ZARZĄDZENIE 141.2022
Wójta Gminy Raciąż
z dnia 29 września 2022 r.

w sprawie wprowadzenia: „Polityki bezpieczeństwa informacji w Urzędzie Gminy Raciąż"

Na podstawie: 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 (Dz. Urz. UE.L 2016 Nr 119, str. 1) zarządzam, co następuje:

§ 1. Uchyla się treść „Polityki Ochrony Danych Osobowych i Instrukcji Zarządzania Systemem Informatycznym w Urzędzie Gminy Raciąż" wprowadzonych Zarządzeniem nr 3.2018 przez Wójta Gminy Raciąż z dnia 7 maja 2018 r.

§ 2. Przyjmuje się „Politykę bezpieczeństwa informacji w Urzędzie Gminy Raciąż" stanowiącą **Załącznik** do niniejszego Zarządzenia. Załącznik do zarządzenia ma charakter dokumentu wewnętrznego i nie podlega publikacji w BIP.

§ 3. 1. Z zarządzeniem zobowiązani są zapoznać się wszyscy pracownicy Urzędu Gminy Raciąż oraz osoby, które przetwarzają na zlecenie Administratora dane osobowe.

2. Prawo do wglądu do „Polityki bezpieczeństwa informacji" w sekretariacie Urzędu mają wszyscy właściciele danych osobowych, które przetwarza Urząd oraz podmioty, które wykażą cel publiczny oraz organy kontrolne.

§ 4. Wykonanie zarządzenia powierza się sekretarzowi Urzędu i inspektorowi ochrony danych.

§ 5. Zarządzenie wchodzi w życie z dniem podpisania.

Wójt Gminy Raciąż

Zbigniew Sadowski

Załącznik
do Zarządzenia 141.2022
Wójta Gminy Raciąż
z dnia 29 września 2022 r.
w sprawie wprowadzenia „Polityki bezpieczeństwa informacji
w Urzędzie Gminy Raciąż"

„POLITYKA BEZPIECZEŃSTWA INFORMACJI W URZĘDZIE GMINY RACIĄŻ"

§ 1

Wstęp

1. Niniejszy dokument reguluje sprawy ochrony danych osobowych przetwarzanych w **Urzędzie Gminy Raciąż**, zwanej dalej „**jednostką**".
2. Jednostka jako administrator danych osobowych deklaruje dołożyć wszelkich starań, aby przetwarzanie tych danych odbywało się w zgodności z obowiązującymi przepisami prawa.
3. Podstawę prawną niniejszego dokumentu stanowi :
   1) rozporządzenie parlamentu europejskiego i rady (UE) 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, zwane dalej w treści „RODO;
   2) ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, zwanej dalej „Ustawą".

§ 2

Deklaracja kierownictwa

1. Wójt Gminy Raciąż, stojąc na stanowisku, że informacja jest newralgicznym zasobem każdej organizacji, wdraża w Urzędzie Gminy Raciąż „Politykę Bezpieczeństwa Informacji", zwanej dalej „**Polityką**".
2. Polityka stanowi zbiór spójnych, precyzyjnych reguł i procedur, według których jednostka buduje, zarządza oraz udostępnia zasoby i systemy informacyjne, informatyczne i stanowi kodeks postępowania w rozumieniu art. 40 RODO.

§ 3

Definicje

Ilekroć w dokumencie jest mowa o:

1) **RODO** – należy przez to rozumieć Rozporządzenie parlamentu europejskiego i rady (UE) 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;
2) **jednostce** – należy przez to rozumieć Urząd Gminy Raciąż z siedzibą przy ul. Kilińskiego 2, 09-140 Raciąż;
3) **Administratorze** – należy przez to rozumieć **Urząd Gminy w Raciążu** reprezentowaną przez **Wójta Gminy Raciąż,** który decyduje o celu i sposobie przetwarzania danych

osobowych w jednostce;

4) **Administratorze Systemu Informatycznego (ASI)** – należy przez to rozumieć osobę, nadzorująca funkcjonowanie systemu informatycznego oraz stosowanie technicznych i organizacyjnych środków ochrony użytkowanych w tych systemach;

5) **danych osobowych** – należy przez to rozumieć informację o zidentyfikowanej lub możliwej do identyfikacji w sposób pośredni lub bezpośredni osobie fizycznej;

6) **Inspektorze Danych Osobowych (IOD)** – należy przez to rozumieć osobę wyznaczoną przez Administratora na podstawie art. 37 RODO, w celu zapewnienia realizacji zadań wskazanych w art. 39 RODO, a w szczególności do monitorowania przestrzegania zasad przetwarzania danych osobowych oraz wymagań w zakresie ich ochrony, określonych w Polityce Bezpieczeństwa Informacji oraz wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych;

7) **informacji** – należy przez to rozumieć wszelkie dane, w tym dane osobowe, przetwarzane w celu i zakresie wskazanym w przepisach prawa lub na podstawie zgody osoby, której dane dotyczą, niezbędne do realizacji zadań urzędu niezależnie od formy przetwarzania lub środków, za pomocą których są udostępniane lub przechowywane;

8) **danych wrażliwych** (szczególnej kategorii danych) – należy przez nie rozumieć dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej, dane dotyczące zdrowia, seksualności lub orientacji seksualnej oraz dane dotyczące wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa;

9) **PUODO** – należy przez to rozumieć Prezesa Urzędu Ochrony Danych Osobowych, będącego organem powołanym do spraw z zakresu ochrony danych osobowych;

10) **przetwarzaniu** – należy przez to rozumieć jakiekolwiek operację lub zestaw operacji wykonywanych na danych, w tym danych osobowych, w tym: zbieranie, przeglądanie, utrwalanie, przechowywanie, zmienianie, udostępnianie i usuwanie;

