Wielozawodowy Zespół Szkół w Zatorze
ul Kongresowa 11
32-640 Zator

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA I OCHRONY DANYCH OSOBOWYCH W WIELOZAWODOWYM ZESPOLE SZKÓŁ W ZATORZE

Rejestr zmian w dokumencie:

Wersja	Data	Opracował	Opis nowelizacji
1		Karol Matyjasik	----------

Dokumenty powiązane:

1. **Instrukcja zarządzania systemem informatycznym w Wielozawodowym Zespole Szkół w Zatorze.**

Zawartość

Rozdział I. Postanowienia ogólne

§1

Dokument Polityka bezpieczeństwa przetwarzania danych osobowych w **Wielozawodowym Zespole Szkół w Zatorze**, zwany dalej Polityką bezpieczeństwa, została opracowana w oparciu o:

Ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2015 r. poz. 2135 z późn. zm.)

a) Ustawę z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U z 2010 r. Nr 182, poz. 1228)

b) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. 2004 nr 100 poz. 1024 z późn. zm.)

1. Polityka bezpieczeństwa opisuje zasady dotyczące bezpieczeństwa danych osobowych przetwarzanych w Wielozawodowym Zespole Szkół w Zatorze.
2. Przy przetwarzaniu danych osobowych w systemach informatycznych Technikum i Zasadniczej Szkoły Zawodowej należy stosować **wysoki poziom bezpieczeństwa**.
3. Polityka dotyczy wszystkich danych osobowych, przetwarzanych w Szkole, niezależnie od formy ich przetwarzania.
4. Bezpieczeństwo systemów informatycznych odnosi się do wszystkich procesów związanych z informacją to jest: wytwarzania, przetwarzania, przechowywania, archiwizowania, przesyłania, zbierania, prezentowania oraz niszczenia.
5. **Polityka bezpieczeństwa** określa tryb postępowania w przypadku, gdy:
   c) Stwierdzono naruszenie zabezpieczenia systemu informatycznego,
   d) Stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci informatycznej mogą wskazywać na naruszenie zabezpieczeń tych danych.

Rozdział II. Cele polityki bezpieczeństwa

§ 2.

Celem **Polityki bezpieczeństwa** jest przyjęcie, wdrożenie i realizacja takich działań przy wykorzystaniu środków technicznych i organizacyjnych, które zapewnią maksymalny poziom bezpieczeństwa procesu przetwarzania danych osobowych, chroniąc je przed nieautoryzowanym dostępem, przetwarzaniem z naruszeniem przepisów określających zasady postępowania przy przetwarzaniu danych osobowych oraz przed zmianą, uszkodzeniem lub zniszczeniem.

§ 3.

Cele **Polityki** realizowane są poprzez zapewnienie danym osobowym następujących cech:

1. poufności – właściwości zapewniającej, że dane nie są udostępniane nieupoważnionym podmiotom;
2. integralności – właściwości zapewniającej, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
3. rozliczalności – właściwości zapewniającej, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
4. zgodności z prawem – właściwości zapewniającej, że gromadzone są wyłącznie dane niezbędne do właściwego funkcjonowania szkoły i realizowania przez nią zadań określonych w odrębnych przepisach. W związku z tym Szkoła może przetwarzać tylko takie informacje o pracownikach, które maja bezpośredni i jednoznaczny związek ze stosunkiem pracy oraz tylko takie informacje o uczniach, które związane są z procesem dydaktycznym i ochroną zdrowia podczas nauki w Szkole. Szczegółowy zakres danych osobowych uczniów, jakie może gromadzić szkoła, podaje rozporządzenie Ministra Edukacji Narodowej z dnia 19 kwietnia 1999 r w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (Dz.U. nr 41 poz. 414). Zakres danych dotyczących pracowników określa rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 28 maja 1996 r. w sprawie zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracownika (Dz.U. 1996, nr 62, poz. 286, z późn. zm.)

Rozdział III. Deklaracja Dyrekcji Szkoły

§ 4.

