ZESPÓŁ SZKÓŁ NR 2
Z ODDZIAŁAMI INTEGRACYJNYMI
W PUŁTUSKU
ul. POLNA 7, 06-100 PUŁTUSK
tel./fax (0-23) 692 02 01
REGON 130949410, NIP 568-152-25-57

ZARZĄDZENIE 37/2020

Dyrektora Zespołu Szkół nr 2 z Oddziałami Integracyjnymi w Pułtusku

z dnia 31 grudnia 2020 r.

w sprawie wprowadzenia: „Polityki bezpieczeństwa informacji w Zespole Szkół nr 2 z Oddziałami Integracyjnym w Pułtusku"

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) zarządzam, co następuje:

§ 1

Uchyla się treść „Polityki bezpieczeństwa informacji" wprowadzonej Zarządzeniem nr 6a/2018 przez Dyrektora Zespołu Szkół nr 2 z Oddziałami Integracyjnymi w Pułtusku z dnia 8 maja 2018 r.

§ 2

Przyjmuje się „Politykę bezpieczeństwa informacji w Zespole Szkół nr 2 z Oddziałami Integracyjnymi w Pułtusku" stanowiącą **Załącznik** do niniejszego Zarządzenia.

§ 3

1. Z zarządzeniem zobowiązani są zapoznać się wszyscy pracownicy oraz osoby, które przetwarzają na zlecenie Zespołu dane osobowe.

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

§ 4

Wykonanie zarządzenia powierza się sekretarzowi zespołu i inspektorowi ochrony danych.

§ 5

Zarządzenie wchodzi w życie z dniem z dniem publikacji.

DYREKTOR
ZESPOŁU SZKÓŁ NR 2
Z ODDZIAŁAMI INTEGRACYJNYMI
W PUŁTUSKU
mgr Krystyna Laskowska

ZESPÓŁ SZKÓŁ NR 2
Z ODDZIAŁAMI INTEGRACYJNYMI
w PUŁTUSKU
ul. POLNA 7, 06-102 PUŁTUSK
tel./fax (0-23) 692 02 01
REGON 130[illegible]410, NIP 568-152-25-57

Załącznik
do Zarządzenia 37./2020
Dyrektora Zespołu Szkół nr 2 z Oddziałami Integracyjnymi w Pułtusku
z dnia 31 grudnia 2020 r.
w sprawie wprowadzenia „Polityki bezpieczeństwa informacji
w Zespole Szkół nr 2 z Oddziałami Integracyjnymi w Pułtusku"

„POLITYKA BEZPIECZEŃSTWA INFORMACJI W ZESPOLE SZKÓŁ NR 2 Z ODDZIAŁAMI INTEGRACYJNYMI W PUŁTUSKU"

§ 1

Wstęp

1. Niniejszy dokument reguluje sprawy ochrony danych osobowych przetwarzanych w **Zespole Szkół nr 2 z Oddziałami Integracyjnymi w Pułtusku,** zwanym 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. Dyrektor Zespołu Szkół, stojąc na stanowisku, że informacja jest newralgicznym zasobem każdej organizacji, wdraża w Zespole Szkół nr 2 z Oddziałami Integracyjnymi w Pułtusku „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 Zespół Szkół nr 2 z Oddziałami Integracyjnymi w Pułtusku (06-100) ul. Polna 7.

3) **Administratorze** - należy przez to rozumieć Zespół Szkół nr 2 z Oddziałami Integracyjnymi w Pułtusku reprezentowany przez Dyrektora Zespołu Szkół, który decyduje o celach 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 zespołu szkół 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 Dyrektor Zespołu 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:
   a) zasoby sytemu informatycznego;
   b) zagrożenia;
   c) podatności;
   a) 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 2016r. 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 oszacowanei 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	[redacted]	Poziom ryzyka akceptowalny – działania podejmowane w zależności od wymaganych nakładów
5 – 8		Poziom ryzyka nieakceptowany – działanie może zostać usunięte w czasie, ale wymaga okresowego monitorowania
9 – 12		Poziom ryzyka nieakceptowany – działanie może zostać przesunięte w czasie, ale wymaga stałego monitorowania
13 - 16		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 rekrutacji dzieci oraz ich pobytu w placówce oświatowej wykorzystuje się klauzulę informacyjną dla rodziców/prawnych opiekunów, których dane i dane ich dzieci są przetwarzane przez placówkę oświatową. 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, których 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 bezpieczeństwa – Załącznik nr 14** do Polityki.