11) **powierzeniu** – należy przez to rozumieć powierzenie przez jednostkę innemu podmiotowi (podmiotowi przetwarzającemu), danych osobowych na podstawie art. 28 RODO;

12) **zbiorze danych osobowych** – należy przez to rozumieć uporządkowany zestaw danych dostępnych za pomocą wybranych kryteriów wyszukiwania, niezależnie czy jest on scentralizowany, zdecentralizowany lub rozproszony geograficznie lub funkcjonalnie;

13) **Systemie Informatycznym** – należy przez to rozumieć zespół współpracujących ze sobą urządzeń, oprogramowanie, zastosowane narzędzia programowe, procedury przetwarzania danych i informacji oraz dane eksploatowane w tych urządzeniach;

14) **programach komputerowych** – należy przez to rozumieć program lub zestaw programów tworzących system, służące do przetwarzania danych;

15) **użytkownikach** – należy przez to rozumieć osoby przetwarzające dane osobowe, działające na podstawie upoważnienia lub udokumentowanego polecenia Administratora, niezależnie od formy zatrudnienia. Użytkownikiem systemu informatycznego może być osoba której Administrator Systemu Informatycznego nadał identyfikator i hasło dostępu do systemu informatycznego i programów komputerowych;

16) **zasobach** – należy przez to rozumieć wszelkie informacje wytworzone, przetwarzane i przechowywane w jednostce niezależnie od ich postaci i formy przetwarzania, w tym dokumentacja papierowa zawierająca informacje o funkcjonowaniu jednostki, w tym rejestry, ewidencje, księgi, wykazy oraz inne zbiory danych, środki materialne (fizyczne np. serwery, stacje robocze, urządzenia aktywne sieci) i niematerialne (oprogramowanie) oraz personel;

17) **przesyłaniu** – należy przez to rozumieć przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;

18) **identyfikatorze** - należy przez to rozumieć ciąg znaków literowych identyfikujących osobę, której ASI nadał uprawnienia do systemu informatycznego jednostki;

19) **haśle** - należy przez to rozumieć ciąg znaków literowych, cyfrowych lub znaków specjalnych znanych jedynie osobie uprawnionej do pracy w systemie informatycznym,

20) **uwierzytelnianiu** - należy przez to rozumieć działanie, którego celem jest weryfikacja deklarowanej tożsamości osoby, polegająca na podaniu identyfikatora osoby upoważnionej oraz związanego z nim hasła.

§ 4

Cel wdrożenia Polityki Bezpieczeństwa Informacji

1. W Polityce określono zasady przetwarzania danych osobowych, które są przestrzegane i stosowane w jednostce, w celu ich zabezpieczenia przed nieuprawnionym dostępem, naruszeniem integralności, dostępności lub zniszczeniem, nieuprawnionym przetwarzaniem i przechowywaniem.
2. Priorytetowym celem Polityki, jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych w zakresie ochrony danych osobowych, sposobu przetwarzania informacji zawierających dane osobowe. Informacje zawierające dane osobowe są przetwarzane i składowane zarówno w postaci tradycyjnej (dokumentacja papierowa) jak i elektronicznej.
3. Utrzymanie bezpieczeństwa przetwarzanych przez jednostkę informacji rozumiane jest jako zapewnienie ich poufności, integralności i dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka związanego z zasobem stanowiącym przedmiot niniejszej Polityki.
4. Niniejszą Politykę należy odczytywać łącznie ze stanowiącą **Załącznik nr 1** do Polityki **„Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych”,** która określa zasady użytkowania Systemu Informatycznego.
5. **Celem wprowadzenia Polityki jest:**
   1) zapewnienie zgodności działania jednostki z przyjętymi na podstawie procesu szacowania ryzyka środków środkami ochrony, wymaganiami RODO oraz wymaganiami wynikającymi z realizacji zawartych umów;
   2) zapewnienie ciągłości działania i minimalizacji ryzyka związanego z utratą poufności, integralności oraz dostępności, w systemach informatycznych oraz poza nimi oraz zapewnienie zgodności przetwarzania danych osobowych z RODO;
   3) Minimalizacja ryzyk związanych z przetwarzaniem danych osobowych;
   4) Zapewnienie osobom uprawnionym do przetwarzania informacji niezbędnej wiedzy w zakresie ochrony przetwarzanych informacji, poprzez zapewnienie szkoleń wymaganych przez RODO.

§ 5

Zakres stosowania i przegląd Polityki

1. Zasady i procedury określone w Polityce stosuje się do wszystkich użytkowników informacji oraz innych osób mogących mieć dostęp do danych i informacji lub obszarów i pomieszczeń ich przetwarzania.

2. Dla zapewnienia aktualności Polityki jednostka zobowiązuje się do wykonania planowego lub doraźnego jej przeglądu oraz aktualizacji za pomocą wyznaczonych przez Administratora osób. Przegląd Polityki dokonuje się nie rzadziej niż raz w roku.
3. Ochrona w ramach Polityki ma zastosowanie do całego systemu informacyjnego jednostki, a w szczególności do:
   1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są informacje podlegające ochronie;
   2) informacji będących własnością jednostki;
   3) informacji dot. interesantów pozyskanych w celu realizacji obowiązku prawnego ciążącego na Administratorze lub na podstawie zgody;
   4) informacji będących własnością klientów jednostki, uzyskanych na podstawie zawartych umów;
   5) wszystkich lokalizacji jednostki, czyli budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie,
   6) wszystkich pracowników w rozumieniu przepisów Kodeksu pracy, Ustawy o pracownikach samorządowych, stażystów i innych osób mających dostęp do informacji podlegających ochronie.