Polityka zakłada pełne zaangażowanie Dyrekcji oraz pracowników Szkoły dla zapewnienia bezpieczeństwa danych osobowych przetwarzanych zarówno w sposób tradycyjny, jak i w systemie informatycznym.

§ 5.

Zarządzanie bezpieczeństwem zasobów danych osobowych stanowi proces ciągły, na który składają się takie elementy, jak: identyfikacja oraz analiza zagrożeń i ryzyka, stosowanie odpowiednich zabezpieczeń, monitorowanie wdrażania i eksploatacji zabezpieczeń, wykrywanie i reagowanie na incydenty.

§ 6.

Niniejsza Polityka oraz dokumenty z nią powiązane powinny być aktualizowane wraz ze zmieniającymi się przepisami prawnymi o ochronie danych osobowych oraz zmianami faktycznymi, które mogą powodować, że zasady ochrony danych osobowych określone w obowiązujących dokumentach będą nieaktualne lub nieadekwatne.

1. Fakty wystąpienia poważnych naruszeń ochrony danych osobowych powinny skutkować zmianami w dokumencie niniejszej Polityki i dokumentach powiązanych.
2. Wszelkie znaczące zmiany Polityki powinny być zatwierdzane przez Dyrekcję

Rozdział IV. Definicje

- **Administrator Danych Osobowych**–w **Wielozawodowym Zespole Szkół w Zatorze** jest dyrektor Szkoły.

- **Administrator Bezpieczeństwa Informacji - Dyrektor Szkoły**.
- **Administrator Systemu Informatycznego** - osoba wyznaczona przez **Administratora Bezpieczeństwa Informacji,** odpowiedzialna za funkcjonowanie infrastruktury informatycznej oraz za stosowanie technicznych i organizacyjnych środków bezpieczeństwa w systemach informatycznych.
- **Dane Osobowe** - każda informacja dotycząca żyjącej osoby fizycznej, która pozwala na bezpośrednią lub pośrednią identyfikacje tej osoby.
- **Dyrekcja** – dyrektor Szkoły.
- **Osoba upoważniona** - osoba posiadająca upoważnienie wydane przez administratora danych osobowych (lub osobę uprawnioną przez niego)i dopuszczona jako użytkownik do przetwarzania danych osobowych w zakresie wskazanym upoważnieniu.
- **Przetwarzanie danych osobowych** - wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie.
- **Stacja robocza** – stacjonarny lub przenośny komputer wchodzący w skład systemu informatycznego umożliwiający użytkownikom systemu dostęp do danych osobowych znajdujących się w systemie.
- **System informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
- **Użytkownik systemu** - osoba posiadająca uprawnienia do przetwarzania danych osobowych w systemie informatycznym.
- **Ustawa** – ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.
- **Rozporządzenie** - rozporządzenie Ministra Spraw Wewnętrznych i Administracji zdania 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.
- **Właściciel zasobów danych osobowych**— osoba wyznaczona przez **Administratora Bezpieczeństwa Informacji,** odpowiedzialna za gromadzenie i przetwarzanie danych osobowych w podległej komórce organizacyjnej.
- **Zbiór danych osobowych** - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
- **Szkoła - Wielozawodowy Zespół Szkół w Zatorze**.

Rozdział V. Obowiązki i odpowiedzialność w zakresie zarządzania bezpieczeństwem

§ 7.

Dyrekcja jest odpowiedzialna za przetwarzanie i ochronę danych osobowych zgodnie z przepisami prawa, w tym wprowadzenie do stosowania procedur postępowania zapewniających prawidłowe przetwarzanie danych osobowych, rozumiane jako ochronę danych przed ich udostępnieniem osobom nieupoważnionym, zmian, lub zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem Ustawy oraz utratą, uszkodzeniem lub zniszczeniem.

