ZARZĄDZENIE NR 733/2024
BURMISTRZA MIASTA I GMINY ŁASIN

z dnia 3 stycznia 2024 r.

w sprawie wprowadzenia „Polityki Bezpieczeństwa Informacji Urzędu Miasta i Gminy Łasin”.

Na podstawie art. 13 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2023, poz. 57 ze zm.) oraz § 20 ust.1 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacjiw postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.Uz 2017 r., poz. 2247), zarządza się co następuje:

§ 1. Wprowadzam „Politykę Bezpieczeństwa Informacji Urzędu Miasta i Gminy Łasin”, która stanowi załącznik nr 1 do niniejszego zarządzenia.

§ 2. Zobowiązuję pracowników Urzędu Miasta i Gminy w Łasinie do zapoznania się z „Polityką Bezpieczeństwa Informacji Urzędu Miasta i Gminy Łasin”, w terminie siedmiu dni od dnia wejścia w życie niniejszego zarządzenia.

§ 3. Zobowiązuję pracowników Urzędu Miasta i Gminy Łasin do stosowania zasad określonych w „Polityce Bezpieczeństwa Informacji Urzędu Miasta i Gminy Łasin”.

§ 4. Wykonanie zarządzenia powierzam inspektorowi ds. informatyki oraz inspektorowi ochrony danych osobowych.

§ 5. Zarządzenie wchodzi w życie z dniem podpisania.

Burmistrz Miasta i Gminy
Łasin

mgr inż. Rafał Kobylski

ZATWIERDZAM

Załącznik nr 1 do Zarządzenia Nr 733/2024
Burmistrza Miasta i Gminy Łasin
z dnia 3 stycznia 2024 r.

.....

IOD.142.1.2024

POLITYKA BEZPIECZEŃSTWA INFORMACJI

Urzędu Miasta i Gminy Łasin

ŁASIN 2023

METRYKA DOKUMENTU

Nazwa	**Urząd Miasta i Gminy Łasin**		
Tytuł dokumentu	**Polityka Bezpieczeństwa Informacji**		
Rodzaj dokumentu	**Dokument wykonawczy**		
Zastosowanie	**Urząd Miasta i Gminy Łasin**		
Status	**przyjęty**	**Liczba stron**	**34**

WERSJA DOKUMENTU / HISTORIA ZMIAN

Wersja	Data wersji	Opis zmiany	Rozdział	Autor zmiany
1	grudzień 2023	dokument pierwszy	całość	IOD

SPIS TREŚCI

DEKLARACJA O WDROŻENIU POLITYKI BEZPIECZEŃSTWA INFORMACJI

Przywiązując szczególną wagę do problematyki bezpieczeństwa informacji tworzonych i przetwarzanych zarówno w formie tradycyjnej, jak i elektronicznej, Kierownictwo Urzędu Miasta i Gminy Łasin deklaruje pełne zaangażowanie w procesy służące wdrożeniu Systemu Zarządzania Bezpieczeństwem Informacji.

Fundamentem i jednym z kluczowych elementów Systemu Zarządzania Bezpieczeństwem Informacji jest Polityka Bezpieczeństwa Informacji. Przyczynia się ona do zapewnienia ochrony informacji, w szczególności prawnie chronionej, poprzez zapewnienie jej poufności, integralności i dostępności. Polityka Bezpieczeństwa Informacji, jako akt wewnętrzny, stanowi podstawę wszystkich procedur, instrukcji, czy innych regulacji odnoszących się bardziej szczegółowo do bezpieczeństwa informacji. Taka konstrukcja służy jak najpełniejszemu zdefiniowaniu wszystkich obszarów bezpieczeństwa, zapobieganiu ewentualnym zagrożeniom oraz podjęciu niezbędnych działań w sytuacjach kryzysowych, dając w efekcie gwarancję właściwego poziomu ochrony informacji oraz procesu ciągłości jej przetwarzania.

Osiągnięcie wyżej wymienionych celów, poprzez stworzenie systemu bezpieczeństwa informacji, wzbogaconego o stosowne narzędzia jego zarządzania, jest niezwykle ważne dla ochrony aktywów i wizerunku każdej instytucji, dlatego ze strony Kierownictwa UMiG deklaruję wdrożenie i utrzymanie niezbędnych zabezpieczeń organizacyjnych i technicznych w urzędzie, a także uczestnictwo w procesach ciągłej weryfikacji i doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji, którego elementem jest wprowadzona Polityka Bezpieczeństwa Informacji.

Zobowiązuję jednocześnie wszystkich pracowników do bezwzględnego stosowania zasad wyznaczonych przez Politykę Bezpieczeństwa Informacji oraz dokumentów z nią powiązanych.

Łasin, dnia ……..

.....
(podpis)

1. WYKAZ PODSTAWOWYCH DEFINICJI I SKRÓTÓW

1.1. Skróty

SZBI	System Zarządzania Bezpieczeństwem Informacji
PBI	Polityka Bezpieczeństwa Informacji
GAI	Główny Administrator Informacji
AI	Administratorzy Informacji (lokalni)
ADO	Administrator Danych Osobowych
IOD	Inspektor Ochrony Danych
ASI	Administrator Systemów Informatycznych
PODO	Polityka Ochrony Danych Osobowych
IZSI	Instrukcja Zarządzania Systemami Informatycznymi
UMiG	Urząd Miasta i Gminy Łasin

1.2. Definicje

System Zarządzania Bezpieczeństwem Informacji	to część całościowego systemu zarządzania odnosząca się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji.
Bezpieczeństwo informacji	zachowanie poufności, integralności i dostępności informacji.
Poufność	właściwość polegająca na tym, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom.
Integralność danych	funkcja bezpieczeństwa zapewniająca, że dane nie zostały zmodyfikowane, dodane lub usunięte w nieautoryzowany sposób.
Dostępność	właściwość bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu.
Autentyczność informacji	zapewnienie, że informacja jest zgodna z prawdą, oryginalna.
Rozliczalność działań	zapewnienie, że wszystkie istotne czynności wykonane przy przetwarzaniu informacji zostały zarejestrowane i dają możliwość zidentyfikowania osoby, która tę czynność wykonała.

Niezawodność działań	zapewnienie, że wykonywane czynności prowadzą do zamierzonych skutków.
Zarządzanie ryzykiem	proces, którego celem jest identyfikacja, kontrolowanie i minimalizowanie ryzyka związanego z bezpieczeństwem informacji i ciągłością działania.
Analiza ryzyka	systematycznie wykorzystanie informacji do zidentyfikowania źródeł i oszacowania ryzyka.
Aktywa	wszystko co ma wartość dla organizacji.
Zdarzenie związane z bezpieczeństwem informacji	zdarzenie związane z bezpieczeństwem informacji jako określonym stanem systemu, usługi lub sieci, który wskazuje na możliwe naruszenie Polityki Bezpieczeństwa Informacji, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem.
Incydent związany z bezpieczeństwem informacji	jest to pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne zakłócenia zadań biznesowych i zagrażają bezpieczeństwu informacji.
System teleinformatyczny	to zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci urządzenia końcowego w rozumieniu ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne.
System informatyczny	zbiór współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych stosowanych w celu przetwarzania danych.
Niezaprzeczalność nadania	zdolność systemu do udowodnienia, że nadawca informacji rzeczywiście ją nadał lub wprowadził do systemu w określonym czasie i miejscu .
Niezaprzeczalność odbioru	zdolność systemu do udowodnienia, że adresat informacji otrzymał ją w określonym czasie i miejscu.
Komórka organizacyjna	Wydzielona organizacyjnie część UMiG, w tym także stanowisko wieloosobowe lub samodzielne.
Kierownik komórki organizacyjnej	osoba kierująca komórką organizacyjną lub osoba wyznaczoną do wykonywania jej zadań.

2. KONTEKST PRZYJĘCIA POLITYKI BEZPIECZEŃSTWA INFORMACJI

Miarą i wyznacznikiem skuteczności działania każdej jednostki organizacyjnej jest stopień osiągania zamierzonego celu. Istotnym elementem sprawnej realizacji wyznaczonych i zdefiniowanych celów jest niezakłócone działanie systemów informacyjnych oraz właściwe zabezpieczenie przetwarzanych informacji przed istniejącymi zagrożeniami.