§ 6

Odpowiedzialność

1. Osobą odpowiedzialną za realizacje zasad bezpieczeństwa jest Wójt Gminy Raciąż lub wyznaczona przez niego osoba, która w oparciu o swój zakres obowiązków realizuje zadania w zakresie ochrony danych, a w szczególności:
   1) ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach systemów informatycznych jednostki,
   2) podejmowania stosownych działań zgodnie z niniejszą Polityką w przypadku wykrycia nieuprawnionego dostępu do baz danych lub naruszenia zabezpieczenia danych znajdujących się w systemie informatycznym,
   3) niezwłocznego informowania Administratora, inspektora ochrony danych osobowych lub inne upoważnione przez Administratora osoby o przypadkach naruszenia przepisów ustawy o ochronie danych osobowych.
2. Bezpieczeństwo informacji chronionej, która jest przetwarzana w jednostce zależy w głównej mierze od postawy osób mających do niej dostęp. Do stosowania zasad określonych przez Politykę Bezpieczeństwa są wszyscy pracownicy w rozumieniu Kodeksu pracy, Ustawy o pracownikach samorządowych, konsultanci, stażyści oraz inne osoby mające dostęp do informacji podlegających ochronie, a także do pomieszczeń, w których są takie informacje przetwarzane. Nadzór nad przestrzeganiem przez pracowników zasad Polityki sprawuje Administrator lub upoważniona przez niego osoba.

§ 7

Role i odpowiedzialność osób zaangażowanych w realizację Polityki

W celu realizacji zadań związanych z bezpieczeństwem przetwarzania informacji, w jednostce wyznaczono osoby, którym przypisano określone funkcje w ramach wdrożonych

środków ochrony oraz przypisano odpowiednio zakres odpowiedzialności:

1. **Administrator** w rozumieniu art. 4 pkt. 8 RODO realizuje zadania w zakresie:
   1) podejmowania decyzji o celach i środkach przetwarzania danych osobowych z uwzględnieniem przede wszystkim zmian w obowiązującym prawie, organizacji oraz technik zabezpieczenia danych i informacji, w tym danych osobowych;
   2) wydawania upoważnień do przetwarzania danych osobowych osobom dopuszczonym do ich przetwarzania w zakresie, odpowiadającym zakresowi ich obowiązków, wykonywanych na ich stanowisku pracy;
   3) wyznaczania i dokonuje zgłoszenia do jawnego rejestru prowadzonego przez organ nadzorczy Inspektora Ochrony Danych zgodnie z art. 37 RODO oraz art. 10 ust.4, zapewniając mu zasoby i niezależność niezbędne do realizacji zadań określonych w art. 39 RODO i publikuje jego dane na stronie Internetowej;
   4) wyznaczania Administratora Systemu Informatycznego, określając zakres jego zadań i obowiązki;
   5) podejmowania działania i decyzji w przypadku naruszenia lub podejrzenia naruszenia bezpieczeństwa danych osobowych oraz zatwierdza procedury bezpiecznego przetwarzania danych osobowych;
   6) prowadzenia rejestru osób posiadających dostęp do Systemu Informatycznego, w zakresie:
      - imienia i nazwiska oraz nadanego do systemu informatycznego identyfikatora,
      - zakresu dostępu (nazwy aplikacji, przydzielonych zasobów);
2. **Inspektor Ochrony Danych,** należy przez to rozumieć osobę wyznaczaną i zgłoszoną do jawnego rejestru prowadzonego przez organ nadzorczy przez Administratora, posiadającą niezbędne kwalifikację zawodowe oraz wiedzę fachową na temat praktyk i prawa w dziedzinie ochrony danych, odpowiedzialną za realizację zadań określonych w art. 39, w tym za:
   1) monitorowanie przestrzegania RODO oraz innych obowiązujących przepisów prawa w zakresie ochrony danych osobowych;
   2) współpracę z organem nadzorczym;
   3) pełnienie funkcji punktu kontaktowego w kwestiach związanych z przetwarzaniem danych osobowych oraz kontaktu z organem nadzorczym, o których mowa w art. 36 RODO;
   4) dokonywanie przeglądu i aktualizacji Polityki Bezpieczeństwa, pełniącej funkcję kodeksu postępowania z danymi osobowymi w jednostce;
   5) nadzór nad wdrożeniem i stosowaniem środków ochrony danych osobowych, w celu zapewnienia bezpieczeństwa danych osobowych;
   6) opiniowanie i akceptowanie procedur i regulaminów;
   7) dokonywanie okresowych kontroli przestrzegania przepisów o ochronie danych osobowych;
   8) zapewnienie realizacji zasad przetwarzania danych osobowych określonych w art. 5 RODO;
3. **Administrator Systemu Informatycznego** realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad funkcjonowaniem Systemu Informatycznego, w szczególności:
   1) zapewnienia dbałości o poprawne i efektywne działanie administrowanych systemów;

2) udostępnienia zasobów informatycznych użytkownikom we wnioskowanym zakresie;

3) instalacji i konfigurowania oprogramowania;

4) zapewnienia stosowania ochrony antywirusowej;

5) zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych;

6) nadawania użytkownikom systemu informatycznego identyfikatorów oraz zapewniania wymuszania haseł dostępu do systemu informatycznego jednostki, zgodnie z zasadami określonymi w Instrukcji zarządzania Systemami Informatycznymi;

7) nadawania praw dostępu do systemu informatycznego i oprogramowania przetwarzającego dane osobowe na podstawie pisemnego polecenia Administratora;

8) modyfikacji uprawnień, usuwania kont oraz wyrejestrowywania użytkowników zgodnie z zasadami określonymi w Instrukcji zarządzania Systemami Informatycznymi;

9) konfiguracji stacji roboczych, w tym przygotowania profili użytkowników;

10) aktualizacji zasobów Systemu Informatycznego jednostki;

