decyzję o nadaniu uprawnień innym użytkownikom.

Wrażliwość – atrybut informacji wskazujący, że jej ujawnienie przynosi straty Urzędu;

Współpracownik – osoba fizyczna wykonująca zadania w ramach zawartej z Urzędem umowy cywilnoprawnej;

Zabezpieczenie – środki techniczne i fizyczne oraz metody proceduralno - organizacyjne utrzymania pożądanych atrybutów informacji: jej poufność, integralność, dostępność, rozliczalność, autentyczność oraz pożądane atrybuty systemu teleinformatycznego – integralność i niezawodność;

Zagrożenie – potencjalna możliwość naruszenia bezpieczeństwa systemu informatycznego;

Zarządzanie ryzykiem – skoordynowanie działania kierowania i zarządzanie organizacją z uwzględnieniem ryzyka. Zarządzanie ryzykiem odbywa się na zasadach określonych w odrębnej procedurze;

Zasoby informacyjne – ogół informacji będących w posiadaniu Urzędu, niezależnie od klasyfikacji i stopnia wymaganej ochrony. Obejmuje zarówno informacje przechowywane i przetwarzane

w systemie jak i te które występują poza systemem;

Zdarzenie związane z bezpieczeństwem informacji – jest to określony stan systemu, usługi sieci, który wskazuje na możliwe naruszenie polityki bezpieczeństwa informacji, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana ze zmianą poziomu bezpieczeństwa;

6. Zasady ogólne

Każdy pracownik powinien być zapoznany z regulaminem oraz kompletnymi i aktualnymi procedurami ochrony informacji.

Poniższe uniwersalne zasady są podstawą realizacji polityki bezpieczeństwa informacji:

- **zasada uprawnionego dostępu.** Każdy pracownik przechodzi szkolenie z zasad ochrony informacji, spełnia kryteria dopuszczenia do informacji i podpisuje stosowne oświadczenie o zachowaniu poufności.
- **zasada przywilejów koniecznych.** Każdy pracownik posiada prawo dostępu do informacji, ograniczone wyłącznie do tych, które są konieczne do wykonywania powierzonych zadań.
- **zasada wiedzy koniecznej.** Każdy pracownik posiada wiedzę o systemie, do którego ma dostęp, ograniczoną wyłącznie do zagadnień, które są mu konieczne do realizacji powierzonych zadań.
- **zasada asekuracji.** Każdy mechanizm zabezpieczający musi być ubezpieczony drugim, innym (podobnym). W przypadkach szczególnych może być stosowane trzeci (dodatkowe zabezpieczenie).
- **zasada świadomości zbiorowej.** Wszyscy pracownicy są świadomi konieczności ochrony zasobów informacyjnych i aktywnie uczestniczą w tym procesie.
- **zasada indywidualnej odpowiedzialności.** Za bezpieczeństwo poszczególnych elementów odpowiadają konkretne osoby.
- **zasada obecności koniecznej.** Prawo przebywania w określonych miejscach mają tylko osoby upoważnione.
- **zasada stałej gotowości.** System jest przygotowany na wszelkie zagrożenia. Niedopuszczalne jest tymczasowe wyłączenie mechanizmów zabezpieczających.
- **zasada najsłabszego ogniwa.** Poziom bezpieczeństwa wyznacza najsłabszy (najmniej zabezpieczony) element.
- **zasada kompletności.** Skuteczne zabezpieczenie jest tylko wtedy, gdy stosuje się podejście kompleksowe uwzględniające wszystkie stopnie i ogniwa pojętego procesu przetwarzania

informacji.

- **zasada ewolucji.** Każdy system musi ciągle dostosowywać mechanizmy wewnętrzne do zmieniających się warunków zewnętrznych.
- **zasada odpowiedzialności.** Używane mechanizmy muszą być adekwatne do sytuacji.
- **zasada akceptowanej równowagi.** Podejmowane środki zaradcze nie mogą przekraczać poziomu akceptacji.
- **zasada świadomej konwersji.** Nie zawsze i wszędzie trzeba mówić co się wie, ale zawsze i wszędzie trzeba wiedzieć co, gdzie i do kogo się mówi

7. Definicja bezpieczeństwa informacji

Bezpieczeństwo informacji oznacza zapewnienie następujących cech:

Poufność – właściwość zapewniająca, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom albo procesom.

Integralność danych – właściwości zapewniającej, że dane (forma prezentacji informacji) nie zostały zmienione lub zniszczone w sposób nieautoryzowany, są dokładne i kompletne.