Mając powyższe na względzie, wprowadzona zostaje do stosowania przez wszystkich pracowników UMiG **Polityka Bezpieczeństwa Informacji** (dalej także jako PBI).

Ma ona na celu udokumentowanie działań wdrażających **System Zarządzania Bezpieczeństwem Informacji** (dalej także jako SZBI)

PBI opisuje ogólne zasady obowiązujące w UMiG w procesie przetwarzania informacji, sposób zarządzania ryzykiem, odpowiedzialności poszczególnych osób zaangażowanych w proces przetwarzania informacji, procedurę reagowania na incydenty, a także nakreśla model systemu zarządzania bezpieczeństwem informacji.

3. CEL POLITYKI BEZPIECZEŃSTWA INFORMACJI.

Celem *Polityki Bezpieczeństwa Informacji* jest zdefiniowanie ogólnych zasad i mechanizmów ochrony informacji, które będą filarem wszystkich dokumentów i działań związanych z bezpieczeństwem informacji tworzących System Zarządzania Bezpieczeństwem Informacji.

Definiując bardziej szczegółowe zakładane do osiągnięcia cele w dziedzinie bezpieczeństwa informacji należy wskazać głównie na:

1) **ochronę zasobów informacyjnych** UMiG niezależnie od ich postaci i zapewnienie ciągłości działania procesów;

2) uzyskanie i utrzymanie odpowiedniego poziomu bezpieczeństwa zasobów UMIG, rozumianego jako zapewnienie **poufności**, **integralności** i **dostępności** informacji oraz **rozliczalności** podejmowanych działań;

3) zapewnienie **poprawności działania** i **bezpieczeństwa systemów teleinformatycznych** przetwarzających informacje oraz gwarancji niezaprzeczalności odbioru i nadania oraz rozliczalności zadań;

4) maksymalne zredukowanie prawdopodobieństwa wystąpienia zagrożeń dla bezpieczeństwa informacji wynikających z celowej, bądź niezamierzonej działalności człowieka w kontekście ewentualnej szkody poniesionej przez UMiG;

5) zapewnienie gotowości podejmowania natychmiastowych działań w sytuacji zagrożenia bezpieczeństwa informacji.

Realizacja tak określonych celów może nastąpić poprzez podejmowanie działań związanych z:

1) wyznaczeniem odpowiedniej struktury organizacyjnej umożliwiającej optymalny przydział zadań i odpowiedzialności związanych z bezpieczeństwem informacji i powiązanych aktywów, jak również zapewniający właściwą koordynację tych działań;

2) wdrożeniem i utrzymaniem zabezpieczeń technicznych i organizacyjnych;

3) zarządzaniem ryzykiem w celu jego minimalizacji do akceptowanego poziomu;

4) wdrażaniem i eksploatowaniem systemów informacyjnych z zachowaniem wszelkich zasad bezpieczeństwa;

5) zobowiązaniem wszystkich pracowników do zapoznania się i przestrzegania zasad wprowadzonych przez SZBI;

6) sukcesywnym podnoszeniem świadomości wagi bezpieczeństwa informacji wśród pracowników UMiG;

7) ciągłym monitorowaniem realizacji polityk i procedur w celu ich doskonalenia.

4. ZAKRES POLITYKI BEZPIECZEŃSTWA INFORMACJI.

Polityka Bezpieczeństwa Informacji zawiera w szczególności:

- deklaracje Kierownictwa,
- podstawowe cele i definicje bezpieczeństwa informacji,
- sposób organizacji Systemu Zarządzania Bezpieczeństwem Informacji,
- podstawy prawne odnoszące się do źródeł ogólnie obowiązujących,
- odnośniki do innych dokumentów wewnętrznych UMiG, powiązanych i opracowywanych w ramach tworzonego systemu.

Niniejszy dokument ma zastosowanie do sprecyzowanych poniżej w tekście kategorii informacji, niezależnie od sposobu ich przetwarzania i przechowywania.

Swoim zakresem obejmuje wszystkie komórki organizacyjne UMiG, pracowników w rozumieniu przepisów Kodeksu Pracy, a także inne osoby mające dostęp do informacji na podstawie zawartych umów cywilnoprawnych, czy odbywających w UMiG staż, praktykę lub wolontariat.

5. PODSTAWY PRAWNE.

PBI oraz dokumenty szczegółowe z nią powiązane powinny być zgodne z obowiązującymi w tym zakresie przepisami prawa, normą ISO 27001 oraz innymi uwarunkowaniami i standardami obowiązującymi w UMiG.

Akty prawne związane z SZBI wyszczególniono w załączniku nr 1 do niniejszej PBI.

6. RODZAJE INFORMACJI PRZETWARZANYCH PRZEZ UMiG.

6.1. Klasyfikacja informacji.

Podstawą osiągnięcia spójnej ochrony **informacji** w UMiG jest rozpoznanie wszystkich informacji, obszarów i środków przetwarzania, które powinny podlegać ochronie.

W UMiG występują następujące zdefiniowane rodzaje informacji:

1) **Informacje prawnie chronione** – których ujawnienie może spowodować istotne straty finansowe, problemy prawne lub naruszenie dóbr osoby fizycznej, co do których stosuje się w szczególności przepisy o ochronie informacji niejawnych lub o ochronie danych osobowych.
2) **Informacje publiczne/jawne** – informacje, które mogą być przedstawione na forum i do wiadomości publicznej;

W celu zapewnienia ochrony i sposobów zabezpieczenia informacji, wprowadza się dodatkowy rodzaj informacji – **informację wewnętrzną**, będącą w posiadaniu lub przetwarzaniu pracowników UMiG, z rozróżnieniem na:

1) informacje wewnętrzne udostępnione **wszystkim pracownikom** UMiG,
2) informacje wewnętrzne dostępne dla **pracowników upoważnionych**.

6.2. Ogólne zasady ochrony sklasyfikowanych informacji.

6.2.1. Informacje publiczne.

1. Problematykę dostępu do informacji publicznej definiuje ustawa z dnia 6 września 2001 r. *o dostępie do informacji publicznej* oraz regulacje wewnętrzne.

2. Informacja publiczna chroniona jest ze względu na integralność i dostępność.

3. Dokumenty zawierające informacje publiczne są publikowane w Biuletynie Informacji Publicznej UMiG.

4. Informacje nieudostępnione w Biuletynie Informacji Publicznej, są udostępniane na pisemny wniosek.

5. Informacje, które mogą być udzielone niezwłocznie, są udostępniane w formie ustnej lub pisemnej bez wymaganego wniosku pisemnego.

6. Informacja publiczna może być przechowywana na dowolnym nośniku i przesyłana w systemach teleinformatycznych przy zachowaniu jej **dostępności** i **integralności**.

7. Dodatkowo, problematykę udostępniania dla celów dalszego wykorzystywania informacji sektora publicznego reguluje ustawa z dnia 11 sierpnia 2021 r. *o otwartych danych i ponownym wykorzystaniu informacji sektora publicznego*, co w szczególności dotyczy przypadków eksploatacji danych udostępnionych w dedykowanym portalu danych (m.in. BIP) lub innym systemie teleinformatycznym – tzw. dane otwarte, jak również upubliczniania danych na potrzeby ich dalszej eksploatacji na podstawie wniosku o ponowne wykorzystanie informacji sektora publicznego.

6.2.2. Informacje prawnie chronione.

Informacje prawnie chronione podlegają ochronie według kryteriów zachowania ich **poufności**, **integralności** i **dostępności**.

1. **Informacje niejawne.** Ochrona informacji niejawnej prowadzona jest w oparciu o ustawę z dnia 5 sierpnia 2010 r. *o ochronie informacji niejawnych* oraz dokumenty wewnętrzne powiązane z Polityką Bezpieczeństwa Informacji.

   Za organizację sytemu ochrony informacji niejawnej odpowiada Pełnomocnik ds. informacji niejawnych UMiG. Informacje niejawne posiadają własny system ochrony zgodny z zapisami ustawy o ochronie informacji niejawnych.

2. **Dane osobowe.** Obowiązki w zakresie ochrony danych osobowych precyzuje Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. *w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE* (ogólne rozporządzenie o ochronie danych) (Dz. U. UE z 2016 r., L 119, poz. 1).