11) sprawowania nadzoru nad wykonywaniem napraw zasobów Systemu Informatycznego, a w szczególności stacji roboczych, drukarek oraz urządzeń aktywnych sieci oraz ich konserwacji zgodnie z wytycznymi producenta oraz likwidacji w przypadku wycofania ich z dalszej eksploatacji;

12) informowanie Inspektora Ochrony Danych w sytuacji stwierdzenia naruszenia zabezpieczeń Systemu Informatycznego oraz współdziałanie z nim przy usuwaniu skutków naruszenia;

4. **Użytkownicy** należy przez to rozumieć osoby upoważnione do przetwarzania danych osobowych, posiadające indywidualny identyfikator i hasło umożliwiające dostęp do Systemu informatycznego oraz aplikacji przetwarzających dane osobowe. Użytkownik jest zobowiązany do:

1) przetwarzania danych osobowych wyłącznie w zakresie i celu wykonywania nałożonych obowiązków oraz w zakresie udzielonego przez Administratora upoważnienia;

2) dostęp do Systemu Informatycznego oraz aplikacji służącej do przetwarzania danych osobowych jest możliwy wyłącznie dla uwierzytelnionych użytkowników za pomocą przypisanego identyfikatora i hasła, niezbędnego do rozpoczęcia pracy w systemie;

3) zachowania tajemnicy danych osobowych pozyskanych w trakcie realizacji zadań służbowych oraz sposobu ich zabezpieczenia przez cały okres zatrudnienia, a także po ustaniu zatrudnienia;

4) przestrzegania procedur i zasad bezpiecznego przetwarzania danych osobowych obowiązujących w jednostce;

5) zapoznania się z przepisami prawa w zakresie ochrony danych osobowych oraz postanowieniami Polityki Bezpieczeństwa i Instrukcji Zarządzania Systemami Informatycznymi obowiązującymi w jednostce;

6) zabezpieczania danych i informacji przed ich udostępnieniem osobom nieupoważnionym;

7) uczestniczenia w okresowych szkoleniach dotyczących zasad ochrony danych osobowych;

8) bezwzględnego przestrzegania procedur rozpoczęcia, zawieszenia i zakończenia pracy w systemie;

9) wykonywania kopii bezpieczeństwa danych osobowych i dokumentów przechowywanych na stacjach roboczych;

10) przechowywania wymiennych, elektronicznych, nośników informacji w sposób uniemożliwiający nieautoryzowany do nich dostęp;

11) przechowywania dokumentacji papierowej przetwarzanych informacji zgodnie z zasadami określonymi w Polityce;

12) przechowywania wydruków zawierających dane i informacje w sposób uniemożliwiający dostęp do nich osób nieupoważnionych;

13) udostępniania danych i informacji zgodnie z decyzją Administratora;

14) niszczenia danych i informacji oraz wydruków zgodnie z decyzją Administratora;

15) informowania Administratora Systemu Informatycznego o każdym nieprawidłowym działaniu systemu informatycznego i eksploatowanych aplikacji;

16) informowania Inspektora Ochrony Danych o sytuacjach naruszenia bezpieczeństwa przetwarzania danych osobowych.

§ 8

Proces szacowania ryzyka.

1. W jednostce przeprowadzono proces szacowania ryzyka, który obejmuje:

   1) Analizę ryzyka na którą składa się:

      a) identyfikacja ryzyka,

      b) określenie wartości ryzyka,

      c) ocena ryzyka;

2. W ramach identyfikacji ryzyka określono:

   1) zasoby sytemu informatycznego;

   2) zagrożenia;

   3) podatności;

   4) zabezpieczenia – środki ochrony fizycznej, technicznej lub organizacyjnej zmniejszające ryzyko.

3. Analiza ryzyka bezpieczeństwa systemu informatycznego została przeprowadzona na podstawie norm:

   1) PN-ISO/IEC:17799:2007,

   2) PN-ISO/IEC:27005:2014,

   3) ustawy o prawie autorskim i prawach pokrewnych z dnia 4 lutego 1994 r.,

   4) rozporządzenia parlamentu europejskiego i rady (UE) 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

4. Ryzyko zostanie oszacowane i przeprowadzone w kontekście zachowania:

1) **Poufności** – właściwość określająca, że informacja nie jest ujawniona podmiotom do tego nieuprawnionym,

2) **Integralności** – własność określająca, że zasób systemu teleinformatycznego nie został zmodyfikowany w sposób nieuprawniony,

3) **Dostępności** – własność określająca, że zasób systemu teleinformatycznego jest możliwy do wykorzystania na żądanie, w określonym czasie, przez podmiot uprawniony do pracy w systemie teleinformatycznym.

I. Określenie zasobów jednostki

1. Wynikiem procesu identyfikacji zasobów w jednostce, jest lista zasobów podlegających ochronie:

   1) Informacje, w tym:
      - zbiory danych osobowych,
      - dokumenty;

   2) dobra materialne (infrastruktura IT),

   3) użytkownicy systemu informatycznego,

   4) dobra niematerialne (oprogramowanie),

   5) infrastrukturę jednostki, w tym:
      - obszary przetwarzania danych osobowych,
      - środki techniczne i organizacyjne służące zabezpieczeniu danych osobowych.

II. IDENTYFIKACJA ZAGROŻEŃ I OKREŚLENIE JEGO POZIOMU

1. Zagrożenie może stanowić potencjalną przyczynę wystąpienia incydentu bezpieczeństwa. Przy identyfikacji zagrożeń oparto się na normie PN-ISO/IEC 27005:2014 „Technika informatyczna - Techniki bezpieczeństwa - Zarządzanie ryzykiem w bezpieczeństwie informacji.

