Załącznik nr 1 do Zarządzenia nr ...../.....
z dnia ..... Dyrektora Szkoły
Wersja 2.0 z dnia .....

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Szkoła Podstawowa im. Józefa Piłsudskiego w Przytocznie

Przytoczno 25, 21-146 Jeziorzany

*Niniejszy dokument jest wyłącznie dokumentem wewnętrznym stanowiącym własność administratora danych osobowych.

*Dokument zawiera zestaw praw, procedur i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji danych osobowych, wewnątrz jak i na zewnątrz organizacji.

*Polityka odnosi się całościowo do problemu zabezpieczenia danych przetwarzanych tradycyjnie – w formie papierowej, jak i danych przetwarzanych w systemach informatycznych.

*Celem polityki jest wskazanie działań, jakie należy wykonać. Dokument ustanawia zasady i reguły postępowania, które należy stosować, aby właściwie wykonywać obowiązki administratora danych w zakresie zabezpieczenia danych osobowych.

*Dokument stanowi tajemnicę organizacji i nie należy go publikować, lecz rozpowszechniać jedynie wśród pracowników Szkoły Podstawowej w Przytocznie.

SPIS TREŚCI

1. DEFINICJE

1. **„dane osobowe”** oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
2. **„przetwarzanie”** oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
3. **„RODO”** – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);
4. **„administrator - ADO”** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;
5. **„podmiot przetwarzający”** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
6. **„inspektor – IOD”** oznacza osobę powołaną do pełnienia funkcji Inspektora Ochrony Danych w organizacji, inspektor odgrywa kluczową rolę w zakresie wspierania „kultury ochrony danych” oraz pomaga w implementacji niezbędnych elementów RODO w codziennej działalności organizacji. Administrator oraz podmiot przetwarzający zapewniają, by inspektor był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych. Inspektor bezpośrednio podlega najwyższemu kierownictwu administratora lub podmiotu przetwarzającego. Osoby, których dane dotyczą, mogą kontaktować się z inspektorem we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO. Inspektor jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań – zgodnie z prawem Unii oraz prawem państwa członkowskiego;
7. **„pracownik”** oznacza każdą osobę świadczącą pracę na rzecz administratora na podstawie umowy o pracę oraz innych form zatrudnienia, upoważnioną do przetwarzania danych osobowych w organizacji,

8. **„polityka – PBDO”** oznacza dokument Polityki Bezpieczeństwa Danych Osobowych, jest to zestaw praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji danych osobowych, wewnątrz określonej organizacji. Polityka odnosi się całościowo do problemu zabezpieczenia danych przetwarzanych tradycyjnie – w formie papierowej, jak i danych przetwarzanych w systemie informatycznym. Celem polityki jest wskazanie działań jakie należy wykonać oraz ustanowienie zasad i reguł postępowania, które należy stosować aby właściwie wykonywać obowiązki administratora w zakresie zabezpieczenia danych osobowych;
9. **„zgoda”** oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;
10. **„naruszenie ochrony danych osobowych”** oznacza 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;
11. **„Szkoła”** oznacza Szkołę Podstawową im. Józefa Piłsudskiego w Przytocznie, Przytoczno 25, 21-146 Jeziorzany.

2. CHARAKTER I ZADANIA ORGANIZACJI

Szkoła realizuje cele i zadania określone w ustawie – Prawo oświatowe oraz w przepisach wykonawczych wydanych na jej podstawie, a także zawarte w programie wychowawczo- profilaktycznym, dostosowanym do potrzeb rozwojowych uczniów oraz potrzeb danego środowiska. Zgodnie ze statutem główne zadania Szkoły to m.in.:

1) zapewnianie bezpiecznych i higienicznych warunków pobytu uczniów w Szkole oraz zapewnianie bezpieczeństwa na zajęciach organizowanych przez Szkołę;
2) zorganizowanie systemu opiekuńczo-wychowawczego odpowiednio do istniejących potrzeb;
3) kształtowanie środowiska wychowawczego, umożliwiającego pełny rozwój umysłowy, emocjonalny i fizyczny uczniów w warunkach poszanowania ich godności osobistej oraz wolności światopoglądowej i wyznaniowej;
4) realizacja programów nauczania, które zawierają podstawę programową kształcenia ogólnego dla przedmiotów, objętych ramowym planem nauczania;
5) rozpoznawanie możliwości psychofizycznych oraz indywidualnych potrzeb rozwojowych i edukacyjnych uczniów, a także wykorzystywanie wyników diagnoz w procesie uczenia i nauczania;
6) organizowanie pomocy psychologiczno - pedagogicznej uczniom, rodzicom i nauczycielom stosownie do potrzeb, zgodnie z odrębnymi przepisami;
7) organizowanie obowiązkowych i nadobowiązkowych zajęć dydaktycznych z zachowaniem zasad higieny psychicznej;
8) dostosowywanie treści, metod i organizacji nauczania do możliwości psychofizycznych uczniów lub poszczególnego ucznia;
9) wyposażenie Szkoły w pomoce dydaktyczne i sprzęt umożliwiający realizację zadań dydaktycznych, wychowawczych i opiekuńczych oraz innych statutowych zadań Szkoły;

10) organizacja kształcenia, wychowania i opieki dla uczniów niepełnosprawnych oraz niedostosowanych społecznie w formach i na zasadach określonych w odrębnych przepisach;
11) wspomaganie wychowawczej roli rodziców;
12) umożliwianie uczniom podtrzymywania poczucia tożsamości narodowej, etnicznej, językowej i religijnej;
13) zapewnienie, w miarę posiadanych środków, opieki i pomocy materialnej uczniom pozostającym w trudnej sytuacji materialnej i życiowej;
14) sprawowanie opieki nad uczniami szczególnie uzdolnionymi poprzez umożliwianie realizowania indywidualnych programów nauczania oraz ukończenia Szkoły w skróconym czasie.

3. PODSTAWA PRAWNA

Akty prawne:

1. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Ogólne Rozporządzenie o Ochronie Danych Osobowych – RODO);
2. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych,Dz.U. z 2018 r., poz. 1000;
3. Ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania 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 (ogólne rozporządzenie o ochronie danych), Dz.U. z 2019 r., poz. 730.

Inne dokumenty:

1. Norma PN-EN ISO 19011:2012;
2. Norma PN-EN ISO/IEC 27001:2017-06;
3. Norma PN-EN ISO/IEC 27002;
4. Komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony M.P. 2019 poz. 666;
5. Wytyczne Grupy Roboczej Art. 29oraz Wytyczne Europejskiej Rady Ochrony Danych;
6. Bieżące wskazówki Urzędu Ochrony Danych Osobowych.

4. DEKLARACJA STOSOWANIA KIEROWNICTWA

Zmieniająca się rzeczywistość prawna związana z obowiązywaniem RODO wymusiła na administratorzeinwentaryzację zasobów danych osobowych i procesów ich przetwarzania. Z uwagi na pojawienie się nowych regulacji administrator deklaruje, że wdroży niezbędne procedury oparte na zasadach i podstawach przetwarzania zawartych w obowiązujących przepisach dotyczących ochrony danych osobowych.

Administrator świadomy wagi problemów i zagrożeń związanych z ochroną danych osobowych, w celu właściwej i skutecznej ochrony tych danych, wprowadza Politykę Bezpieczeństwa Danych Osobowych zwaną dalej „Polityką Bezpieczeństwa". Opracowanie niniejszego dokumentu wynika ze zrozumienia znaczenia bezpieczeństwa danych we współczesnym świecie. Polityka Bezpieczeństwa zawiera wypracowane reguły i procedury takie jak:

a. reguły bezpiecznego przechowywania danych osobowych,
b. procedura udostępniania danych osobowych (wewnątrz oraz na zewnątrz organizacji),
c. procedura realizacji uprawnień wynikających z RODO,
d. stosowanie zasady privacy by design, privacy by default.

Ponadto, administrator zobowiązuje się do prowadzenia nadzoru nad przestrzeganiem założeń niniejszego dokumentu. W tym celu ustala coroczny plan sprawdzeń oraz wprowadza obowiązek cyklicznych szkoleń z zakresu ochrony danych osobowych oraz wprowadzonych w Szkole procedur bezpiecznego przetwarzania danych podnoszących świadomość pracownika.

W związku z pojawiającymi się zagrożeniami wynikającymi z rozwoju technologicznego administrator zobowiązuje się do cyklicznego szacowania ryzyka związanego z procesami przetwarzania danych osobowych.

5. ZASADY PRZETWARZANIA DANYCH

Każdy upoważniony do przetwarzania danych osobowych w imieniu administratora jest zobowiązany do przestrzegania poniższych reguł:

1. Pracownikjest zobowiązany do przetwarzania danych osobowych zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą.
2. Pracownikprzed zebraniem danych osobowych od osoby fizycznej zobowiązany jest do umożliwienia zapoznania się z klauzulą informacyjną zawierającą wszelkie informacje dotyczące operacji przetwarzania oraz jej celach.
3. Pracownik czuwa by dane osobowe były zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami.
4. Jeżeli pozyskane dane osobowe mają być wykorzystane w innym celu niż cel, w którym zostały zebrane, przed takim dalszym przetwarzaniem pracownik zobowiązany jest do poinformowania o tym zamiarze osoby, których dane dotyczą oraz udzielenia im wszelkich innych stosownych informacji tj. o przysługujących prawach, nowym celu przetwarzania, podstawie przetwarzania.
5. Dane osobowe gromadzone przez pracownika muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do realizacji celów, w których są przetwarzane.
6. Pracownik odpowiada za zakres przetwarzanych danych. Zakazuje się gromadzenia danych zbędnych dla osiągnięcia określonego celu przetwarzania danych tj. nadmiarowych.
7. Pracownik nadzoruje by dane osobowe były prawidłowe i w razie konieczności je uaktualnia.
8. Pracownik winien podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane.

9. Administratorodpowiada za wprowadzenie procedur wyznaczających terminy przechowania danych (okresy retencji) lub procedur określających terminy okresowych przeglądów danych, a pracownik zobowiązany jest do ich przestrzegania.
10. Pracownik ma obowiązek przetwarzać dane w sposób zapewniający odpowiednie bezpieczeństwo w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem.
11. Jeżeli pracownik gromadzi dane na podstawie zgody to zobowiązany jest do prowadzenia ewidencji uzyskanych zgód od osób fizycznych, których dane dotyczą.

6. ORGANIZACJA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH

Podstawowymi zasadami przy tworzeniu struktur zarządzających bezpieczeństwem danych osobowych są:

1. bezwzględne oddzielenie funkcji zarządzających i kontrolnych od funkcji wykonawczych,
2. uniemożliwienie nadużyć i maksymalne ograniczenie błędów popełnianych przez pojedyncze osoby w ramach ich odpowiedzialności,
3. zapewnienie niezależności i obiektywizmu osób dokonujących audytu bezpieczeństwa, przy zapewnieniu gwarancji zachowania tajemnicy.

Wszystkie procesy bezpieczeństwa, a także organizacja bezpieczeństwa, muszą być zgodne z powyższymi zasadami. PBDO określa konkretną strukturę zarządzania danymi osobowymi oraz zapewnia bezpieczeństwo ich przetwarzania.

6.1. ODPOWIEDZIALNOŚĆ ADO

Administrator Danych Osobowych zapewnia, aby odpowiedzialność i uprawnienia osób pełniących istotną rolę w procesie ochrony danych osobowych w Organizacji zostały odpowiednio przydzielone i bezpośrednio zakomunikowane.

Do najważniejszych obowiązków Administratora Danych Osobowych należą:

1. sprawowanie nadzoru nad bezpieczeństwem oraz przetwarzaniem danych osobowych w Organizacji,
2. zapewnienie środków technicznych i organizacyjnych przetwarzania danych osobowych z uwzględnieniem przede wszystkim zmian w obowiązującym prawie, organizacji administratora oraz technik zabezpieczenia informacji w tym danych osobowych,
3. wprowadzenie w Organizacji procedur zapewniających wysoki poziom zabezpieczenia ochrony przetwarzanych informacji,
4. upoważnianie oraz odwoływanie upoważnień poszczególnych osób do przetwarzania danych osobowych w określonym indywidualnie zakresie, odpowiadającym zakresowi obowiązków,
5. wyznaczanie Administratora Systemu Informatycznego oraz określenie zakresu jego zadań i czynności;

6. wyznaczanie osoby odpowiedzialnej za prowadzenie rejestru osób upoważnionych: do przetwarzania danych osobowych, posiadających dostęp do zasobów sieci informatycznej Organizacji.
7. wyznaczanie osoby odpowiedzialnej za prowadzenie rejestru umów powierzenia danych osobowych, rejestru czynności przetwarzania danych osobowych, rejestru kategorii czynności przetwarzania, rejestru incydentów oraz rejestru umów powierzenia.
8. wyznaczanie osoby odpowiedzialnej za prowadzenie rejestru realizacji praw osób, których dane dotyczą,
9. podejmowanie odpowiednich działań w przypadku naruszenia lub podejrzenia naruszenia procedur bezpiecznego przetwarzania danych osobowych, w tym m.in. zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu oraz zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych,
10. podejmowanie odpowiednich działań w przypadku naruszenia lub podejrzenia naruszenia bezpieczeństwa informacji w tym m.in. zgłaszanie naruszenia bezpieczeństwa informacji do Zespołu CERT Polska,
11. zapewnianie prowadzenia szkoleń w Organizacji lub podejmowanie innych działań w celu podnoszenia kwalifikacji swoich pracowników w zakresie ochrony danych i bezpiecznego przetwarzania danych osobowych,
12. zapewnienie możliwości zapoznania się pracowników z obowiązującymi w przepisami oraz przyjętymi w Organizacji procedurami dotyczącymi bezpiecznego przetwarzania danych osobowych,
13. zlecanie okresowego szacowania ryzyka zagrożeń dla procesów przetwarzania danych osobowych,
14. zlecanie okresowej oceny skutków dla ochrony danych osobowych,
15. dokonywanie przeglądu oraz uaktualniania środków organizacyjnych i technicznych zastosowanych w Organizacji w tym zapewnienie okresowych audytów wewnętrznych PBDO,
16. dbanie o ciągłe doskonalenie systemu ochrony danych osobowych.