Integralność systemu – właściwości polegającej na tym, że system realizuje swoją zamierzoną funkcję w sposób nienaruszony, wolny od nieautoryzowanej manipulacji celowej lub przypadkowej.

Dostępność – właściwość bycia dostępnym, możliwym do wykorzystania na żądanie w założonym czasie, poprzez autoryzowany podmiot.

Rozliczalność – właściwości zapewniającej, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

§ 2

Deklaracja Burmistrza Miasta i Gminy w Osieku

Bezpieczeństwo informacji oraz systemów, w których są przetwarzane jest jednym z kluczowych elementów jakości oferowanej klientom przez wszystkie referaty oraz warunkiem ciągłego rozwoju Urzędu. Gwarancją sprawnej i skutecznej ochrony informacji jest zapewnienie odpowiedniego poziomu kultury bezpieczeństwa oraz zastosowanie przemyślanych rozwiązań technicznych.

Priorytetowym celem systemu jest spełnienie wymagań prawnych oraz zapewnienie ciągłości działania organizacji, poufności danych wrażliwych i dostępności wymaganych informacji.

Burmistrz Miasta i Gminy w Osieku wprowadzając politykę Bezpieczeństwa Informacji deklaruje, że

wdrożony system będzie podlegał ciągłemu doskonaleniu, aż do osiągnięcia wymagań *normy PN-ISO/IEC 27001*

Cele główne stawiane przed systemem zarządzanie bezpieczeństwem informacji:

1. Zapewnienie spełniania wymagań prawnych;
2. Ochrona systemów przetwarzania informacji przed nieuprawnionym dostępem bądź zniszczeniem;
3. Podnoszenie świadomości pracowników;
4. Zmniejszenie ryzyka utraty informacji;
5. Zaangażowanie wszystkich pracowników w ochronę informacji.

Podejście do bezpieczeństwa informacji wywodzi się z następujących kwestii:

1. zapewnienie, że informacja jest udostępniana jedynie osobom upoważnionym (tzw. reguła poufności informacji);
2. zapewnienia dokładności i kompletności informacji oraz metod jej przetwarzania (tzw. reguła integralności informacji);
3. zapewnienie, że osoby upoważnione mają dostęp do informacji związanych i związanych z nią aktywów tylko wtedy, gdy istnieje taka potrzeba (tzw. reguła dostępności informacji);

W Urzędzie Miasta i Gminy w Osieku kierownictwo zapewnia bezpieczeństwo informacji poprzez:

1. Zarządzanie ryzykiem, na które składa się identyfikacja zagrożeń, analiza ryzyka, ocena prawdopodobieństwa wystąpienia czynnika ryzykownego oraz określenie skutków jakie może wywołać ryzyko, określenie i wdrożenie mechanizmów kontrolnych oraz sposobów reagowania na powyższe zjawisko.
2. Zarządzanie zmianą na które składa się analiza wpływu zmiany na poziom bezpieczeństwa oraz zapewnienie pełnej koordynacji podczas wprowadzania zmian.
3. Zarządzanie ciągłością organizacji poprzez określenie i wdrożenie instrukcji i procedur awaryjnych.

Kierownictwo Urzędu zapewnia środki niezbędne do realizacji Polityki Bezpieczeństwa Informacji.

Szczegółowe rozwinięcie zagadnień objętych Deklaracją jest udokumentowane w Polityce Bezpieczeństwa Informacji.

§ 3
Dziedziny bezpieczeństwa

Zapewnienie bezpieczeństwa informacji oznacza zapewnienie bezpieczeństwa informacji w następujących obszarach:

- Organizacja Bezpieczeństwa Informacji
- Zarządzanie aktywami

1. Organizacja bezpieczeństwa informacji

1) Struktura zarządzania bezpieczeństwem

Przyjmuje się, że podstawowymi zasadami przy tworzeniu struktur zarządzających bezpieczeństwem są:

- bezwzględne oddzielenie funkcji zarządzających i kontrolnych od funkcji wykonawczych
- uniemożliwienie i maksymalne ograniczenie błędów popełnionych przez pojedyncze osoby w sferze jednoosobowej odpowiedzialności

2) Koncepcja dokumentacji systemu zarządzania bezpieczeństwem informacji

Dokumentacja systemu zarządzania bezpieczeństwem składa się z elementów Polityki Bezpieczeństwa Informacji

- Deklaracja stosowania
- Procedury i instrukcje bezpieczeństwa, które określają szczegółowo zasady postępowania
- Raporty z analiz ryzyka i plany postępowania z ryzykiem

3) Struktura zarządzania bezpieczeństwem i podział odpowiedzialności

Odpowiedzialność za ochronę informacji w UMiG ponoszą wszyscy pracownicy zgodnie z posiadanym zakresem obowiązków.

