Załącznik nr 23
do polityki bezpieczeństwa-
regulaminu przechowywania
i ochrony danych osobowych w szkole

Instrukcja zarządzania informatycznym systemem przetwarzania danych osobowych w Szkole Podstawowej nr 2 z Oddziałami Dwujęzycznymi im. Aleksandry Piłsudskiej w Suwałkach

Modyfikacja: 11.01.2021 r.

ZATWIERDZAM

DYREKTOR SZKOŁY
mgr Ewa Brzozowska

.....

podpis Dyrektora

SPIS TREŚCI

1. Wstęp

1.1. Informacje ogólne

Niniejszy dokument w postaci Instrukcji zarządzania systemem informatycznym został opracowany przez Administratora Danych –w Szkole Podstawowej nr 2 z Oddziałami Dwujęzycznymi im. Aleksandry Piłsudskiej w Suwałkach , w celu zapewnienia zgodności przetwarzania danych osobowych z polskim prawem.

Wszelkie wątpliwości dotyczące sposobu interpretacji zapisów niniejszego dokumentu Instrukcji zarządzania systemem informatycznym, powinny być rozstrzygane na korzyść zapewnienia możliwie najwyższego poziomu ochrony danych osobowych oraz realizacji praw osób, których dane dotyczą.

Każda osoba mającą dostęp do danych osobowych na podstawie upoważnienia Administratora Danych, została zapoznana z Instrukcją zarządzania systemem informatycznym i zobowiązana do jej przestrzegania w zakresie wynikającym z przydzielonych zadań. Dotyczy to w szczególności pracowników zatrudnionych przez Administratora Danych. Wyżej wymienione osoby złożyły na piśmie oświadczenie o zapoznaniu się z treścią Instrukcji zarządzania systemem informatycznym oraz zobowiązały się do stosowania zawartych w niej postanowień. Oświadczenia przechowywane są w aktach osobowych pracowników.

1.2. Cel przygotowania instrukcji zarządzania

Niniejsza Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwana dalej „instrukcją", przyjęta została w celu wykazania, że dane osobowe w systemach informatycznych Szkoły Podstawowej nr 2 z Oddziałami Dwujęzycznymi im. Aleksandry Piłsudskiej w Suwałkach przetwarzane są w sposób zgodny z przepisami prawa mającymi zastosowanie do takiej czynności, zgodnie z zasadą art. 5 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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.

1.3. Zakres informacji objętych instrukcją zarządzania

Dokument Instrukcji zarządzania systemem informatycznym opisuje zasady i procedury przetwarzania danych osobowych i ich zabezpieczenia przed nieuprawnionym dostępem. Obejmuje on ogólne informacje o systemie informatycznym i zbiorach danych osobowych, które są przy ich użyciu przetwarzane, o zastosowanych rozwiązaniach technicznych, jak również o procedurach eksploatacji i zasadach użytkowania, jakie zastosowano w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych. Na instrukcję zarządzania składają się w szczególności następujące informacje:

1) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności;
2) stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;
3) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;
4) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;
5) sposób, miejsce oraz okres przechowywania:
    a) elektronicznych nośników informacji zawierających dane osobowe,
    b) kopii zapasowych;
6) sposób zabezpieczenia systemu informatycznego przed wirusami i szkodliwym oprogramowaniem;
7) sposób realizacji wymogów, dotyczących przetwarzania danych;
8) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

1.3. Wyjaśnienie terminów używanych w dokumencie instrukcji zarządzania

1) **ustawa** – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (tj. Dz. U. 2018 poz. 1000 z późn. zm.), zwana dalej „ustawą",
2) **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),
3) **Administrator Danych Osobowych (Administrator)** – Szkoła Podstawowa nr 2 z Oddziałami Dwujęzycznymi im. Aleksandry Piłsudskiej w Suwałkach,
4) **dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
5) **instrukcja zarządzania systemem informatycznym** – niniejszy dokument Instrukcji zarządzania systemem informatycznym obowiązujący u Administratora, zwany dalej „instrukcją",
6) **zbiór danych** – uporządkowany zastaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie,
7) **przetwarzanie danych osobowych**– jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,
8) **system informatyczny** – zbiór powiązanych ze sobą elementów: serwerów z systemami operacyjnymi, systemu zarządzania bazami danych osobowych, oprogramowania (programów użytkowych),urządzeń służących do komunikacji między sprzętowymi elementami systemu,
9) **zabezpieczenie danych w systemie informatycznym** – wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
10) **usuwanie danych** – zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,