Za system ochrony danych osobowych odpowiedzialny jest Administrator Danych Osobowych, którym w rozumieniu ustawy jest Burmistrz.

Szczegółowe zapisy dotyczące zasad przetwarzania, ochrony i zabezpieczenia danych osobowych zawiera *Polityka Ochrony Danych Osobowych*.

3. **Informacje wewnętrzne** – chronione ustawowo, to grupa tajemnic pracodawcy określona na podstawie art. 100 § 2 pkt 5 *ustawy z dnia 26 czerwca 1974 r. Kodeks Pracy* oraz odrębnych przepisów.

6.2.3. Informacje wewnętrzne.

1. Zasady przetwarzania informacji wewnętrznej w sposób tradycyjny i w systemach informatycznych:

   1) dostęp do dokumentów mają wyłącznie pracownicy UMiG;

   2) niedopuszczalne jest przekazywanie w jakiejkolwiek postaci, w całości bądź części dokumentów, bądź zawartych w nich treści osobom nie będącym pracownikami;

   3) powielanie, kopiowanie, drukowanie, czy przenoszenie dokumentów na nośniki elektroniczne możliwe jest wyłącznie dla celów realizacji obowiązków służbowych;

   4) przechowywanie informacji wewnętrznej w formie tradycyjnej, jak i w systemach informatycznych, oraz bieżące ich wykorzystywanie, musi odbywać się w sposób uniemożliwiający dostęp do nich osób nieuprawnionych;

   5) do przechowywania informacji w urządzeniach przenośnych wynoszonych poza obszar przetwarzania stosuje się ochronę poprzez ich szyfrowanie;

   6) niszczenie informacji na elektronicznych nośnikach danych powinno się odbywać w sposób nieodwracalny;

   7) wysyłka informacji e-mail może odbywać się tylko za pomocą poczty służbowej.

2. Kategorię informacji wewnętrznej nadaje właściciel informacji.

3. Wszelkie informacje niesklasyfikowane, podlegające ochronie, traktuje się jako informację wewnętrzną.

7. ORGANIZACJA SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI.

7.1. Definicja SZBI

SZBI wdrażany jest na podstawie § 20 *Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych*. SZBI obejmuje swą właściwością realizację zadań publicznych określonych przepisami prawa.

SZBI rozumiany jest jako zespół wszelkich działań organizacyjnych i technicznych, których celem jest zapewnienie, aby istotne dla Jednostki informacje – i dotyczy to wszystkich przetwarzanych informacji – były odpowiednio chronione.

7.2. Cel praktyczny ochrony informacji

Odpowiednia ochrona informacji ma na celu zapewnienie, że informacje są:

Dostępne	co oznacza, że informacja jest możliwa do wykorzystania na żądanie, w założonym czasie, przez podmiot uprawniony do pracy;
Poufne	co oznacza, że informacja nie jest udostępniana lub ujawniana nieupoważnionym osobom fizycznym;
Integralne	co oznacza, że informacja nie została zmodyfikowana w sposób niepożądany lub nieuprawniony;

7.3. Cechy podstawowe SZBI:

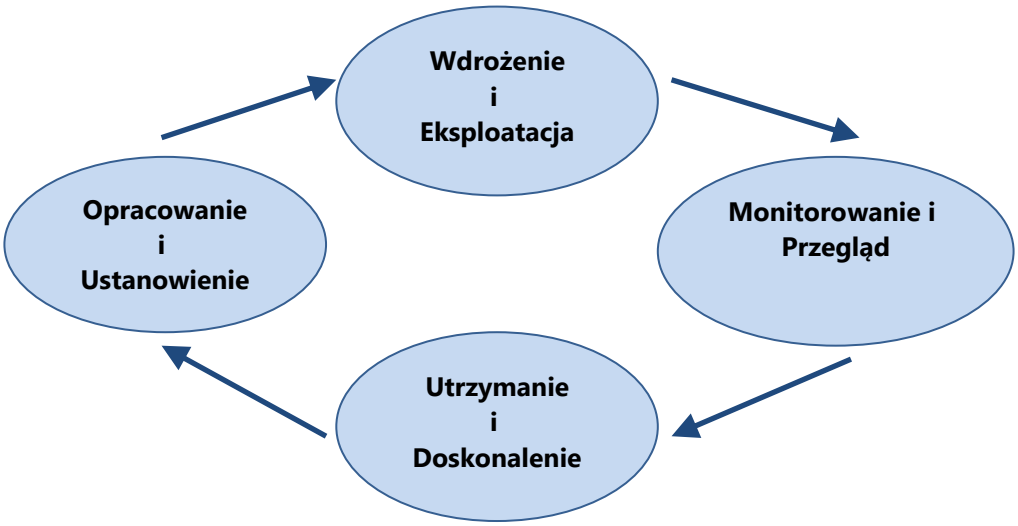
Odpowiednio zorganizowany system zarządzania bezpieczeństwem informacji powinien charakteryzować następujący zestaw cech/atrybutów:

Autentyczność	właściwość polegającą na tym, że pochodzenie lub zawartość danych (informacji) opisujących obiekt są takie, jak deklarowane (autentyczne);
Rozliczalność	właściwość systemu pozwalającą przypisać określone działanie w systemie do konkretnej osoby fizycznej lub procesu oraz umiejscowić je w czasie;
Niezaprzeczalność	brak możliwości zanegowania swego uczestnictwa w całości lub w części wymiany informacji przez jeden z podmiotów uczestniczących w tej wymianie;
Niezawodność	właściwość systemu pozwalająca na jego odpowiednie

(dobre) funkcjonowanie przez cały czas.

7.4. Doskonalenie SZBI

Odpowiednie funkcjonowanie SZBI zapewnia się poprzez cykliczną, powtarzalną realizację czynności wymienionych na poniższym schemacie:



Efektem przyjęcia wskazanej ścieżki ma być wdrożenie modelu „0" SZBI, a następnie stałe podnoszenie jakości, tzn. udoskonalanie funkcjonowania SZBI, m.in. w oparciu o wyniki bieżącego monitorowania oraz okresowych audytów systemu.

7.5. Poziomy zarządzania bezpieczeństwem informacji.

Przyjęta w UMiG konstrukcja SZBI opiera się na trzech poziomach zarządzania bezpieczeństwem informacji:

7.5.1. Poziom pierwszy SZBI – strategiczny

Związany jest z wytyczaniem określonych celów do zrealizowania w odniesieniu do dynamiki zmian otoczenia prawnego i technologicznego, przy uwzględnieniu wyników analizy ryzyka, przeprowadzanej w kontekście zarządzania przez UMiG zasobami (aktywami) dla zapewnienia im wymaganego poziomu bezpieczeństwa.

Aktywa w tym znaczeniu to: informacje, procesy i działania, a także zasoby kadrowe, sprzętowe i oprogramowanie.

Przyjmując analogię przeniesioną z uregulowań z zakresu kontroli zarządczej w UMiG, wspomniana analiza ryzyka powinna zostać przeprowadzona przynajmniej raz w roku, w oparciu o kryterium eliminacji ryzyka maksymalnej wartości w obszarze o najwyższym ryzyku. Tak pozyskane informacje, mają dać podstawę i bazę do aktualizacji dotychczasowych rozwiązań lub wdrażania nowych.

7.5.2. Poziom drugi SZBI - taktyczny

Związany z tworzeniem standardów i mechanizmów w przedmiotowym zakresie oraz ich dalszym egzekwowaniem w praktyce.

O ile w realizację pierwszego poziomu zaangażowane są osoby z kierownictwa, tak drugi poziom odnosi się również do osób mających ściśle określone funkcje związane między innymi z ochroną danych osobowych, takich jak IOD i ASI oraz do kierowników komórek organizacyjnych, będących lokalnymi administratorami danych.

7.5.3. Trzeci poziom SZBI - operacyjny

Ostatni z poziomów to operacyjny, w ramach którego prowadzona jest ochrona bezpieczeństwa informacji pod kątem wypełniania standardów bezpieczeństwa oraz rozwiązywania zakłóceń wynikających z zaistniałych sytuacji naruszeń tych standardów.