- **Burmistrz oraz kierownicy referatów** – są odpowiedzialni za zapewnienie zasobów niezbędnych dla opracowania wdrożenia i funkcjonowania oraz utrzymania i doskonalenia systemu zarządzania bezpieczeństwem informacji oraz utrzymania i doskonalenia systemu

zarządzania bezpieczeństwem informacji oraz poszczególnych zabezpieczeń. Burmistrz wydaje zgodę na użytkowanie urządzeń służących do przetwarzania informacji i zabezpieczeń. Burmistrz decyduje także o współpracy w zakresie bezpieczeństwa z innymi podmiotami. Burmistrz wyraża zgodę na udostępnienie informacji stronom trzecim, także informacji stanowiącej tajemnicę Urzędu. Codzienne postępowanie Burmistrza oraz kierowników referatów stanowi przykład dla innych pracowników, wskazanie, iż aspekty bezpieczeństwa informacji posiada wysoki priorytet we wszystkich podejmowanych działaniach.

- **Właściciel aktywu** odpowiada za bieżące nadzorowanie oraz zarządzanie aktywem
- **Administrator systemu** – odpowiada za realizację i nadzór nad technicznymi aspektami aktywu w kooperacji z właścicielem aktywu

Powołana do ryzyka grupa wykonuje zadania związane z bezpieczeństwem informacji. Do zadań grupy należą:

- dokonywanie przeglądu aktualności Polityki Bezpieczeństwa Informacji;
- monitorowanie ważnych zmian narażania aktywów informacyjnych na podstawowe zagrożenia;
- monitorowanie naruszeń bezpieczeństwa informacji;
- podejmowanie przedsięwzięć zmierzających do podniesienia poziomu bezpieczeństwa informacji;
- upowszechnienie dobrych praktyk bezpieczeństwa informacji w komórkach wewnętrznych.

4) Zasady współpracy z osobami trzecimi

Każda osoba, która wykonuje prace zlecone na terenie Urzędu jest zobligowana do:

- przestrzegania tajemnicy służbowej
- przestrzegania tajemnicy danych osobowych i personalnych
- przestrzeganie Polityki Bezpieczeństwa Informacji
- przestrzegania zasad i reguł BHP i ppoż.

Dostęp do pomieszczeń biurowych, gdzie przechowywane są informacje nadzorowany jest przez pracowników Urzędu.

Współpraca Urzędu z innymi podmiotami oparta jest na umowach, regulaminach lub zarządzeniach, porozumieniach.

5) Polityka kontroli dostępu do informacji

Dostęp do informacji przetwarzanych i przechowywanych w Urzędzie Miasta i Gminy jest poddawany kontroli wynikającej z przepisów prawa powszechnie obowiązującego. Kontrola polega na:

- wydzieleniu obszarów przeznaczonych do przechowywania oraz przetwarzania poszczególnych zbiorów danych i zapewnieniu odpowiednich barier fizycznych przeciwdziałających nieuprawnionemu dostępowi
- zarządzaniu uprawnieniami poszczególnych użytkowników w sposób zapewniający dostęp do danych wymaganych do wykonywania obowiązków służbowych, jeśli dane te podlegają ochronie z jakiejkolwiek przyczyny
- stosowaniu bezpiecznych systemów przetwarzania informacji
- nadzorowaniu działalności stron trzecich mogących wpłynąć na bezpieczeństwo informacji.
- bieżącym informowaniu pracowników o wszystkich zmianach w zakresie regulacji dotyczących przechowywania, przetwarzania i udostępnienia informacji

2. Zarządzanie aktywami

1) Chronione aktywa

W ramach zapewnienia bezpieczeństwa informacji w Urzędzie ochronie podlegają aktywa, na które składają się:

- informacje jawne – informacje publiczne udostępnione
- informacje wewnętrzne – informacje których przetwarzanie i udostępnienie podlegają restrykcjom z uwagi na szczególne znaczenie dla Urzędu (właściciela informacji):
- informacje wewnętrzne dostępne – informacje dostępne dla wszystkich pracowników Urzędu (zarządzenia, procedury postępowania, sposoby zabezpieczeń danych)
- informacje wewnętrzne wrażliwe – informacje dostępne dla grup pracowników, które pracownik wykorzystuje zgodnie z przydzielonym zakresem odpowiedzialności
- informacje stanowiące tajemnicę Urzędu – informacje których ujawnienie może narazić Urząd na szkody (np. kody, hasła, dane osobowe), urządzenia i infrastruktura techniczno – systemowa, dokumentacja systemowa eksploatacyjna, podwykonawcza zarówno w wersji papierowej jak i elektronicznej. Dostęp do tych danych posiadają wyłącznie pracownicy upoważnieni.

W zakres niniejszej Polityki nie wchodzi ochrona informacji niejawnych, ponieważ obecnie informacje te nie są gromadzone, przetwarzane lub przechowywane.

Urząd zarządza swoimi aktywami informacyjnymi w celu zapewnienia im wymaganego poziomu bezpieczeństwa. Szczególnie traktowane są informacje dotyczące danych osobowych.

Ważnym elementem zarządzania aktywami i bezpieczeństwem informacji jest przeprowadzenie określonej, nie rzadkiej niż raz w roku analizy ryzyka i opracowywania planów postępowania z ryzykiem. Analiza jej wyników stanowi podstawę podejmowania wszelkich działań w zakresie doskonalenia ochrony zasobów. Proces szacowania ryzyka obejmujący identyfikację, analizę i ocenę ryzyka w zakresie bezpieczeństwa informacji. Odbywa się na zasadach określonych w odrębnej procedurze zarządzania ryzykiem.

2) Autoryzacja nowych urządzeń

Każde nowe lub zmienione urządzenie służące do przetwarzania informacji lub mogące w jakikolwiek sposób wpływać na bezpieczeństwo informacji musi zostać zweryfikowane na zgodność z wymaganiami systemu bezpieczeństwa informacji i zaakceptowane przez informatyka.

3) Bezpieczeństwo zasobów ludzkich

Urząd dba o zapewnienie kompetentnych pracowników do realizacji wyznaczonych w procesach zadań. Celem takiego postępowania jest ograniczenie ryzyka błędu ludzkiego, kradzieży, nadużycia lub niewłaściwego użytkowania zasobów.

Skuteczna realizacja ograniczenia ryzyka możliwa jest dzięki ustanowionym praktykom i podziałowi odpowiedzialności związanym z weryfikacją kandydatów do pracy podczas naboru, zasadom zatrudnienia pracowników oraz ustalonym w przepisach prawa ogólnie obowiązującego procedurom rozwiązywania umów o pracę.

Pracownicy są okresowo oceniani pod względem spełniania wymagań bezpieczeństwa oraz szkoleni z tej tematyki.

Zasoby ludzkie są ważnym czynnikiem analizowanym podczas przeprowadzenia określonej analizy ryzyka. Tylko kompetentni i zaufani pracownicy są gwarantem bezpieczeństwa informacji.

4) Bezpieczeństwo fizyczne i środowiskowe

Urząd dba o zapewnienie wysokiego poziomu bezpieczeństwa fizycznego i środowiskowego.

Cele takiego postępowania jest zapewnienie bezpieczeństwa informacji przed dostępem osób niepowołanych, uszkodzeniem lub zakłóceniami w siedzibie Urzędu w odniesieniu do informacji.

W przypadku danych osobowych najistotniejsze jest zapewnienie wszystkich trzech podstawowych aspektów bezpieczeństwa poufności danych oraz ich dostępności i integralności.

Skuteczna realizacja postawionego celu możliwa jest dzięki ustanowionym praktykom i podziałowi odpowiedzialności związanemu z wyznaczeniem stref bezpieczeństwa, zasadami pracy oraz administrowaniem prawami dostępu do nich. Kluczowe systemy informatyczne wyposażone są w systemy podtrzymujące zasilanie.

5) Zarządzanie systemami i sieciami

Urząd dba o przestrzeganie zasad związanych z utrzymaniem, użytkowaniem systemów informatycznych i sieci w celu zapewnienia poufności, integralności i dostępności przetwarzanej przez nie informacji własnych.