11) **zgoda osoby, której dane dotyczą** – oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści,
12) **identyfikator użytkownika** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
13) **hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym,
14) **sieć telekomunikacyjna** – sieć telekomunikacyjna oraz publiczna sieć telekomunikacyjna w rozumieniu odpowiednio art.2 pkt 35 oraz art. 2 pkt 29 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2017 r. poz. 1907 ze zm.), w tym w szczególności Internet,
15) **teletransmisja** – przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej,
16) **rozliczalność** – właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,
17) **integralność danych** – właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
18) **raport** – przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych,
19) **poufność danych** – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom,
20) **uwierzytelnianie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

2. PROCEDURY NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH I REJESTROWANIA TYCH UPRAWNIEŃ W SYSTEMACH INFORMATYCZNYCH ORAZ WSKAZANIE OSOBY ODPOWIEDZIALNEJ ZA TE CZYNNOŚCI

2.1. Procedury nadawania/ cofnięcia lub anulowania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemach informatycznych

1. Uprawnienia do przetwarzania danych osobowych w systemach informatycznych nadaje każdorazowo Administrator Systemów Informatycznych. Wzór upoważnienia stanowi załącznik nr 1a i 1b do instrukcji.
2. Uprawnienie do przetwarzania danych osobowych w systemach informatycznych może zostać nadane wyłącznie pracownikom, którzy uzyskali upoważnienie do przetwarzania danych osobowych.
3. Administrator Systemów Informatycznych każdorazowo decyduje, czy istnieje konieczność (w celu wykonywania obowiązków zawodowych) nadania upoważnionemu pracownikowi uprawnienia do przetwarzania danych osobowych w systemach informatycznych.
4. Zakres uprawnienia (zakres dostępu do danych osobowych przetwarzanych w systemach informatycznych) nie może być szerszy niż w wydanym wcześniej upoważnieniu.
5. Przydzielanie poszczególnym pracownikom Administratora Danych Osobowych uprawnień do przetwarzania danych osobowych w systemach informatycznych jest jednoznaczne z nadaniem im loginu oraz hasła tymczasowego pozwalającego na dostęp do danego systemu informatycznego.
6. Administrator Systemów Informatycznych prowadzi ewidencję nadanych uprawnień do przetwarzania danych w systemach informatycznych.
7. Jeśli Administrator Systemów Informatycznych uzna to za stosowne, uprawnienie dostępu do danego systemu informatycznego może zostać w każdej chwili cofnięte.
8. Pracownikowi anuluję się uprawnienia do przetwarzania danych oraz uprawnienia dostępu do danego systemu informatycznego z chwilą zakończenia pracy w szkole. Wzór upoważnienia stanowi załącznik nr 1c i 1d do instrukcji.
9. Cofnięcie uprawnienia dostępu do danego systemu informatycznego Administrator Systemów Informatycznych odnotowuje w prowadzonym przez siebie rejestrze nadanych uprawnień.

2.2. Osoby odpowiedzialne za nadawanie uprawnień do przetwarzania danych i rejestrowanie tych uprawnień w systemach informatycznych

Zakres odpowiedzialności	Osoba odpowiedzialna
Przegląd przestrzegania Instrukcji	Inspektor ochrony danych, Administrator Systemów Informatycznych
Przegląd aktualności Instrukcji	Inspektor ochrony danych, Administrator Systemów Informatycznych
Nadawanie uprawnień do przetwarzania danych w systemach informatycznych	Administrator Systemów Informatycznych
Rejestrowanie uprawnień do przetwarzania danych w systemach informatycznych	Administrator Systemów Informatycznych
Wyrejestrowanie uprawnień do przetwarzania danych w systemach informatycznych	Administrator Systemów Informatycznych

3. OPIS STOSOWANYCH METOD I ŚRODKÓW UWIERZYTELNIENIA ORAZ PROCEDUR ZWIĄZANYCH Z ZARZĄDZANIEM I UŻYTKOWANIEM STOSOWANYCH METOD I ŚRODKÓW UWIERZYTELNIENIA

