Polityka Bezpieczeństwa Informacji w Zespole Szkół nr 1 im. Anny Wazówny w Golubiu-Dobrzyniu

§1Cel powstania i przedmiot dokumentu

1. Polityka odnosi się do wszelkich informacji znajdujących się w zasobach Administratora danych obejmując w szczególności obszar ochrony danych osobowych, została opracowana i wdrożona w celu zapewnienia zgodności przetwarzania danych osobowych z wymogami obowiązujących w tym zakresie, polskich i europejskich aktów prawnych.
2. Przedmiotem Polityki jest określenie, opisanie i zawarcie, w tym i w innych wskazanych w Polityce dokumentach, a stanowiących jej część, zastosowanych środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych informacji w tym danych osobowych, odpowiednią do zagrożeń oraz kategorii danych osobowych objętych ochroną, a w szczególności zabezpieczeń przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, zniszczeniem, bezprawną modyfikacją, utratą, uszkodzeniem.

§2 Słownik/Definicje

1. ***Polityka***– polityka bezpieczeństwa informacji- ochrony informacji, w tym ochrony danych osobowych, regulująca kwestie opisane w niniejszym dokumencie, jak i w innych pozostałych już wytworzonych lub w przyszłości wytworzonych, odnoszących się do szeroko rozumianej ochrony informacji, ochrony danych osobowych przetwarzanych w jednostce lub powierzanych innym podmiotom.
2. ***Administrator*** - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Placówka reprezentowana przez dyrektora.
3. ***Administrator systemu informatycznego*** - osoba odpowiedzialna za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego- Informatyk. Osoba kontaktowa z ***CSIRT NASK*** w sprawie incydentów bezpieczeństwa komputerowego.
4. ***Analiza ryzyka*** - analiza możliwości wystąpienia naruszenia bezpieczeństwa informacji, naruszenia ochrony danych osobowych w konkretnym zasobie przetwarzającym dane oraz zawierająca działania służące mitygowaniu ryzyka.
5. ***Dane osobowe*** - wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.
6. ***IOD*** - inspektor ochrony danych - osoba wyznaczona zgodnie z obowiązującymi przepisami przez Administratora, w celu informowania i doradzania Administratorowi i pracownikom w zakresie obowiązującego prawa o ochronie danych osobowych oraz w celu monitorowania jego przestrzegana oraz działania, jako punkt kontaktowy dla osób, których dane są przetwarzane i organu nadzorczego.
7. ***Naruszenie bezpieczeństwa informacji***- każdy przypadek naruszenia poufności, integralności i dostępności, niespełnienie wymagań bezpieczeństwa informacji aktywów jednostki.
8. ***Naruszenie ochrony danych osobowych*** - naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania,

nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

9. ***System informatyczny*** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
10. ***Dostępność danych-*** – właściwość określająca, że zasób systemu informatycznego jest możliwy do wykorzystania na żądanie, w założonym czasie
11. ***Integralność danych*** - rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
12. ***Poufność danych*** - rozumie się przez to własność zapewniającą, że dane nie zostaną udostępniane nieupoważnionym podmiotom.
13. ***Przetwarzanie danych*** - operacja lub zestaw operacji wykonywanych na danych osobowych od momentu pozyskania do momentu usunięcia danych z zasobów Administratora, w sposób zautomatyzowany lub niezautomatyzowany.
14. ***RODO*** - rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
15. ***Pozostałe akty prawne regulujące ochroną informacji i danych osobowych*** – ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne i rozporządzenie wykonawcze o Krajowych Ramach Interoperacyjności, ustawa o ochronie danych osobowych z 10.05. 2018 r., ustawa o Krajowym Systemie Cyberbezpieczeństwa z dnia 5 lipca 2018 r., inne akty europejskie. Ustawa o ochronie danych osobowych z dnia 10 maja 2018 r.
16. ***Upoważnienie*** - pisemne zezwolenie do przetwarzania danych osobowych wydane na zasadach określonych u Administratora. W systemie informatycznym upoważnienie jest nadaniem uprawnień w celu realizacji określonych czynności, w zakresie świadczonej pracy przez użytkownika.
17. ***Użytkownik systemu*** - osoba posiadająca uprawnienia do przetwarzania danych osobowych w systemie informatycznym.
18. ***Właściciel ryzyka*** — osoba upoważniona przez Administratora danych, odpowiedzialna za gromadzenie i przetwarzanie danych osobowych w danym procesie przetwarzania danych osobowych.
19. ***Jednostka***- Zespół Szkół nr 1 im. Anny Wazówny w Golubiu-Dobrzyniu.