2. **Postępowanie Upoważnionego 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 bezpieczeństwa** 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 ustala 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:

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.

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;

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.

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 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

mgr Marek Rochna
Audytor Normy ISO/IEC 27001
tel. 602 523 360

Zatwierdził:

DYREKTOR
ZESPOŁU SZKÓŁ NR 2
Z ODDZIAŁAMI INTEGRACYJNYMI
W PUŁTUSKU
mgr Krystyna Sułkowska

.....

(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 – Klauzule informacyjne dla rodziców/prawnych opieńków, których dane i dane ich dzieci są przetwarzane przez placówkę oświatową;

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.

ZESPÓŁ SZKÓŁ NR 2
Z ODDZIAŁAMI INTEGRACYJNYMI
w PUŁTUSKU
ul. POLNA 7, 06-102 PUŁTUSK
tel./fax (0-23) 692 02 01
REGON 130949410, NIP 568-152-25-57

Załącznik nr 1
„Polityki bezpieczeństwa informacji
w Zespole Szkół nr 2 z Oddziałami Integracyjnymi w Pułtusku"
z dnia 31 grudnia 2020 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W ZESPOLE SZKÓŁ NR 2 Z ODDZIAŁAMI INTEGRACYJNYMI W PUŁTUSKU

I. Wprowadzenie

1. Niniejszy dokument, zwany dalej **Instrukcją** stanowi załącznik do dokumentu Polityki Bezpieczeństwa Informacji, stosowanej w Zespole Szkół nr 2 z Oddziałami Integracyjnymi w Pułtusku, zwana dalej **„Administratorem"**.
2. Instrukcja stanowi zbiór obowiązków, zasad i procedur regulujących sposób przetwarzania i ochrony danych osobowych przez Administratora przy użyciu systemu informatycznego.
3. Instrukcja określa zasady bezpieczeństwa przetwarzania danych osobowych, które powinny być przestrzegane i stosowane w jednostce, przez wszystkie osoby zaangażowane w przetwarzanie danych osobowych przy użyciu systemu informatycznego.
4. Instrukcja reguluje zasady organizacji pracy przy zbiorach danych osobowych przetwarzanych w systemie informatycznym.
5. Instrukcja spełnia także funkcję informacyjną i edukacyjną, poprzez zaprezentowanie obowiązków i odpowiedzialności osób związanych z przetwarzaniem danych osobowych przy użyciu systemu informatycznego.

II. Zasady ogólne

1. Instrukcja zarządzania systemem informatycznym stanowi integralną część Polityki Bezpieczeństwa i jest dokumentem obowiązującym w Zespole Szkół nr 2 z Oddziałami Integracyjnymi w Pułtusku w zakresie wdrażania, przestrzegania weryfikacji zasad ochrony danych osobowych.
2. Instrukcja jest dokumentem obowiązującym wszystkie osoby uczestniczące w przetwarzaniu danych osobowych przy użyciu systemu informatycznego.
3. Każda osoba dopuszczona do przetwarzania danych osobowych u Administratora ma obowiązek zapoznania się z niniejszą Instrukcją przed przystąpieniem do przetwarzania danych.
4. Instrukcja ustanawia procedury obowiązujące dla:
   a) zbierania i przetwarzania danych osobowych przy użyciu systemu informatycznego;
   b) udostępnienia danych osobowych przetwarzanych przy użyciu systemu informatycznego upoważnionym podmiotom zewnętrznym;
   c) zasady uwierzytelnienia dostępu do systemu informatycznego służącego do przetwarzania danych osobowych;
   d) zapewnienia bezpieczeństwa systemu informatycznego, wykorzystywanego przy przetwarzaniu danych osobowych;
   e) zapewnienia bezpieczeństwa zbiorów danych osobowych przetwarzanych przy użyciu systemu informatycznego;
   f) korzystania ze stacji roboczej, sieci Internet i poczty e-mail przy użyciu systemu informatycznego;
   g) zapewnienia bezpieczeństwa i korzystania z aplikacji stosowanych przy przetwarzaniu danych przy użyciu systemu informatycznego;
   h) postępowania w przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego.

