Zarządzenie Nr 71/2019
Kierownika Miejsko-Gminnego Ośrodka
Pomocy Społecznej w Łasku
z dnia 31 grudnia 2019 r.

w sprawie wprowadzenia zmian do Polityki Bezpieczeństwa Informacji w Miejsko-Gminnym Ośrodku Pomocy Społecznej w Łasku

Na podstawie 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 (Dz. Urz. UE L 119/1 z 4.5.2016 r.)§ 2 ust. 5 Regulaminu Organizacyjnego Miejsko-Gminnego Ośrodka Pomocy Społecznej w Łasku zatwierdzonego Zarządzeniem nr 245/2015 Burmistrza Łasku z dnia 30 listopada 2015 r. ze zm.) oraz Zarządzenia Nr 14/2018 Kierownika Miejsko-Gminnego Ośrodka Pomocy Społecznej w Łasku z dnia 25 maja 2018 roku w sprawie wprowadzenia Polityki bezpieczeństwa informacji, Instrukcji zarządzania systemem informatycznym, Procedury szacowania ryzyka i oceny skutków, Procedury zarządzania incydentami oraz Procedury zarządzania zmianą w Miejsko-Gminnym Ośrodku Pomocy Społecznej w Łasku ***zarządzam, co następuje***:

§ 1. Załącznik Nr 1 do Zarządzenia Nr 14/2018 Kierownika Miejsko-Gminnego Ośrodka Pomocy Społecznej w Łasku z dnia 25 maja 2018 roku w sprawie wprowadzenia Polityki bezpieczeństwa informacji, Instrukcji zarządzania systemem informatycznym, Procedury szacowania ryzyka i oceny skutków, Procedury zarządzania incydentami oraz Procedury zarządzania zmianą w Miejsko-Gminnym Ośrodku Pomocy Społecznej w Łasku otrzymuje nowe brzmienie zgodnie z załącznikiem do niniejszego zarządzenia.

§ 2. Zobowiązuję pracowników Miejsko-Gminnego Ośrodka Pomocy Społecznej w Łasku do zapoznania się i ścisłego przestrzegania wprowadzonych zmian.

§ 3. Wykonanie zarządzenia powierzam Kierownikom Działów i Sekcji w Miejsko-Gminnym Ośrodku Pomocy Społecznej w Łasku.

§ 4. Zarządzenie wchodzi w życie z dniem podjęcia.

Kierownik Miejsko-Gminnego
Ośrodka Pomocy Społecznej w Łasku
mgr Tamara Szymko

Nie wnoszę zastrzeżeń
formalno-prawnych

RADCA PRAWNY
Paweł Kubiński

Załącznik do Zarządzenia nr 71/2019
Kierownika Miejsko-Gminnego Ośrodka Pomocy Społecznej w Łasku
z dnia 31 grudnia 2019 r.

Polityka bezpieczeństwa informacji

Miejsko – Gminnego

Ośrodka Pomocy Społecznej

w Łasku

Wydanie – 2/2019

1. Cel dokumentu

Wprowadzenie Polityki Bezpieczeństwa Informacji, zwanej dalej Polityką, ma na celu spełnienie obowiązków wynikających z powszechnie obowiązującego prawa, które określa art. 24 ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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. Ponadto niniejsza polityka stanowi nadrzędny dokument Systemu Zarządzania Systemem Informacji, którego celem jest ochrona interesów osób, których dane dotyczą poprzez zapewnienie należytej i adekwatnej do przewidywanych zagrożeń oraz kategorii przetwarzanych danych, ochrony posiadanych zasobów informacyjnych oraz świadczenie usług o wysokim standardzie, realizowanych przez Miejsko – Gminny Ośrodek Pomocy Społecznej w Łasku, zwany dalej MGOPS lub Ośrodkiem.

2. Zakres dokumentu

Niniejsza Polityka obejmuje wszystkich pracowników oraz osoby i podmioty przetwarzające dane osobowe w imieniu Ośrodka. W związku z powyższym stosowanie niniejszej Polityki obejmuje wszystkie dane osobowe przetwarzane przez MGOPS, który zapewnia bezpieczeństwo podczas ich zbierania, utrwalania, organizowania, porządkowania, przechowywania, adaptowania lub modyfikowania, pobierania, przeglądania, wykorzystywania, ujawniania poprzez przesłanie, rozpowszechniania lub innego rodzaju udostępniania, dopasowywania lub łączenia, ograniczania, usuwania lub niszczenia.