2. Źródłem rozpatrywanych zagrożeń są czynniki wewnętrzne jednostki lub zewnętrzne, które dzielą się na:

   1) **Zagrożenia globalne** – zagrożenia ze strony grup przestępczych, zagrożenia terrorystyczne, środowiskowe (takie jak np. wypadki, awarie zasilania), lokalizacja.

   2) **Zagrożenia lokalne** – zagrożenia ze strony personelu, osób nieupoważnionych, poziomu przeszkolenia.

III. OCENA SKUTKÓW, UTRATY POUFNOŚCI, INTEGRALNOŚCI I DOSTĘPNOŚCI DLA ZIDENTYFIKOWANYCH ZASOBÓW

Ocena skutków utraty poufności, integralności i dostępności zasobów jednostki ma postać liczbową, gdzie:

Przedział	Poziom ryzyka	Opis działania
1 – 4	Niski (N)	Poziom ryzyka akceptowalny – działania podejmowane w zależności od wymaganych nakładów
5 – 8	Średni (Ś)	Poziom ryzyka nieakceptowany – działanie może zostać usunięte w czasie, ale wymaga okresowego monitorowania
9 – 12	Wysoki (W)	Poziom ryzyka nieakceptowany – działanie może zostać przesunięte w czasie, ale wymaga stałego monitorowania
13 - 16	Krytyczny (K)	Poziom ryzyka nietolerowany – wymaga natychmiastowego działania

Wynik procesu szacowania ryzyka stanowi **Załącznik nr 2** Polityki.

§ 9

Upoważnienia do przetwarzania danych osobowych

1. Jednym z elementów składających się na prawidłowe wdrożenie zasad Polityki Bezpieczeństwa w zakresie bezpieczeństwa jest szkolenie pracowników. Szkolenia są istotnym etapem wdrożenia, gdyż stanowią gwarancję zrozumienia przez uczestników systemu informacyjnego zagrożeń i potrzeby zabezpieczenia informacji.
2. Kolejnym elementem zapewnienia bezpieczeństwa jest podpisywanie **oświadczeń o zachowaniu w poufności** informacji chronionej pozyskanej w trakcie wykonywania czynności służbowych i sposobu ich zabezpieczenia oraz o przestrzeganiu Polityki Bezpieczeństwa, stanowiący **Załącznik nr 3** do Polityki. Takie zobowiązanie jest dołączone do akt osobowych pracownika.
3. Administrator upoważnia pracowników do przetwarzania danych osobowych, w zakresie niezbędnym do realizacji zadań służbowych określonych w Regulaminie Organizacyjnym jednostki na zajmowanym stanowisku. Wzór upoważnienia stanowi **Załącznik nr 4** do Polityki.
4. Upoważnienie dotyczy również przebywania w obszarze przetwarzania danych osobowych wszystkim pracownikom obsługi, w zakresie niezbędnym do wykonywania przez nich obowiązków służbowych.
5. Dla zapewnienia ciągłości działania Systemu Informatycznego jednostki, służącego do przetwarzania danych osobowych lub usuwania skutków wystąpienia awarii, Administrator wydaje upoważnienie do wykonania wszystkich czynności związanych z naprawą i konserwacją Systemu Informatycznego lub czynności te są wykonywane pod nadzorem osób upoważnionych.
6. Osoby firm trzecich dopuszczone do czynności konserwacji lub naprawy systemu informatycznego działają na pisemne upoważnienie Administratora. Treść upoważnienia jest elementem zawartej umowy wraz ze zobowiązaniem do zachowania poufności pozyskanych informacji oraz sposobu ich zabezpieczenia i ich nieujawnianiu osobom nieuprawnionym.
7. Administrator podpisuje upoważnienia dla osób, które mają zostać dopuszczone do przetwarzania danych oraz prowadzi ewidencję osób upoważnionych do przetwarzania danych, dokonuje wpisów i aktualizacji w ewidencji. **Ewidencja upoważnień** zapewnia rozliczalność wobec poufności i integralności danych osobowych, o którym mowa w art. 5 RODO i stanowi **Załącznik nr 5** Polityki.

§ 10

Kategoria przetwarzanych danych

1. **W jednostce przetwarzane są następujące kategorię danych:**
   1) **dane zwykłe** przetwarzane na podstawie przesłanek przetwarzania określonych w art. 6 ust.1 RODO;
   2) **dane szczególnej kategorii**, przetwarzane na podstawie przesłanek wskazanych w art. 9 ust. 2 oraz art.10 RODO.
2. Przetwarzanie informacji w jednostce odbywa się:
   1) w formie analogowej (papierowej) – w sposób tradycyjny, poza systemem informatycznym;
   2) w formie elektronicznej – w ramach systemu informatycznego jednostki.
3. Przetwarzanie danych osobowych w jednostce odbywa się na podstawie przesłanek dopuszczalności przetwarzania, określonych w art. 6 ust. 1 lit. a, b, c, art.9 ust. 2 lit. b, h oraz 10 RODO. Przesłanki przetwarzania danych osobowych w poszczególnych zbiorach danych osobowych oraz kategorią przetwarzanych danych odnotowuje się w **„Rejestrze czynności przetwarzania"**, stanowiącym **Załącznik nr 6** do Polityki.
4. Przetwarzane w jednostce dane osobowe są pozyskiwane od:
   1) osób, których dane dotyczą;
   2) innych podmiotów, w tym podmiotów publicznych.