5. Administrator dochowuje należytej staranności przy zapewnianiu ochrony danych osobowych przetwarzanych w toku jej działalności w ramach systemu informatycznego, którym się posługuje, w szczególności poprzez zapewnienie i wdrożenie:
   a) procedur przetwarzania danych w sposób zgodny z prawem;
   i) procedur korzystania z sieci Internet, poczty e-mail oraz jednostki roboczej, używanych przy przetwarzaniu danych z zastosowaniem systemu informatycznego;
   j) procedur powierzania danych osobowych przetwarzanych przy użyciu systemu informatycznego upoważnionym podmiotom wewnętrznym i zewnętrznym;
   k) procedur tworzenia kopii zapasowych zbioru przetwarzanych danych osobowych;
   l) procedur kontroli oprogramowania i systemu informatycznego używanych przy przetwarzaniu danych osobowych przez Administratora;
   m) zbierania danych w celach oznaczonych i zgodnych z prawem;
   n) zbierania danych merytorycznie poprawnych i adekwatnych w stosunku do celów ich zbierania;
   o) przechowywania danych w sposób zgodny z prawem, w szczególności uniemożliwiając ich nieuprawnione udostępnienie i przechowywanie przez dłuższy czas, niż jest to konieczne dla osiągnięcia celów przetwarzania danych.
6. Przestrzeganie procedur ustanowionych w Instrukcji jest konieczne dla realizacji zasad zgodnego z prawem przetwarzania danych osobowych.

III. Definicje

Ilekroć w niniejszej Instrukcji jest mowa o:

a) **identyfikatorze** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
b) **integralności danych** – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
c) **haśle** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
d) **osobie upoważnionej** – rozumie się przez to użytkownika systemu informatycznego uprawnionego do przetwarzania danych osobowych;
e) **poufności danych** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
f) **raporcie** – rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;
g) **rozliczalności** – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
h) **systemie informatycznym** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
i) **uwierzytelnianiu** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
j) **użytkownikach** – należy przez to rozumieć osoby przetwarzające dane osobowe w Systemie Informatycznym, 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;

k) **zabezpieczeniu danych w systemie informatycznym** – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.

IV. Poziom bezpieczeństwa systemu informatycznego

1. Poziom bezpieczeństwa systemu informatycznego przetwarzających dane osobowe określono jako wysoki. Wszystkie działania, procedury wdrażane i cele ochrony danych osobowych w jednostce muszą być zgodne z wytycznymi zawartymi w niniejszym rozdziale Instrukcji.
2. Obszar przetwarzania danych osobowych określony w Polityce zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.
3. Przebywanie osób nieuprawnionych w obszarze przetwarzania danych osobowych jest dopuszczalne za zgodą Administratora lub w obecności osoby upoważnionej do przetwarzania danych osobowych.
4. W systemie informatycznym służącym do przetwarzania danych osobowych stosuje się mechanizmy kontroli dostępu do tych danych.
5. Jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas zapewnia się, aby:
   a) w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator;
   b) dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.
6. System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed:
   a) działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego;
   b) utratą danych spowodowana awarią zasilania lub zakłóceniami w sieci zasilającej.
7. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.
8. W przypadku gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni. Hasło składa się co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.
9. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych.
10. Kopie zapasowe:
    a) przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem;
    b) usuwa się niezwłocznie po ustaniu ich użyteczności.

11. Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych osobowych określonym w Polityce, w tym stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.
12. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
    a) likwidacji – pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
    b) przekazania podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
    c) naprawy – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez Administratora.
13. System informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.
14. Zabezpieczenia logiczne, o których mowa w pkt 13 obejmują w szczególności:
    a) kontrolę przepływu informacji pomiędzy systemem informatycznym administratora a siecią publiczną;
    b) kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora danych.
15. Administrator stosuje środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej.
16. Administrator monitoruje wdrożone zabezpieczenia systemu informatycznego, stosując na poziomie wysokim środki bezpieczeństwa.
17. Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych szczegółowo określone zostały w Polityce.

V. Procedura nadawania upoważnień do przetwarzania danych osobowych

1. Upoważnienia do przetwarzania danych osobowych są nadawane w związku z wykonywaniem przez osobę upoważnioną obowiązków lub zadań związanych z przetwarzaniem danych osobowych.
2. Upoważnienia nadaje i odwołuje Administrator.
3. Upoważnienie i jego odwołanie sporządza się na piśmie, w dwóch jednobrzmiących egzemplarzach – jeden jest przeznaczony dla osoby, której nadano lub odebrano upoważnienie, drugi – dla administratora.
4. Wzór upoważnienia do przetwarzania danych osobowych stanowi **Załącznik nr 4** do Polityki.
5. Upoważnienia nie sporządza się dla Administratora.
6. Administrator prowadzi ewidencję upoważnień, która stanowi **Załącznik nr 5** do Polityki.