Skuteczna realizacja postawionego celu jest możliwa dzięki:

- kompetencjom świadomości pracowników
- opracowanym zasadom konserwacji urządzeń w celu zapewnienia ich ciągłości
- kontrolowaniu wprowadzenia wszelkich zmian do infrastruktury technicznej
- usługi dostarczane przez osoby trzecie są nadzorowane, a w szczególności wszelkie wprowadzane do nich zmiany. Po zakupie lub wprowadzeniu zmiany do systemu jest on odbierany i akceptowany w sposób świadomy, uwzględniający jego wpływ na istniejący system bezpieczeństwa
- wdrożone są zabezpieczenia chronione przed oprogramowaniem złośliwym i mobilnym
- usystematyzowanemu tworzeniu kopii bezpieczeństwa
- bieżącemu monitorowaniu aktywów informacyjnych w tym informatycznych, pod kątem wcześniejszego wykrycia wszelkich niebezpieczeństw mogących zagrozić bezpieczeństwu systemów
- monitorowaniu incydentów w systemach informatycznych oraz stosowaniu mechanizmów reagowania w przypadkach ich wystąpienia

Szczegółowe zasady bezpieczeństwa informacji przetwarzanych w systemie określają procedury zarządzane systemami informatycznymi służącymi do przetwarzania danych osobowych oraz

Instrukcja bezpieczeństwa informacji w systemach informatycznych stanowiąca załącznik Nr 1 do Polityki.

6) Kontrola dostępu

Urząd zarządza kontrolą dostępu w celu zapewnienia dostępu do informacji miejsc i urządzeń oraz systemów wyłącznie osobom upoważnionym.

Skuteczna realizacja postawionego celu jest możliwa dzięki ustanowionym praktykom i podziałowi odpowiedzialności związanemu z nadzorowaniem ruchu osobowego w pomieszczeniach biurowych.

Pomieszczenia biurowe są zamykane na klucz.

Największa uwaga poświęcona jest kontroli dostępu do danych powierzonych przez klientów – danych osobowych

7) Wymiana informacji

Każda informacja udostępniana osobom trzecim podlega ochronie.

Przed udostępnieniem każdy pracownik jest odpowiedzialny za upewnienie się, że może informację przekazać. W przypadku wątpliwości decyduje właściwy przełożony pracownika.

8) Pozyskiwanie, rozwój i utrzymanie systemów informatycznych

Urząd zapewnia, że wszelkie procesy związane z pozyskaniem, rozwojem lub utrzymaniem systemów prowadzone jest w sposób nadzorowany, gwarantujący utrzymanie poziomu bezpieczeństwa.

Na to składa się:

- uwzględnienie wymogów bezpieczeństwa podczas zakupu nowych systemów
- wdrożone procedury kontroli zmian/aktualizacji oprogramowania

9) Zarządzanie incydentami

W przypadku wszelkich incydentów powiadamiany jest Administrator systemów informacyjnych. Z jego udziałem dokonywana jest wstępna analiza incydentów, po czym podejmowane są działania zgodne z zasadami reakcji na zdarzenie.

Po wystąpieniu incydentu natychmiast podejmowane są działania mające na celu usunąć ewentualne skutki, a następnie incydent jest analizowany i podejmowane są właściwe decyzje.

10) Zarządzanie ciągłością działania

Urząd dba o zapewnienie ciągłości funkcjonowania usług związanych z przetwarzaniem danych w celu przeciwdziałania przerwom w wydajności biznesowej oraz ochrony krytycznych procesów przed awariami.

Realizacja postawionego celu jest możliwa poprzez: ustanowione praktyki, podział odpowiedzialności związanej z zarządzeniem ciągłości działania poszczególnych systemów informatycznych. Podział odpowiedzialności związanej z zarządzaniem ogranicza się do poziomu akceptowanego skutki wypadków i awarii.

11) Zgodność

Urząd dba o zapewnienie zgodności zasad postępowania z przepisami obowiązującego prawa, przyjętych uwarunkowań normatywnych oraz własnych standardów w celu uniknięcia naruszania przepisów prawa, ustaw, rozporządzeń i innych wymagań bezpieczeństwa.

Prowadzony jest nadzór nad komplementarnością techniczną stosowanych urządzeń oraz prowadzone są aktywy wewnętrzne funkcjonowania systemu.

§ 3

Postanowienia końcowe

Wszyscy pracownicy Urzędu są zapoznani z Polityką Bezpieczeństwa Informacji.

Naruszenie świadome bądź przypadkowe niniejszej instrukcji oraz dokumentów wykonawczych powoduje skutki prawne zgodnie z regulaminem Pracy, a w przypadkach zastrzeżonych przez ustawodawcę – karne wynikające z odpowiedzialności określonej przez sąd.