6.2. ODPOWIEDZIALNOŚĆ ASI

Administrator Systemów Informatycznych nadzoruje cały system informatyczny, zainstalowane oprogramowanie, aktualność zabezpieczeń oprogramowania służącego do przetwarzania informacji w tym danych osobowych. W przypadku braku powołania ASI jego odpowiedzialność spoczywa na **Administratorze.**

Do zakresu obowiązków ASI należy:

1. zarządzanie systemami informatycznymi oraz przeciwdziałanie dostępowi osób niepowołanych do systemów informatycznych,
2. nadawanie pracownikom uprawnień dostępu do danych w systemach informatycznych wprowadzonych w Organizacji poprzez:
   a. tworzenie kont użytkowników w systemach informatycznych,
   b. przypisywanie do kont startowych haseł uwierzytelniających użytkowników tych kont,
   c. resetowanie utraconych haseł i nadawanie nowych.

3. podejmowanie niezwłocznych działań w sytuacji utraty uprawnień do systemu poprzez usuwanie kont i uprawnień dla kont osób, które utraciły uprawnienia,
4. zarządzanie hasłami użytkowników i nadzór nad przestrzeganiem procedur określających częstotliwość ich zmiany,
5. wprowadzenie procedury awaryjnego odtwarzania systemu informatycznego i sprawowanie nadzoru nad hasłem Administratora,
6. prowadzenie i bieżąca aktualizacja rejestru/ewidencji stosowanych programów oraz sprzętu komputerowego wraz z ich konfiguracją,
7. zabezpieczenie systemów przetwarzania danych osobowych, poprzez instalację programów antywirusowych,
8. planowanie i wykonywanie zadań związanych z tworzeniem kopii bezpieczeństwa systemów i danych,
9. wprowadzenie procedury testowania wykonanych kopii zapasowych pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego w środowisku neutralnym,
10. prowadzenie działań konserwacyjnych w systemie oraz systematyczne aktualizowanie oprogramowania systemowego, aplikacyjnego i ochronnego,
11. monitorowanie stanu środowiska IT, stanu sprzętu IT i wykorzystywanego oprogramowania oraz aktywności sieciowej użytkowników,
12. kontrola przepływu informacji pomiędzy systemami informatycznym a siecią publiczną oraz kontrola działań inicjowanych z sieci publicznej a systemem informatycznym,
13. sprawowanie nadzoru nad wykonywaniem napraw, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe,
14. zapewnienie bezawaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych osobowych,
15. zapewnienie okresowej analizy logów systemowych,
16. prowadzenie szkoleń dla użytkowników systemu informatycznego dotyczących bezpiecznej pracy w systemie,
17. planowanie inwestycji oraz dostaw i usług niezbędnych dla utrzymania i rozwoju środowiska IT w Organizacji.

6.3. ODPOWIEDZIALNOŚĆ IOD

Inspektor Ochrony Danych realizuje zadania w zakresie nadzoru nad przestrzeganiem zasad ochrony danych osobowych obowiązujących w Ośrodku Pomocy Społecznej w Jeziorzanach.

Wewnętrzne obowiązki IOD:

1. monitorowanie przestrzegania przepisów prawa o ochronie danych oraz polityk i procedur przyjętych przez Administratora w dziedzinie ochrony danych osobowych,
2. informowanie Administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o spoczywających na nich obowiązkach,

3. aktualizacja oraz bieżący nadzór nad dokumentacją wprowadzoną w Organizacji w tym, między innymi nad:
   a. dokumentacją opisującą sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych,
   b. dokumentacją pracowniczą związaną z przetwarzaniem danych osobowych (upoważnienie do przetwarzania danych osobowych oraz rejestry osób upoważnionych do przetwarzania danych osobowych),
   c. oświadczeniami pracowników o zapoznaniu się z obowiązującymi procedurami i zachowaniu poufności,
4. zatwierdzanie wzorów dokumentów, w tym również projektów umów powierzenia danych osobowych przygotowywanych przez pracowników Administratora oraz otrzymanych bezpośrednio od kontrahentów,
5. nadzorowanie prowadzenia rejestrów upoważnień do przetwarzania danych osobowych, umów powierzenia, incydentów, czynności oraz kategorii czynności przetwarzania, a także realizacji praw osób, których dane dotyczą,
6. prowadzenie działań zwiększających świadomość pracowników Organizacji poprzez prowadzenie cyklicznych szkoleń personelu uczestniczącego w operacjach przetwarzania,
7. udzielanie odpowiedzi na bieżące pytania i wątpliwości z zakresu ochrony danych osobowych kierowane na dedykowany adres poczty elektronicznej przez pracowników Organizacji,
8. przeprowadzanie audytów w zakresie przestrzegania przepisów dotyczących ochrony danych osobowych i przyjętych przez administratora procedur,
9. nadzorowanie oraz podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń lub podejrzenia naruszenia,
10. udzielanie na żądanie administratora zaleceń co do oceny skutków dla ochrony danych.

Zewnętrzne obowiązki IOD:

1. współpraca z organem nadzorczym,
2. pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami,
3. w stosownych przypadkach prowadzenie konsultacji z organem nadzorczym we wszelkich innych sprawach niż wynikające z art. 36 RODO,
4. zapewnienie kontaktu dla osób, których dane dotyczą.

6.4. Odpowiedzialność Pracowników

Każdy **Pracownik**Szkoły w Przytocznie, zobowiązany jest do:

1. zapoznania się z wprowadzonymi przez Administratora procedurami w tym zwłaszcza PBDO, instrukcją postępowania w sytuacji naruszenia bezpieczeństwa ochrony danych osobowych oraz procedurą realizacji praw osób, których dane dotyczą i postępowania zgodnie z nimi,

2. przetwarzania danych osobowych wyłącznie w zakresie ustalonym indywidualnie przez administratora w upoważnieniu i tylko w celu wykonywania nałożonych na niego obowiązków,
3. brania czynnego udziału w szkoleniach dotyczących bezpieczeństwa informacji, ochrony danych osobowych oraz bezpiecznej pracy w systemie IT,
4. w sytuacji pobierania danych osobowych od klientów/interesantów Organizacji zapewniania możliwości zapoznania się osoby, której dane dotyczą z klauzulą informacyjną,
5. stosowania określonych przez ADO, procedur i środków mających na celu zabezpieczenie informacji przed ich udostępnieniem osobom nieupoważnionym,
6. w związku z brakiem mechanizmu automatycznej zmiany hasła, każdy pracownik zobowiązany jest do stosowania procedury zmiany i ustanawiania haseł zawartej w niniejszym dokumencie,
7. zachowania w tajemnicy informacji w tym danych osobowych oraz informacji o sposobach ich zabezpieczania, przy czym przestrzeganie tajemnicy obowiązuje przez cały okres zatrudnienia u ADO, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji,
8. ochrony informacji oraz danych osobowych przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem.

7. PROCEDURAREALIZACJI OBOWIĄZKU INFORMACYJNEGO

W celu wypełnienia obowiązku informacyjnego wprowadza się następujące reguły:

1. Przed podjęciem działań z danymi osobowymi należy umożliwić osobie, której dane dotyczą, zapoznanie się z klauzulą informacyjną.
2. Informowanie powinno się dokonać bez prośby zainteresowanego.
3. Obowiązek informacyjny spełnia się poprzez pozostawienie treści klauzuli w miejscu dostępnym dla osób fizycznych (np. tablica informacyjna znajdująca się przy wejściu do Szkoły), od których pozyskiwane są dane osobowe oraz poprzez zamieszczenie treści klauzuli informacyjnej na stronie internetowej w zakładce RODO.
4. Klauzule informacyjne w formie skróconej stosuje się również w treści podania o przyjęcie do Szkoły Podstawowej w Przytoczenie.
5. Treść klauzuli należy skonsultować każdorazowo z inspektorem w celu potwierdzenia zgodności z obowiązującymi przepisami prawa.
6. Treść klauzuli informacyjnej jest zamieszczana w regulaminach konkursów i innych wydarzeń kulturalnych.
7. Treść każdej nowej, tworzonej przez pracownika klauzuli należy skonsultować każdorazowo z inspektorem w celu potwierdzenia zgodności z obowiązującymi przepisami prawa.

8. PROCEDURA OBSŁUGI PRAW WYNIKAJĄCYCH Z RODO

Obsługa uprawnień, które zostały zawarte w przepisach rozdziału III RODO stanowi gwarancję poszanowania praw i wolności osób fizycznych i jako podstawowe prawo realizowane jest poprzez wypełnienie poniższych reguł.

1. Administrator gwarantuje by wszelkie przekazywane informacje były sformułowane w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.
2. Administrator w miejscu ogólnodostępnym (w tym na stronie internetowej w zakładce RODO) zamieszcza informację, do kogo i w jakiej formie należy kierować żądanie realizacji praw.
3. Realizacja żądania osób fizycznych w zakresie realizacji praw wynikających z RODO (a w szczególności wskazanych w klauzuli informacyjnej) należy do obowiązków inspektora.
4. Zgłoszenie żądania osoby fizycznej powinno zawierać:
   a. imię, nazwisko osoby której zgłoszenie dotyczy,
   b. opis zgłaszanego żądania wraz ze wskazaniem ewentualnych zastrzeżeń,
   c. podpis osoby zgłaszającej żądanie w przypadku zgłoszeń pisemnych,
   d. pełnomocnictwo jeśli w imieniu zgłaszającego żądanie kieruje pełnomocnik,
   e. informacje o preferowanej formie odpowiedzi, jeżeli kanał odpowiedzi ma być inny niż zgłoszone żądanie.
5. Pracownik może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby składającej żądanie w przypadku, gdy ma co do niej uzasadnione wątpliwości.
6. Jeżeli zgłoszenie nastąpiło w formie ustnej, pracownik zobowiązany jest do sporządzenia notatki, zawierającej dane o których mowa w punkcie 4.
7. W przypadku skierowania żądania realizacji praw bezpośrednio pracownikowi, zobowiązany jest on najpóźniej w terminie 7 dni przesłać treść żądania inspektorowi.
8. Pracownik jest zobowiązany do udzielania informacji inspektorowi niezbędnych do realizacji żądania osoby fizycznej.
9. Wprowadza się obowiązek rejestracji każdego wniosku o realizację praw osób wpływający bezpośrednio do siedziby Szkoły lub na skrzynki mailowe pracowników, poprzez wpisanie do rejestru obsługi praw osób fizycznych wraz ze wskazaniem daty otrzymania wniosku.

9. ŚRODKI ORGANIZACYJNE I TECHNICZNE

Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża niniejsze środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z rozporządzeniem RODO i aby móc to wykazać.

9.1. ŚRODKI ORGANIZACYJNE

1. Opracowano i wdrożono PolitykęBezpieczeństwa Danych Osobowych.

2. Opracowano i wdrożono procedurę postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych.
3. Powołano Inspektora Ochrony Danych.
4. Zastosowano upoważnienia adekwatne do zakresu przetwarzania zgodnego z zajmowanym stanowiskiem służbowym.
5. Upoważnienia do przetwarzania danych pracowników mających dostęp do pomieszczeń szczególnie chronionych (archiwum),akt osobowych oraz danych szczególnej kategorii, powinny zawierać szczegółowe umocowania.
6. Wprowadzono rejestr upoważnień pracowników.
7. Wprowadzono obowiązek odbierania oświadczenia pracowników o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych wraz z obowiązkiem zachowania poufności wszelkich informacji uzyskanych w ramach wykonywanych obowiązków, również po ustaniu zatrudnienia.
8. Wprowadzono obowiązek bezpiecznego udostępniania danych osobowych podmiotom zewnętrznym poprzez zawieranie umów powierzenia (lub innych instrumentów prawnych) oraz zobowiązania do zachowania danych osobowych w poufności.
9. Wprowadzono obowiązek cyklicznego szkolenia pracowników z obowiązujących przepisów dotyczących ochrony danych osobowych jak i wewnętrznych regulacji bezpieczeństwa danych osobowych stosowanych przez administratora.
10. Wprowadzono obowiązek cyklicznego szkolenia pracowników w zakresie bezpiecznej obsługi urządzeń i programów służących do przetwarzania danych osobowych.
11. Zakazano pracownikom dorabiania kluczy do budynku, w którym znajduje się siedziba Szkoły.
12. Zakazano pracownikom pozostawiania kluczy w zamkach drzwi i szaf.