VI. Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

1. Administrator lub osoba przez niego upoważniona odpowiada za nadzór nad dostępem pracowników do systemu informatycznego, w szczególności za:
   a) nadawanie/zmianę/blokowanie identyfikatorów i haseł osobom upoważnionym;
   b) tworzenie kopii zapasowych;
   c) monitorowanie funkcjonowania zabezpieczeń wdrożonych w celu ochrony danych osobowych;
   d) zabezpieczenia haseł administratorów systemu informatycznego;
   e) właściwą konfigurację systemu informatycznego, zapewniającą jego bezpieczeństwo i zapewnienie niezakłóconego działania systemów.
2. Środkiem uwierzytelnienia dostępu do Systemu Informatycznego służącego do przetwarzania danych osobowych to identyfikator (email) i hasło dostępu.
3. W celu korzystania z systemu informatycznego służącego do przetwarzania danych osobowych wymaga się uwierzytelnienia przy użyciu indywidualnego identyfikatora i hasła użytkownika systemu. Celem procedury jest zapewnienie, że do systemu informatycznego przetwarzających dane osobowe mają dostęp jedynie osoby do tego upoważnione.
4. Identyfikatorami i hasłami użytkowników, korzystających z systemu informatycznego zarządza Administrator Systemu Informatycznego.
5. Uwierzytelnianie jest każdorazowo konieczne:
   a) przy uruchamianiu sprzętu komputerowego;
   b) przy uruchamianiu programów przetwarzających dane osobowe.
6. Zasady tworzenia hasła:
   a) hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów;
   b) hasło składa się z dużych i małych liter oraz z cyfr lub znaków specjalnych i liczy co najmniej 8 znaków;
   c) zmiana hasła do systemu następuje nie rzadziej, niż co 30 dni oraz niezwłocznie w przypadku podejrzenia, że hasło mogło zostać ujawnione;
   d) użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności, hasło nie może być wyświetlane w sposób jawny na ekranie;
   e) w przypadku złamania poufności hasła, użytkownik zobowiązany jest niezwłocznie je zmienić i poinformować o tym fakcie Administratora;
   f) System Informatyczny może wymuszać dokonanie zmiany hasła. Jeśli System Informatyczny nie ma takiej funkcji Użytkownik jest zobowiązany do samodzielnej zmiany hasła, przy zachowaniu wskazanych wytycznych.
7. Nadany użytkownikowi identyfikator nie może być zmieniany, a po wyrejestrowaniu użytkownika z Systemu Informatycznego, nie powinien być przydzielany innej osobie.
8. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych osobowych, należy niezwłocznie zablokować w Systemie Informatycznym oraz unieważnić przyznane mu hasła.
9. Administrator Systemu Informatycznego przekazuje w zabezpieczonej kopercie hasła administracyjne do serwerów i urządzeń sieci informatycznej. Administrator przechowuje przekazane hasła w sposób uniemożliwiający dostęp osobom niepowołanym.

VII. Obowiązki osób upoważnionych do przetwarzania danych w systemie informatycznym

1. Każda osoba upoważniona do przetwarzania danych jest zobowiązana do:
   a) zachowania w tajemnicy danych osobowych, do których ma dostęp poprzez systemy informatyczne w związku z wykonywaniem zadań służbowych lub obowiązków pracowniczych;
   b) zachowania w tajemnicy sposobów zabezpieczenia danych osobowych o ile nie są one jawne;
   c) korzystania ze sprzętu komputerowego oraz oprogramowania wyłącznie w związku z wykonywaniem obowiązków pracowniczych;
   d) wykorzystywania jedynie legalnego oprogramowania pochodzącego od Administratora;
   e) należytej dbałości o sprzęt i oprogramowanie zgodnie z dokumentacją ochrony danych osobowych;
   f) przestrzegania procedur korzystania z Internetu, poczty elektronicznej oraz innych wytycznych wskazywanych przez Administratora;
   g) korzystania z komputerów przenośnych zgodnie z dokumentacją ochrony danych osobowych.
2. Postępowanie sprzeczne z powyższymi zobowiązaniami, może być uznane przez Pracodawcę za ciężkie naruszenie obowiązków pracowniczych w rozumieniu art. 52 § 1 pkt 1 Kodeksu Pracy lub za naruszenie przepisów karnych wynikających z przepisów prawa.