BURMISTRZ
Miasta i Gminy
Magdalena Małgowska

Instrukcja bezpieczeństwa informacji w systemach informatycznych Urzędu Miasta i Gminy w Osieku

1. Cel i zakres dokumentu

Instrukcja określa zasady organizacyjne i techniczne zapewniające bezpieczeństwo informacji, w tym danych osobowych, przetwarzanych w systemach informatycznych Urzędu Miasta i Gminy w Osieku. Obowiązuje wszystkich pracowników, współpracowników i inne osoby upoważnione do korzystania z systemów informatycznych Urzędu.

2. Podstawy prawne

- Rozporządzenie Parlamentu Europejskiego 2016/679 (RODO),
- Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U z 2019 r. poz. 1781)
- Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz. U z 2025 r. poz. 1703)

3. Definicje

- **System informatyczny** – zespół współpracujących ze sobą urządzeń, oprogramowania i procedur służących do przetwarzania danych.
- **Użytkownik** – osoba posiadająca indywidualne uprawnienia dostępu do systemu informatycznego.
- **Administrator Systemu Informatycznego (ASI)** – osoba odpowiedzialna za zarządzanie systemami i ich bezpieczeństwem.
- **IOD** – Inspektor Ochrony Danych, nadzoruje przestrzeganie zasad RODO.

4. Zasady ogólne

- Dane osobowe i inne informacje chronione muszą być zabezpieczone przed utratą, nieuprawnionym dostępem, ujawnieniem, modyfikacją lub zniszczeniem.
- Systemy informatyczne muszą być wykorzystywane wyłącznie do celów służbowych.
- Pracownicy przetwarzający dane są zobowiązani do zachowania poufności i podpisania stosownych oświadczeń.

5. Nadawanie i zarządzanie dostępem

- Każdy użytkownik systemu otrzymuje indywidualny login i hasło.
- Uprawnienia dostępu są nadawane przez ASI na podstawie pisemnego upoważnienia wydanego przez Burmistrza Miasta i Gminy.
- Po zakończeniu współpracy użytkownik traci dostęp do systemów informatycznych.

- Hasła muszą być zmieniane co najmniej raz na 30 dni i mieć minimalnie 8 znaków (w tym cyfry, wielkie/małe litery).

6. Bezpieczeństwo fizyczne i środowiskowe

- Pomieszczenia z serwerami i sprzętem informatycznym muszą być zabezpieczone tj. zamykane na klucz, do którego mają dostęp tylko upoważnione osoby.
- Nośniki danych muszą być przechowywane w sposób chroniący przed kradzieżą lub zniszczeniem.
- W urządzeniach wielofunkcyjnych z funkcją kopiowania/skanowania dane powinny być regularnie kasowane lub szyfrowane.

7. Ochrona techniczna

- Urządzenia muszą być chronione programami antywirusowymi oraz zaporami sieciowymi (firewall).
- System operacyjny i oprogramowanie muszą być aktualizowane.
- Wymagane jest stosowanie polityki haseł i blokady ekranu po 10 minutach bezczynności.
- Kopie zapasowe danych wykonuje się codziennie oraz przechowywane są na serwerze (odrębne dyski)

8. Postępowanie w przypadku naruszeń

- Każdy użytkownik jest zobowiązany do zgłaszania incydentów bezpieczeństwa (włamania, utraty danych, awarii) do ASI lub IOD.
- Incydenty są dokumentowane i analizowane pod kątem wpływu na bezpieczeństwo danych.
- W przypadku poważnego naruszenia IOD informuje Prezesa UODO w terminie do 72 godzin.

9. Przeglądy i audyty

- Przynajmniej raz w roku przeprowadza się audyt bezpieczeństwa systemów informatycznych.
- Wszelkie nieprawidłowości skutkują wprowadzeniem działań korygujących.

10. Szkolenia

- Nowi pracownicy są obowiązkowo szkoleni z zasad bezpiecznego korzystania z systemów informatycznych.
- Szkolenia okresowe odbywają się co najmniej raz na 2 lata.

11. Postanowienia końcowe

- Instrukcja wchodzi w życie z dniem zatwierdzenia
- Dokument jest być aktualizowany przez Administratora Danych lub ASI w przypadku zmiany technologii, prawa lub struktury organizacyjnej urzędu.

BURMISTRZ
Miasta i Gminy
Magdalena Maryńowska