§ 11

Realizacja obowiązków i uprawnień

1. Dla zapewnienia bezpieczeństwa osobowego oraz realizacji obowiązku informacyjnego wobec kandydatów na pracowników i pracowników jednostki Administrator:
   1) w procesie rekrutacji umieszcza się w ogłoszeniu rekrutacyjnym **klauzulę informacyjną dla kandydata do pracy**, której wzór stanowi **Załącznik nr 7** do Polityki;
   2) dla zapewnienia realizacji obowiązku informacyjnego w procesie zatrudnienia stosuje **klauzulę informacyjną dla pracowników**, która jest przechowywana w teczce osobowej pracownika. Wzór klauzuli stanowi **Załącznik nr 8** do Polityki;
   3) w procesie załatwiania spraw urzędowych udostępnia się **klauzulę informacyjną dla klientów, interesantów i petentów, których dane są przetwarzane przez Administratora**. Wzór klauzuli stanowi **Załącznik nr 9** do Polityki.
2. Dostęp do systemu informatycznego jednostki nadaje Administrator Systemu Informatycznego przekazując użytkownikowi identyfikator i hasło, rejestruje użytkownika w systemie informatycznym oraz przyznaje określone uprawnienia na zasadach określonych w Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych.
3. Wszystkie osoby zatrudnione przy przetwarzaniu danych osobowych w jednostce są zobowiązane do dołożenia szczególnej staranności w celu ochrony interesów oraz realizacji obowiązku informacyjnego wobec osób, których dane dotyczą, w zakresie określonym w RODO.
4. Obowiązek informacyjny jest realizowany przez jednostkę w oparciu o następujące zasady:
   1) informacja kierowana do osób, których dane dotyczą musi zostać formułowana jasnym i prostym językiem, w sposób zwięzły i zrozumiały;

2) w przypadku zbierania danych od osoby, której dane dotyczą zapewnia się przekazanie informacji w zakresie wskazanym w art. 13 ust. 1 i 2, poprzez umieszczenie informacji na stronie internetowej i Biuletynie Informacji Publicznej (BIP) oraz w pomieszczeniach przeznaczonych do obsługi klienta/interesanta, korzystając z formularzy wzorów klauzul informacyjnych stanowiących **Załączniki 10 – 12** Polityki;

3) wszystkim osobom, których dane dotyczą realizującym prawo dostępu do informacji wynikające z art. 15 RODO, Administrator lub osoby przez niego wyznaczone są zobowiązane bez zbędnej zwłoki, a nie później niż w terminie jednego miesiąca udzielić informacji w zakresie wskazanym w art. 15 ust. 1 i 2 RODO oraz informacji o działaniach podjętych w związku z realizacją żądań przez osobę, której dane dotyczą na podstawie art. 16-22.

5. W przypadku przetwarzania danych osobowych na podstawie przesłanki dotyczącej wyrażenia zgody przez osobę, której dane dotyczą **(klauzula zgody),** należy taką zgodę uzyskać, korzystając ze wzoru stanowiącego **Załącznik nr 13** Polityki.

6. **Inspektor Ochrony Danych prowadzi zgodnie:**

1) z art. 30 RODO - **rejestr czynności przetwarzania danych,** w zakresie wskazanym w art. 30 ust.1. Rejestr ma formę papierową i elektroniczną stanowiący **Załącznik nr 6** do Polityki;

2) **Rejestr naruszeń ochrony danych**, o którym mowa w art. 33 stanowiący **Załącznik nr 14** do Polityki.

7. Dane osobowe gromadzone w zbiorach danych osobowych są udostępniane lub powierzane innym podmiotom lub osobom fizycznym zgodnie z obowiązującymi przepisami prawa. na zasadach określonych w Polityce.

§ 12

Powierzenie przetwarzania danych osobowych

1. Powierzenie przetwarzania danych osobowych może odbywać się wyłącznie na podstawie pisemnej umowy, o której mowa w art. 28 ust. 3 RODO regulującej wzajemne stosunki prawne pomiędzy administratorem, a podmiotem przetwarzającym w rozumieniu art. 4 pkt. 8 RODO.
2. Podmiot przetwarzający przetwarza dane osobowe w imieniu administratora, który korzysta wyłącznie z usług podmiotów zapewniających wystarczające gwarancje wdrożenia środków technicznych i organizacyjnych oraz realizację obowiązków określonych w art. 32-36 RODO, by przetwarzanie spełniało wymogi rozporządzenia.
3. Przetwarzanie danych może odbywać się wyłącznie w zakresie i celu przewidzianym w umowie.
4. **Wzór umowy powierzenia** stanowi **Załącznik nr 15** do Polityki.
5. **Ewidencja umów powierzenia** stanowi **Załącznik nr 16** do Polityki.

§ 13

Zagrożenia bezpieczeństwa danych osobowych

1. Incydentem jest sytuacja naruszenia bezpieczeństwa informacji i utrata ich dostępności, integralności i poufności. Incydenty powinny być wykrywane, rejestrowane i monitorowane w celu zapobieżenia ich ponownemu wystąpieniu.
2. Przykładowy katalog incydentów:

1) losowe zdarzenie wewnętrzne, np. awaria komputera, serwera, twardego dysku, błąd użytkownika, informatyka, zgubienie danych;

2) losowe zdarzenie zewnętrzne, np. klęski żywiołowe, zalanie, awaria zasilania, pożar;

3) incydent umyślny, np. wyciek informacji, ujawnienie danych nieupoważnionym osobom, świadome zniszczenie danych, działanie wirusów komputerowych, włamanie do pomieszczeń lub systemu informatycznego (wewnętrzne i zewnętrzne).

§ 14

Instrukcja postępowania w przypadku incydentów bezpieczeństwa danych osobowych

1. **Postępowanie Administratora Danych Osobowych lub właściwej osoby przez niego upoważnionej w przypadku stwierdzenia wystąpienia incydentu:**

   1) ustalenie czasu zdarzenia będącego incydentem;

   2) ustalenie zakresu incydentu;

   3) określenie przyczyn, skutków oraz szacowanych zaistniałych szkód;

   4) zabezpieczenie dowodów;

   5) ustalenie osób odpowiedzialnych za naruszenie;

   6) usunięcie skutków incydentu;

   7) ograniczenie szkód wywołanych incydentem;

   8) zainicjowanie działań dyscyplinarnych;

   9) zarekomendowanie działań zapobiegawczych w kierunku wyeliminowania podobnych zagrożeń w przyszłości;

   10) udokumentowanie prowadzonego postępowania w **Rejestrze naruszeń ochrony danych osobowych – Załącznik nr 14** do Polityki.