3. Deklaracja najwyższego kierownictwa

Na podstawie niniejszej Polityki Kierownik MGOPS deklaruje świadomość potrzeby ochrony informacji oraz wskazuje zabezpieczenia, mechanizmy i procesy umożliwiające zapewnienie bezpieczeństwa przetwarzanych danych, a ponadto rozpoznaje ciągłe doskonalenie Systemu Zarządzania Bezpieczeństwem Informacji poprzez realizowane przeglądy.

4. Podstawa prawna

4.1. Tworząc System Zarządzania Bezpieczeństwem Informacji Miejsko-Gminny Ośrodek Pomocy Społecznej w Łasku uwzględnia przy tym regulacje prawne, które określa:

a) 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,

b) Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych oraz

c) Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych.

5. Definicje

5.1. Definicje oraz pojęcia użyte w niniejszej Polityce są wspólne dla wszystkich dokumentów powiązanych, przyjętych przez Ośrodek w zakresie ochrony danych osobowych. Ilekroć jest mowa o:

- **Administratorze danych osobowych**, tj. ADO – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę organizacyjną, lub inny podmiot lub osobę, która samodzielnie lub wspólnie
  z innymi ustala cele i sposoby przetwarzania danych osobowych;

- **Administratorze systemów informatycznych**, tj. ASI – rozumie się przez to osobę fizyczną wyznaczoną przez ADO, która odpowiada za zapewnienie sprawności, należytej konserwacji i wdrażania technicznych zabezpieczeń systemów informatycznych oraz odpowiada za to, aby systemy informatyczne, w których przetwarzane są dane osobowe, zgodnie z zakresem przypisanych uprawnień oraz obowiązków;
- **Bezpieczeństwie informacji** – należy przez to rozumieć zapewnienie poufności, integralności oraz dostępności informacji;
- **danych osobowych** – rozumie się przez to wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
- **Danych „wrażliwych"**, tj. szczególnych kategorii – rozumie się przez to dane osobowe objęte szczególną ochroną, ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne umożliwiające jednoznaczne zidentyfikowanie osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej osoby, której te dane dotyczą;
- **Dostępności** – należy przez to rozumieć, że informacja jest zawsze dostępna, kiedy zachodzi taka potrzeba ;
- **Incydencie** – oznacza niepożądane i niespodziewane, pojedyncze zdarzenie związane z bezpieczeństwem informacji lub serie takich zdarzeń, które stwarzają znaczne prawdopodobieństwo zakłócenia prowadzonych działań;
- **Inspektorze ochrony danych**, tj. IOD – rozumie się przez to osobę posiadającą odpowiednie kwalifikacje zawodowe, w szczególności posiadającą wiedzę fachową na temat prawa i praktyk w zakresie ochrony danych oraz umiejętność wypełnienia zadań określonych w RODO;
- **Integralności** – rozumie się przez to właściwość informacji polegająca na jej modyfikacji, która zapewnia że zapis informacja nie został zmieniony w nieautoryzowany sposób;
- **Naruszeniu ochrony danych osobowych** – rozumie się przez to naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
- **Organie nadzorczym** – rozumie się przez to Prezesa Urzędu Ochrony Danych Osobowych, zgodnie z art. 51 RODO;
- **Osobach uprawnionych** – rozumie się przez to wszystkie osoby uprawnione do przetwarzania informacji w ramach wykonywanych obowiązków służbowych lub działających na podstawie przepisów prawa;
- **osobie upoważnionej** – rozumie się przez to osobę, która otrzymała upoważnienie do przetwarzania danych, przez które rozumie się oświadczenie nadawane przez ADO wskazujące z imienia i nazwiska osobę, która ma prawo przetwarzać dane osobowe w Ośrodku,
- **Poufności** – należy przez to rozumieć właściwość, która zapewnia, że informacje nie zostaną udostępnione osobom nieuprawnionym;
- **przetwarzaniu danych osobowych** – rozumie się przez to operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie,

porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

- **RODO** – rozumie się przez to 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;
- **Strukturze informatycznej** – oznacza to zespół środków technicznych i ich zabezpieczeń, tj. urządzeń (komputerów, drukujące, łączności, wraz z okablowaniem i oprogramowaniem) oraz oprogramowania (systemów operacyjnych, oprogramowania urządzeń), a także sieć informatyczna i udostępniane przez nią zasoby;
- **Systemie informatycznym** – rozumie się przez to system przetwarzania informacji składający się z urządzeń komputerowych, oprogramowania oraz zewnętrznych nośników informacji;
- **Systemie Zarządzania Bezpieczeństwem Informacji**, tj. SZBI – oznacza zbiór wszystkich zasad, procedur i procesów realizowanych w celu zapewniania bezpieczeństwa informacji;
- **Ustawie** – rozumie się przez to Ustawę z dnia z dnia 10 maja 2018 r. o ochronie danych osobowych;
- **Usuwaniu danych** – rozumie się przez to zniszczenie lub modyfikację danych osobowych w sposób niepozwalający identyfikacji osoby, której dane dotyczą;
- **Użytkowniku** – rozumie się przez to osobę upoważnioną, posiadającą prawo dostępu do informacji, która otrzymała dostęp do sieci LAN umożliwiający korzystanie z sieci Internet oraz identyfikator użytkownika, w tym hasło dostępu do systemu;
- **Zbiorze danych osobowych** – rozumie się przez to każdy zestaw danych o charakterze osobowym, posiadający strukturę, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony, czy podzielony funkcjonalnie;
- **Zdarzeniu** – rozumie się przez to zdarzenie związane z bezpieczeństwem informacji oraz oznacza stwierdzone wystąpienie stanu systemu, usługi lub sieci, który wskazuje na możliwe naruszenie polityki bezpieczeństwa informacji lub błąd zabezpieczenia, lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem informacji.

6. Klasyfikacja informacji

W ramach Systemu Zarządzania Bezpieczeństwem Informacji przyjmuje się następującą klasyfikację informacji, identyfikując przy tym poniższe poziomy ochrony informacji:

I. **Poziom 1** – dotyczący informacji jawnych oraz informacji publicznej. Oznacza zapewnienie integralności oraz dostępności informacji, bez wymogu zachowania ich poufności.

II. **Poziom 2** – dotyczący informacji chronionych, tj. danych osobowych, danych „wrażliwych", tajemnicy przedsiębiorstw oraz tajemnicy skarbowej. Informacjom tej kategorii zapewnia się poufność, integralność oraz dostępność.

III. **Poziom 3** – dotyczący informacji niejawnych, zgodnie z Ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych

6.1. SZBI swoim zakresem obejmuje informacje z wyłączeniem poziomu 3 z uwagi na informacje niejawne, które wynikają z odrębnych regulacji prawnych oraz są zarządzane przez wyznaczone osoby spełniające określone warunki, zgodnie z obowiązującymi przepisami prawa.

6.2. Informacje jawne stanowią informacje udostępniane za pośrednictwem stron internetowych Ośrodka, takie jak dane kontaktowe, czy dane pracowników.

6.3. Informacje publiczne stanowią informacje udostępniane zgodnie z Ustawą z dnia 6 września 2001 r. o dostępie do informacji publicznej.

6.4. W ramach współpracy z podmiotami zewnętrznymi podczas realizacji zamówień publicznych istnieją przypadki informacji objętych tajemnicą przedsiębiorstwa.

6.5. Informacje stanowiące tajemnicę przedsiębiorstwa zabezpiecza się zgodnie z przyjętymi zasadami bezpieczeństwa w ramach zawartej umowy.

6.6. W ramach zapewnienia bezpieczeństwa informacji stosuje się środki ochrony fizycznej oraz ograniczenia dostępu do pomieszczeń, o których mowa w punkcie 9 Polityki Ochrony Danych Osobowych.

6.7. W przypadku informacji przetwarzanych za pomocą systemów informatycznych środki bezpieczeństwa określa Instrukcja Zarządzania Systemami Informatycznymi.