1. Do kompetencji **Dyrekcji** należy w szczególności:
   a) Wyznaczenie **Administratora Bezpieczeństwa Informacji** oraz jego zastępcy.
   b) Wyznaczanie **Właścicieli** zasobów danych osobowych.
   c) Podział zadań i obowiązków związanych z organizacją ochrony danych osobowych.

2. Do obowiązków **Dyrekcji** należy:
   a) Zapewnienie szkoleń dla pracowników w zakresie przepisów o ochronie danych osobowych oraz zagrożeń związanych z ich przetwarzaniem.
   b) Przyjmowanie i zatwierdzanie niezbędnych, wymaganych przez przepisy prawa dokumentów regulujących ochronę danych osobowych w Szkole
   c) Zapewnienie środków finansowych na ochronę fizyczną pomieszczeń, w których przetwarzane są dane osobowe.
   d) Zapewnienie środków finansowych niezbędnych do ochrony danych osobowych przetwarzanych w systemach informatycznych oraz w zbiorach nieinformatycznych.
   e) Zapewnienie realizacji obowiązku zgłoszenia i aktualizacji zbiorów danych osobowych do rejestracji GIODO.

§ 8.

Administrator Bezpieczeństwa Informacji odpowiada za nadzorowanie stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie ochrony danych osobowych.

1. Do kompetencji Administratora Bezpieczeństwa Informacji należy:
   a) Określenie zasad ochrony danych osobowych.
   b) Wnioskowanie o ukaranie osób winnych naruszenia przepisów i zasad dotyczących ochrony danych osobowych.
2. Do obowiązków Administratora Bezpieczeństwa Informacji należy:
   a) Nadzór nad wdrożeniem stosownych środków organizacyjnych, technicznych i fizycznych w celu ochrony przetwarzanych danych osobowych.
   b) Nadawanie, zmienianie oraz cofanie uprawnień do przetwarzania danych osobowych.
   c) Zapoznawanie pracowników oraz współpracowników Szkoły z przepisami i zasadami ochrony danych osobowych oraz informowanie o zagrożeniach związanych z ich przetwarzaniem.
   d) Reprezentowanie Szkoły w kontaktach z Biurem GIODO.
   e) Przygotowywanie zgłoszeń zbiorów danych osobowych do rejestracji w Biurze GIODO.
   f) Reagowanie na zgłaszane incydenty związane z naruszeniem ochrony danych osobowych oraz analizowanie ich przyczyn i kierowanie wniosków dotyczących ukarania winnych naruszeń.
   g) Sprawdzanie wypełnienia obowiązków technicznych i organizacyjnych związanych z ochron danych osobowych.
   h) Prowadzenie pełnej dokumentacji związanej z ochroną danych osobowych, zawierającej:
      (1) ewidencję zbiorów danych osobowych,
      (2) ewidencje osób upoważnionych do przetwarzania danych osobowych (odwołanie upoważnienia),
      (3) wykaz obszarów przetwarzania danych osobowych,
      (4) dokumenty z audytów i przeglądów bezpieczeństwa,

(5) oryginały i kopie dokumentów dotyczących ochrony danych osobowych, w szczególności uchwały Zarządu, polityki bezpieczeństwa, instrukcje, regulaminy, procedury,

(6) programy szkoleń, listę przeszkolonych osób,

(7) kopie wniosków o rejestrację zbiorów,

(8) raport z wypełnienia obowiązku informacyjnego (kopie wniosków, pism z klauzulami informacyjnymi).

(9) raporty, analizy, protokoły, zestawienia dotyczące przetwarzania i ochrony danych osobowych.

§ 9.