Zabezpieczenia we własnym zakresie

Pracownik zobowiązany jest do przestrzegania zasady czystego biurka i ekranu w szczególności poprzez:

1. Schowanie wszystkich dokumentów, nośników zawierających dane osobowe w miejsce niedostępne dla innych osób w trakcie pracy, w trakcie sprzątania pomieszczeń oraz po zakończeniu pracy.
2. Dbanie o porządek, poprzez pozostawienie na stanowisku pracy wyłącznie dokumentów, które są niezbędne do wykonywania czynności służbowych.
3. Blokowanie dostępu lub wylogowanie się z systemu przy czasowym opuszczaniu stanowiska pracy.
4. Zamknięcie wszystkich aplikacji, wylogowanie się z systemu i wyłączenie komputera po zakończeniu pracy.
5. Zachowanie porządku na pulpicie komputera poprzez cotygodniowy przegląd połączony z porządkowaniem oraz usuwaniem zbędnych folderów i plików znajdujących się na pulpicie systemu.

Pracownik zobowiązanyjest również do:

1. Nieprzechowywania plików prywatnych (w tym poczty prywatnej, zdjęć, dokumentów prywatnych, skanówitp.) na powierzonym sprzęcie elektronicznym tj. komputerach, telefonach, aparatach fotograficznych, dyskach zewnętrznych.
2. Wylogowania się z systemu operacyjnego lub używanego programu przy każdorazowym odejściu od komputera.
3. Pilnego strzeżenia dokumentów w formie papierowej, płyt CD/DVD, pamięci i komputerów przenośnych, oraz wszelkich innych urządzeń przenośnych, na których mogą znajdować się dane osobowe.
4. Nieużywania powtórnie dokumentów zadrukowanych jednostronnie.
5. Niezapisywania hasła wymaganego do uwierzytelnienia się w systemie informatycznym na papierze lub innym nośniku.
6. Nieudostępniania hasła wymaganego do uwierzytelnienia się do systemu informatycznego innym osobom, w tym zarówno pracownikom organizacji jak i osobom postronnym.
7. Dbania o prawidłową wentylację komputerów (zabrania się zasłaniania kratek wentylatorów meblami, zasłonami lub stawiania komputerów tuż przy ścianie).
8. Niepodłączania do listew podtrzymujących napięcie przeznaczonych dla sprzętu komputerowego innych urządzeń, szczególnie tych łatwo powodujących spięcia (np. grzejniki, czajniki, wentylatory).
9. Powstrzymywania się od samodzielnej ingerencji w oprogramowanie i konfigurację powierzonego sprzętu, nawet gdy z pozoru mogłoby to usprawnić pracę lub podnieść poziom bezpieczeństwa danych.
10. Przestrzegania przez pracowników swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła oraz stosowania się do zaleceń osoby nadzorującej system informatyczny.
11. Ustawiania monitora w sposób uniemożliwiający przeglądanie wyświetlanych treści osobom nieupoważnionym.
12. Niszczenia w niszczarce lub chowania do szaf zamykanych na klucz wszelkich wydruków zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończeniu dnia pracy.
13. Zamykania okien w razie opadów czy innych zjawisk atmosferycznych, które mogą zagrozić bezpieczeństwu danych osobowych.
14. Zamykania szafek z dokumentami i drzwi na klucz po zakończeniu pracy w danym dniu.

9.2. ŚRODKI TECHNICZNE

1. Dane osobowe przechowywane są w uporządkowanych zbiorach tj.skoroszytach, segregatorach, itp.
2. Zbiory danych osobowych przechowywane powinny być w pomieszczeniach zabezpieczonych drzwiami zamykanymi na klucz.
3. Pomieszczenia, w których przetwarza się dane są zabezpieczone przed skutkami pożaru za pomocą wolnostojącej gaśnicy.
4. Zaleca się, aby zbiory danych osobowych przechowywane były w pomieszczeniach, w których okna zabezpieczone są za pomocą krat, rolet lub folii antywłamaniowej.
5. Szkoła wyposażona jest w zabezpieczenia alarmowe.

6. W szkole znajduje się również monitoring.

Dokumenty papierowe

1. Dane w formie papierowej przechowywane powinny być w zamkniętych, metalowych jak i niemetalowych szafkach i szufladach.
2. Kopie zapasowe danych osobowych w formie papierowej przechowywane powinny być w zamkniętych, metalowych bądź niemetalowych szafkach i szufladach.
3. Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów, uniemożliwiających ich odtworzenie.

Dokumenty elektroniczne

1. Dokumenty elektroniczne przechowywane powinny być na zabezpieczonych urządzeniach końcowych, serwerach, urządzeniach przenośnych.
2. Zaleca się stosowanie urządzeń typu UPS chroniących system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania.
3. Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
4. Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity, w postaci programów antywirusowych.
5. Zaleca się stosowanie systemu Firewall do ochrony dostępu do sieci komputerowej.
6. Zaleca się stosowanie środków technicznych pozwalających na rejestrację i kontrolę zmian wykonywanych na danych osobowych w systemie informatycznym.
7. Zastosowano środki umożliwiające określenie oraz ograniczenie i zmianę prawa dostępu do wskazanego zakresu danych osobowych przetwarzanych w systemie informatycznym.
8. Zaleca się stosowanie mechanizmu wymuszającego okresową zmianę haseł dostępu do systemu służącego do przetwarzania danych.
9. W sytuacji braku możliwości stosowania mechanizmu wymuszającego zmianę haseł dostępu do systemu informatycznego, w którym przetwarzane są dane osobowe,administrator wprowadza procedurę ustanawiania i zmiany hasła.
10. Zaleca się zainstalowanie wygaszaczy ekranów na stanowiskach, na których przetwarzane są dane osobowe.
11. Zaleca się stosowanie mechanizmu automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika, poprzez automatyczne wylogowanie się z systemu.
12. Zaleca się stosowanie mechanizmu tworzenia kopii zapasowych z systemu informatycznego.
13. Kopie zapasowe przechowywane winny być na dysku zewnętrznym, innych urządzeniach przenośnych, które przechowywane powinny być w metalowych zamykanych szafach

14. Dokumenty elektroniczne z nośników przenośnych niebędących kopiami zapasowymi po wprowadzeniu do systemu informatycznego są trwale usuwane z tych nośników przez fizyczne zniszczenie (np. płyty CD-ROM) lub usunięcie danych programem trwale usuwającym pliki.

10. PROCEDURA DOSTĘPU DO POMIESZCZEŃ SZCZEGÓLNIE CHRONIONYCH

1. Pracownikom, którzy zgodnie z pełnioną funkcją lub zakresem obowiązków maja dostęp do pomieszczeń szczególnie chronionych tj. pomieszczenia archiwum, atakże do akt osobowych pracowników, w upoważnieniu do przetwarzania danych określa się w sposób szczegółowy zakres czynności, które wykonują.
2. W rejestrze upoważnień odnotowuje się zakres udzielonego umocowania.
3. Administrator lub osoba upoważniona prowadzi rejestr wydanych kluczy dostępu do pomieszczeń szczególnie chronionych.
4. Pracownik posiadający dostęp do pomieszczeń szczególnie chronionych zobowiązany jest do:
   a. przechowywania kluczy dostępu w sposób bezpieczny,
   b. przebywania w pomieszczeniu bez udziału osób nieupoważnionych,
   c. każdorazowego upewnienia się, że po opuszczeniu pomieszczenia jest ono zamknięte w sposób prawidłowy.

11. STRATEGIE OCHRONY DANYCH W FAZIE PROJEKTOWANIA I FAZIE DOMYŚLNEJ

Uwzględniając koncepcje ochrony danych w fazie projektowania administrator już podczas planowania systemu ochrony danych osobowych wdraża takie środki, by od samego początku chronić przetwarzane dane oraz prywatność osób, których dane dotyczą. W tym celu administrator wprowadza następujące reguły:

1. Każde planowane przedsięwzięcie w Szkole musi zostać poprzedzone analizą wpływu planowanych zmian na bezpieczeństwo danych osobowych.
2. Jako planowane procesy, w których administrator zobowiązany jest wziąć pod uwagę bezpieczeństwo danych osobowych wyróżnia się w szczególności:
   a. przystąpienie do projektów realizowanych ze środków europejskich,
   b. zakup nowego systemu bądź aktualizacja obecnego systemu informatycznego,
   c. zakup nowych systemów ochrony fizycznej (systemy alarmowe, monitoring) jak i systemów bezpieczeństwa IT,
   d. wprowadzenie nowych technologii organizacyjnych,
   e. rozwój organizacji poprzez tworzenie nowych działów, oddziałów itp.,
   f. restrukturyzacja Szkoły,
   g. zatrudnienie nowych pracowników,
   h. zmiana celów przetwarzania.

3. **ADMINISTRATOR BĄDŹ WYZNACZONY PRZEZ NIEGO PRACOWNIK ZOBOWIĄZANYJEST NA ETAPIE PLANOWANIA PROCESU WDROŻYĆ**odpowiedne środki techniczne i organizacyjne zapewniające bezpieczeństwo danych osobowych, a w szczególności zobowiązany jest do stosowania:
    a. pseudonimizacji,
    b. szyfrowania,
    c. minimalizacji danych,
    d. prawidłowości i przejrzystości zbieranych danych,
    e. ograniczenia do niezbędnej ilości zbieranych danych osobowych,
    f. ograniczenia do niezbędnego zakresu przetwarzania danych,
    g. ograniczenia do niezbędnego okresu przechowywania danych,
    h. technik zapewniających odpowiedni poziom dostępności.
4. Na etapie planowania procesów administrator bądź wyznaczony przez niego pracownik zobowiązany jest również:
    a. rozważyć na jakiej przesłance legalności zostanie oparty proces przetwarzania danych, przy czym jeśli będzie to zgoda należy przygotować odpowiednio wcześniej jej treść oraz ustalić sposób jej zbierania i odwołania;
    b. opracować treść oraz sposób przekazania klauzul zawierających obowiązek informacyjny;
    c. administrator zobowiązany jest poinformować IOD o wszystkich planowanych przedsięwzięciach oraz umożliwić mu podjęcie wszelkich koniecznych działań niezbędnych do zapewnienia bezpieczeństwa przetwarzania danych osobowych;
    d. przy wyborze kontrahenta, partnera biznesowego, kooperanta – rozważyć, który z nich w najpełniejszy sposób realizuje zasadę bezpiecznego przetwarzania danych osobowych;
    e. przy wyborze nowego systemu informatycznego, sytemu ochrony bądź wprowadzaniu zmian technologicznych, kierować się również zapewnieniami producenta dotyczącymi bezpieczeństwa przetwarzania danych osobowych oraz dostosowaniu do wymogów RODO.

Administrator świadomy jest, że zasada ochrony danych w fazie projektowania nie ogranicza się jedynie do procesu planowania, gdyż z przepisów RODO jasno wynika, że ocena zgodności z przepisami dotyczy również etapu realizacji procesu. Wobec powyższego administrator wprowadza zasadę regularnego przeglądu funkcjonowania procesów przetwarzania danych oraz jego elementów składowych poprzez:

1. Audyty systemu informatycznego (uwzględniającego zasady cyberbezpieczeństwa jak i adekwatnego przetwarzanych w systemach danych osobowych).
2. Sprawdzenie poprawności metod zbierania i przechowywania zgód na przetwarzanie danych osobowych (w tym zasadność ich zbierania, możliwość ich wycofania oraz treści samej zgody).
3. Sprawdzenie realizacji wypełniania obowiązków informacyjnych.
4. Audyty procesów przetwarzania danych osobowych pod względem adekwatności ich przetwarzania oraz ograniczenia do niezbędnej ilości zbieranych danych. W tym celu administrator zobowiązuje:
    a. pracowników odpowiedzialnych za prowadzenie rekrutacji – do przestrzegania procedury rekrutacyjnej określonej w niniejszej Polityce Bezpieczeństwa,

b. pracowników odpowiedzialnych za prowadzenie projektów realizowanych z funduszy unijnych – do czuwania nad realizacją obowiązków, które spoczywają na Szkole jako administratorze danych przetwarzanych w projekcie (np. w zakresie spełnienia obowiązku informacyjnego),
c. pracowników do wykonywania cyklicznej inwentaryzacji zasobów poczty służbowej i usuwania wiadomości, które utraciły znaczenia dla wypełniania obowiązków służbowych,
d. pracowników upoważnionych do obsługi monitoringu do dokonania analizy obszaru, który obejmie system monitoringu wizyjnego do upewnienia się, czy swoim działaniem nie narusza on godności oraz innych dóbr osób objętych rejestracją.