2. **Postępowanie w przypadku stwierdzenia wystąpienia zagrożenia do czasu przybycia Administratora Danych Osobowych lub upoważnionej przez niego osoby:**

   1) powiadomienie Administratora o wystąpieniu incydentu;

   2) powstrzymanie się od rozpoczęcia lub kontynuowania pracy, jak również od podejmowania jakichkolwiek czynności, mogących spowodować zatarcie śladów naruszenia bądź innych dowodów;

   3) zabezpieczenie elementów systemu informatycznego lub kartotek, przede wszystkim poprzez uniemożliwienie dostępu do nich osób nieupoważnionych;

   4) podjęcie, stosownie do zaistniałej sytuacji, wszelkich niezbędnych działań celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych.

3. **Postępowanie Inspektora Ochrony Danych w przypadku stwierdzenia wystąpienia zagrożenia:**

   1) ustalenie zakresu i przyczyn zagrożenia oraz jego ewentualnych skutków;

   2) w miarę możliwości przywrócenie stanu zgodnego z zasadami ochrony danych osobowych;

3) w razie konieczności zainicjowanie działań dyscyplinarnych;

4) zarekomendowanie działań zapobiegawczych w kierunku wyeliminowania podobnych zagrożeń w przyszłości;

5) udokumentowanie prowadzonego postępowania w **Rejestrze naruszeń ochrony danych osobowych** stanowiącym **Załącznik nr 14** do Polityki.

§ 15

Polityka monitorowania i reagowania na naruszenia danych osobowych

1. W przypadku naruszenia ochrony danych osobowych, Administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie **72 godzin** po stwierdzeniu naruszenia – zgłasza je PUODO, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.
2. Inspektor Ochrony Danych dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze w Rejestrze naruszeń bezpieczeństwa.
3. Zgłoszenie do PUDO musi zawierać co najmniej:
   1) opis charakteru naruszenia ochrony danych osobowych - w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
   2) imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
   3) opis możliwych konsekwencji naruszenia ochrony danych osobowych;
   4) opis środków ochrony zastosowanych w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
4. Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, można ich udzielać sukcesywnie bez zbędnej zwłoki.

§ 16

Zawiadomienie osoby o naruszeniu

1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.
2. Zawiadomienie, o którym mowa powyżej, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w pkt. 21.1 lit. b), c) i d) powyżej.
3. Zawiadomienie, o którym mowa powyżej nie jest wymagane, w następujących przypadkach:
   1) Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;

2) Administrator zastosował w następstwie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa powyżej;

3) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

§ 17

Szkolenia

1. Każdy użytkownik przed dopuszczeniem do pracy powinien zapoznać się z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej, a ponadto winien być poddany przeszkoleniu w zakresie ochrony danych osobowych.
2. **Szkolenia dzielą się na dwa rodzaje:**
   1) wstępne (przeprowadzane w momencie zatrudnienia);
   2) okresowe (związane z przypomnieniem standardów ochronnych danych osobowych i danych szczególnie wrażliwych).
3. Termin ważności szkoleń okresowych uzależnia się od ryzyka występującego w obszarze przetwarzania ochrony danych osobowych jednak nie rzadziej niż raz na 5 lat.
4. Za organizację szkolenia odpowiada Administrator i osoby przez niego upoważnione.
5. Za przeprowadzenie szkolenia odpowiedzialny jest Inspektor ochrony danych osobowych.
6. Zakres szkolenia powinien obejmować zaznajomienie użytkownika z przepisami ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz instrukcjami obowiązującymi u Administratora, a także o zobowiązaniu się do ich przestrzegania.
7. Szkolenie zostaje zakończone podpisaniem przez słuchacza oświadczenia o wzięciu udziału w szkoleniu i jego zrozumieniu oraz zobowiązaniu się do przestrzegania przedstawionych w trakcie szkolenia zasad ochrony danych osobowych.
8. Dokument ten jest przechowywany w aktach osobowych użytkowników i stanowi podstawę do podejmowania działań w celu nadania im uprawnień do przetwarzania danych osobowych w tym korzystania z systemu informatycznego przetwarzającego dane osobowe.

§ 18

Odpowiedzialność karna

1. Pracownik, który przetwarza dane osobowe:
   1) do których przetwarzania nie jest upoważniony;
   2) których przetwarzanie jest zabronione;
   3) niezgodne z celem stworzenia zbioru danych;
   4) udostępnia lub umożliwia dostęp do danych osobowych osobom nieupoważnionym;
   5) nie dopełnia obowiązku poinformowania osoby, której dane dotyczą, o przysługujących jej prawach;
   6) uniemożliwia osobie, której dane dotyczą, korzystanie z przysługujących jej praw - podlega odpowiedzialności dyscyplinarnej.
2. Wobec osoby, która w przypadku naruszenia zasad bezpieczeństwa lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonych w niniejszej Polityce, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna

się postępowanie dyscyplinarne.