1. Do kompetencji **Właścicieli** zasobów danych osobowych należy:
   a) Określanie celów w jakich mają być przetwarzane dane osobowe, zakresu, sposobu oraz czasu trwania przetwarzania danych osobowych.
   b) Ustalenie, czy dane przetwarzane dla określonego celu mają mieć charakter poufny.
2. Do obowiązków Właścicieli zasobów danych osobowych należy:
   a) Zapewnienie podstaw prawnych do przetwarzania danych osobowych od chwili zebrania danych osobowych do chwili ich usunięcia.
   b) Zapewnienie aktualności, adekwatności oraz merytorycznej poprawności danych osobowych przetwarzanych w określonym przez nich celu.
3. Realizację obowiązku informowania o przetwarzaniu danych osobowych osób, których dane osobowe są pozyskiwane.
4. Zapewnienie na żądanie uprawnionych osób, udostępniania informacji o przetwarzanych danych osobowych oraz podmiotach, którym zostały one udostępnione.

§ 10.

Odpowiedzialność **pracowników** i **użytkowników** systemu

1. Pracownicy są odpowiedzialni za bezpieczeństwo danych, do których maja dostęp. W szczególności w systemach informatycznych odpowiadają oni za poprawne wprowadzanie informacji do tych systemów oraz za użycie, zniszczenie lub uszkodzenie sprzętu oraz znajdujących się na nim danych i oprogramowania.
2. Pracownicy Szkoły są zobowiązani do informowania o wszelkich podejrzeniach naruszenia lub zauważonych naruszeniach oraz słabościach systemu przetwarzającego dane osobowe bezpośrednio do Administratora Bezpieczeństwa Informacji.
3. Pracownicy Szkoły są zobowiązani do:
   a) Postępowania zgodnie z Polityką.
   b) Zachowania w tajemnicy danych osobowych oraz informacji o sposobach ich zabezpieczenia.
   c) Ochrony danych osobowych oraz środków przetwarzających dane osobowe przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem.
   d) Pracownicy powinni mieć świadomość możliwości zaistnienia sytuacji naruszenia ochrony danych osobowych. W tym celu powinni przestrzegać procedur związanych

z otwieraniem i zamykaniem pomieszczeń, a także z wejściem do obszarów przetwarzania danych osobowych osób nieupoważnionych.

Rozdział VI. Sankcje za naruszenie zasad ochrony danych osobowych

§ 11.

W przypadku naruszenia przepisów lub zasad postępowania, osoba upoważniona do przetwarzania danych osobowych podlega odpowiedzialności służbowej i karnej. Naruszenie zasad ochrony danych osobowych a także sposobu ich zabezpieczania, może skutkować postawieniem pracownikowi zarzutu popełnienia, jednego z przestępstw określonych w Rozdziale 8 Ustawy lub przestępstwa określonego w art. 266 Kodeksu Karnego.

Rozdział VII. Obowiązek informacyjny

§ 12.

W przypadku zbierania danych osobowych na formularzach, umowach, drukach (zarówno papierowych jak i elektronicznych) należy umieszczać na nich odpowiednią klauzulę informacyjną. Klauzula taka powinna informować osobę, której dane zbierane są:

1. Adresie siedziby i pełnej nazwie Wielozawodowego Zespołu Szkół w Zatorze.
2. Celu zbierania danych, a także o znanych lub przewidywanych odbiorcach danych.
3. Prawie dostępu do treści swoich danych oraz ich poprawiania.
4. Dobrowolności albo obowiązku podania danych, a jeśli taki obowiązek istnieje, o jego podstawie prawnej.

Rozdział VIII. Przetwarzanie danych osobowych w obszarach bezpiecznych

§ 13.

Dane osobowe w Szkole mogą być przetwarzane wyłącznie w pomieszczeniach przetwarzania danych osobowych.

1. Wykaz pomieszczeń lub części pomieszczeń, w których przetwarzane są dane osobowe w Szkole stanowi **Załącznik nr 4** do niniejszego dokumentu i może być zmieniany decyzją **Administratora Bezpieczeństwa Informacji**.
2. Za obszar przetwarzania danych należy rozumieć obszar, w którym wykonywana jest choćby jedna z czynności wymienionych w art. 7 pkt. 2 Ustawy.

Rozdział IX. Wymiana informacji dotyczących danych osobowych

§ 14.