VIII. Procedura korzystania z Internetu

1. Użytkownicy systemu informatycznego mają prawo korzystać z Internetu przede wszystkim w celu wykonywania obowiązków służbowych.
2. Przy korzystaniu z Internetu, użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i praw autorskich.
3. Użytkownicy systemu informatycznego mają prawo korzystać z Internetu dla celów prywatnych wyłącznie okazjonalnie i nie może to wpływać na jakość i ilość świadczonej przez nich pracy oraz na prawidłowe i rzetelne wykonywanie obowiązków służbowych, a także na wydajność systemu informatycznego Administratora.
4. Zabrania się zgrywania na dysk twardy komputera oraz uruchamia jakichkolwiek programów nielegalnych oraz plików pobranych z niepewnego źródła.
5. Osoba korzystająca ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie ściągnięte z Internetu i przez niego zainstalowane.
6. Zabrania się w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.
7. Należy korzystać wyłącznie z przeglądarek posiadających odpowiednie opcje zabezpieczeń.
8. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka, protokół https).
9. W zakresie dozwolonym przepisami prawa, Administrator zastrzega sobie prawo kontrolowania sposobu korzystania przez użytkowników systemu informatycznego

z Internetu pod kątem wyżej opisanych zasad. Administrator może również blokować dostęp do niektórych treści dostępnych przez Internet.

IX. Procedura korzystania z poczty elektronicznej

1. Przesyłanie danych osobowych poza jednostkę może odbywać się tylko przez osoby upoważnione, za zgodą Administratora.
2. W przypadku przesyłania danych osobowych należy wykorzystywać mechanizmy kryptograficzne (pakowanie i zabezpieczanie hasłem wysyłanych plików lub podpis elektroniczny).
3. Należy zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu;
4. Przy rozsyłaniu korespondencji wielu adresatom należy czynić to w taki sposób, że odbiorcy nie widzą wzajemnie swoich adresów.
5. Zaleca się, aby użytkownik systemu informatycznego podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.
6. Nie należy otwierać załączników (plików) w korespondencji elektronicznej nadesłanej przez nieznanego nadawcę.
7. Należy okresowo kasować niepotrzebne wiadomości pocztowe.
8. Użytkownik jest świadomy, że wszelkie wiadomości o charakterze prywatnym utworzone lub odebrane za pośrednictwem służbowej poczty elektronicznej przetwarzane są wyłącznie na jego własną odpowiedzialność.
9. Użytkownik wyraża zgodę na prowadzenie kontroli tych wiadomości przez Administratora lub osobę przez niego upoważnioną. Administrator nie będzie w tej sytuacji odpowiadać za przypadkowe naruszenie dóbr osobistych użytkownika systemu informatycznego w postaci naruszenia tajemnicy korespondencji.

X. Procedura korzystania z komputerów przenośnych

1. Komputery przenośne można wynosić z obszaru przetwarzania danych osobowych określonego w Polityce tylko w szczególnych przypadkach, po poinformowaniu i uzyskaniu zgody Administratora.
2. Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych osobowych.
3. Dane osobowe na komputerach przenośnych zabezpieczone są dodatkowo środkami ochrony kryptograficznej.
4. Osoba użytkująca komputer przenośny nie może logować się do hotspotów i innych niezabezpieczonych punktów dostępu do sieci Internet.
5. W przypadku zaginięcia komputera przenośnego lub nośników danych, na których były zgromadzone dane osobowe, użytkownik posługujący się komputerem niezwłocznie powiadamia Administratora lub upoważnioną przez niego osobę, a w przypadku kradzieży dodatkowo zawiadamia jednostkę policji.
6. W powyższej sytuacji Administrator lub upoważniona przez niego osoba podejmuje niezbędne kroki do wyjaśnienia okoliczności zdarzenia, sporządza protokół z zajęcia, który powinna podpisać także osoba, której skradziono lub, której zaginął sprzęt.
7. W przypadku kradzieży komputera razem z nośnikiem danych Administrator lub upoważniona przez niego osoba podejmuje działania zmierzające do odzyskania utraconych danych oraz nadzoruje proces przebiegu wyjaśnienia sprawy.