Realizując zasadę ochrony prywatności i bezpieczeństwa jako właściwości domyślnych *(pivacy by default)* administrator bądź pracownik nadzorujący pracę systemu informatycznego zobowiązany jest do:

1. Konfiguracji systemu informatycznego w taki sposób, aby od momentu jego uruchomienia system zapewniał odpowiedni poziom ochrony według ustawień domyślnych.
2. Konfiguracja systemu informatycznego powinna zapewniać:
   a. aby system nie pozwalał na zbieranie nadmiernej ilości danych osobowych,
   b. aby system wskazywał bądź umożliwiał wprowadzenie danych dotyczących okresu przechowywania danych,
   c. aby system umożliwiał dostęp do danych jedynie upoważnionym w danym zakresie pracownikom.
3. Wprowadzenia zakazu dokonywania jakichkolwiek samodzielnych zmian przez pracowników w ustawieniach fabrycznych komputerów oraz w ustawieniach systemu informatycznego.

12. SZACOWANIE RYZYKA DLA DANYCH OSOBOWYCH I OCENA SKUTKÓW

Administrator powinien przeprowadzić ogólną ocenę ryzyka oraz szczegółową ocenę ryzyka, ukierunkowaną naskutki w zakresie naruszenia praw lub wolności osób fizycznych (tzw. ocenę skutków dla ochrony danych).

Ogólną ocenę ryzyka w zakresie bezpieczeństwa przetwarzania informacji, w tym danych osobowych, należy przeprowadzić, biorąc pod uwagę potencjalne negatywne skutki (straty materialne i niematerialne) zarówno dla Szkoły, jak i osób, których dane dotyczą. Ocenę skutków dla ochrony danych przeprowadza się natomiast wtedy, gdy istnieje wysokie ryzyko naruszenia praw i wolności osób, których dane dotyczą.

12.1. IDENTYFIKACJA I KLASYFIKACJA AKTYWÓW ORGANIZACJI

Zarządzanie aktywami, jest realizowane w celu zapewnienia wymaganego poziomu bezpieczeństwa ochrony danych osobowych. Należy zidentyfikować i sklasyfikować wszystkie aktywa organizacji, które wiążą się z przetwarzaniem danych osobowych. Aktywa to wszystko, co ma wartość dla Szkoły. Rozumieć przez to należy zarówno informacje, w tym dane osobowe, jak i inne zasoby organizacji, takie jak: posiadana wiedza, personel, sprzęt, oprogramowanie oraz inne środki techniczne i organizacyjne związane z przetwarzaniem danych osobowych. Identyfikacja i klasyfikacja aktywów powinna być przeprowadzana na takim poziomie szczegółowości, aby zapewnić niezbędne informacje wymagane w procesie szacowania ryzyka.

Posługując się schematem zaczerpniętym z normy ISO/IEC 27005, aktywa te można podzielić na podstawowe i wspierające. Aktywa podstawowe to procesy i działania biznesowe oraz informacje. Aktywa wspierające to sprzęt,oprogramowanie,sieć,personel,siedziba,struktura organizacyjna.Aktywa są chronione ze względu na wymagania wynikające zarówno z przepisów prawa oraz regulacji wewnętrznych, z których wynika ochrona właściwych aktywów, a także z zasad bezpieczeństwa wymaganych przez Szkołę,postanowień umów zawieranych pomiędzy organizacją, a podmiotami zewnętrznym, czy z warunków licencji.

12.2. ZASADY ZARZĄDZANIA AKTYWAMI

Zarządzanie aktywami w organizacjiodbywa się zgodnie z poniższymi zasadami:

1. Ustalenie odpowiedzialności za aktywa: należy określić właścicieli wszystkich aktywów oraz przydzieloną im odpowiedzialność za utrzymanie odpowiednich zabezpieczeń. Wdrożenie określonych zabezpieczeń może być delegowane przez właściciela aktywów, jednak pozostaje on nadal odpowiedzialny za adekwatną ochronę aktywów.
2. Identyfikacji aktywów: w wyniku identyfikacji aktywów powinno się uzyskać listę aktywów istotnych z punktu widzenia zarządzaniaryzykiem oraz listę procesów biznesowych, w których aktywa te są wykorzystywane. Kolejnym istotnym krokiem podczas identyfikacji aktywów jest określenie ich wartości.
3. Akceptowalnego użycia aktywów: w dokumentacji są określone i wdrażane przez administratora zasady dopuszczalnego korzystania z aktywów i zasobów związanych z przetwarzaniem danych osobowych.
4. Klasyfikacji aktywów (szczegółowy opis stosowanych zabezpieczeń): określona jest metoda oraz sposób klasyfikacji aktywów odzwierciedlający wymagania ich ochrony na odpowiednim poziomie.
5. Oznaczania aktywów: stosowane są regulacje wewnętrzne wyznaczające zasady oznaczanie aktywów informacji i postępowania z nimi.

12.3. SZACOWANIE RYZYKA

1. Szacowanie ryzyka ma na celu określenie, jakie potencjalne wydarzenia w zakresie naruszenia ochrony danych osobowych mogą mieć miejsce w organizacji(kiedy, gdzie, jak i dlaczego) i jak dotkliwe straty mogą wskutek naruszenia powstać. W ramach tego działania dla zidentyfikowanych procesów przetwarzania danych i występujących tam aktywów należy wskazać, przeanalizować i oszacować:
   a. występujące zagrożenia dla bezpieczeństwa przetwarzanych danych,
   b. zastosowane środki bezpieczeństwa,
   c. podatność przyjętych rozwiązań z uwzględnieniem zastosowanych środków bezpieczeństwa na urzeczywistnienie się zidentyfikowanych zagrożeń,
   d. potencjalne następstwa w przypadku zaistnienia określonych zagrożeń.
2. **PROCES ZARZĄDZANIA RYZYKIEM W BEZPIECZEŃSTWIE INFORMACJI REALIZUJE SIĘ ZGODNIE Z WYTYCZNYMI NORMY** PN-ISO/IEC 27005:2014.
3. Wszyscy pracownicy podczas realizacji zadań biorą pod uwagę ryzyka związane z bezpieczeństwem przetwarzania danych.

4. Administrator zobowiązany jest do:
   a. identyfikacji i klasyfikacji aktywów oraz zasobów informacyjnych na potrzeby analizyszacowania ryzyka,
   b. identyfikacji scenariuszy wykorzystania podatności na zagrożenie,
   c. szacowania strat dla zasobów użytych w realizacji procesów objętych przeglądem analizy ryzyka,
   d. wykonania oceny skutków zgodnie z art. 35 RODO dla operacji przetwarzania danych osobowych (jeżeli jest wymagana przepisami prawa),
   e. wykonania analizy szacowania ryzyka i przeprowadzenia oceny skutków zgodnie z art. 35 RODO, w przypadku wdrożenia nowej technologii (np. nowego systemu informatycznego) w organizacji, służącej do przetwarzania danych osobowych,
   f. w razie potrzeby po dokonaniu oceny skutków, przeprowadzenia zgodnie z art. 36 RODO konsultacji z Urzędem Ochrony Danych Osobowych w sytuacji, gdy administrator nie jest w stanie zminimalizować wysokiego ryzyka naruszenia praw lub wolności osób fizycznych.
5. Do zadań inspektora oraz pracownika nadzorującego system informatyczny należy:
   a. przygotowanie Procedury szacowania ryzyka,
   b. przygotowanie wykazu aktywów organizacji wraz z ich klasyfikacją,
   c. przeprowadzenie analizy szacowania ryzyka i przygotowanie raportu (wyników) szacowania ryzyka w Rejestrze ryzyka,
   d. przygotowanie planu postępowania z ryzykami,
   e. ewentualne konsultowanie oceny skutków i wsparcie administratora w jej wykonaniu.
6. Do zadań Administratora należy:
   a. zatwierdzenie wykazu aktywów Szkoły (informacyjnych),
   b. zatwierdzenie rejestru ryzyka organizacji,
   c. zatwierdzenie planów postępowania z ryzykami,
   a. przeprowadzenie i zatwierdzenie oceny skutków (jeżeli została wykonana).

Ocena skutków jest wykonywana zgodnie z metodologią wskazaną przez Urząd Ochrony Danych Osobowych.

13. ORGANIZACJA PRZETWARZANIA DANYCH OSOBOWYCH (WEWNĄTRZ SZKOŁY)

Organizacja realizując niniejszą Politykę Bezpieczeństwa w zakresie udostępniania danych osobowych w ramach własnej (wewnętrznej) struktury, zezwala na ich przetwarzanie w systemie informatycznym lub w wersji papierowej wyłącznie pracownikom (w niektórych przypadkach praktykantom, stażystom). Zezwolenie na przetwarzanie danych osobowych realizowane jest poprzez nadanie stosownego upoważnienia.

13.1. ZASADY NADAWANIA UPOWAŻNIENIA DO PRZETWARZANIA DANYCH

1. Upoważnienie do przetwarzania danych osobowych wydawane jest każdemu z pracowników osobno, w zakresie adekwatnym do pełnionych obowiązków służbowych.

2. Upoważnienia wydawane są na czas określony i ustają po terminie na jaki zostały wydane.
3. Od pracownika odbiera się oświadczenia o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych oraz wewnętrznymi regulacjami bezpieczeństwa danych osobowych administratora.
4. Pracownika zobowiązuje się do zachowania w poufności wszelkich informacji uzyskanych w ramach wykonywanych obowiązków, również po ustaniu zatrudnienia.
5. Fakt nadawania upoważnienia jest odnotowywany w rejestrze upoważnień, w tym również w rejestrze prowadzonym w formie elektronicznej.
6. Ewidencjaosób upoważnionych do przetwarzania danych podlega przeglądowi każdorazowo z przeglądem organizacyjnych i technicznych środków bezpieczeństwa, czyli nie rzadziej niż raz w roku.

13.2. ZASADY ODBIERANIA UPOWAŻNIEŃ DO PRZETWARZANIA DANYCH

Upoważnienie do przetwarzania danych w określonych sytuacjach może być odebrane pracownikowi przez administratora:

1. Gdy pracownik posługuje się danymi w sposób niewłaściwy, przetwarza je w zakresie wykraczającym poza nadane upoważnienie.
2. Rażącego naruszenia zasad Polityki Bezpieczeństwa.
3. Rozwiązania stosunku pracy bądź innego stosunku prawnego łączącego osobę upoważnioną z administratorem.
4. Zmiany stanowiska pracy, na stanowisko uzasadniające konieczność posiadania upoważnienia w innym zakresie.

W sytuacji odebrania upoważnienia do przetwarzania danych stosuje się niniejsze zasady:

1. Administrator lub osoba wyznaczona informuje pracownika o przebiegu przekazywania obowiązków i rozliczeniu się tej osoby z pobranego sprzętu, materiałów i dokumentów należących do pracodawcy według przyjętych procedur.
2. Osoba nadzorująca system informatyczny blokuje dostęp pracownika do poczty elektronicznej oraz systemu informatycznego.
3. Administrator lub osoba nadzorująca system informatyczny, zabezpiecza skrzynkę poczty elektronicznej, zasoby serwera lub dysku twardego przypisane do pracownika.
4. Po zablokowaniu dostępu do imiennej skrzynki poczty elektronicznej, osoba nadzorująca system informatyczny, zmienia ustawienia skrzynki poprzez ustawienie przekierowania poczty przychodzącej na adres osoby przejmującej obowiązki, a także, o ile to możliwe, uruchomienie komunikatu w formie (autorespondera) automatycznej odpowiedzi/informacji do nadawcy o przekazaniu niniejszej korespondencji do innego odbiorcy.
5. Pracownikowi odbiera się możliwość dostępu do budynków i pomieszczeń należących do organizacji (klucze).
6. W przypadku zmiany stanowiska pracy powyższe reguły stosuje się odpowiednio.
7. Fakt odebrania upoważnienia odnotowuje się w rejestrze upoważnień wraz ze wskazaniem daty.

14. ORGANIZACJA PRZETWARZANIA DANYCH OSOBOWYCH (NAZEWNĄTRZ SZKOŁY)

Udostępnianie danych osobowych może nastąpić wyłącznie za zgodąadministratora, dane osobowe mogą być udostępniane w następujących przypadkach:

a. na podstawie wniosku od podmiotu uprawnionego do otrzymywania danych osobowych na podstawie przepisów,
b. na podstawie umowy z innym podmiotem, w ramach której istnieje konieczność udostępnienia danych,
c. na podstawie wniosku osoby, której dane dotyczą.