W celu zabezpieczenia należytej ochrony dane osobowe przesyłane do organów nadrzędnych Szkoły (Biuro Edukacji, OKE) przekazywane są drogą elektroniczną poprzez szyfrowane kanały z zastosowaniem uwierzytelnionych haseł.

1. Za bezpieczeństwo programów do przesyłania informacji a także za sposób bezpiecznego przekazywania haseł odpowiadają odpowiednie organy (Biuro Edukacji, Okręgowa Komisja Egzaminacyjna).

2. Za zabezpieczenie techniczne komputerów przed programami szpiegującymi i wirusami odpowiada **Administrator Systemu Informatycznego.**

Rozdział X. Wykaz zbiorów danych oraz programów zastosowanych do przetwarzania danych osobowych

§ 15.

Wykaz zbiorów danych oraz programów zastosowanych do przetwarzania danych osobowych w Szkole stanowi **Załącznik nr 5** do niniejszego dokumentu i może być zmieniany decyzją **Administrator Bezpieczeństwa Informacji**.

Rozdział XI. Struktury zbiorów danych oraz przepływ danych pomiędzy systemami

§ 16.

W Szkole dane osobowe mogą być przetwarzane w zbiorach danych, przy zastosowaniu systemów informatycznych oraz zbiorów ewidencyjnych w postaci kartotek, skorowidzów, ksiąg i wykazów.

§ 17.

Zawartość pól informacyjnych, występujących w systemach zastosowanych w celu przetwarzania danych osobowych, musi być zgodna z przepisami prawa, które uprawniają lub zobowiązują Administratora Bezpieczeństwa Informacji do przetwarzania danych osobowych.

§ 18.

Na żądanie Administrator Bezpieczeństwa Informacji lub osoby przez niego upoważnionej, Administrator Systemu Informatycznego zobowiązany jest do wskazania powiązań między polami informacyjnymi, które zawierają dane osobowe w systemie.

1. Przepływ danych pomiędzy systemami zastosowanymi w celu przetwarzania danych osobowych może odbywać się w postaci przepływu jednokierunkowego lub przepływu dwukierunkowego.
2. Przepływ jednokierunkowy oznacza, że system informatyczny udostępnia dane ze zbioru (bazy) danych tylko w trybie „do odczytu”.

3. Przepływ dwukierunkowy umożliwia upoważnionemu użytkownikowi korzystanie z danych w trybach „do odczytu” i „do zapisu”, tj. umożliwia wprowadzanie nowych danych i modyfikację istniejących.

§ 19.

Przesyłanie danych pomiędzy systemami może odbywać się w sposób manualny, przy wykorzystaniu nośników zewnętrznych (np. płyta CD, DVD, dysk wymienny, Pendrive itp.) lub w sposób półautomatyczny, przy wykorzystaniu funkcji eksportu/ importu danych za pomocą teletransmisji (np. poprzez szyfrowaną sieć teleinformatyczną).

§ 20.

Przesyłanie danych może odbywać się zarówno w obrębie szkoły, jak i na zewnątrz (do organu prowadzącego szkołę lub podmiotów współpracujących ze szkołą w organizowaniu zadań związanych z procesem edukacyjnym, w szczególności organizujących egzamin maturalny i proces rekrutacyjny).

Rozdział XII. Środki ochrony

§ 21.

Administrator Bezpieczeństwa Informacji zapewnia zastosowanie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

1. Środki ochrony, zastosowane przez Administratora Bezpieczeństwa Informacji dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych, obejmują:
   a) środki fizyczne;
   b) środki osobowe;
   c) środki techniczne.

§ 22.

Środki ochrony fizycznej obejmują:

1. Zastosowanie elektronicznego systemu monitoringu w celu kontroli ruchu osób na terenie szkoły;
2. nadzorowanie pobytu osób nie będących pracownikami Szkoły w obszarach bezpiecznych, chyba że ich dostęp został wcześniej zaakceptowany;
3. lokalizację miejsc przetwarzania danych osobowych w pomieszczeniach o ograniczonym i kontrolowanym dostępie;
4. ustalenie zasad pobierania kluczy do pomieszczeń i szaf;
5. składowanie zbiorów danych osobowych (w tym nośników wymiennych i nośników kopii zapasowych) w odpowiednio zabezpieczonych pomieszczeniach i szafach.