§3 Zakres informacji objętych Polityką oraz zakres jej stosowania

1. Politykę stosuje się do wszelkich czynności stanowiących przetwarzanie informacji w tym danych osobowych, niezależnie od źródła ich pochodzenia, zakresu, celu zebrania, sposobu lub czasu przetwarzania. Odnosi się do wszystkich danych osobowych przetwarzanych w Jednostce, a także poza jej obszarem, niezależnie od formy, celu oraz zakresu ich przetwarzania (tradycyjnego, elektronicznego).
2. Polityka obowiązuje we wszystkich pomieszczeniach jednostki.
3. Polityka ma zastosowanie do wszystkich pracowników, którzy w zakresie swoich obowiązków służbowych przetwarzają dane osobowe, jak również innych osób, które z upoważnienia Administratora uzyskały dostęp do danych osobowych.

4. Każda z osób, o których mowa w ust. 3 została zobowiązana do zapoznania się z procedurami bezpieczeństwa danych opisanymi w Polityce bezpieczeństwa informacji wraz z załącznikami, do ich przestrzegania w zakresie wynikającym z przydzielonych zadań oraz do złożenia w tym zakresie stosownego oświadczenia o zachowaniu poufności.
5. Każde naruszenie zasad Polityki może być uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych lub wynikających z umów cywilnych o współpracy i może skutkować konsekwencjami zgodnie z Kodeksem pracy lub odpowiednimi przepisami dotyczącymi zasad współpracy, jak również odpowiedzialnością przewidzianą w przepisach regulujących zasady przetwarzania, w tym ochrony danych osobowych.
6. W przypadku, gdy naruszenie miałoby charakter umyślnego przestępstwa, wówczas zastosowanie powinny znaleźć przepisy karne, a konkretnie art. 107 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.

§4 Podstawowe zasady przetwarzania danych osobowych

1. Przetwarzanie danych osobowych w Jednostce odbywa się przy zachowaniu zasad **opisanych i w art. 5 RODO**, do których należą:
   - zgodność z prawem, rzetelność i przejrzystość (dane mają być przetwarzane zgodnie z prawem i rzetelnie oraz przy zastosowaniu niezbędnych środków technicznych i organizacyjnych, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia);
   - ograniczenie celu (dane mają być przetwarzane w konkretnych i uzasadnionych celach)
   - minimalizacja danych (dane mają być adekwatne, stosowne i nienadmierne do celów, dla których są przetwarzane);
   - prawidłowość (dane mają być prawidłowe i w razie potrzeby uaktualniane);
   - ograniczenie przechowywania (dane należy przechowywać w formie umożliwiającej identyfikację osób, których dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów ich przetwarzania);
   - integralność i poufność (dane należy przetwarzać w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą środków technicznych i organizacyjnych odpowiednich do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczone przed ich udostępnieniem osobom nieupoważnionym lub wejściem w posiadanie przez osobę nieuprawnioną);
   - rozliczalność - Administrator jest odpowiedzialny za przestrzeganie zasad dotyczących przetwarzania danych osobowych i prawidłową realizację czynności w tym zakresie oraz ma obowiązek prowadzić dokumentację dotyczącą realizacji tych czynności.
2. Za bezpieczeństwo danych osobowych odpowiedzialna jest każda osoba realizująca zadania w Jednostce w zakresie swoich obowiązków służbowych i uprawnień, jakie zostały jej nadane w systemach informatycznych.