14.1. UDOSTĘPNIANIE DANYCH

1. W przypadku udostępniania danych osobowych na zewnątrz administrator dokonuje oceny sposobu przygotowania danych, a także analizuje sposób i prawidłowość przygotowania danych do udostępnienia.
2. Odmowa udostępnienia danych osobowych następuje wówczas, gdy spowodowałoby to istotne naruszenia dóbr osobistych osób, których dane dotyczą, lub innych osób oraz jeżeli dane osobowe nie mają istotnego związku ze wskazanymi we wniosku motywami działania wnioskodawcy.
3. Informacje zawierające dane osobowe powinny być przekazywane uprawnionym podmiotom lub osobom za potwierdzeniem odbioru np. e-mailem, listem poleconym za potwierdzeniem nadania lub innym bezpiecznym sposobem, pozwalającym na udokumentowanie spełnienia prawa.
4. Udostępniając dane osobowe innym podmiotom należy odnotowywać informacje o udostępnieniu bezpośrednio w systemie informatycznym, z którego udostępniono dane lub w inny zatwierdzony sposób.
5. Administratorprowadzi ewidencję podmiotów, którym udostępniono przetwarzane dane. Odnotować należy: informacje o odbiorcy danych, dacie i zakresie udostępnionych danych osobowych.

14.2. POWIERZANIE PRZETWARZANIA DANYCH OSOBOWYCH

Powierzenie przetwarzania danych osobowych może mieć miejsce wyłącznie na podstawie pisemnej (w tym elektronicznej) umowy lub innego instrumentu prawnego, określającej w szczególności przedmiot i czas trwania przetwarzania oraz charakter i cel przetwarzania danych. Umowa musi określać również obowiązki
i zakres odpowiedzialności podmiotu, któremu powierzono przetwarzanie danych z tytułu niewykonania lub nienależytego wykonania umowy. Regulacje dotyczące sposobu przetwarzania danych oraz obowiązków ciążących na stronach umowy winny zawierać również zapisy dotyczące:

1. Zobowiązania o zachowaniu poufności przez podmiot przetwarzający oraz osoby biorące udział w przetwarzaniu.
2. Obsługi praw jednostki, w szczególności obowiązków informowania administratora o otrzymaniu zgłoszenia i sposobie jego realizacji.

3. Niezwłocznego zgłaszania administratorowi wszelkich podejrzeń o naruszeniu ochrony powierzonych danych.
4. Sposobu przekazania danych po zakończeniu trwania przetwarzania.
5. Realizacji uprawnień kontrolnych.
6. Dalszego powierzania danych przez podmiot przetwarzający.

Procedura zawarcia umowy powierzenia przetwarzania danych osobowych

1. Pracownik informuje administratora lub inspektora o potrzebie powierzenia danych osobowych do przetwarzania.
2. Inspektor w porozumieniu z pracownikiem przygotowuje projekt umowy powierzenia danych osobowych innemu podmiotowi.
3. Pracownik w projekcie umowy określa procesy przetwarzania powierzonych danych osobowych orazich zakres.
4. Sporządzony projekt umowy przedkładany jest administratorowi do podpisu.
5. Zawarta umowa powierzenia odnotowywana jest w rejestrze umów powierzenia.

15. PROCEDURA REKRUTACYJNA

Przetwarzanie danych osobowych kandydatów do pracy odbywa się z należytym poszanowaniem prawa do prywatności wobec czego wprowadza się następujące zasady przy prowadzeniu rekrutacji:

1. Administrator (lub pracownik odpowiedzialny za rekrutację) zamieszczając ogłoszenie rekrutacyjne zobowiązany jest do zawarcia w jego treści klauzuli informacyjnej dotyczącej przetwarzania danych osobowych kandydata oraz oświadczeń tj.:
   a. oświadczenia o wyrażeniu zgody na przetwarzanie danych osobowych zawartych w CV, liście motywacyjnym lub innych załączonych dokumentach (jeśli przekazane dane obejmują szczególne kategorie danych, bądź wykraczają poza dane, o których mowa w art. 22^1k.p.),
   b. oświadczenia o wyrażeniu zgody na przetwarzanie danych osobowych w celu wykorzystania ich w kolejnych rekrutacjach prowadzonych przez Szkołę – o ile w danym przypadku administrator zdecyduje o woli pozostawienia dokumentów rekrutacyjnych osób niewybranych na potrzeby przyszłych rekrutacji.
2. W przypadku braku zawarcia w dokumentach aplikacyjnych stosownej zgody z punktu 1 lit. a powyżej, pracownik kontaktuje się z kandydatem w celu odebrania stosownego oświadczenia o wyrażeniu zgody. Jeżeli pracownik nie uzyska oświadczenia, zobowiązany jest do usunięcia dokumentów aplikacyjnych w sposób trwały.
3. W przypadku braku zawarcia w dokumentach aplikacyjnych stosownej zgody z punktu 1 lit. b powyżej (o ile administrator żądał takiego oświadczenia w ogłoszeniu) i niezatrudnienia kandydata, administrator zobowiązany jest po zakończeniu rekrutacji do usunięciajego dokumentów aplikacyjnych w sposób trwały.

4. W przypadku wymagań wynikających z zapisów odpowiednich przepisów prawa, po zakończeniu procesu rekrutacji dokumenty zawierające dane osobowe kandydatów do pracy są archiwizowane zgodnie
z zapisami tych przepisów.
5. Pracownik odpowiedzialny za rekrutację przechowuje dokumenty aplikacyjne w miejscu zabezpieczonym przed dostępem osób nieuprawnionych.
6. Administrator określił czas w jakim dokumenty aplikacyjne są przechowywane, tj. 9 miesięcy. Po jego upływie dokumenty są niszczone w sposób trwały – stosując procedurę niszczenia dokumentów i utylizacji nośników.

16. SZKOLENIA

Kompetencje oraz świadomość personelu mają wpływ na zgodność osiąganych wyników pracy z wymaganiami dotyczącymi zapewnienia bezpiecznego przetwarzania danych osobowych. W tym celu Szkoła zapewnia, aby pracownicy mieli możliwość czynnego udziału w szkoleniach z zakresu bezpiecznego przetwarzania danych osobowych.

16.1. SZKOLENIE WSTĘPNE

Szkolenie wstępne, dla nowoprzyjętych pracowników Szkoły, odbywa się przed udostępnieniem stanowiska pracy i przeprowadzane jest przez administratora bądź osobę przez niego wskazaną. Tematyka szkolenia powinna obejmować m.in.:

1. terminologię z zakresu ochrony danych osobowych,
2. podstawy prawne obowiązywania ochrony danych osobowych,
3. omówienie roli i odpowiedzialności osób uczestniczących w przetwarzaniu danych osobowych,
4. omówienie istniejących zagrożeń bezpieczeństwa danych osobowych,
5. stosowane przez administratora środki zabezpieczenia danych osobowych i ochronę stanowiska pracy,
6. obowiązki pracownika w razie naruszenia ochrony danych osobowych.

16.2. SZKOLENIA OKRESOWE

Szkolenia okresowe pracowników w zakresie przetwarzania danych osobowych, przeprowadza administrator bądź osoba przez niego upoważniona. Szkolenia osób zaangażowanych w proces przetwarzania danych osobowych powinny być prowadzone cyklicznie w związku ze zmieniającymi się zagrożeniami bezpieczeństwa danych osobowych i zmieniającymi się zabezpieczeniami. Szkolenia powinny być przeprowadzane nie rzadziej niż raz na rok.Szkolenia okresowe dotyczą również wprowadzanych zmian i aktualizacji systemu bezpieczeństwa danych osobowych.

Tematyka szkolenia powinna obejmować m.in.:

1. zagrożenia bezpieczeństwa danych osobowych;
2. aktualności o zagrożeniach, skutkach i zabezpieczeniach danych osobowych;

3. skutki naruszenia zasad bezpieczeństwa danych osobowych w stosunku do wszystkich osób uczestniczących w procesie przetwarzania informacji, w tym odpowiedzialność prawna;
4. obowiązki pracownika w razie naruszenia ochrony danych osobowych;
5. wybrane elementy dokumentacji ochrony danych osobowych przyjętej w organizacji;
6. sposoby zabezpieczenia danych w systemie informatycznym oraz w formie papierowej w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich.

16.3. ORGANIZACJA SZKOLEŃ

Planowanie szkoleń

1. Szkolenia związane z podnoszeniem kwalifikacji oraz poszerzania wiedzy w zakresie bezpieczeństwa przetwarzania danych osobowych są traktowane jako jedno z priorytetowych zadań organizacji i obowiązków każdego pracownika.
2. Plany szkoleń sporządzane są przez administratora na podstawie zaistniałych potrzeb (nowi pracownicy) oraz zgłoszeń zapotrzebowania (np. po wystąpieniu incydentu, naruszenia bezpieczeństwa ochrony danych osobowych).
3. Zmiany i uzupełnienia planów szkoleń mogą być wprowadzane na podstawie zgłoszeń pracowników oraz administratora.

Realizacja szkoleń

1. Szkolenia odbywają się w siedzibie Szkoły, po uprzednim uzgodnieniu terminu.
2. Szkolenia mogą również odbywać się za pomocą platform do przeprowadzania szkoleń online.
3. Administrator bądź pracownik przez niego wyznaczony zobowiązany jest sporządzić listę osób uczestniczących w szkoleniu.

Dokumentowanie szkoleń

1. Po zakończonym szkoleniu prowadzący szkolenie zobowiązany jest przekazać do administratora konspekt (program) przeprowadzonego szkolenia.
2. Dokumentem potwierdzającym odbyte szkolenie jest również podpisana lista obecności osób uczestniczących w szkoleniu przekazywana po zakończonym szkoleniu administratorowi.
3. Szkołazobowiązana jest do wyznaczenia osoby odpowiedzialnej za prowadzenie rejestru szkoleń, w którym odnotowuje się każde przeprowadzone szkolenie z zakresu ochrony danych osobowych.

17. PROCEDURA MONITORINGU

Zapewniając ochronę wizerunku osób fizycznych objętych monitoringiem, wprowadza się następujące reguły.

1. Administrator zapewnia prawidłowe funkcjonowanie monitoringu mając na względzie by nie naruszał on prawa do prywatności osób fizycznych oraz czuwa by przetwarzanie danych odbywało się w granicach prawa.

2. Monitoring wizyjny wykorzystywany jest w celuzapewnienia bezpieczeństwa uczniów i pracowników, a także ochrony mienia.
3. Obowiązek informacyjny realizowany jest poprzez oznaczenie strefy objętej systemem monitoringu tabliczką zawierającą piktogram kamery wraz ze skróconym obowiązkiem informacyjnym.
4. Klauzula informacyjna zawierająca pełny obowiązek informacyjny jest udostępniona wewnątrz budynku na tablicy ogłoszeń oraz na stronie internetowej w zakładce RODO.
5. Regulamin użytkownika monitoringu wizyjnego udostępniony jest w sekretariacie oraz na stronie internetowej Szkoły w zakładce RODO.
6. Przed rozpoczęciem pracy monitoringu wizyjnego administrator (lub wskazana przez niego osoba) dokonuje analizy obszaru, który obejmie system monitoringu wizyjnego upewniając się, iż swoim działaniem nie naruszy on godności oraz innych dóbr pracownika. Monitoring wizyjny może obejmować jedynie obszar przylegający do organizacji i to w takim zakresie jakim nie narusza on prywatności osób postronnych.
7. System monitoringu działa całą dobę.
8. Rejestracji i zapisaniu na nośniku fizycznym podlega tylko obraz. System monitoringu nie rejestruje dźwięku.
9. Zapis z monitoringu przechowuje się przez okres nie dłuższy niż 3 miesiące. Po upływie tego terminu dane są automatycznie nadpisywane.
10. W uzasadnionych przypadkach, gdy urządzenia monitoringu wizyjnego zarejestrowały zdarzenie związane z naruszeniem bezpieczeństwa osób i mienia, okres przechowywania danych może ulec wydłużeniu o czas niezbędny do zakończenia postępowania, którego przedmiotem jest zdarzenie zarejestrowane przez monitoring wizyjny.
11. Rejestrator umieszcza się w pomieszczeniu, do którego dostęp mają tylko upoważnione osoby.
12. Dostęp do poglądu z kamer w czasie rzeczywistym ma pracownik upoważniony do tego procesu.
13. Stanowisko komputerowe z monitorem, na którym jest wyświetlany obraz z kamer znajduje się w wyznaczonej strefie a widok z monitora jest niedostępny dla osób postronnych.
14. Zapis z systemu monitoringu może być udostępniony uprawnionym organom w zakresie realizowania przez nie ustawowych zadań np. policji, sądom, prokuraturom na ich pisemny wniosek.
15. Osoba zainteresowana zabezpieczeniem danych z monitoringu zwraca się pisemnie do administratora z prośbą o ich zabezpieczenie przed automatycznym usunięciem. Wniosek musi zawierać informacje takie jak:
    a. dane osoby zgłaszającej,
    b. opis zdarzenia wraz ze wskazaniem przybliżonego czasu i miejsca,
    c. cel wykorzystania nagrania.
16. Pracownik sporządza kopię nagrania z monitoringu wizyjnego za okres, którego dotyczy wniosek osoby zainteresowanej oraz oznacza ją w sposób trwały poprzez:
    a. numer porządkowy kopii,
    b. datę sporządzenia kopii,

c. okres, którego dotyczy nagranie,
d. źródła danych.