§ 23.

Środki ochrony osobowej obejmują:

1. dopuszczenie do przetwarzania danych osobowych wyłącznie osób posiadających upoważnienie wydane przez Administratora Bezpieczeństwa Informacji;

2. zapoznanie tych osób z zasadami przetwarzania danych osobowych oraz obsługą systemu służącego do przetwarzania danych;
3. odebranie stosownych zobowiązań i oświadczeń; tj.: zobowiązania do zachowania w tajemnicy danych i sposobów ich zabezpieczenia oraz oświadczenia o zapoznaniu z treścią przepisów określających zasady postępowania przy przetwarzaniu danych osobowych, a także z dokumentacją opisującą sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ich ochronę.

§ 24.

Środki ochrony technicznej obejmują:

1. mechanizmy kontroli dostępu do systemów i zasobów;
2. zastosowanie odpowiednich i regularnie aktualizowanych informatycznych narzędzi ochronnych;
3. regularne tworzenie kopii zapasowych zbiorów danych przetwarzanych w systemach informatycznych;

Rozdział XIII. Zasady ochrony danych osobowych w zbiorach nieinformatycznych

§ 25.

Zbiory nieinformatyczne powinny być odpowiednio zabezpieczone przed nieuprawnionym dostępem i zniszczeniem.

1. Dokumenty i wydruki, zawierające dane osobowe, należy przechowywać w zamykanych pomieszczeniach, do których dostęp mają jedynie uprawnione osoby.
2. Na czas nieużytkowania, dokumenty i wydruki zawierające dane osobowe powinny być zamykane w szafach biurowych lub zamykanych szufladach.
3. Wydruki robocze, błędne lub zdezaktualizowane powinny być niezwłocznie niszczone przy użyciu niszczarki do papieru lub w inny sposób zapewniający skuteczne ich usunięcie lub zanonimizowanie.

Rozdział XIV. Dopuszczenie osób do przetwarzania danych osobowych

§ 26.

Dyrekcja Szkoły upoważniona jest do przetwarzania danych osobowych, których Administratorem Danych jest Wielozawodowy Zespół Szkół w Zatorze oraz danych osobowych, które są przetwarzane na podstawie art. 31 Ustawy.

§ 27.

Przetwarzanie danych osobowych jest możliwe wyłącznie po uzyskaniu przez pracownika formalnego upoważnienia do przetwarzania danych osobowych wystawianego przez Administratora Bezpieczeństwa Informacji. W tym celu Administratora Bezpieczeństwa Informacji lub jego zastępca przed dopuszczeniem pracownika do pracy przy przetwarzaniu danych osobowych:

1. Zapoznaje pracownika z przepisami dotyczącymi ochrony danych osobowych oraz uregulowaniami wewnętrznymi obowiązującymi w tym zakresie w Wielozawodowym Zespole Szkół w Zatorze.
2. Przyjmuje od pracownika podpisane oświadczenie o zachowaniu danych osobowych i sposobów ich zabezpieczania w tajemnicy, przetwarzania danych osobowych zgodnie z przepisami oraz oświadczenia o znajomości niniejszego dokumentu a także o znajomości „Instrukcji bezpieczeństwa przetwarzania danych osobowych w Wielozawodowym Zespole Szkół w Zatorze", którego wzór stanowi **załącznik nr 1** niniejszej Polityki.
3. Wystawia pracownikowi formalne upoważnienie pracownika do przetwarzania danych osobowych sporządzane wg wzoru stanowiącego **załącznik nr 2** niniejszej Polityki.
4. Oświadczenia i upoważnienia, o których mowa w ust. 2 przechowuje się w aktach osobowych pracownika.