3. Mając na względzie zapisy art. 32 RODO Administrator w Polityce określa odpowiednie środki techniczne oraz niezbędne zabezpieczenia stosowane przy przetwarzaniu danych osobowych w celu skutecznej realizacji zasad ochrony danych osobowych oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń.

§5 Przetwarzanie danych osobowych na podstawie RODO

1. Na podstawie ogólnego rozporządzenia o ochronie danych osobowych - RODO, przetwarzane są dane osobowe gromadzone w związku z realizacją przepisów prawa oraz realizacją zadań w interesie publicznym, w szczególności: realizacja obowiązków związanych z edukacją , wychowaniem, realizowaniem programów, udzielaniem odpowiedzi na informację publiczną, realizacją zadań w zakresie wykonywanych projektów, programów unijnych, realizacją obowiązków wynikających z zatrudnienia, oraz związanych z bezpieczeństwem i higieną pracy.

§6 Struktura organizacji bezpieczeństwa informacji oraz danych osobowych

1. Za przetwarzanie danych osobowych oraz ich ochronę zgodnie z powszechnie obowiązującymi przepisami, postanowieniami Polityki oraz procedurami wewnętrznymi z zakresu ochrony danych osobowych, bezpieczeństwa informacji oraz cyberbezpieczeństwa wdrożonych w Jednostce, odpowiadają:
   1) Administrator,
   2) IOD,
   3) ASI,
   4) Pracownicy administracji,
   5) Pracownicy pedagogiczni.
2. Administrator jest odpowiedzialny za:
   - przetwarzanie danych osobowych zgodnie z przepisami o ochronie informacji i danych osobowych;
   - prowadzenie rejestru czynności przetwarzania - Administrator musi prowadzić rejestr czynności przetwarzania danych,
   - przeprowadzenie analizy ryzyka naruszenia bezpieczeństwa informacji oraz naruszenia ochrony danych osobowych, w tym praw i wolności osób fizycznych oraz coroczne przeglądy analizy ryzyka;
   - informowanie osób, których dane dotyczą - Administrator musi informować osoby, których dane dotyczą, w jaki sposób ich dane są przetwarzane, jakie prawa przysługują im w związku z przetwarzaniem danych i w jaki sposób mogą skorzystać z tych praw;
   - zapewnienie bezpieczeństwa danych - Administrator musi zapewnić odpowiednie środki techniczne i organizacyjne, aby zapobiec nieuprawnionemu dostępowi do danych, ich zmianom, zniszczeniu lub utracie;
   - powiadamianie o naruszeniu bezpieczeństwa danych osobowych Organ nadzorczy – PUODO oraz osoby których dane zostaną naruszone;

- informowanie o incydentach bezpieczeństwa komputerowego odpowiedni CSIRT-NASK-Centrum Reagowania na Incydenty Bezpieczeństwa Komputerowego;
- prowadzenie oceny skutków dla ochrony danych - w przypadku przetwarzania danych, które mogą powodować wysokie ryzyko naruszenia prywatności osób, administrator musi przeprowadzić ocenę skutków dla ochrony danych;
- współpraca z organem nadzorczym- Prezesem Urzędu Ochrony Danych.

3. Inspektor ochrony danych odpowiedzialny jest za realizację obowiązków wymienionych w art. 39 RODO oraz za:
   - informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
   - monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
   - udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35;
   - współpraca z organem nadzorczym;
   - pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach;
   - aktualizację Rejestru czynności przetwarzania danych;
   - szkolenia z zakresu ochrony danych- wstępne, okresowe;
   - przeprowadzanie doraźnych audytów w zakresie ochrony danych osobowych.

§8 Wymogi i informacje dotyczące ochrony i przetwarzania danych osobowych

1. Wykaz budynków, pomieszczeń, obiektów i lokalizacji, tworzących obszar, w którym przetwarzane są dane osobowe, został określony w załączniku do niniejszej Polityki.
2. Osobą upoważnioną do przetwarzania danych osobowych jest osoba, która odbyła szkolenie wstępne, posiada wydane upoważnienie przez Administratora oraz nadane uprawnienie dostępu do systemów informatycznych zgodnie z zakresem obowiązków.