17. Nagrania są udostępniane na nośniku elektronicznym w postaci płyty CD bądź pendrive, w sposób nienaruszający wizerunku osób trzecich widocznych na nagraniu.
18. Kopia nagrania przechowywana jest w szafie zamkniętej na klucz.
19. Po upływie 6 miesięcy zabezpieczona na wniosek osoby zainteresowanej kopia nagrania podlega zniszczeniu.
20. Kopia nagrania podlega zaewidencjonowaniu w rejestrze kopii z monitoringu wizyjnego.
21. Rejestr zawiera następujące informacje:
    a. numer porządkowy kopii,
    b. datę sporządzenia kopii,
    c. okres, którego dotyczy nagranie,
    d. źródło danych,
    e. informację o udostępnieniu ze wskazaniem daty,
    f. informację o zniszczeniu kopii ze wskazaniem daty.

    Nośnik z kopią nagrania przekazuje się wnioskodawcy za pokwitowaniem odbioru.

18. ARCHIWIZACJA

1. Administrator lub wyznaczony przez niego pracownik odpowiada za przeprowadzenie archiwizowania akt dokumentów, danych, poczty, faktur i innych dokumentów księgowych oraz finansowych w przyjętych ramach czasowych.
2. Dokumenty podlegające archiwizacji umieszczane są w opisanych segregatorach lub teczkach.
3. Administrator w miarę możliwości powinien wyznaczyć pomieszczenie przeznaczone na archiwum.
4. Pomieszczenie archiwum stanowi obszar przetwarzania danych osobowych i jest pomieszczeniem szczególnie chronionym w Szkole.
5. Pomieszczenie archiwum powinno być wyposażone w środki bezpieczeństwa fizycznego podnoszące bezpieczeństwo przechowywanych tam dokumentów przynajmniej o jeden poziom wyżej, niż pozostałe pomieszczenia będące obszarem przetwarzania.
6. Za środki bezpieczeństwa fizycznego podnoszące poziom bezpieczeństwa uznaje się:
    a. pomieszczenie znajdujące się na innej kondygnacji niż 0,
    b. pomieszczenie bez okna,
    c. pomieszczenie w oknach którego znajduje się krata lub roleta antywłamaniowa,
    d. pomieszczenie do którego zastosowano drzwi antywłamaniowe i ogniotrwałe,
    e. zastosowano system alarmowy,
    f. zainstalowano zamek magnetyczny otwierany indywidualnymi kartami lub kodami,
    g. zainstalowano dodatkową kamerę monitoringu wizyjnego skierowaną na drzwi wejściowe,
    h. pomieszczenie archiwum wyposażono w higrometr i termometr.

7. Zabrania się umieszczania dokumentacji bezpośrednio na podłodze.
8. W przypadku kiedy organizacja nie dysponuje warunkami lokalowymi umożliwiającymi wydzielenie pomieszczenia archiwum, administrator powinien przeznaczyć przynajmniej jedną szafę metalową/sejf na dokumenty archiwalne.

19. UTRZYMANIE CZYSTOŚCI

Pomieszczenia, w których znajdują się dane osobowe zarówno w postaci papierowej jak i elektronicznej, które przechowywane są na stacjach komputerowych bądź innych urządzeniach umożliwiających dostęp do danych, stanowią obszar przetwarzania danych osobowych. Dostęp do tych obszarów powinien być kontrolowany zwłaszcza w zakresie w jakim jest on udostępniany osobom sprzątającym. Niezależnie od tego czy osoby sprzątające pomieszczenia, w których przetwarza się dane osobowe są zatrudnione wewnątrz struktury organizacyjnej administratora czy są to osoby świadczące usługi z zewnątrz, administratorwprowadza następujące reguły:

1. Wszystkie osoby sprzątające zobowiązane są do zachowania w tajemnicy danych osobowych znajdujących się w obszarze przetwarzania danych osobowych podczas wykonywania czynności.
2. Oświadczenie o zachowaniu w tajemnicy powinno być odbierane przez administratora przed przystąpieniem osoby sprzątającej do wykonywania czynności.
3. Oświadczenie o zachowaniu w tajemnicy danych osobowych może stanowić oddzielny dokument bądź zostać zawarte w treści umowy o pracę bądź innej podstawy świadczenia usług.
4. Przed rozpoczęciem sprzątania pracownicy zobowiązani są zastosować się do zasady czystego biurka oraz zasady czystego ekranu oraz umożliwić wejście i rozpoczęcie wykonywanych czynności przez osobę sprzątającą.
5. Osoby sprzątające pomieszczenia, w których przetwarzane są dane osobowe powinny wykonywać czynności sprzątania pod nadzorem i w obecności pracowników.
6. W przypadku realizacji usług bez nadzoru pracownika, pracownik zobowiązany jest do zabezpieczenia obszaru przetwarzania poprzez umieszczenie dokumentacji/nośników w szafkach zamykanych na klucz oraz wylogowania z systemu informatycznego.
7. Powyższe zasady mają również zastosowanie do innych osób świadczących usługi np. remontowe, serwisowe.

20. PROCEDURA PRACY NA URZĄDZENIACH PRZENOŚNYCH

Pracownik przy wykonywaniu swoich obowiązków służbowych zarówno w siedzibie administratora jak i poza nią, korzysta z urządzeń przenośnych takich jak laptop czy pendrive. Bez względu na ilość przetwarzanych za pomocą tych urządzeń danych osobowych, uwzględniając stopień ryzyka naruszenia ochrony danych osobowych, stosuje się odpowiednie zabezpieczenia tych urządzeń.

1. Przetwarzanie danych osobowych na komputerach przenośnych powinno być ograniczone do niezbędnych przypadków (regulacje dotyczące komputerów przenośnych stosuje się odpowiednio do innych urządzeń przenośnych).

2. Administrator bądź wyznaczony przez niego pracownik zobowiązany jest do podejmowania działań mających na celu zabezpieczenie komputerów przenośnych poprzez:
   a. przeprowadzenie konfiguracji oprogramowania na komputerach przenośnych, która będzie wymuszać korzystanie z haseł dostępu do urządzenia oraz okresową ich zmianę,
   b. w przypadku braku możliwości powyższej konfiguracji oprogramowania, każdy z pracowników korzystający z urządzeń przenośnych odpowiedzialny jest we własnym zakresie za ustanowienie hasła dostępu do urządzenia oraz jego zmianę zgodnie z procedurą ustanawiania i zmiany haseł zawartą w niniejszej Polityce Bezpieczeństwa,
   c. zabezpieczenie danych na urządzeniach przenośnych poprzez zastosowanie mechanizmu szyfrującego, który uniemożliwi zapoznanie się z danymi w razie zgubienia urządzenia,
   d. w przypadku braku możliwości skorzystania z takiego mechanizmu, pracownik po zakończeniu wykonywania obowiązków służbowych na urządzeniach przenośnych samodzielnie szyfruje dane w taki sposób, by ich odczyt przez osoby niepowołane był niemożliwy,
   e. zainstalowanie i skonfigurowanie na komputerach przenośnych programu antywirusowego,
   f. oznaczenie każdego urządzenia przenośnego w sposób identyfikujący pracownika/pracowników korzystającego tego urządzenia,
   g. wprowadzenie systemu kontroli pozwalającego na zdalną blokadę lub usunięcie danych osobowych z urządzenia przenośnego.

Ponadto pracownik korzystający z urządzenia przenośnego zobowiązany jest:

1. Nie przechowywać plików prywatnych (w tym poczty prywatnej, zdjęć, dokumentów prywatnych, skanów etc.) na powierzonym sprzęcie elektronicznym tj. komputerach, telefonach.
2. Zwracać szczególną uwagę na zabezpieczenie przetwarzanych danych osobowych, zwłaszcza przed dostępem do nich osób nieupoważnionych (np. poprzez wykonywanie pracy na danych w sposób uniemożliwiający podgląd danych osobom trzecim), a także przed ich zniszczeniem.
3. Nie pozostawiać urządzeń przenośnych bez nadzoru w miejscach publicznych lub samochodach. Komputery przenośne pracownik przewozi w torbach, zapewniających ich bezpieczeństwo fizyczne w razie upadku.
4. Chronić dane osobowe przechowywane na urządzeniach przenośnych przed uszkodzeniami fizycznymi, poprzez przestrzeganie zaleceń producentów dotyczących ochrony sprzętu.
5. Nie udostępniać domownikom lub innym osobom postronnym urządzeń przenośnych nawet do chwilowego korzystania.
6. Nie udostępniać domownikom lub innym osobom postronnym identyfikatora lub hasła dostępu do urządzeń przenośnych.
7. Nie korzystać z niezabezpieczonych, publicznych sieci zwłaszcza przy wykonywaniu jakichkolwiek czynności na danych osobowych.
8. Wyłączyć porty komunikacyjne (bluetooth, wi-fi itp.) w czasie kiedy nie są one wykorzystywane do pracy.
9. Przestrzegać wewnętrznych regulacji administratora dotyczących serwisowania urządzeń przenośnych oraz tworzenia kopii zapasowych danych przetwarzanych na urządzeniach przenośnych.

21. PROCEDURA KORZYSTANIA Z SIECIINTERNET

Niniejsza procedura dotyczy korzystania z sieci Internet podczas wykonywania obowiązków pracowniczych. Poniższe zasady mają na celu poprawę jakości i zgodności wykonywanych obowiązków służbowych z procedurami obowiązującymi w Szkole, ochronę tajemnicy służbowej, a także zabezpieczenie danych osobowych przetwarzanych w organizacji.

1. Korzystanie z sieci Internet nie może zagrażać bezpieczeństwu oprogramowania, systemu informatycznego, a także przetwarzanych danych osobowych.
2. Zabronione jest pobieranie, instalowanie oraz wykorzystywanie jakiegokolwiek oprogramowania pobranego z sieci Internet bez wiedzy i udziału osoby nadzorującej pracę w systemie informatycznym.
3. Pracownikowi zabrania się korzystania z sieci Internet w sposób, który mógłby narazić Szkołę na utratę dobrego imienia (np. otwieranie stron wątpliwej reputacji czy potencjalnie niebezpiecznych, udostępnianie chronionych informacji na portalach społecznościowych, przesyłanie pocztą elektroniczną danych osobowych bez stosownych zabezpieczeń),udostępniania łącza internetowego dostarczonego przez organizację osobom nieupoważnionym.
4. Zabrania się obciążania sieci Internet poprzez pobieranie aplikacji, gier, filmów, plików muzycznych, plików graficznych niezwiązanych z pełnionymi obowiązkami służbowymi.
5. Dostęp do sieci wewnętrznej oraz urządzeń (np. router) zabezpieczony jest hasłem dostępu.
6. Zaleca się stosowanie podziału oraz stopniowania dostępu do zasobów sieci. Dopuszczalne jest także zastosowanie blokady dostępu do stron, które organizacja uznaje za potencjalnie niebezpieczne.

22. PROCEDURA TWORZENIA ORAZ ZMIANY HASŁA

22.1. TWORZENIE HASŁA

1. Pracownicy korzystają z bezpiecznych haseł.
2. Za hasło, które nie spełnia wymogów bezpieczeństwa uznaje się hasło:
   a. zbyt krótkie,
   b. zawierające znaki tylko jednego rodzaju,
   c. składające się wyłącznie lub niemal wyłącznie z nazw własnych jak np. nazwa miejscowości, imiona, marka samochodu itp.,
   d. zawierające dane osobiste np. data urodzenia, imiona dzieci, małżonka, nr pesel, nr rejestracji samochodowej,
   e. nie zmieniane przez dłuży czas (ponad 3 miesiące).
3. Pracownicy nie mogą tworzyć haseł poprzez ustalenie stałego trzonu hasła i dodawanie w kolejnym miesiącu odpowiednio cyfry 01, 02, 03 zgodnie z aktualnym miesiącem bądź samej nazwy miesiąca tj. styczeń, luty, marzec itd.
4. Hasło, z którego korzystają pracownicy powinno być hasłem złożonym z co najmniej 8 znaków i zawierać jeden z co najmniej trzech rodzajów znaków tj.:

a. małe litery,
b. wielkie litery,
c. cyfry,
d. znaki specjalne.