Rozdział XV. Ewidencja osób upoważnionych do przetwarzania danych osobowych

§ 28.

Osoby upoważnione do przetwarzania danych osobowych powinny być wpisywane do ewidencji. Ewidencja osób upoważnionych do przetwarzana danych osobowych powinna być prowadzona przez Administratora Bezpieczeństwa Informacji lub jego zastępcę i powinna zawierać:

1. Imię i nazwisko osoby upoważnionej do przetwarzania danych osobowych.
2. Zakres upoważnienia do przetwarzania danych osobowych.
3. Wskazanie komórki organizacyjnej, w której osoba upoważniona pracuje.
4. Identyfikator, jeśli osoba upoważniona została zarejestrowana w systemie informatycznym, służącym do przetwarzania danych osobowych.
5. Datę nadania i odebrania uprawnień.

§ 29.

Jakakolwiek zmiana w zakresie informacji zawartych w ewidencji powinna podlegać natychmiastowemu odnotowaniu.

§ 30.

Wykazy zawierające ewidencję osób upoważnionych do przetwarzania danych osobowych powinny być przechowywane w szafie zamykanej, do której ma dostęp Administrator Bezpieczeństwa Informacji lub osoba przez niego upoważniona.

§ 31.

Wzór karty z rejestru ewidencji stanowi **załącznik nr 3**niniejszej Polityki.

Rozdział XVI. Rejestracja zbiorów danych osobowych

§ 32.

Upoważnieni pracownicy są zobowiązani do wnioskowania Administratorowi Bezpieczeństwa Informacji zamiaru utworzenia nowego zbioru danych osobowych wraz ze wskazaniem podstawy przetwarzania danych, uzasadnieniem celowości zakresu i sposobu zbierania danych osobowych (którego wzór stanowi załącznik nr 8).

Administrator Bezpieczeństwa Informacji weryfikuje wniosek o utworzenie nowego zbioru danych osobowych oraz analizuje nowy zbiór danych pod kątem obowiązku zgłoszenia zasobu, jako zbioru danych do rejestracji w GIODO.

1. W sytuacji, jeżeli rejestracja nowo powstałego zbioru danych osobowych jest ustawowo wymagana, Administrator Bezpieczeństwa informacji przygotowuje projekt zgłoszenia zbioru danych osobowych do rejestracji w GIODO.
2. Dyrekcja wyznacza Właściciela zasobów danych osobowych dla zarejestrowanego zbioru danych osobowych.

Rozdział XVII. Aktualizacja zbiorów danych osobowych

§ 33.

Właściciel zasobów danych osobowych zgłasza do Administratora Bezpieczeństwa Informacji w ciągu 7 dni od daty modyfikacji zbioru danych osobowych wszelkie zmiany dotyczące przetwarzania danych w zarejestrowanym zbiorze danych osobowych mające wpływ na wniosek rejestracyjny, tj. tych wskazanych wart. 41 ust. 1 pkt3 -7 Ustawy.

§ 34.

Administrator Bezpieczeństwa Informacji przygotowuje wniosek aktualizacyjny zarejestrowanego zbioru danych osobowych w terminie 30 dni od dnia dokonania zmiany w zbiorze.

Rozdział XVIII. Udostępnianie danych osobowych

§ 35.

Dane osobowe mogą być udostępniane podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa, osobom, których dotyczą oraz w szczególnych przypadkach na podstawie art. 31 ust. 1 Ustawy.

Rozdział XIX. Postanowienia końcowe

§ 36.

Niezależnie od odpowiedzialności określonej w przepisach prawa powszechnie obowiązującego, naruszenie zasad określonych w niniejszej Polityce może być podstawą rozwiązania stosunku pracy bez wypowiedzenia z osobą która dopuściła się naruszenia.

§ 37.

W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz. U. z 2015 r. poz. 2135 z późna. zm.) oraz przepisy wykonawcze do tej Ustawy.