7. Ogólne zasady bezpieczeństwa informacji

7.1. Podstawą Systemu Zarządzania Bezpieczeństwem Informacji oraz stosowanych zabezpieczeń są wymagania prawne, wyniki przeprowadzanego szacowania ryzyka utraty bezpieczeństwa informacji oraz wyniki monitorowania realizowanego przez IOD i audytów zewnętrznych lub wewnętrznych oraz przeglądy zarządcze.

7.2. Bezpieczeństwo informacji jest realizowane poprzez stosowanie zabezpieczeń organizacyjnych, technicznych, fizycznych oraz środowiskowych.

7.3. Przez informacje objęte ochroną opisaną w dokumentacji SZBI należy rozumieć dane osobowe, w rozumieniu artykułu 4 RODO.

7.4. Przez zapewnienie bezpieczeństwa informacji rozumie się zapewnienie każdego z tych atrybutów informacji:

a) poufności – rozumianej jako właściwość zapewniająca, że informacje nie są udostępniane nieupoważnionym osobom,

b) integralności – rozumianej jako właściwość zapewniająca, że informacja nie została zmieniona lub zniszczona w sposób nieautoryzowany,

c) dostępności – rozumianej jako zapewnienie, że informacja jest dostępna zawsze wtedy, kiedy zachodzi taka potrzeba.

7.5. W MGOPS obowiązują następujące zasady bezpieczeństwa:

a) „Zasada wiedzy koniecznej" – osoby uprawnione posiadają informacje niezbędne do wykonywania przez nich obowiązków.

b) „Zasada potrzeby koniecznej" – osoby uprawnione mają dostęp jedynie do zasobów, które są niezbędne do wykonywania przez nich obowiązków.

c) „Zasada zachowania poufności" – osoby uprawnione są zobowiązane do zachowania poufności o informacjach, które zdobyły przez realizowanie swoich czynności zawodowych oraz o stosowanych w Ośrodku zabezpieczeniach obejmujących te informacje.

7.6. We wszystkich sytuacjach spornych lub specyficznych wymaganiach nieujętych w dokumentacji SZBI, zezwolenia na odstępstwa może wydać Kierownik MGOPS lub w uzasadnionych sytuacjach zmian może dokonać KKO. Sytuacje wymagające odstępstw mogą być podstawą do dalszego rozwijania dokumentacji.

8. Odpowiedzialności w bezpieczeństwie informacji

8.1. Administrator Danych Osobowych

- ✓ Kierownik MGOPS (jako realizujący zadania ADO) – odpowiada za zapewnianie środków na realizowanie postanowień wynikających z wymagań prawnych, zatwierdzanie dokumentacji SZBI, przydzielanie obowiązków w zakresie bezpieczeństwa informacji oraz prowadzenie nadzoru nad zgodnością przetwarzania danych osobowych,
- ✓ Do obowiązków ADO należy w szczególności:

a) Realizacja zadań wynikających z przepisów prawa określonych w punkcie 4,
b) Powyższe realizuje przez wyznaczone osoby, zgodnie z postanowieniami niniejszej Polityki oraz dokumentacji powiązanej

- ✓ ADO wyznacza Inspektora Ochrony Danych, zgodnie z art. 37 RODO,
- ✓ W związku z powyższym ADO zapewnia, że:
  a) inspektor ochrony danych jest właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych;
  b) wspiera inspektora, w wypełnianiu jego obowiązków, o których mowa w punkcie 8.2, zapewniając przy tym niezbędne środki do ich wykonania oraz dostęp do danych osobowych
  i operacji przetwarzania, a także zasoby umożliwiające rozwój posiadanej wiedzy z zakresu ochrony danych osobowych,
- ✓ Ponadto ADO może wyznaczyć Administratora Systemów Informatycznych (ASI), który odpowiada za zapewnienie przestrzegania zasad ochrony danych osobowych przetwarzanych za pomocą systemów informatycznych określonych w Instrukcji Zarządzania Systemem Informatycznym.

8.2. Inspektor Ochrony Danych

- ✓ Do obowiązków IOD należy:
  a) nadzór nad przestrzeganiem zasad bezpieczeństwa danych osobowych,
  b) monitorowanie zgodności z przepisami ochrony danych osobowych,
  c) opiniowanie przeprowadzonych szacowań ryzyka oraz oceny skutków naruszeń,
  d) nadzór nad dokumentacją bezpieczeństwa danych osobowych,
  e) prowadzenie ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych,
  f) podejmowanie działań mających na celu zwiększanie świadomości i szkolenia personelu Administratora uczestniczącego w operacjach przetwarzania danych,
  g) współpraca z organem nadzorczym, w tym pełnienie funkcji punktu kontaktowego w sprawach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO.