22.2. ZMIANA I PRZECHOWYWANIE HASŁA

1. System informatyczny automatycznie powinien wymuszać zmianę hasła nie rzadziej niż raz na 3 miesiące.
2. Osoba sprawująca nadzór nad systemem informatycznym wprowadza w systemie informatycznym oraz w aplikacjach, które służą do przetwarzania danych osobowych funkcję automatycznego wymuszania zmiany hasła przez pracownika.
3. Jeżeli brak jest możliwości ustawienia wymuszania automatycznej zmiany hasła, każdy z pracowników jest za to odpowiedzialny we własnym zakresie.
4. W przypadku podejrzenia lub stwierdzenia ujawnienia hasła, każdy z pracowników niezwłocznie zmienia hasło na nowe.
5. Hasła nie mogą być przechowywane w formie dostępnej dla osób nieupoważnionych.
6. Pracownik ponosi pełną odpowiedzialność za utworzenie hasła i jego bezpieczne przechowywanie.
7. Pracownik utrzymuje swoje hasło w tajemnicy również po upływie jego ważności.

23. OBSŁUGA KONTA POCZTY ELEKTRONICZNEJ

1. Administrator lub wyznaczony pracownik tworzy, nadaje i odbiera dostęp do konta poczty elektronicznej.
2. Konta poczty elektronicznej tworzone są dla pracownika, zgodnie z zakresem pełnionych przez niego obowiązków służbowych.
3. W organizacjidopuszcza się tworzenie kont imiennych, a także kont funkcyjnych.
4. Dostęp do kont funkcyjnych w Szkole może posiadać kilku pracowników.
5. Dostęp do danego konta imiennegomoże posiadać wyłącznie pracownik, do którego konto jest przyporządkowane.
6. Nowo zatrudniony pracownik po przydzieleniu jednorazowego hasła zobowiązany jest do jego zmiany przy pierwszym logowaniu się do poczty elektronicznej.
7. Właścicielem wszystkich treści znajdujących się na koncie pocztowym jest Szkoła.
8. Pracownik odpowiedzialny jest za treść wysyłanych widomości oraz załączników.
9. Pracownik przed wysłaniem wiadomości upewnienia się co do poprawności adresata.
10. Zabrania się prowadzenia korespondencji zbiorowej (wielu adresatów) wysyłanej poza organizację w sposób jawny dla pozostałych adresatów. W takim przypadku można wykorzystać pole adresu UDW.
11. Przed odczytaniem wiadomości elektronicznej pracownik upewnia się w pierwszej kolejności, że znany jest mu adres nadawcy.

12. Pracownik zwraca szczególną uwagę na treść i załączniki, pod kątem próby wykorzystania fałszywych podpisów, sfałszowanego adresu nadawcy, użycia nazw firm i instytucji powszechnych np. Urząd Skarbowy, DHL, Poczta Polska, Zakład Energetyczny.
13. Podejrzane wiadomości e-mail pracownik zgłasza administratorowi lub osobie nadzorującej systemem informatyczny bez wykonywania jakichkolwiek działań mogących uruchomić linki (odnośniki) w treści e-mail lub otwarcia załączników do wiadomości.
14. Zabrania się przesyłanie danych osobowych w innym celu, niż wykonywanie obowiązków służbowych.
15. Nie zaleca się korzystać z prywatnej poczty elektronicznej do realizacji celów służbowych.
16. Korzystanie ze służbowej poczty elektronicznej do celów rejestracji jakichkolwiek innych kont niezwiązanych z obowiązkami służbowymi (np. portale społecznościowe, sklepy internetowe) jest zabronione.
17. Pracownik zobowiązany jest do cyklicznej inwentaryzacji zasobów poczty elektronicznej poprzez usunięcie zbędnej korespondencji oraz jej archiwizację.

24. AKTUALIZACJA OPROGRAMOWANIA

Celem procedury jest zapewnienie ciągłości działania systemu informatycznego oraz zabezpieczenie danych osobowych przed ich nieuprawnionym udostępnieniem.

1. Sprzęt komputerowy oraz oprogramowanie, z którego korzystają pracownicy jest zgodne ze standardami obowiązującymi w Szkole, w tym oprogramowanie instalowane w systemie informatycznym, jest legalne.
2. Wszelkie działania związane z utrzymaniem i eksploatacją systemu informatycznego podejmowane są wyłącznie przez wykwalifikowanych pracowników.
3. Wyznaczona przez administratora osoba nadzorująca systemem informatycznym dba o prawidłowe korzystanie ze sprzętu komputerowego i oprogramowania oraz zapewnia jego aktualizację.
4. Przegląd i konserwacja systemu informatycznego są wykonywane w terminach określonych przez producentów systemu jednak nie rzadziej, niż raz w roku.W miarę możliwości aktualizacja systemu informatycznego odbywa się po godzinach pracy organizacji.
5. Osoba nadzorująca system informatyczny monitoruje na bieżąco pojawiające się aktualizacje i zalecenia producentów oprogramowania, z którego korzysta administrator.

25. KOPIE ZAPASOWE

Niniejsze zasady maja na celu zabezpieczenie przetwarzanych danych przed ich trwała utratą.

1. Przez kopię zapasową rozumie się kopię (roboczą) wykonywaną po każdym dniu pracy lub po zamknięciu jakiegoś etapu pracy. Kopiowaniu podlegają wyłącznie pliki, na których pracownik wykonywał zmiany.
2. Kopia bezpieczeństwa – jest kopią systemową, sporządzaną rzadziej ale obejmuje ona wszystkie pliki, katalogi oraz systemy, w których pracownik przetwarza dane osobowe.

3. Osoba nadzorująca system informatyczny w organizacji wspólnie z administratorem ustala częstotliwość sporządzania kopii zapasowych, bezpieczeństwa oraz ich ilość.
4. Osoba nadzorująca system informatyczny wprowadza w oprogramowaniu stacji roboczych zmiany, po których kopia wykonywana jest automatycznie w oparciu o zaplanowany interwał czasowy.
5. Jeśli oprogramowanie dysku sieciowego uniemożliwia ustawienie polecenia automatycznego wykonywania kopii zapasowych, osoba nadzorująca system informatyczny w Szkole wykonuje kopię zapasową w sposób ręczny.
6. Kopie zapasowe zapisuje się na:
   a. dysku zewnętrznym;
   b. pamięciach flash USB;
   c. innych nośnikach.
7. W sytuacji przechowywania dysków z kopiami zapasowymi w lokalizacjach nienależących do administratora (archiwum, hosting) podpisuje się z takimi podmiotami umowy powierzenia danych osobowych.
8. Organizacja powinna wykonywać dwie niezależne kopie. Kopię zapasową Szkoła powinna wykonywać przynajmniej raz w miesiącu zapisując ją na oddzielnym dysku. Kopie bezpieczeństwa powinny być wykonywane regularnie w terminie wyznaczonym przez administratora (nie rzadziej niż raz na 3 miesiące) i zapisywane na zewnętrznym dysku, przechowywanym w zamykanej, metalowej szafie.
9. Pracownik odpowiada indywidualnie za sporządzanie kopii zapasowych z urządzenia końcowego na którym wykonuje swoją pracę.
10. Dla czynności cyklicznych comiesięcznych pracownik np. kadr wykonuje kopię zapasową ze swojego urządzenia we własnym zakresie nie rzadziej niż raz w miesiącu lub częściej jeżeli cykl przetwarzania jest krótszy.
11. Dla czynności cyklicznych, których cykl jest dłuższy niż jeden miesiąc, kopia zapasowa wykonywana jest po realizacji każdego projektu, jeśli zaś projekt jest istotny dla organizacji kopia wykonywana jest w trakcie trwania projektu, po zamknięciu jego istotnych etapów.
12. Zabrania się wykonywania kopii zapasowych z urządzeń końcowych na nośniki nie będące własnością administratora bez konsultacji z administratorem lub osobą nadzorującą system informatyczny.
13. Kopie zapasowe i kopie bezpieczeństwa podlegają okresowemu przeglądowi pod względem ich wydajności i przydatności.
14. Kopie, które straciły swą przydatność dla organizacji, należy usunąć zgodnie z procedurą archiwizacji.
15. Zabrania się wyrzucania do śmietnika nośników danych, na których zapisane były kopie zapasowe (bezpieczeństwa).

26. KONSERWACJA I NAPRAWA SPRZĘTU

Administrator stosując się do ogólnych zasad przetwarzania danych osobowych, w tym w szczególności do zapewnienia ochrony danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem

przez osobę nieuprawnioną oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, ma obowiązek zabezpieczenia danych przy udostępnianiu sprzętu lub dostępu do obszarów przetwarzania osobom trzecim. Wobec tego administrator wprowadza następujące reguły postępowania:

1. W przypadku wykonywania prac remontowych, montażowych bądź naprawczych (w tym również sprzętu komputerowego) przez podmioty zewnętrzne, dane osobowe zostają należycie zabezpieczone przed nieupoważnionym dostępem.
2. Ryzyko utraty bezpieczeństwa danych osobowych przetwarzanych przez administratora pojawiające się ze strony osób trzecich, które mają do nich dostęp (typu bieżąca konserwacja i naprawy wykonywane przez firmy zewnętrzne), jest zabezpieczone poprzez podpisanie umów powierzenia przetwarzania danych osobowych.
3. Umowa powierzenia danych osobowych jest zawierana przed przystąpieniem przez podmiot zewnętrzny do wykonywanych czynności.
4. Jeśli jest to konieczne dopuszcza się konserwowanie oraz naprawę sprzętu poza siedzibą organizacji jedynie po jego zabezpieczeniu. Przed przekazaniem uszkodzonego sprzętu, wykonuje się kopię zapasową danych oraz stosuje się przynajmniej jedną z poniższych czynności:
   a. wymontowanie nośników z danymi jeśli to możliwe,
   b. trwałe usunięcie danych,
   c. szyfrowanie danych.
5. Wszystkie awarie, działania konserwacyjne i naprawy systemu informatycznego są opisywane w protokołach podpisywanych przez osoby w tych działaniach uczestniczące.
6. Doraźne czynności konserwacyjne i naprawcze wykonywane bez zawarcia umowy o powierzeniu danych osobowych muszą być przeprowadzane pod stałym nadzorem pracowników. Ryzyko ze strony osób, które potencjalnie mogą w łatwiejszy sposób uzyskać dostęp do danych osobowych, jest zabezpieczane poprzez zobowiązywanie ich do zachowania tajemnicy na podstawie pisemnych oświadczeń.

27. NISZCZENIE DOKUMENTÓW I UTYLIZACJA NOŚNIKÓW

Niniejsza procedura utylizacji dotyczy zarówno nośników w formie papierowej, jak i elektronicznej.

1. Nośniki przeznaczone do zniszczenia przechowywane są w wydzielonym i zabezpieczonym miejscu.
2. Dokumenty papierowe zawierające dane osobowe, niszczone są w niszczarce, w sposób uniemożliwiający ich odczytanie.
3. Wycofane z użytku nośniki elektroniczne (uszkodzone, wyeksploatowane) przeznaczone do utylizacji pozbawia się wcześniej zapisu danych lub w sposób mechaniczny pozbawia się możliwości ich odczytu.
4. Poprzez trwałe usunięcie danych rozumie się wykorzystanie specjalistycznego oprogramowania, uniemożliwiającego odtworzenie danych.
5. Pracownik niszczy dokumentację papierową samodzielnie, a niepotrzebne lub uszkodzone nośniki elektroniczne przekazuje administratorowi.

6. Utylizacja nośników elektronicznych odbywa się po uzyskaniu zgody administratora i zostaje potwierdzona protokołem zniszczenia.
7. Wzór protokołu zniszczenia ustala administrator. Protokół powinien zawierać w szczególności datę, przyczynę zniszczenia nośników oraz podpisy osób uprawnionych do zniszczenia nośników.
8. W przypadku korzystania z usług zewnętrznego podmiotu utylizującego dokumentację zawierającą dane osobowe niezbędne jest uprzednie zawarcie umowy powierzenia danych osobowych. Administrator zobowiązany jest do odebrania protokołu zniszczenia wystawionego przez podmiot zewnętrzny.

28. PROCEDURA POSTĘPOWANIA W SYTUACJI NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Celem procedury jest określenie ogólnych zasad postępowania w przypadku naruszenia bezpieczeństwa danych osobowych przetwarzanych zarówno tradycyjnie, jak również w systemie informatycznymSzkoły. Niniejsza procedura zapewnia, że zdarzenia związane z bezpieczeństwem danych oraz zagrożeniazwiązane z funkcjonowaniem systemu informatycznego, zgłaszane są w sposób umożliwiający niezwłoczne podjęcie działań naprawczych oraz eliminację negatywnych skutków związanych z zaistniałym incydentem.

Zasady postępowania w przypadku naruszenia ochrony danych osobowych obowiązują wszystkie osoby biorące udział w procesie przetwarzania danych.