W tym poziomie mają udział już wszyscy pracownicy UMiG – użytkownicy sytemu informatycznego.

7.6. Główne zadania w ramach SZBI

W procesie zarządzania bezpieczeństwem informacji można wyszczególnić następujące grupy zadań:

1) Zarządzanie ryzykiem.
2) Monitorowanie SZBI.
3) Utrzymanie oraz wdrażanie działań korygujących i doskonalących SZBI.
4) Nadzór nad dokumentacją SZBI.
5) Zarządzanie dostępem do informacji.
6) Zarządzanie incydentem w zakresie bezpieczeństwa informacji.

7.6.1. Zarządzanie ryzykiem.

Proces zarządzania ryzykiem w UMiG jest niezwykle istotnym elementem zarządzania aktywami i bezpieczeństwem informacji.

Zarządzanie ryzykiem polega na systematycznym stosowaniu procedur dotyczących identyfikacji i oceny ryzyk, a następnie planowaniu i wdrażaniu reakcji na ich wystąpienie.

Rozpoczyna go każdorazowo identyfikacja ryzyka poprzez określenie słabych punktów i zagrożeń. Jest to etap wstępny, po którym następuje określenie wpływu zidentyfikowanego ryzyka na działalność UMiG.

Oszacowane ryzyko poddawane jest następnie ocenie w kontekście wyznaczonych poziomów jego akceptowalności z uwzględnieniem kryterium mającego na celu eliminację ryzyka maksymalnej wartości w obszarze o najwyższym ryzyku oraz związanego z wystąpieniem niezgodności z obowiązującym prawem. Na tej podstawie sporządzany jest plan postępowania z ryzykiem przekraczającym wyznaczone poziomy akceptowalności.

Dalszą konsekwencją przeprowadzonego procesu analizy ryzyka jest dobranie odpowiednich zabezpieczeń fizycznych, technicznych i organizacyjnych, mających na celu zapewnienie wymagalnego poziomu bezpieczeństwa zasobów UMiG.

Analiza ryzyka wykonywana jest systematycznie, nie rzadziej niż raz w roku, bądź częściej w sytuacji zmian mających istotne znaczenie dla SZBI.

Z wynikami analizy ryzyka zapoznawany jest każdorazowo Administrator SZBI (Burmistrz) oraz zainteresowane komórki organizacyjne UMiG.

Metodologia analizy ryzyka oraz zasady zarządzania ryzykiem w przetwarzaniu informacji zawierających dane osobowe określono w dokumencie "*Procedura szacowania i zarządzania ryzykiem związanym z przetwarzaniem danych osobowych w Urzędzie Miasta i Gminy Łasin*". Jeśli przepisy prawa nie stanowią inaczej, zasady opisane we wskazanych uregulowaniach wewnętrznych mają odniesienie także do informacji niebędących danymi osobowymi (z wyjątkiem informacji niejawnych, gdzie zasady te opisuje dokument niejawny pn. "*Szczególne Wymagania Bezpieczeństwa*").

7.6.2. Monitorowanie i ocena SZBI.

Monitorowanie SZBI opiera się w głównej mierze na jego weryfikacji pod kątem zgodności z obowiązującym prawem, jak również zapewnienia stosowalności do realizowanych zadań publicznych oraz możliwości obsługi interesantów w każdych warunkach niezależnie od okoliczności i zmian w UMiG.

Działania monitorujące wykonywane są corocznie poprzez przegląd dokumentacji SZBI. Dodatkowo, w zależności od potrzeb przegląd SZBI może być dokonywany częściej, po stwierdzeniu istotnego naruszenia bezpieczeństwa, czy pojawieniu się zasadniczych zmian w UMiG, jego strukturze lub jego otoczeniu (nowe zagrożenia, nowe technologie itp.).

Okresowo wykonywane są również oceny funkcjonowania SZBI poprzez wewnętrzne, bądź zewnętrzne audyty bezpieczeństwa informacji wykonywane zgodnie z dyspozycją *§ 20 ust. 1 pkt 14 Rozporządzenia o KRI*.

7.6.3. Utrzymanie oraz wdrażanie działań korygujących i doskonalących SZBI.

Utrzymanie oraz doskonalenie SZBI w UMiG realizowane jest w szczególności poprzez podejmowanie następujących działań:

1. **Działania zapobiegawcze.**

Wdrażanie takich działań jest wynikiem przeprowadzonej analizy ryzyka i ma na celu przeciwdziałanie w jak najwyższym stopniu potencjalnym zidentyfikowanym zagrożeniom oraz szybką identyfikację zagrożeń dotąd niezidentyfikowanych.

2. **Działania korygujące.**

   Podejmowane są w sytuacji konieczności poprawy istniejących uregulowań wewnętrznych. Są one konsekwencją zarówno analizy ryzyka, jak i przeglądu (monitorowania) dokumentacji SZBI.

Zarówno w pierwszym, jak i drugim punkcie, konieczna jest właściwa koordynacja przepływu informacji o podejmowanych i wdrażanych działaniach pomiędzy wszystkimi punktami przetwarzania informacji z uwzględnieniem Kierownictwa UMiG.

Cykliczność wykonywania w/w działań uzależniona jest od potrzeb oraz zmieniającego się otoczenia prawnego, technologicznego, czy fizycznego w jakim funkcjonuje UMiG. Opisane wyżej działania mają za zadanie dążenie do osiągnięcia i utrzymania odpowiednio wysokiego i pełnego poziomu bezpieczeństwa informacji przetwarzanych w UMiG.

7.6.4. Nadzór nad dokumentacją SZBI.

Sprawowanie nadzoru nad dokumentacją SZBI obejmuje zarówno samo opracowanie dokumentacji, jak i jej kompletność. Nadzorowi podlega dodatkowo zgodność zapisów systemowych z obowiązującymi przepisami prawa, regulacjami wewnętrznymi, jak również ze stanem faktycznym. Poszczególne elementy są nadzorowane w ramach wykonywanych planowych audytów, albo na podstawie zgłoszenia osoby wykonującej obowiązki określone w PBI, czy informacji osoby trzeciej.

7.6.5. Zarządzanie dostępem do informacji.

Zasadą ogólną zarządzania dostępem do zasobów informacji jest uzyskanie lub przyznanie uprawnień w ramach określonego rodzaju informacji, bądź systemu teleinformatycznego.

Szczegóły w tym zakresie zostały zawarte w dokumentach wewnętrznych powiązanych z niniejszą PBI, w szczególności w *Polityce ochrony danych osobowych.*

7.6.6. Zarządzanie incydentem w zakresie bezpieczeństwa informacji.

Ogólne zasady postępowania z incydentem związanym z bezpieczeństwem informacji.

Szczegółowe regulacje odnoszące się do incydentów związanych z przetwarzaniem danych osobowych czy incydentów związanych z systemami informatycznymi, określają stosowne regulacje wewnętrzne powiązane z niniejszą PBI, tj. zał. nr 10 do PODO - "*Instrukcja postępowania w sytuacji naruszenia systemu ochrony danych osobowych*" oraz zał. nr 11 - "*Tabela form naruszeń bezpieczeństwa danych osobowych*". W zakresie informacji niejawnych uregulowania takie występują w dokumencie niejawnym pn. "*Szczególne Wymagania Bezpieczeństwa*", który zawiera zał. nr 4 pn. "*Metodyka szacowania ryzyka*" oraz zał. nr 9 "*Tabela oceny istotności czynników zagrożeń*".

7.7. Struktura dokumentacji SZBI.

Dokumentacja SZBI została podporządkowana formie zhierarchizowanej w oparciu o następującą strukturę:

7.7.1. Poziom pierwszy

Poziom pierwszy stanowi *Polityka Bezpieczeństwa Informacji*, obejmująca obowiązujące wymagania i zasady bezpieczeństwa informacji oraz sposób zorganizowania SZBI w UMiG.

7.7.2. Poziom drugi

Dokumentacja drugiego poziomu odnosi się do polityk i planów w zakresie przetwarzania informacji prawnie chronionych. Dokumenty wewnętrzne, nie są publikowane.