- ✓ W celu realizacji powyższych zadań IOD ma prawo:
  a) kontrolować komórki organizacyjne oraz osoby przetwarzające dane osobowe, w zakresie właściwego zabezpieczenia wykorzystywanych zasobów oraz pomieszczeń, w których przetwarzane są dane osobowe,
  b) wydawać polecenia Kierownikom komórek organizacyjnych w zakresie bezpieczeństwa danych osobowych – jeśli zagrożone jest bezpieczeństwo danych osobowych,
  c) informować ADO o przypadkach naruszenia bezpieczeństwa danych osobowych,
  d) raportować ADO wyniki z przeprowadzonych monitorowań oraz zalecać działania jakie należy podjąć w celu naprawy niezgodności,
  e) żądać wyjaśnień w sytuacjach naruszenia bezpieczeństwa danych osobowych od wszystkich osób przetwarzających.

8.3. Administrator Systemu Informatycznego

W ramach zarządzania infrastrukturą teleinformatyczną ASI odpowiada za:

- ✓ zapewnienie przestrzegania zasad ochrony danych osobowych przetwarzanych za pomocą systemów informatycznych, które określa Instrukcja Zarządzania Systemem Informatycznym,
- ✓ realizacje zadań, zgodnie z dokumentacją SZBI

- ✓ Ponadto bierze udział w ocenie zdarzeń naruszających bezpieczeństwo informacji, dotyczących struktury informatycznej oraz w zależności od sytuacji w ocenie skutków naruszeń, oraz uczestniczy w procesie analizowania wpływu na bezpieczeństwo informacji przy wprowadzanych zmianach.

8.4. Kierownicy komórek organizacyjnych

- ✓ Przez Kierowników komórek organizacyjnych tj. KKO, uważa się Kierowników Działów lub Sekcji jak również osoby pełniące funkcje przełożonych oraz zajmujące samodzielne stanowiska, które wyznaczono w ramach struktury Ośrodka,
- ✓ KKO odpowiadają za:
  a) Nadzór nad przetwarzaniem danych w ramach swoich komórek.
  b) Uczestnictwo w procesach nadawania upoważnień i uprawnień, zarządzania naruszeniami bezpieczeństwa oraz realizacji praw osób, których dane dotyczą.
  c) Analizę wpływu na bezpieczeństwo informacji przy wprowadzaniu zmian

8.5. Pracownik ds. kadrowych

- ✓ W zakresie niniejszej Polityki pracownik ds. kadrowych zobowiązany jest do:
  a) Realizacji obowiązku informacyjnego w ramach prowadzonych rekrutacji oraz
  b) Przekazywania informacji do IOD, KKO oraz ASI na temat zatrudnienia pracowników, w tym informowanie o podjęciu pracy, zwolnieniach oraz rozwiązaniu stosunku pracy.

8.6. *Osoby uprawnione*

- ✓ Do obowiązków osób posiadających upoważnienie do przetwarzania danych w Ośrodku należy:
  a) przestrzeganie przepisów prawa oraz zasad bezpieczeństwa informacji,
  b) zwracanie uwagi na obce osoby bez nadzoru w obszarach z ograniczonym dostępem,
  c) zgłaszanie zdarzeń potencjalnie naruszających bezpieczeństwo informacji,
  d) zgłaszanie słabości lub niepoprawnego działania stosowanych zabezpieczeń,
  e) zgłaszanie wszelkich zmian w zakresie procesów przetwarzania danych osobowych, w tym rozszerzania lub zmniejszania zakresu przetwarzanych danych, usuwania lub tworzenia nowych procesów.

8.7. Pozostali pracownicy

- ✓ Pozostali pracownicy, tj. nie związani z przetwarzaniem informacji, są zobowiązani w szczególności do:
  a) zgłaszania zdarzeń potencjalnie naruszających bezpieczeństwo informacji – pozostawionych dokumentów poza zamykanymi obszarami, szafami lub otwartych pomieszczeń po godzinach pracy, itp. oraz
  b) zgłaszania źle funkcjonujących zabezpieczeń, zwłaszcza fizycznych.