XI. Polityka czystego biurka i ekranu

1. Polityka czystego biurka ma na celu zabezpieczenie dokumentów podczas pracy z dokumentami w wersji papierowej.
2. Dane osobowe w formie papierowej mogą znajdować się na biurkach tylko na czas niezbędny na dokonanie czynności służbowych a następnie muszą być chowane do odpowiednio zabezpieczonych szaf.
3. Na biurku nie powinny znajdować się dokumenty zawierające dane osobowe innych osób niż w danej chwili obsługiwanej.
4. Odchodząc od biurka nie wolno pozostawiać dokumentów bez nadzoru.
5. Po zakończeniu pracy dokumenty należy zabezpieczyć w zamkniętej szafie.
6. Nie należy magazynować zbędnych wydruków.
7. Zbędne wydruki i inne dokumenty konwencjonalne (na nośnikach papierowych), zawierające dane osobowe, powinny być zniszczone w niszczarce dokumentów lub podarte na drobne fragmenty w sposób uniemożliwiający ich odczytanie.
8. Za prawidłowe zniszczenie zbędnych dokumentów papierowych, zawierających dane osobowe, odpowiada osoba, która przetwarzała dane.
9. Nadzór nad prawidłowym niszczeniem dokumentów zawierających dane osobowe sprawuje Administrator.
10. Ustawienia monitorów muszą zapewniać ograniczenie możliwości podglądania wyświetlanych danych osobom trzecim.
11. W przypadku konieczności czasowego opuszczenia stanowiska pracy, przyłączonego do sieci informatycznej lub służącego przetwarzaniu danych, wiążącego się ze utratą z pola widzenia swojego stanowiska, użytkownik powinien:
    a) wylogować się z programu lub sieci informatycznej, lub zablokować stację roboczą odpowiednią kombinacją klawiszy, przy czym odblokowanie może nastąpić dopiero po podaniu hasła, lub
    b) aktywować wygaszacz ekranu w ten sposób, aby powrót do normalnej pracy był możliwy dopiero po podaniu hasła.

XII. Procedura dostępu do danych osobowych podmiotów zewnętrznych

1. Administrator prowadzi ewidencję podmiotów zewnętrznych, którym udostępnia dane osobowe oraz podmiotów, którym powierzono przetwarzanie danych osobowych w formie usługi zewnętrznej.
2. Administrator powierza dane osobowe do przetwarzania w formie usługi zewnętrznej podmiotom zewnętrznym w oparciu o pisemną umowę powierzenia przetwarzania danych.
3. Administrator udostępnia dane na pisemny i umotywowany wniosek, chyba że szczególny przepis prawa stanowi inaczej. Wniosek powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać ich zakres i przeznaczenie.
4. Szczegółowe informacje o formie i obowiązkach związanych z udostępnianiem i powierzaniem danych osobowych zawarte są w Polityce.

XIII. Odpowiedzialność użytkowników za zabezpieczenie systemów i stosowanie środków ochrony informatycznej

1. Każdy Użytkownik zobowiązany jest do ochrony danych dostępowych oraz haseł dostępu do Systemu Informatycznego.
2. Przez dane dostępowe rozumie się:
   a) hasła dostępu;
   b) klucze sprzętowe i softwareowe (pliki umożliwiające dostęp – np. certyfikaty do VPN) – jeśli mają zastosowanie;
   c) inne mechanizmy umożliwiające dostęp do systemów IT.
3. Metody ochrony danych dostępowych obejmują:
   a) nieujawnianie haseł dostępu innym osobom, hasło jest poufne;
   b) nieprzechowywanie danych w miejscach publicznych (np. zapisywanie haseł dostępowych w łatwo dostępnych miejscach).
4. Zabrania się pracy w Systemie Informatycznych z użyciem danych dostępowych innych użytkowników.

XIV. Procedura rozpoczęcia, zawieszenia i zakończenia pracy

1. Przed rozpoczęciem przetwarzania danych osobowych Upoważniony powinien sprawdzić, czy nie ma oznak fizycznego naruszenia zabezpieczeń. W przypadku wystąpienia jakichkolwiek nieprawidłowości, należy powiadomić Administratora.
2. Przystępując do pracy w Systemie Informatycznym służącym do przetwarzania danych osobowych, Użytkownik jest zobowiązany wprowadzić swój identyfikator oraz hasło dostępu. Zabrania się wykonywania jakichkolwiek operacji w systemie informatycznym służącym do przetwarzania danych osobowych z wykorzystaniem identyfikatora i hasła dostępu innego Użytkownika.
3. W przypadku czasowego opuszczenia stanowiska pracy, Użytkownik musi wylogować się z Systemu Informatycznego służącego do przetwarzania danych osobowych lub zastosować wygaszacz ekranu chroniony hasłem.
4. Zakończenie pracy w Systemie Informatycznym służącym do przetwarzania danych osobowych następują poprzez wylogowanie się z tego systemu.
5. Prowadząc pracę z użyciem Systemu Informatycznego, służącego do przetwarzania danych osobowych, Upoważniony jest zobowiązany dochowywać należytej staranności w celu uniemożliwienia nieuprawnionym osobom trzecim wglądu w informacje obejmujące dane osobowe przetwarzane w ramach systemu, które wyświetlane są na ekranie komputera.