Na dokumentację w tym zakresie składają się:

1) Polityka Ochrony Danych Osobowych w UMiG.
2) Procedura szacowania i zarządzania ryzykiem związanym z przetwarzaniem danych osobowych w UMiG wraz z kartami ryzyka bezpieczeństwa informacji.
3) Plan Ochrony Informacji Niejawnych w UMiG.
4) Szczególne Wymagania Bezpieczeństwa Systemu Teleinformatycznego służącego w UMiG do przetwarzania informacji niejawnych.

7.7.3. Poziom trzeci

Poziom trzeci związany jest z określeniem procedur, instrukcji i regulaminów w zakresie bezpieczeństwa systemów teleinformatycznych. Dokumenty wewnętrzne, nie są publikowane.

Wśród nich wymienić należy:

1) Instrukcję Zarządzania Systemem Informatycznym w UMiG (załącznik nr 1 do Polityki Ochrony Danych Osobowych);
2) Procedury Bezpiecznej Eksploatacji Systemu Teleinformatycznego służącego w UMiG do przetwarzania informacji niejawnych.

7.8. Role i odpowiedzialności za bezpieczeństwo informacji.

Wszyscy pracownicy, a także inne osoby mające dostęp do informacji na podstawie zawartych umów cywilnoprawnych, czy odbywających w UMiG staż, praktykę lub wolontariat, postępują zgodnie z zasadami niniejszej Polityki Bezpieczeństwa Informacji oraz uzupełniającymi ją dokumentami, jeśli mają zastosowanie.

7.8.1. Obowiązki pracowników

Pracownicy zobowiązani są dbać o bezpieczeństwo powierzonych im do przetwarzania, bądź przechowywania informacji, a w szczególności:

1. przestrzegać i stosować opisane w PBI oraz innych dokumentach wewnętrznych zasady;
2. chronić informacje przed dostępem osób nieupoważnionych;
3. chronić informacje przed przypadkowym lub umyślnym zniszczeniem, modyfikacją, czy utratą;
4. zabezpieczać sprzęt i nośniki danych, a także wykonywane wydruki;
5. stosować się do określonych w IZSI zasad w zakresie pracy w systemach informatycznych, w tym odnoszących się do polityki haseł, ochrony antywirusowej itp.;
6. zachować w tajemnicy podczas zatrudnienia, jak i po jego ustaniu, szczegóły technologiczne związane z dostępem i obsługą systemów teleinformatycznych;
7. uczestniczyć w organizowanych szkoleniach z zakresu bezpieczeństwa informacji;
8. powiadamiać każdorazowo IOD oraz bezpośredniego przełożonego o przypadkach:
    1) ujawnienia, bądź możliwości ujawnienia informacji chronionych osobom nieupoważnionym;
    2) utraty lub zniszczenia informacji;
    3) nieautoryzowanej modyfikacji informacji, lub jej próbie;
    4) wadliwego działania systemów teleinformatycznych, czy też braku dostępu do nich.

7.8.2. Obowiązki osób trzecich

Do obowiązków osób trzecich należy między innymi:

1. przestrzeganie tajemnicy prawnie chronionej w zakresie przewidzianym przez prawo;
2. zgłaszanie wszelkich przypadków działań niezgodnych z politykami i regulaminami noszącymi znamiona incydentami bezpieczeństwa;
3. przeciwdziałanie próbom naruszenia bezpieczeństwa informacji.

7.8.3. Przypisanie ról w SZBI

W celu opracowania, wdrożenia i doskonalenia SZBI w UMiG, zdefiniowano role mające szczególne obowiązki w obszarze ochrony informacji.

Określono je według dwóch pionów:

1. Administracyjnego – zarządzającego informacją,
2. Bezpieczeństwa – zarządzającego bezpieczeństwem informacji.

W ramach obydwóch pionów, wyodrębniono następujące funkcje:

1) Głównego Administratora Informacji,
2) Administratorów Informacji,
3) Inspektora Ochrony Danych,
4) Administratora Systemów Informatycznych.

7.8.4. Główny Administrator Informacji (GAI).

Głównym Administratorem Informacji jest Burmistrz, który odpowiada za:

1) wdrożenie, funkcjonowanie, zarządzanie i nadzór nad SZBI;
2) określa rodzaje zasobów podlegających ochronie w UMIG;
3) wyznacza cele i środki przetwarzania danych;
4) w rozumieniu Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (RODO) jest Administratorem Danych Osobowych;
5) zatwierdza i wprowadza Politykę Bezpieczeństwa Informacji oraz dokumenty z nią powiązane;
6) wyznacza Inspektora Ochrony Danych i Administratora Systemów Informatycznych oraz Pełnomocnika ds. Ochrony Informacji Niejawnych;
7) zatwierdza procedury awaryjne związane z potencjalnymi zagrożeniami bezpieczeństwa informacji;
8) dopuszcza i upoważnia do przetwarzania określonych grup informacji, w tym również w systemach informatycznych.

7.8.5. Administratorzy Informacji (AI).

Rolę Administratorów Informacji pełnią kierownicy komórek organizacyjnych UMIG. Do ich obowiązków należy w szczególności:

1) wdrożenie, utrzymanie i doskonalenie systemu zarządzania bezpieczeństwem w podległej komórce;
2) czuwanie nad merytoryczną poprawnością gromadzonych danych przez podległą komórkę;
3) określenie wrażliwości zasobów ze względu na ich poufność, integralność i dostępność;
4) zapewnienie odpowiedniego poziomu bezpieczeństwa przetwarzanych informacji, w tym danych prawnie chronionych;
5) wdrożenie zabezpieczeń dla zasobów, nad którymi sprawują nadzór, stosownie do PBI;

6) nadzór nad wypełnianiem przez komórkę organizacyjną i jej pracowników obowiązków związanych z bezpieczeństwem informacji;

7) monitorowanie funkcjonowania systemów informatycznych wykorzystywanych w komórkach organizacyjnych;

8) wnioskowanie o nadanie, modyfikację lub odebranie uprawnień do przetwarzania danych, w tym przetwarzania w systemach informatycznych;

9) identyfikacja zagrożeń związanych z bezpieczeństwem informacji w komórce organizacyjnej – przekazywanie takich informacji do GAI, IOD i ASI;

10) określenie i realizacja działań w przypadku wykrycia naruszenia bezpieczeństwa informacji, współpraca w tym zakresie z IOD i ASI;

11) wnioskowanie o dokonanie niezbędnych zmian rozwiązań zawartych w PBI i dokumentach powiązanych.

7.8.6. Inspektor Ochrony Danych (IOD).

Inspektor Ochrony Danych:

1) opracowuje wewnętrzne dokumenty w zakresie bezpieczeństwa danych osobowych - przedkłada do zatwierdzenia i zaopiniowania stosowne projekty;

2) wnioskuje o niezbędne zmiany i aktualizacje w prowadzonej dokumentacji SZBI;

3) sprawuje nadzór nad przyznawaniem praw dostępu do przetwarzania danych osobowych, w tym prowadzi rejestr osób upoważnionych;

4) nadzoruje proces nadawania identyfikatora i konta w systemach informatycznych;

5) monitoruje zachowanie odpowiedniego poziomu bezpieczeństwa dla poszczególnych rodzajów informacji;

6) dokonuje okresowych audytów i przygotowuje okresowe raporty dotyczącego stanu bezpieczeństwa informacji w UMiG;

7) przeprowadza analizę ryzyka informacji, w szczególności dla danych osobowych;

8) odpowiada za przeprowadzenie szkoleń z zakresu bezpieczeństwa informacji zawierających dane osobowe.