9. Przegląd i rozwój systemu zarządzania bezpieczeństwem informacji

9.1. Kierownik Ośrodka, jako realizujący zadania ADO zobowiązany jest do przeprowadzania okresowych audytów, w tym mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania, zgodnie z art. 32 ust. 1 lit. d) RODO, w celu weryfikowania zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz efektywności zasad bezpieczeństwa wdrożonych na podstawie niniejszej Polityki.

9.2. Audyty obejmują przegląd systemu ochrony danych osobowych, w tym audyt systemu ochrony danych osobowych, analizę ryzyka związanego z bezpieczeństwem zasobów uczestniczących w operacjach przetwarzania danych oraz ocenę skutków przetwarzania dla ochrony danych, jeśli ADO jest zobowiązany do wykonania takiej oceny, bądź podejmie decyzję o jej wykonaniu pomimo braku takiego obowiązku. Dokonując przeglądu wykonywanych operacji przetwarzania danych osobowych, należy dokonać oceny podmiotów przetwarzających, o ile takie istnieją, w zakresie spełnienia obowiązków dotyczących powierzenia danych osobowych wynikających z art. 28 RODO.

9.3. Rozwój SZBI jest realizowany zgodnie z Procedurą zarządzania zmianą oraz podejmowanymi na tej podstawie działaniami udoskonalającymi.

9.4. Okresowo przeprowadzane jest szacowanie ryzyka utraty bezpieczeństwa informacji zgodnie z procedurą przeprowadzania szacowania ryzyka i oceny skutków.

9.5. Przegląd SZBI jest realizowany wewnętrznie, poprzez bezpośredni nadzór nad przestrzeganiem przyjętych zasad, zgodnie z podziałem obowiązków oraz w związku z realizacją procedur zarządzania incydentami oraz zarządzania zmianą.

9.6. Przegląd jest również realizowany poprzez audyty wewnętrzne w zakresie bezpieczeństwa informacji. Audyty mogą być realizowane siłami wewnętrznymi lub zewnętrznie.

9.7. Na potrzeby rozwoju dokumentacji SZBI oraz zapewniania jej przestrzegania, wprowadza się numery wydania. Przed wypełnieniem postanowień danej regulacji, należy zweryfikować jej aktualne wydanie, zgodnie z poniższym wykazem dokumentów.

10. Dokumenty powiązane

W ramach SZBI niniejsza Polityka stanowi nadrzędny dokument, a ponadto wyróżnia się:

10.1. Politykę Ochrony Danych Osobowych

10.2. Instrukcje Zarządzania Systemem Informatycznym

10.3. Procedurę przeprowadzania szacowania ryzyka i oceny skutków

10.4. Procedurę realizacji praw osób, których dane dotyczą

10.5. Politykę zarządzania incydentami

10.6. Procedurę zarządzania zmianą

11. Sankcje

Nieprzestrzeganie zasad bezpieczeństwa opisanych w dokumentacji SZBI oraz przepisów prawa określających ochronę danych osobowych stanowi naruszenie obowiązków pracowniczych i może być przyczyną postępowania dyscyplinarnego lub wiązać się z konsekwencjami określonymi przepisami Ustawy lub RODO.

Kierownik Miejsko-Gminnego
Ośrodka Pomocy Społecznej w Łasku

mgr Tamara Szymko

12.Historia zmian dokumentacji

Dokument	Wydanie	Opis zmian	Data wprowadzenia
Polityka Bezpieczeństwa Informacji	1	Rozszerzono opis celu dokumentu, o którym mowa w punkcie 1; Wprowadzono klasyfikacje informacji, zgodnie z opisem punktu 6; Uwzględniono konsekwencje za nieprzestrzeganie zasad w obowiązującym SZBI (punkt 11)	31 grudnia 2019 r.
Polityka Bezpieczeństwa Danych Osobowych	1	Zaktualizowano informacje stosowanych zabezpieczeń fizycznych (punkt 9); Usunięto informacje dotyczące sankcji i konsekwencji (punkt 11)	31 grudnia 2019 r.