XV. Procedury tworzenia i przechowywania kopii zapasowych

1. Za sporządzanie kopii zapasowych zbiorów danych odpowiedzialny jest upoważniony użytkownik Systemu Informatycznego służącego do przetwarzania danych osobowych.
2. Kopie zapasowe tworzone są:
   a) raz na miesiąc – w przypadku danych płacowo-kadrowych;
   b) raz na rok – w przypadku zbiorów dot. organizacji roku szkolnego (dziennik elektroniczny, sekretariat).
3. Kopie zapasowe powinny być kontrolowane przez sporządzającego kopie oraz Administratora, w szczególności pod kątem prawidłowości ich wykonania poprzez częściowe lub całkowite odtworzenie na wydzielonym sprzęcie komputerowym.

4. Nośniki informatyczne zawierające dane osobowe lub kopie systemu informatycznego służącego do przetwarzania danych osobowych są przechowywane w sposób uniemożliwiający ich utratę, uszkodzenie lub dostęp osób nieuprawnionych.
5. W przypadku likwidacji nośników informatycznych zawierających dane osobowe lub kopie zapasowe systemu informatycznego służącego do przetwarzania danych osobowych należy przed ich likwidacją usunąć dane osobowe lub uszkodzić je w sposób uniemożliwiający odczyt danych osobowych.

XVI. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe

1. Procedura określa sposób postępowania z nośnikami danych osobowych takimi jak: twarde dyski, płyty CD/DVD, pendrive, na których znajdują się dane osobowe, celem zabezpieczenia ich przez niszczeniem, kradzieżą, dostępem osób nieupoważnionych.
2. Nie należy przechowywać zbędnych nośników informacji zawierających dane osobowe oraz kopii zapasowych, a także wydruków i innych dokumentów zawierających dane osobowe.
3. Po upływie okresu ich użyteczności lub przechowywania, dane osobowe powinny zostać skasowane lub zniszczone tak, aby nie było możliwe ich odczytanie.
4. Zabrania się wynoszenia poza obszar przetwarzania danych określony w Polityce wymiennych nośników informacji, a w szczególności twardych dysków z zapisanymi danymi osobowymi bez zgody Administratora.
5. Elektroniczne nośniki informacji zawierające dane osobowe oraz kopie zapasowe, a także wydruki i inne dokumenty zawierające dane osobowe przechowywane są w zamykanych szafach w pomieszczeniach stanowiących obszar przetwarzania danych osobowych, w sposób zabezpieczający je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem i zniszczeniem.
6. W przypadku uszkodzenia lub zużycia nośnika informacji zwierających dane osobowe należy go fizycznie zniszczyć tak, aby nie było możliwe odczytanie danych osobowych.
7. W sytuacji przekazywania nośników z danymi osobowymi poza obszar przetwarzania danych należy stosować następujące zasady bezpieczeństwa:
   a) adresat powinien zostać powiadomiony o przesyłce;
   b) nadawca powinien sporządzić kopię przesyłanych danych;
   c) dane przed wysłaniem powinny zostać zaszyfrowane, a hasło podane adresatowi inną drogą;
   d) stosować bezpieczne koperty depozytowe;
   e) przesyłkę należy przesyłać korzystając z usług kuriera;
   f) adresat powinien powiadomić nadawcę o otrzymaniu przesyłki.

XVII. Procedury zabezpieczania systemu informatycznego z uwzględnieniem ochrony przed wirusami komputerowymi

1. Celem procedury jest zabezpieczenie systemu informatycznego przed szkodliwym oprogramowaniem (np. typu robaki, wirusy, konie trojańskie, rootkity) oraz nieautoryzowanym dostępem do systemów przetwarzających dane osobowe.
2. Do ochrony przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do Systemu Informatycznego służącego do przetwarzania danych osobowych stosowane jest oprogramowanie antywirusowe.
3. Za zaplanowanie i zapewnienie ochrony antywirusowej, w tym za zapewnienie odpowiedniej ilości licencji programów antywirusowych dla użytkowników systemu informatycznego odpowiada Administrator.
4. Na każdym stanowisku wyposażonym w dostęp do sieci Internet musi być zainstalowanie oprogramowanie antywirusowe. Niedopuszczalne jest stosowanie dostępu do sieci Internet bez aktywnej ochrony antywirusowej oraz zabezpieczenia przed dostępem szkodliwego oprogramowania.
5. Aktualizacja definicji wirusów odbywa się automatycznie przez system.
6. W przypadku stwierdzenia pojawienia się wirusa, każdy użytkownik systemu informatycznego powinien niezwłocznie powiadomić Administratora.