7.8.7. Administrator Systemów Informatycznych (ASI).

Administratorem Systemów Informatycznych jest wyznaczony przez GAI pracownik. Funkcję tę pełni równolegle jako ASI w procesie przetwarzania danych osobowych. Wśród jego obowiązków wymienić należy:

1) zapewnienie ciągłości działania systemów teleinformatycznych;

2) monitorowanie i kontrola wydajności oraz skuteczności systemów teleinformatycznych;

3) opracowywanie i aktualizacja dokumentacji IZSI;

4) prowadzenie dokumentacji systemów teleinformatycznych, którymi administruje;

5) administrowanie oprogramowaniem systemowym w kontekście zapewnienia bezpieczeństwa informacji;

6) nadzór nad wdrażanymi aplikacjami, współpraca w tym zakresie z dostawcami oprogramowania;

7) zabezpieczenie systemów przed nieautoryzowanym dostępem do nich;

8) instalowanie i konfiguracja nowego sprzętu, systemów i aplikacji;

9) nadawanie użytkownikom uprawnień, identyfikatorów i haseł startowych w systemach informatycznych, zgodnie z przedłożonymi wnioskami;

10) zakładanie i administracja kont pocztowych;

11) zarządzanie kopiami zapasowymi i awaryjnymi;

12) ocenianie pracy systemów informatycznych w celu identyfikacji zagrożeń i nieprawidłowości;

13) określanie i realizacja planów działań awaryjnych na wypadek zagrożenia bezpieczeństwa informacji przetwarzanych w systemach teleinformatycznych;

14) opiniowanie wewnętrznych dokumentów związanych z bezpieczeństwem informacji;

15) wnioskowanie o zmianę i aktualizację dokumentacji SZBI;

16) współpraca z osobami odpowiedzialnymi za bezpieczeństwo informacji określonymi przez PBI;

7.9. Zarządzanie aktywami w ramach SZBI.

UMiG zarządza zasobami (aktywami) dla zapewnienia im wymaganego poziomu bezpieczeństwa. Aktywa służące do przetwarzania informacji lub będące w bezpośredniej korelacji z zapewnieniem tego bezpieczeństwa, muszą zostać zinwentaryzowane i zweryfikowane pod kątem ich zgodności z SZBI.

W załączniku nr 2 do niniejszej Polityki zamieszczono formularz inwentaryzacyjny dla aktywów informatycznych wykorzystywanych w przetwarzaniu informacji, w tym danych osobowych. Ponadto spis aktywów informatycznych wykorzystywanych w przetwarzaniu informacji/danych osobowych stanowi dokumentację zmian w systemach informatycznych.

Do zasobów chronionych zalicza się między innymi:

1) informacje – bazy danych (papierowe i elektroniczne), pliki, regulacje wewnętrzne (np. polityki, regulaminy, instrukcje), dokumentacje systemowe, umowy z dostawcami, kopie zapasowe;
2) aktywa fizyczne – nośniki danych, sprzęt teleinformatyczny;
3) usługi – związane z: przetwarzaniem i przesyłaniem informacji, zapewnieniem ciągłości działalności UMiG;
4) oprogramowanie – wykorzystywane aplikacje i systemy informatyczne;
5) kapitał ludzki – wiedza i doświadczenie pracowników UMiG;
6) wartości niematerialne – wizerunek na zewnątrz, dobre imię UMiG.

Wyszczególnione powyżej aktywa chronione są w oparciu o wartość materialną i intelektualną na podstawie:

1) przepisów prawa ogólnie obowiązującego;
2) zapisów umów cywilnoprawnych;
3) warunków licencji.

Aktywa informacyjne są identyfikowane zgodnie z wymaganiami w zakresie ich ochrony. Zasadą nadrzędną jest określnie odrębnych szczegółowych regulacji z określeniem grupy pracowników posiadających do nich dostęp. Zgodnie z uregulowaniami prawnymi, rodzaje informacji przetwarzanych przez UMiG zostały sklasyfikowane w rozdziale „*Rodzaje informacji przetwarzanych przez UMiG*”.

7.10. Zarządzanie bezpieczeństwem zasobów ludzkich.

UMiG w swojej działalności dąży do zapewnienia wykwalifikowanej obsady personalnej dla realizacji zadań gminnych. Dążenie do realizacji tak zdefiniowanego celu jest możliwe dzięki odpowiedniemu podziałowi kompetencji, a także procedurom związanym z okresową oceną kadry pracowniczej, jak również ustanowionymi zasadami zatrudniania na stanowiska urzędnicze. Dodatkowym źródłem zapewnienia odpowiednich kwalifikacji w tym z zakresu bezpieczeństwa informacji są prowadzone szkolenia.

Odnosząc się nieco szerzej do zasobów ludzkich w kontekście bezpieczeństwa informacji należy stwierdzić, że stanowią one bardzo istotny element zaliczany do źródeł zagrożeń – w związku z powyższym ustanowiono trzy etapy stosowania zabezpieczeń dla tego obszaru obejmujące:

1. Okres przed zatrudnieniem.

Kandydaci do pracy powinni przejść stosowne procedury rozpoczęcia zatrudniania, w skład których wchodzą: szkolenia wstępne z zakresu bhp, bezpieczeństwa informacji oraz szczegółowy instruktaż związany z wykonywanymi obowiązkami na stanowisku pracy, zapoznanie się z regulacjami wewnętrznymi w szczególności PBI, uzyskanie uprawnień do przetwarzania określonego rodzaju informacji.

2. **W okresie zatrudnienia.**

Pracownicy na podstawie stosownych wniosków Administratora Informacji (AI) uzyskują uprawnienia do poszczególnych rodzajów informacji, przetwarzanych tradycyjnie lub systemach teleinformatycznych. Nadane uprawnienia mogą być w każdym czasie modyfikowane, bądź wycofane.

Wszyscy pracownicy UMiG objęci są obligatoryjnie szkoleniem z zakresu bezpieczeństwa informacji, w szczególności informacji prawnie chronionych. Formę i częstotliwość tych szkoleń określają dokumenty powiązane odnoszące się poszczególnych rodzajów informacji.

3. **Po zakończeniu zatrudnienia**

Zakończenie zatrudnienia może być związane z ryzykiem przejęcia, kradzieży lub bezprawnego wykorzystania powierzonych w czasie stosunku pracy informacji. Minimalizacja tych ryzyk odbywa się głównie poprzez niezwłoczne odbieranie uprawnień i dostępów. W proces ten angażuje się merytoryczna komórka organizacyjna zatrudniająca pracownika, komórka organizacyjna odpowiadająca odpowiednio za sprawy kadrowe oraz ASI i ABI.

Szczegółowe zasady nadawania upoważnień określono w *„Polityce Ochrony Danych Osobowych”* w rozdziale III oraz p.2 *"Instrukcji Zarządzania Systemem Informatycznym".*

7.11. Zarządzanie systemami teleinformatycznymi.

Zarządzanie systemami teleinformacyjnymi UMiG ma na celu głównie zapewnienie poufności, integralności i dostępności przetwarzanych informacji. Realizacja tak postawionego celu opiera się o następujące zasady:

1) Wszystkie systemy i aplikacje dopuszczane do użytkowania powinny spełniać minimalne wymogi bezpieczeństwa określone poprzez obowiązujące akty prawe oraz być zgodne ze standardami wewnętrznymi określonymi przez UMiG;
2) Wdrażane są efektywne zabezpieczenia systemów i aplikacji przed oprogramowaniem złośliwym;
3) Egzekwowana jest jakość usług dostarczanych przez podmioty zewnętrzne związana z serwisem lub okresową konserwacją urządzeń przetwarzających informacje;
4) Kontrolowanie wprowadzonych zmian do infrastruktury technicznej;
5) Wykonywanie kopii zapasowych i bezpieczeństwa;
6) Monitorowanie aktywów informacyjnych przetwarzanych w systemach teleinformatycznych pod kątem ich podatności na zagrożenia;
7) Monitorowanie poziomu incydentów w systemach i zapewnienia mechanizmów ich przeciwdziałania.
8) W celu ochrony poufności przesyłanych danych stosuje się zabezpieczenia kryptograficzne.

7.12. Zapewnienie bezpieczeństwa fizycznego.

Zapewnienie odpowiedniego poziomu bezpieczeństwa fizycznego dla informacji przetwarzanych w UMiG realizowane jest poprzez podział odpowiedzialności, wyznaczenie stref bezpieczeństwa, a także określenie zasad organizacji pracy oraz sposobu przydzielania praw dostępu do danych.