§ 19

Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

1. Mając świadomość, że żadne zabezpieczenie techniczne nie gwarantuje 100%-towej szczelności systemu, konieczne jest aby każdy użytkownik systemu, pełen świadomej odpowiedzialności, postępował zgodnie z przyjętymi zasadami i minimalizował zagrożenia wynikające z błędów ludzkich.
2. W celu zapewnienia bezpieczeństwa danych osobowych wyznaczono w jednostce obszar przetwarzania danych osobowych obejmujący wszystkie pomieszczenia dydaktyczne i administracyjne jednostki.
3. W celu należytego zabezpieczenia przetwarzanych danych osobowych, jednostka wprowadziła szereg rozwiązań, natury organizacyjnej i technicznej, w szczególności:

I. Środki organizacyjne

a) została opracowana i wdrożona Polityka bezpieczeństwa;

b) została opracowana i wdrożona Instrukcja zarządzania systemem informatycznym;

c) wprowadzono procedurę udostępniania danych osobowych na podstawie złożonego przez zainteresowane podmioty wniosku. Wzór **wniosku o udostępnienie danych** stanowi **Załącznik nr 17** do Polityki.;

d) jednostka prowadzi **ewidencję udostępniania danych osobowych** na podstawie złożonych wniosków w określonym celu lub na podstawie prawnej przesłanki, która stanowi **Załącznik nr 18** do Polityki;

e) do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające ważne upoważnienia nadane przez Administratora;

f) prowadzona jest ewidencja osób upoważnionych do przetwarzania danych;

g) osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych;

h) przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego;

i) osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy;

j) monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane;

k) przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych;

l) przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych;

m) stosuje się pisemne umowy powierzenia przetwarzania danych dla współpracy z podwykonawcami przetwarzającymi dane osobowe;

n) obowiązuje polityka czystego biurka i ekranu.

II. Środki ochrony fizycznej danych

a) dane osobowe przechowywane są w pomieszczeniach, do których dostęp mają jedynie upoważnione osoby;

b) dokumenty zawierające dane osobowe w formie papierowej przechowywane są w zamykanych szafach;

c) pomieszczenia jednostki zabezpieczone zamkami.

d) kopie zapasowe zbiorów danych osobowych przechowywane są w zamykanych szafach;

e) pomieszczenia, w których przetwarzane są zbiory danych osobowych zabezpieczone są przed skutkami pożaru za pomocą wolnostojącej gaśnicy;

f) dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów;

III. Środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej

a) lokalizacja urządzeń komputerowych (komputerów typu PC, drukarek) uniemożliwia do nich dostęp osobom niepowołanym;

b) programy zainstalowane na komputerach obsługujących przetwarzanie danych osobowych są użytkowane z zachowaniem praw autorskich i posiadają licencje;

c) dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła, zgodnie z polityką haseł wskazaną w Instrukcji zarządzania systemem informatycznym;

d) stosuje się środki kryptograficznej ochrony danych dla danych osobowych na komputerach przenośnych i nośnikach;

e) stosuje się środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji (poczta e-mail);

f) zastosowano system antywirusowy w celu ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie.

IV. Środki ochrony w ramach narzędzi programowych i baz danych

a) zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych;

b) zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego;

c) dostęp do poszczególnych programów przetwarzających dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła, zgodnie z polityką haseł wskazaną w Instrukcji zarządzania systemem informatycznym;

d) zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego;

e) zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.

§ 20

Postanowienia końcowe

1. Polityka bezpieczeństwa jest dokumentem obowiązującym w jednostce w zakresie wdrażania, przestrzegania i weryfikacji zasad ochrony danych osobowych.
2. Każda osoba dopuszczona do przetwarzania danych osobowych w jednostce ma obowiązek zapoznania się z niniejszą Polityką bezpieczeństwa.
3. Naruszenie zasad wynikających z Polityki bezpieczeństwa może stanowić podstawę wszczęcia postępowania dyscyplinarnego przeciwko sprawcy naruszenia.
4. Wszczęcie lub przeprowadzenie postępowania dyscyplinarnego przeciwko osobie naruszającej zasady wynikające z Polityki bezpieczeństwa nie wyklucza możliwości wszczęcia postępowania karnego oraz dochodzenia roszczeń z powództwa cywilnego.
5. Polityka bezpieczeństwa wraz z załącznikami wchodzi w życie z dniem jej podpisania przez Administratora.
6. W przedmiocie spraw nieuregulowanych Polityką bezpieczeństwa, zastosowanie znajdują właściwe przepisy prawa, w szczególności RODO.

Opracował:

mgr Marek Rochna – Inspektor Ochrony Danych

Zatwierdził:

.....

(data oraz podpis Administratora)

Wykaz załączników do polityki:

Załącznik nr 1 – Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych;

Załącznik nr 2 – Proces szacowanie ryzyka;

Załącznik nr 3 – Oświadczenie o zachowaniu w poufności;

Załącznik nr 4 – Wzór upoważnienia do przetwarzania danych osobowych;

Załącznik nr 5 – Ewidencja osób upoważnionych do przetwarzania danych;

Załącznik nr 6 – Rejestrze czynności przetwarzania;

Załącznik nr 7 – Klauzula informacyjna dla kandydata do pracy;

Załącznik nr 8 – Klauzula informacyjna dla pracowników;

Załącznik nr 9 – Klauzula informacyjna dla klientów, interesantów i petentów;

Załącznik nr 10 – Klauzula informacyjna na stronę internetową;

Załącznik nr 11 – Przykład obowiązku informacyjnego;

Załącznik nr 12 – Klauzula informacyjna dla osób korzystających z ZFŚS;

Załącznik nr 13 – Klauzula zgody;

Załącznik nr 14 – Rejestr naruszeń ochrony danych;

Załącznik nr 15 –Wzór umowy powierzenia przetwarzania;

Załącznik nr 16 – Ewidencja umów powierzenia;

Załącznik nr 17 – Wniosek o udostępnienie danych osobowych;

Załącznik nr 18 – Ewidencja udostępnienia danych osobowych.