XVIII. Sposób zapewnienia odnotowania informacji o odbiorcach, którym dane osobowe zostały udostępnione

W Systemie Informatycznym (szczególnie w dzienniku elektronicznym) służącym do przetwarzania danych osobowych odnotowywane są informację o odbiorcach danych, a w szczególności imię i nazwisko lub nazwa odbiorcy, data udostępnienie oraz zakres udostępnienia.

XIX. Procedury realizacji przeglądów i konserwacji systemu informatycznego

1. Celem procedury jest zapewnienie ciągłości działania systemu informatycznego przetwarzających dane osobowe oraz zabezpieczenie danych osobowych przed ich nieuprawnionym udostępnieniem.
2. Przeglądy i konserwacje sprzętu komputerowego oraz nośników informacji służących do przetwarzania danych osobowych, przeprowadzane są w pomieszczeniach stanowiących obszar przetwarzania danych osobowych określony w Polityce przez firmy zewnętrzne na podstawie zawartych umów.
3. Osoba, której zlecono naprawę lub konserwację sprzętu, czynności te wykonuje na podstawie odrębnego upoważnienia Administratora – wzór stanowi **Załącznik nr 4** do Polityki oraz oświadczenia o zachowaniu poufności - **Załącznik nr 3** do Polityki lub zawartych w treści umowy.
4. Nadzór nad przeprowadzaniem przeglądów technicznych, konserwacji i napraw sprzętu komputerowego, na którym zainstalowano system informatyczny służący do przetwarzania danych osobowych, systemu informatycznego służącego do przetwarzania danych osobowych oraz nośników informacji służących do przetwarzania danych osobowych pełni Administrator lub wskazana przez niego osoba.
5. W przypadku przekazywania do naprawy sprzętu komputerowego z zainstalowanym systemem informatycznym służącym do przetwarzania danych osobowych lub nośnikiem informacji służących do przetwarzania danych osobowych, powinien on zostać pozbawiony danych osobowych przez fizyczne wymontowanie dysku

lub skasowanie danych lub naprawa powinna zostać przeprowadzona w obecności Administratora lub osoby przez niego upoważnionej.

6. Przeglądy techniczne wykonywane muszą być nie rzadziej niż raz w roku.
7. Zabronione jest wykonywanie przeglądów i konserwacji systemu informatycznego służącego do przetwarzania danych osobowych oraz nośników informacji służących do przetwarzania danych osobowych samodzielnie przez użytkownika systemu.

XX. Postanowienia końcowe

1. Administrator ma prawo do kontroli stanu zabezpieczeń oraz przestrzegania zasad ochrony danych osobowych w dowolnym terminie.
2. Należy instalować zalecane przez producentów oprogramowania poprawki i uaktualnienia Systemu Informatycznego celem wyeliminowania błędów w działaniu lub poprawienia wydajności działania.
3. Naruszenie zasad wynikających z Polityki i Instrukcji zarządzania systemem informatycznym może stanowić podstawę wszczęcia postępowania dyscyplinarnego przeciwko sprawcy naruszenia.
4. Wszczęcie lub przeprowadzenie postępowania dyscyplinarnego przeciwko osobie naruszającej zasady wynikające z Polityki i Instrukcji zarządzania systemem informatycznym nie wyklucza możliwości wszczęcia postępowania karnego oraz dochodzenia roszczeń z powództwa cywilnego.
5. Instrukcja zarządzania systemem informatycznym wchodzi w życie z dniem jej podpisania przez Administratora.

Opracował:
mgr Marek Rochna – Inspektor Ochrony Danych

mgr Marek Rochna
Audytor Normy ISO/IEC 27001
tel. 602 523 360

Zatwierdził:
DYREKTOR
ZESPOŁU SZKÓŁ NR 2
Z ODDZIAŁAMI INTEGRACYJNYMI
W PUŁTUSKU
mgr Krystyna Estkowska

.....
(data i podpis Administratora)