Jednym z kluczowych elementów zapewnienia bezpieczeństwa informacji jest kontrola dostępu obejmująca:

1) kontrolę do pomieszczeń biurowych i obszarów chronionych związanych z przetwarzaniem danych prawnie chronionych;
2) kontrolę dostępu do systemów teleinformatycznych i sieci publicznych;
3) ustalenie zasad nadawania uprawnień do przetwarzania określonych rodzajów informacji w sposób tradycyjny i w systemach informatycznych;
4) zapewnienie utrzymania i ciągłości działania dla kluczowych w UMiG systemów teleinformatycznych;
5) określenie „polityki haseł" odpowiedniej do poziomu bezpieczeństwa przetwarzanych informacji;
6) realizację tzw. „polityki czystego biurka i ekranu";
7) używanie adekwatnych do sytuacji zabezpieczeń kryptograficznych;

Wyszczególnione powyżej zasady mają na celu zapewnienie bezpieczeństwa informacji przed dostępem osób niepowołanych, uszkodzeniem, lub innymi formami zakłóceń w ich przetwarzaniu.

7.13. Zarządzanie incydentem związanym z bezpieczeństwem informacji.

7.13.1. Istota i definicja incydentów

Postępowanie z incydentami bezpieczeństwa informacji w UMiG stanowi bardzo ważny element SZBI. Wraz z procesami zarządzania ryzykiem, zarządzanie zdarzeniami bezpieczeństwa informacji, ma na celu zapewnienie ciągłości działania oraz ograniczenie wpływu przypadków naruszeń bezpieczeństwa aktywów informacyjnych na działalność całego UMiG.

Incydentem bezpieczeństwa informacji jest zdarzenie, którego bezpośrednim lub pośrednim skutkiem jest lub może być naruszenie bezpieczeństwa aktywów informacyjnych.

Incydenty bezpieczeństwa informacji mogą być związane z przyczynami zewnętrznymi – wyładowania atmosferyczne, powódź, pożar itp., jak również celowymi działaniami ludzkimi (zarówno w celu uzyskania korzyści finansowych, chęci sprawdzenia własnych umiejętności, zemsty), czy niezamierzonymi błędami lub zaniedbaniami. Zatem incydentem mogą być w szczególności:

1) przypadki naruszenia poufności (ujawnienie niepowołanym osobom), integralności (uszkodzenie, zniszczenie) i dostępności (dane nie są dostępne w użytecznej postaci) danych, niezależnie od ich zastosowanego nośnika, w tym także przechowywanych i przetwarzanych w systemach informatycznych oraz transmitowanych przez łącza sieci;

2) niedostępności oraz błędne działanie systemów informatycznych;

3) infekcje i działania szkodliwego oprogramowania, do których zaliczają się między innymi wirus, robak internetowy, koń trojański, keylogger, rootkit, itp.;

4) rozpoznanie, penetracja i próby omijania systemów zabezpieczeń;

5) niewłaściwe wykorzystywanie lub nadużywanie zasobów informacyjnych;

6) próby nieautoryzowanego dostępu do aplikacji, czy systemów informatycznych;

7) kradzież, zagubienie lub zniszczenie urządzeń przetwarzających i przechowujących informacje oraz nośników danych;

8) wyłudzenia lub próby wyłudzeń informacji wrażliwych, np. haseł dostępu czy tajemnicy służbowej;

9) celowe naruszanie przepisów prawa w zakresie bezpieczeństwa informacji powszechnie obowiązującego, regulacji wewnętrznych, czy odnoszących się do nich zapisów w umowach z podmiotami zewnętrznymi.

7.13.2. Proces zarządzania incydentem

Proces zarządzania incydentami bezpieczeństwa składa się z następujących etapów:

1. **Wstępnego przygotowania postępowania z incydentem.**

   Ten etap ma na celu zapewnienie możliwości wykrycia, prawidłowej identyfikacji i kategoryzacji incydentu oraz właściwego postępowania z zaistniałym incydentem. Związany jest on przede wszystkim z opracowaniem stosownej procedury dotyczącej wszystkich pracowników UMiG.

2. **Identyfikacja i zgłoszenie incydentu.**

   Incydenty bezpieczeństwa informacji mogą być identyfikowane na różne sposoby, przez zastosowanie narzędzi pomocniczych oraz przez wszystkich zatrudnionych, jak również przedstawicieli podmiotów zewnętrznych.

   Zgłaszający incydent odpowiada za jego szczegółowe opisanie.

   Incydent powinien być zgłaszany niezwłocznie po jego zaistnieniu, lub wykryciu do GAI, IOD, czy AI, bądź ASI jeżeli dotyczy on poprawności działania systemów informatycznych.

3. **Zebranie i selekcja informacji o incydencie.**

   Kolejnym etapem jest pozyskiwanie informacji dodatkowych o incydencie. Mogą one pochodzić z systemów monitorujących, systemów zabezpieczeń i urządzeń sieciowych, czy dokumentacji opisujących wcześniejsze analogiczne przypadki. Na tym, etapie niezwykle istotne jest gromadzenie informacji niezbędnych dla zabezpieczenia danych tak, aby nie utraciły one atrybutów dostępności, integralności, poufności i autentyczności.

   Zebrane materiały powinny zachować wartość dowodową. W oparciu o nie dokonywana jest analiza czy zaistniałe zdarzenie wyczerpuje znamiona incydentu, a jeżeli tak to jaki jest jego rozmiar i wpływ incydentu na działalność całego UMiG, bądź konkretnej komórki organizacyjnej. Na każdym etapie postępowania z incydentem ta klasyfikacja może być zmieniona, o ile zajdą ku temu przesłanki.

4. **Analiza zgromadzonych informacji**

   Polega na weryfikacji pozyskanego materiału pod kątem poprawności i kompletności. Następnie, określona zostaje istotność zaistniałego incydentu w oparciu o skalę skutków, co determinuje dalsze działania.

   Ważne jest określenie krytyczności incydentu, czyli stopnia jego oddziaływania na procesy, czy infrastrukturę teleinformatyczną, w kontekście zapewnienia bezpieczeństwa informacji.

   ASI zgłasza incydent niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia, do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV. Jeżeli incydent dotyczy danych osobowych to podlega także zgłoszeniu do Prezesa Urzędu Ochrony Danych Osobowych.

5. **Minimalizacja wpływu.**

   Minimalizacja zasięgu zaistniałego incydentu bezpieczeństwa oraz ograniczenie jego wpływu na działalność to etap, który ma na celu natychmiastową identyfikację luk i podatności w zabezpieczeniu systemów i procesów.

   Obejmuję on także planowanie i uruchomienie działań powstrzymujących przebieg i zasięg incydentu. Zastosowane metody muszą być ściśle zależne od rodzaju zaistniałego incydentu.

6. **Działania naprawcze**.

   Wdrożenie postępowania naprawczego dla przywrócenia procesów i systemów do normalnego działania i odtworzenia danych. Postępowanie naprawcze to zaplanowanie i wdrożenie działań związanych z przywróceniem ciągłości operacyjnej, odzyskaniem danych, usunięciem śladów incydentów i zapewnieniem w konsekwencji bezpieczeństwa systemów i procesów.

   W tym etapie wykonywane są m.in. takie czynności jak przywracanie poprawnej konfiguracji z kopii zapasowych, zmiana haseł, wzmacnianie bezpieczeństwa instalacji i ustawień systemów, czy włączanie innych wymaganych zabezpieczeń fizycznych, technicznych lub organizacyjnych.

7. **Dokumentowanie i raport.**

   Dokumentacja dotycząca incydentu powinna być prowadzona na każdym jego etapie; przygotowana i utrzymywana w taki sposób, aby zawierała rzetelne i aktualne informacje o incydencie.

   Metody dokumentowania muszą spełniać wymagania autentyczności i integralności, zwłaszcza kiedy istnieje prawdopodobieństwo ich wykorzystania w charakterze materiału dowodowego np. w sądzie.

   Sporządzana dokumentacja może zawierać dane wrażliwe, w związku z powyższym dostęp do niej musi być ograniczony.

   Po zakończeniu dokumentowania IOD sporządza i przedkłada GAI stosowny raport.

   Wzór raportu zawarto w załączniku nr 9 do PODO.

8. **Plan przeciwdziałania incydentom.**

   Plany zapobiegania incydentom w przyszłości powstają na podstawie rekomendacji zawartych w raportach incydentów oraz danych pozyskanych z oceny ryzyka.

   Głównym celem i zamierzeniem tworzonych planów ma być taki dobór środków zapobiegawczych, aby były one adekwatne do skutecznej eliminacji, bądź minimalizacji ryzyka powtórzenia incydentu w przyszłości.