Reakcja na incydent zależy od jego istotności, mierzonej skutkami i poziomem oddziaływania na organizację lub na osoby, których dane osobowe były objęte incydentem.

Osoby stwierdzające naruszenie zasad ochrony lub zdarzenie, które mogło skutkować takim naruszeniem, zobowiązane są do przestrzegania oraz postępowania według opracowanej i wdrożonej procedury postępowania w sytuacji naruszenia ochrony danych osobowych.

28.1. ISTOTA NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Naruszenie ochrony danych osobowych oznacza naruszenie bezpieczeństwa prowadzące do:

a. "naruszenia poufności" – polegającego na nieuprawnionym lub przypadkowym ujawnieniu lub udostępnieniu danych osobowych,
b. "naruszenia integralności" – polegającego na nieuprawnionym lub przypadkowym zmodyfikowaniu danych osobowych,
c. "naruszenia dostępności" – polegającego na przypadkowej lub nieuprawionej utracie dostępu do danych osobowych lub ich zniszczeniu.

Naruszeniem danych osobowych jest przede wszystkim każdy stwierdzony fakt nieuprawnionego ujawnienia danych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną czy uszkodzenia jakiegokolwiek elementu systemu informatycznego.

Obowiązek zgłoszenia jest wymagany, przede wszystkim w sytuacji, gdy naruszenie polegało na:

1. Zgubieniu lub kradzieży nośnika/urządzenia.
2. Zgubieniu, kradzieży lub pozostawieniu w niebezpiecznej lokalizacji dokumentacji papierowej zawierającej dane osobowe.
3. Utracie korespondencji papierowej przez operatora pocztowego lub otwarcie przed zwróceniem jej do nadawcy.
4. Nieuprawnionym uzyskaniu dostępu do informacji.
5. Nieuprawnionym uzyskaniu dostępu do informacji poprzez złamanie zabezpieczeń.
6. Ingerencji złośliwego oprogramowania ingerującego w poufność, integralność i dostępność danych.
7. Uzyskaniu poufnych informacji przez pozornie zaufaną osobę w oficjalnej komunikacji elektronicznej, takiej jak e-mail, czy też inny komunikator internetowy.
8. Nieprawidłowej anonimizacji danych osobowych w dokumencie.
9. Nieprawidłowym usunięciu/zniszczeniu danych osobowych z nośnika/ urządzenia elektronicznego przed jego zbyciem przez administratora.
10. Niezamierzonej publikacji.
11. Przesłaniu danych osobowych do niewłaściwego odbiorcy.
12. Ujawnieniu danych niewłaściwej osobie.
13. Ustnym ujawnieniu danych osobowych.

28.2. POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Pracownik, który stwierdzi fakt naruszenia danych osobowych ma obowiązek podjąć czynności niezbędne do powstrzymania skutków naruszenia ochrony oraz zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia.
2. Wprzypadku stwierdzenia naruszenia bezpieczeństwa danych należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia oraz powiadomić odpowiednie organy/służby ochrony oraz bezpośredniego przełożonego.
3. Z każdego zdarzenia pracownik sporządza notatkę i przekazuje ją administratorowi. W notatce należy ująć:
   a. datę i miejsce stwierdzenia naruszenia,
   b. sposób stwierdzenia naruszenia (opis sytuacji),
   c. podjęte działania (wykonane czynności po wykryciu naruszenia),
   d. wskazanie osób poinformowanych o zaistniałym incydencie,
   e. czytelny podpis osoby sporządzającej notatkę.
4. Po przedłożeniu notatki z naruszenia administrator lub wyznaczona przez niego osoba informuje Inspektora o zaistniałym zdarzeniu oraz dokonuje jego analizy.
5. W przypadku zakwalifikowania zdarzenia jako naruszenie ochrony danych osobowych, administrator lub osoba przez niego wyznaczona dokonuje oceny istotności naruszenia.

6. Przy ocenie istotności incydentu pod uwagę brane są następujące czynniki:
   a. charakter naruszenia ochrony danych osobowych (naruszenie poufności, integralności, dostępności),
   b. klasyfikacja naruszenia (na czym polegało naruszenie),
   c. przyczyny naruszenia (wewnętrzne działanie niezamierzone/zamierzone, zewnętrzne działanie niezamierzone/zamierzone),
   d. kategorie danych osobowych i przybliżoną liczbę osób, których dane dotyczą,
   e. kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,
   f. środki bezpieczeństwa zastosowane przed naruszeniem,
   g. możliwe konsekwencje naruszenia ochrony danych osobowych (naruszenie praw lub wolności osób fizycznych),
   h. wpływ incydentu na ciągłość działania organizacji,
   i. koszty usunięcia skutków incydentu,
   j. szacowany czas naprawy skutków wywołanych incydentem.
7. Ocena istotności naruszenia prowadzi do zakwalifikowania incydentu według przyjętej skali:
   a. pomijalne,
   b. niskie,
   c. akceptowalne,
   d. wysokie,
   e. maksymalne.
8. W celu dokonania zgłoszenia administrator stosuje formularz udostępniony przez Urząd Ochrony Danych Osobowych.
9. Inspektor dokumentuje zaistniały przypadek naruszenia oraz sporządza raport.
10. Zgłoszenie incydentu rejestrowane jest przez administratora lub wyznaczoną przez niego osobę w rejestrze incydentów.

28.3. KONSEKWENCJE ZANIECHANIA ZGŁOSZENIA NARUSZENIA OCHRONY DANYCH

1. Wobec pracownika, który w przypadku naruszenia danych osobowych nie podjął działania określonego w niniejszym dokumencie, a w szczególności nie powiadomił administratora lub odpowiedniej osoby,zgodnie z określonymi zasadami może zostać wszczęte postępowanie dyscyplinarne lub porządkowe.
2. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych.
3. Kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia administratora o naruszeniu danych osobowych nie wyklucza odpowiedzialności karnej oraz cywilnej zgodnie z obowiązującymi przepisami.

28.4. UDOKUMENTOWANIE SKUTKÓW ORAZ PODJĘTYCH ŚRODKÓW I DZIAŁAŃ

Pracownik, który stwierdził fakt lub uzyskał informację o naruszeniu bezpieczeństwa danych osobowych jest obowiązany niezwłocznie powiadomićadministratora i/lub inspektora oraz osobę nadzorującą system informatyczny. Administrator lub osoba przez niego wyznaczona mają obowiązek:

1. Wygenerować i wydrukować wszystkie dokumenty i raporty, które mogą pomóc w ustaleniu wszelkich okoliczności zdarzenia, opatrzyć je datą i godziną oraz podpisać.
2. Przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, w tym określić skalę zniszczeń, metody dostępu osoby nieuprawnionej do danych osobowych w systemie informatycznym służącym do przetwarzania danych osobowych.
3. Podjąć odpowiednie kroki w celu powstrzymania lub ograniczenia dostępu osoby nieuprawnionej do danych osobowych, zminimalizować szkody i zabezpieczyć przed usunięciem śladów naruszenia ochrony, w szczególności poprzez:
   a. fizyczne odłączenie urządzeń i segmentów sieci, które mogły umożliwić dostęp do danych osobowych osobie nieuprawnionej,
   b. wylogowanie użytkownika podejrzanego o naruszenie ochrony danych osobowych,
   c. zmianę hasła użytkownika, przez konto którego uzyskano nielegalny dostęp do danych osobowych w celu uniknięcia ponownej próby uzyskania takiego dostępu.
4. Dokonać szczegółowej analizy stanu systemu informatycznego w celu potwierdzenia lub wykluczenia faktu naruszenia bezpieczeństwa danych osobowych.
5. Przywrócić prawidłowe działanie systemu informatycznego służącego przetwarzaniu danych osobowych.
6. Po przywróceniu prawidłowego stanu, należy przeprowadzić szczegółową analizę, w celu określenia przyczyn naruszenia ochrony danych osobowych lub podejrzenia takiego naruszenia oraz podjąć kroki, mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.
7. Jeżeli przyczyną zdarzenia był błąd pracownika, należy przeprowadzić szkolenie dotyczące bezpieczeństwa przetwarzania danych osobowych w Szkole.
8. Jeżeli przyczyną zdarzenia była infekcja wirusem lub innym szkodliwym oprogramowaniem, należy ustalić źródło jego pochodzenia i utworzyć zabezpieczenia antywirusowe oraz organizacyjne, wykluczające podobne zdarzenia w przyszłości.

28.5. ZGŁASZANIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH ORGANOWI NADZORCZEMU

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 Prezesowi Urzędowi Ochrony Danych Osobowych, 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. Zgłoszenie, o którym mowa w ust. 1, musi co najmniej:

a. opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,
b. zawierać imię i nazwisko oraz dane kontaktowe inspektora lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,
c. opisywać możliwe konsekwencje naruszenia ochrony danych osobowych,
d. opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

3. Jeżeli informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.
4. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu na weryfikowanie przestrzegania niniejszego artykułu.

28.6. ZAWIADAMIANIE OSOBY, KTÓREJ DANE DOTYCZĄ, O NARUSZENIU OCHRONY DANYCH OSOBOWYCH

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 w ust. 1 niniejszego artykułu, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w art. 33 ust. 3 lit. b), c) i d) RODO.
3. Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, w następujących przypadkach:
   a. administratorwdrożył 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 tych danych osobowych,
   b. administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1,
   c. 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.

29. POSTANOWIENIA KOŃCOWE

1. Administrator zobowiązany jest zapoznać z dokumentem wszystkie osoby przetwarzające dane osobowe.

2. Niezależnie od odpowiedzialności określonej w przepisach prawa powszechnie obowiązującego, naruszenie zasad określonych w niniejszej Polityce Bezpieczeństwa może być podstawą rozwiązania stosunku pracy bez wypowiedzenia z osobą, która dopuściła się naruszenia.
3. W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy RODO oraz przepisy Ustawy.
4. Pracownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce Bezpieczeństwa. W wypadku odrębnych od zawartych w niniejszej Polityce uregulowań występujących w innych procedurach obowiązujących w organizacji pracownicy mają obowiązek stosowania zapisów dalej idących, których stosowanie zapewni wyższy poziom ochrony danych osobowych.
5. W sprawach nieokreślonych w niniejszym dokumencie należy stosować instrukcje obsługi i zalecenia producentów aktualnie wykorzystywanych urządzeń i programów.
6. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się przed dopuszczeniem do przetwarzania danych z niniejszą Polityką Bezpieczeństwa oraz złożyć stosowne oświadczenie, potwierdzające znajomość jej treści.
7. Integralną częścią Polityki są jej załączniki, opisane w wykazie. Zmiana załączników lub ich aktualizacja nie wymaga zmiany dokumentu Polityki.
8. Polityka wchodzi w życie z dniem podpisania.

30. WYKAZ ZAŁĄCZNIKÓW

Załącznikami do Polityki są:

Załącznik nr 1 – Upoważnienie pracownika;

Załącznik nr 2 –Oświadczenie pracownika;

Załącznik nr 3 –Oświadczenie dla osoby sprzątającej;

Załącznik nr 4 – Klauzula informacyjna dla uczniów, rodziców/opiekunów;

Załącznik nr 5 –Klauzula informacyjna skrócona;

Załącznik nr 6–Klauzula informacyjna dla kandydata do pracy;

Załącznik nr 7 –Klauzula informacyjna dla pracownika;

Załącznik nr 8 – Zgoda pracownika na przetwarzanie adresu mailowego – wzór;

Załącznik nr 9 – Klauzula informacyjna pełna do monitoringu;

Załącznik nr 10– Klauzula informacyjna skrócona do monitoringu;

Załącznik nr 11– Regulamin monitoringu;

Załącznik nr 12 –Klauzula informacyjna do formularza kontaktowego;

Załącznik nr 13– Klauzula informacyjna do ZFŚS;

Załącznik nr 14 –Klauzula informacyjna dla osoby odbierającej dziecko;

Załącznik nr 15 – Klauzula informacyjna na Facebook;

Załącznik nr 16 – Oświadczenie pracodawcy o prowadzeniu monitoringu;

Załącznik nr 17 – Wzór umowy powierzenia;

Załącznik nr 18 – Procedura realizacji praw osób fizycznych;

Załącznik nr 19 – Procedura postępowania w sytuacji naruszenia.

Załącznik nr 20 – Zgłoszenie naruszenia ochrony danych formularz alternatywny.

Załącznikiem do Polityki jest również plik Excel – „Rejestry", zawierający: rejestr upoważnień, rejestr umów powierzenia, rejestr naruszeń, rejestr realizacji praw osób, których dane dotyczą, rejestr szkoleń, rejestr zgód.

Dokument sporządzono:	**Opracował**	**Sprawdził**	**Zatwierdził (ADO)**
Data: 09.02.2021 r. Miejsce:			

PLAN SPRAWDZEŃ: Data	**Sprawdził** (AW lub IOD)	**Zatwierdził** (ADO)
……2022 r.		
……2023 r.		
……2024 r.		
……2025 r.		