§9 Zasady udzielania dostępu do danych osobowych

1. Dostęp do danych osobowych otrzymuje osoba, której nadano upoważnienie, zgodnie z zasadami ustalonymi u Administratora.
2. Nadawanie uprawnień do systemu informatycznego, to proces przydzielania określonych poziomów dostępu do różnych funkcji i zasobów systemu informatycznego dla użytkowników.

§10 Obowiązki wobec osób, których dane osobowe są przetwarzane

1. Obowiązek informacyjny wobec osób, których dane są przetwarzane, spełniany jest zgodnie z wymogami art. 12 i 13 RODO, m.in. poprzez umieszczenie:
   - szczegółowych informacji o przetwarzaniu danych osobowych na stronie internetowej jednostki pod adresem: **https://www.wazowna.pl/75,przetwarzanie-danych-osobowych**
   - na tablicy informacyjnej w siedzibie Placówki;
   - obowiązków informacyjnych dołączanych do składanych wniosków podań, zawieranych umów, do zapytań ofertowych, w postępowaniu o zamówienie publiczne, w stopce wiadomości e-mail, w pismach zwrotnych kierowanych do podmiotów danych, itp.

§11 Przetwarzanie danych osobowych poza własnymi strukturami

1. Powierzenie przetwarzania danych może zachodzić wówczas, gdy dotyczy to zlecenia czynności na danych (konkretnych działań – operacji na danych osobowych) do innego administratora lub w imieniu administratora danych zlecającego dany proces przetwarzania danych.

§12 Udostępnienie danych osobowych

1. Administrator dopuszcza, by dane osobowe, których jest administratorem, były przekazywane innym administratorom w formie udostępnienia danych, po wykazaniu interesu przez innego administratora lub w związku z realizacją zadań wynikających z przepisów prawa.
2. Udostępnienie danych osobowych może nastąpić tylko w sytuacji istnienia przynajmniej jednej z podstaw spośród wskazanych w art. 6 ust. 1 Rodo lub art. 6 ust. 1 Rodo oraz art. 9 ust. 2 RODO.
3. W każdym przypadku, kiedy pojawią się wątpliwości, co do zgodności udostępniania danych osobowych pracownicy konsultują się z inspektorem ochrony danych.
4. Podmioty lub kategorie podmiotów, którym udostępnia się dane osobowe, muszą zostać obligatoryjnie wskazane w stosownych informacjach, które kieruje się poprzez obowiązki informacyjne do podmiotów danych.

§13 Współadministrowanie danymi osobowymi

1. Administrator w zakresie przetwarzanych przez siebie danych osobowych dopuszcza możliwość przyjęcia modelu współadministrowania danymi osobowymi zgodnie z art. 26 RODO.
2. Gdy dochodzi do współadministrowania konieczne jest wspólne uzgodnienie wszystkich administratorów, co do zakresu odpowiedzialności dotyczącej wypełnienia obowiązków wynikających z RODO.

§14 Realizacja praw osób, których dane dotyczą

1. Procedura postępowania w sytuacji realizacji praw osób, których dane dotyczą, tj. określonych w art. 15-22 RODO, została zawarta w złączniku do dokumentacji, który stanowi integralną część Polityki.
2. Zlecając przetwarzanie danych osobowych podmiotom przetwarzającym należy uwzględnić w umowach obowiązki realizacji praw podmiotów danych lub pomoc w wykonaniu tych obowiązków przez podmioty przetwarzające.

§15 Ochrona danych w fazie projektowania oraz domyślna ochrona danych

(Privacy by design by default)

1. Administrator przed przystąpieniem do przetwarzania danych w nowym procesie (zbiorze, rejestrze) przetwarzania danych osobowych zobligowany jest do wykonania czynności określonych w procedurze ,,Privacy by design by default.,,.
2. Obowiązkiem Administratora danych jest zadbanie o jak najlepszą ochronę danych osobowych w fazie projektowania (privacy by design).
3. Podstawowym celem powyższej zasady jest ,,wbudowanie,, zasad ochrony prywatności w taki sposób, aby od samego początku istnienia danego procesu ochrona prywatności stanowiła jego część składową.
4. Mając na uwadze powyższą zasadę uwzględniając nowy projekt, nową usługę, nowy proces, w którym występuje przetwarzanie danych należy wdrożyć odpowiednie środki techniczne takie jak: szyfrowanie danych, pseudonimizacja danych jak również minimalizację zbieranych danych.