   Plany powyższe powstają przy zaangażowaniu wszystkich osób związanych z reakcją na już zaistniałe incydenty.

Reakcja na incydenty związane z naruszeniem bezpieczeństwa danych osobowych odbywa się stricte w oparciu o "*Instrukcję postępowania w sytuacji naruszenia systemu ochrony danych osobowych" - załącznik nr 10 do PODO*

Do sposobu postępowania z incydentem w informacji niejawnej stosuje się regulacje z zakresu przetwarzania informacji niejawnych.

Niesklasyfikowane inne incydenty są zgłaszane w trybie przewidzianym niniejszą procedurą.

7.14. Podsumowanie – postanowienia końcowe.

Wdrożenie i utrzymanie *Polityki Bezpieczeństwa Informacji* jako części SZBI ma za zadanie skuteczną ochronę informacji przed szeroką gamą zagrożeń. Zagrożenia te częściowo definiuje dokumentacja SZBI.

Bieżący monitoring i stałe doskonalenie przyjętego systemu zwiększa poziom bezpieczeństwa informacji. Na wspomniany stan zabezpieczeń składa się cały proces zarządzania bezpieczeństwem informacji oraz środki proceduralno-organizacyjne, zabezpieczenia techniczne i fizyczne. Zabezpieczenia te bezwzględnie muszą zostać ustanowione, wdrożone, monitorowane, sprawdzone i udoskonalone, a sama ich eksploatacja powinna odbywać się w powiązaniu z innymi procesami rozwoju i zarządzania UMiG.

Z dokumentacją SZBI powinni się zapoznać i stosować wszyscy pracownicy UMiG, potwierdzając ten fakt podpisem na arkuszu zapoznania się z PBI.

Prawo dostępu w niezbędnym zakresie do *Polityki Bezpieczeństwem Informacji* przysługuje ponadto osobom i instytucjom (w tym stronom umów i porozumień) mającym dostęp do informacji podlegającej ochronie.

Zmiany wprowadzane w załącznikach do niniejszego dokumentu nie wymagają zmiany zarządzenia, które wprowadziło niniejszą *Politykę* w życie.

8. WYKAZ ZAŁĄCZNIKÓW

1) Załącznik nr 1 – Wykaz obowiązujących UMiG aktów prawnych związanych z bezpieczeństwem informacji.

2) Załącznik nr 2 – Spis aktywów informatycznych wykorzystywanych w przetwarzaniu informacji / danych osobowych.

Załącznik nr 1
do *Polityki Bezpieczeństwa Informacji*

WYKAZ OBOWIĄZUJĄCYCH UMiG AKTÓW PRAWNYCH ZWIĄZANYCH Z BEZPIECZEŃSTWEM INFORMACJI

1. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE z 2016 r., L 119, poz. 1);

2. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t. j. Dz. U. z 2019 r. poz. 1781);

3. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t. j. Dz. U. z 2021 r. poz. 2070 z późn. zm.);

4. Rozporządzenia wykonawcze do w/w ustaw:

    1) Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie krajowych ram interoperacyjności minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych

    2) Rozporządzenie Ministra Cyfryzacji z dnia 10 marca 2020 roku w sprawie szczegółowych warunków organizacyjnych i technicznych, które powinien spełniać system teleinformatyczny służący do uwierzytelniania użytkowników

    3) Rozporządzenie Ministra Cyfryzacji z dnia 29 czerwca 2020 roku w sprawie profilu zaufanego i podpisu zaufanego

    4) Rozporządzenie Rady Ministrów z dnia 27 września 2005 roku w sprawie sposobu zakresu i trybu udostępniania danych zgromadzonych w rejestrze publicznym

    5) Rozporządzenie Prezesa Rady Ministrów z dnia 14 września 2011 roku w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępnienia formularzy wzorów i kopii dokumentów elektronicznych

    6) Rozporządzenie Ministra Cyfryzacji z dnia 5 października 2016 roku w sprawie zakresu i warunków korzystania z elektronicznej platformy usług administracji publicznej

5. Opinie i wytyczne Grupy Roboczej art. 29

6. Decyzje i interpretacje w indywidualnych sprawach wydawane przez UODO

7. Normy ISO z grupy 27000 (27001, 27002, 27005)

Regulacje wewnętrzne powiązane z SZBI

1. Zarządzenie nr 220/2020 Burmistrza w sprawie ustalenia "Polityki ochrony danych osobowych w Urzędzie Miasta i Gminy Łasin".

2. Wytyczne nr ORA.0147.3.2017 Burmistrza Miasta i Gminy Łasin z dnia 20 stycznia 2017 r. w sprawie upoważnienia pracowników Urzędu Miasta i Gminy Łasin do wykonywania czynności związanych z zabezpieczeniem pomieszczeń biurowych urzędu.

3. Zarządzenie nr 158/2012 Burmistrza Miasta i Gminy Łasin z dnia 9 lutego 2012 r. w sprawie wyznaczenia i określenia zadań Administratora Bezpieczeństwa Informacji i Administratora Systemu Informatycznego, zmienione zarządzeniem nr 487/2018 Burmistrza Miasta i Gminy Łasin z dnia 15 maja 2018 r. w sprawie wyznaczenia inspektora ochrony danych.

4. Zarządzenie nr 520/2018 z dn. 27 lipca 2018 r. w sprawie funkcjonowania monitoringu wizyjnego na terenie miasta Łasin.

Załącznik nr 2
do *Polityki Bezpieczeństwa Informacji*

SPIS AKTYWÓW INFORMATYCZNYCH WYKORZYSTYWANYCH W PRZETWARZANIU INFORMACJI / DANYCH OSOBOWYCH

System informatyczny	
1. Nazwa systemu	
2. Usługi publiczne świadczone przez system informatyczny	
Organizacja bezpieczeństwa	
1. Dane dostępu do systemów *(loginy, hasła, PINy, kody)* ze wskazaniem których systemów dotyczy	
2. Polityka bezpieczeństwa i inne dokumenty techniczne	
3. Szczegółowe procedury bezpieczeństwa (jakie)	
4. Umowy z dostawcami usług (różnych)	
Oprogramowanie	
1. Systemy operacyjne	
2. Oprogramowanie biurowe	
3. Serwery usługowe	
4. Oprogramowanie administracyjne	
5. Oprogramowanie sprzętowe (firmware wbudowane)	
6. Sterowniki	
7. Oprogramowanie własne	

8. Strony www i aplikacje webowe, poczta mail	
Sprzęt	
1. Serwery (fizyczne i wirtualne)	
2. Stacje robocze (PC, laptopy)	
3. Urządzenia mobilne (smartfony, tablety)	
4. Urządzenia peryferyjne (drukarki, skanery)	
5. Elektroniczne nośniki z danymi	
6. Nośniki instalacyjne	
7. Nośniki licencji	
8. Dokumentacja papierowa	
9. Centrala telefoniczna	
10. Urządzenia telefoniczne (telefony, faxy, modemy)	
11. Łącza (internet, centrala voip)	
Sieć	
1. Okablowanie	
2. Usługi sieciowe	
3. Urządzenia aktywne (switche, routery)	
4. Urządzenia pasywne np. panele krosownicze	
Infrastruktura	
1. Serwerownia	
2. Studzienki i kanały telekomunikacyjne	

3. Rozdzielnia elektryczna	
4. Miejsca przetwarzania danych osobowych	
5. Klimatyzatory	
6. Zasilacze awaryjne i agregaty	
7. Mierniki środowiska (czujniki temperatury, dymu)	
8. Urządzenia do monitoringu (kamery, rejestratory)	
9. Stanowiska monitoringu	
10. Systemy alarmowe	
11. Archiwum (*Archiwista, usługi porządkowe w składnicy akt, likwidacja, niszczenie dokumentów*)	
Pracownicy	
1. Kompetencje (kto i jakie uprawnienia)	
Kontrahenci	
1. Umowy na powierzenie przetwarzania danych osobowych	
2. Dostawcy usług serwisowych i gwarancyjnych	
3. Dostawcy oprogramowania	
4. Wsparcie techniczne, naprawy, instalacje urządzeń IT	