§16 Ocena skutków dla ochrony danych osobowych

1. Administrator przed przystąpieniem do przetwarzania danych osobowych przeprowadza analizę ryzyka, jeśli przetwarzanie może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych, wówczas Administrator zobligowany jest przeprowadzić ocenę skutków dla ochrony danych w trybie art. 35 Rodo, w szczególności, jeśli zamierza przetwarzać dane z użyciem nowych technologii.

2. W strukturze Jednostki ocena skutków dla ochrony danych stanowi obowiązek konsultacji z inspektorem ochrony danych jako forma realizacji jego zadań szczególnie w zakresie informowania Administratora oraz podmiotów przetwarzających.

§17 Naruszenia ochrony danych osobowych

1. Pracownicy powinni mieć świadomość możliwości zaistnienia sytuacji naruszenia ochrony danych osobowych.
2. Zasady postępowania w przypadku naruszeń ochrony danych zostały odrębnie uregulowane w dedykowanej procedurze i stanowią integralną część Polityki.

§17.1 Naruszenia bezpieczeństwa komputerowego- Incydenty Bezpieczeństwa Komputerowego

1. W związku z obowiązkiem jednostek publicznych do zgłaszania i obsługi incydentów cyberbezpieczeństwa, wynikających z przepisów o Krajowym systemie cyberbezpieczeństwa została wprowadzona polityka określająca postępowanie dla wskazanych incydentów.

§18 Najważniejsze zasady bezpieczeństwa przetwarzania danych

1. ***Zasada wiedzy koniecznej*** – oznaczająca, że dostęp do informacji ograniczony jest do tych danych, które są niezbędne do prawidłowego wykonywania obowiązków na danym stanowisku.
2. ***Zasada chronionego pomieszczenia*** – wyrażająca się tym, że pod nieobecność osoby uprawnionej w pomieszczeniach (poza ogólnodostępnymi typu korytarze) nie mogą przebywać osoby postronne. Po opuszczeniu pomieszczenia osoba odpowiedzialna zamyka je na klucz (bez pozostawiania kluczy w zamkach – wyjątek stanowi ewakuacja).
3 ***Zasada czystego biurka*** – oznaczająca, że zarówno dokumentów papierowych, jak i ja-kichkolwiek innych nośników informacji (np. pendrive, płyt CD), nie pozostawia się bez nadzoru.
4. ***Zasada czystego ekranu*** – każdorazowe opuszczenie pomieszczenia w godzinach pracy powinno zostać poprzedzone zablokowaniem komputera. Na wszystkich stacjach aktywny jest wygaszasz ekranu zabezpieczony hasłem, który aktywizuje się automatycznie po przekroczeniu, określonego w minutach, czasu braku aktywności. Każdy użytkownik systemu zobowiązany jest zadbać, aby po zakończeniu pracy sprzęt został poprawnie wyłączony.
5. ***Zasada czystej drukarki*** – wszystkie osoby zobowiązane są do zabierania dokumentów z drukarek zaraz po ich wydrukowaniu.
6. ***Zasada czystego kosza*** – nieprzydatne dokumenty, brudnopisy, zbędne kopie muszą zostać trwale zniszczone w sposób uniemożliwiający odtworzenie zawartych w nich informacji. Zasada ta dotyczy również informacji zapisanych w innej niż papierowa forma

– na nośnikach elektronicznych. Zabrania się wrzucania do kosza na śmieci płyt CD/DVD oraz innych nośników, które powinny zostać zniszczone w specjalistycznych niszczarkach.

7. ***Zasada legalności oprogramowania*** – wyrażająca się zabranianiem pracownikom samodzielnego instalowania oprogramowania a także przechowywania na komputerach stanowiących mienie Administratora treści naruszających prawo.
8. ***Zasada minimalizacji danych*** – Administrator przetwarza dane niezbędne do realizacji celów, w związku z którymi przetwarza dane osobowe.

§18 Audyty systemu ochrony danych osobowych

1. Administrator zobowiązany jest do przeprowadzania regularnych audytów, w tym mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania, zgodnie z art. 32 ust 1 lit. d RODO.

§19 Audyty bezpieczeństwa informacji (KRI)

1. Administrator jest zobowiązany do przeprowadzania audytów zgodnie z wymogiem, o którym mowa w § 20 ust. 2 pkt 14 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, w celu weryfikowania zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz efektywności zasad bezpieczeństwa wdrożonych na podstawie niniejszej Polityki.
2. Audyty bezpieczeństwa informacji KRI przeprowadzone są przez zespół zewnętrznych audytorów ze Starostwa Powiatowego.

§20 Role pracowników określone w polityce

1. W jednostce publicznej, wdrażanie polityki bezpieczeństwa informacji jest zadaniem wielu pracowników, a ich role zależą od hierarchii organizacyjnej oraz specyfiki pracy. Uwzględniając powyższe w kontekście bezpieczeństwa informacji:
   - ***Dyrekcja***- odpowiada za opracowanie i wdrożenie polityki bezpieczeństwa informacji, nadzoruje działania w tym zakresie oraz podejmuje decyzje dotyczące jej aktualizacji i poprawy.
   - ***Inspektor ochrony danych*** – pełni funkcję doradczą oraz nadzoruje wypełnienie obowiązków w zakresie ochrony danych osobowych w Jednostce.
   - ***Administrator systemów informatycznych*** - odpowiada za konfigurację, zarządzanie i utrzymanie systemów informatycznych, zapewnienie ich bezpieczeństwa. Osoba wyznaczona do kontaktu z ***CSIRT NASK*** w sprawie incydentów bezpieczeństwa komputerowego.
   - ***Pracownicy administracji*** - przetwarzają informacje, zgodnie z wytycznymi i procedurami dotyczącymi bezpieczeństwa informacji, zapewniają poufność, integralność i dostępność informacji, wykonują obwiązki informacyjne, zgłaszają

nowe procesy inspektorowi ochrony danych, konsultują się w sprawach związanych biorą udział w procesie szacowania ryzyka.

- ***Pracownicy pedagogiczni***- nauczyciele włączają się w cały proces przetwarzania danych w placówce oświatowej, zwłaszcza danych osobowych i informacji j dotyczących uczniów oraz rodziców.

2. Wszyscy pracownicy są odpowiedzialni za przestrzeganie polityki bezpieczeństwa informacji i przeciwdziałanie zagrożeniom w tym zakresie. Ich aktywny udział i świadomość ryzyka są kluczowe dla zapewnienia bezpieczeństwa informacji, w tym bezpieczeństwa danych osobowych.

§21 Zasady bezpieczeństwa przy przetwarzaniu informacji w tym danych osobowych

1. Pracownicy są zobowiązani do ochrony danych osobowych oraz środków przetwarzających dane osobowe przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem.
2. Zasady bezpieczeństwa przy przetwarzaniu danych osobowych określone zostały w załączniku do niniejszej Polityki, który zawiera wykaz zastosowanych środków technicznych i organizacyjnych w celu przeciwdziałania naruszeniom. Co najmniej raz do roku Administrator dokonuje przeglądu aktualności zastosowanych zabezpieczeń.
3. Każdy pracownik oraz inne osoby przetwarzające dane osobowe z upoważnienia Administratora zobowiązani są do ich stosowania i przestrzegania.

§22 Przeglądy i uaktualnienia Polityki

1. Polityka podlega okresowemu przeglądowi pod kątem jej adekwatności, nie rzadziej niż jeden raz do roku. Przeglądu polityki i załączników do w/w dokumentu dokonuje inspektor ochrony danych w porozumieniu z Administratorem.

2. Załączniki do Polityki stanowią integralną część dokumentacji i podlegają przeglądom oraz aktualizacji w ramach zmieniających się przepisów i regulacji.