1) Hasła tymczasowe do konta użytkownika (w przypadku utworzenia nowego konta, a także w sytuacjach awaryjnych związanych np.: ze zagubieniem, utratą lub zapomnieniem hasła osobistego przez użytkownika konta) tworzone są przez Administratora Systemów Informatycznych.
2) Tryb przekazywania ww. hasła tymczasowego odbywa się osobiście w sposób zapewniający bezpieczeństwo i poufność przekazywanych informacji, w szczególności: w sposób uniemożliwiający innej osobie ich podsłuchanie lub nieuprawnione wykorzystanie.
3) Zakazuje się przekazywania haseł tymczasowych poprzez osoby trzecie lub przy użyciu metod, które nie gwarantują zachowania jego poufności oraz niezaprzeczalnego ustalenia nadawcy i odbiorcy hasła, np. przez niechronione wiadomości przekazywane elektronicznie.
4) Po otrzymaniu hasła tymczasowego użytkownik ma obowiązek niezwłocznego zalogowania się do systemu informatycznego przy użyciu tego hasła oraz może dokonać zmiany na hasło osobiste.
5) Ujawnianie przez użytkownika komukolwiek, jakichkolwiek aktualnych lub poprzednich haseł, haseł osobistych lub innych haseł mu powierzonych, jest zabronione.
6) Autoryzacja do wszystkich programów przetwarzających dane osobowe, opisanych w niniejszej instrukcji zarządzania możliwa jest wyłącznie za pomocą loginu i hasła.
7) Jeżeli do uwierzytelniania użytkowników używa się hasła, jego zmiana musi następować nie rzadziej niż co 30 dni, hasło musi się składać z co najmniej 8 znaków długości oraz jednocześnie zawierać małe i wielkie litery, cyfry lub znaki specjalne.
8) W celu zapewnienia odpowiedniego poziomu bezpieczeństwa haseł i innych identyfikatorów pozwalających na autoryzację w programach przetwarzających dane osobowe nie zaleca się stosowania jakichkolwiek programów i systemów umożliwiających zapamiętywanie identyfikatorów i haseł. Nie ma możliwości zapamiętania hasła użytkownika do systemu operacyjnego.
9) Dostęp do każdego z profili użytkowników ograniczony jest wyłącznie do jednego pracownika.

10) W przypadku, gdy system informatyczny uniemożliwia stworzenie odrębnego profilu użytkownika, osoba która na zlecenie Administratora Danych Osobowych ma dostęp do systemu otrzymuje odrębne upoważnienie wraz ze wskazaniem szczególnej odpowiedzialności użytkownika.

4. PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY PRZEZNACZONE DLA UŻYTKOWNIKÓW SYSTEMU

4.1. Procedura rozpoczęcia pracy przeznaczona dla użytkownika systemu

1. Przed rozpoczęciem pracy, w trakcie rozpoczynania pracy z systemem informatycznym oraz w trakcie pracy, każdy pracownik jest obowiązany do zwrócenia bacznej uwagi, czy nie wystąpiły objawy, mogące świadczyć o naruszeniu zasad ochrony danych osobowych.
2. Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje uruchomienie komputera, wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione oraz ogólne stwierdzenie poprawności działania systemu. Użytkownikowi nie wolno w czasie uruchamiania systemu operacyjnego odchodzić od stanowiska. Jest to dozwolone tylko i wyłącznie zgodnie z procedurą opisującą tryb zawieszenia pracy z systemem, w którym przetwarzane są dane osobowe.
3. Użytkownik informuje Administratora Systemów Informatycznych lub osobę przez niego upoważnioną do opieki nad sprzętem komputerowym o wszelkich nieprawidłowościach w dostępie do systemu informatycznego.

4.2. Procedura zawieszenia pracy przeznaczona dla użytkownika systemu

1. W przypadku konieczności zawieszenia pracy w systemie informatycznym z powodu tymczasowego opuszczenia stanowiska pracy, użytkownik zobowiązany jest, w zależności od przewidywanego okresu swojej nieobecności, do aktywowania wygaszacza ekranu, zabezpieczonego hasłem lub do zablokowania dostępu do użytkowanego systemu komputerowego, np. poprzez jednoczesne naciśnięcie klawiszy {Ctrl + Alt + Delete} i potwierdzenia klawiszem Enter podświetlonej opcji „Zablokuj komputer".

4.3. Procedura zakończenia pracy przeznaczona dla użytkownika systemu

1. Zakończenie pracy polega na wybraniu odpowiedniego polecenia systemowego umożliwiającego zakończenie pracy. Zaleca się zamknięcie wszystkich programów i zapisanie wszystkich otwartych plików. Użytkownik powinien zaczekać przy komputerze do chwili jego wyłączenia.

5. PROCEDURY TWORZENIA KOPII ZAPASOWYCH ZBIORÓW DANYCH ORAZ PROGRAMÓW I NARZĘDZI PROGRAMOWYCH SŁUŻĄCYCH DO ICH PRZETWARZANIA

1. Po zakończeniu pracy w programie, codziennie każdy pracownik archiwizuje dane lokalnie.
2. Raz w tygodniu kopia lokalna przegrywana jest na dysk sieciowy, znajdujący się w pracowni komputerowej (parter budynku dydaktycznego szkoły).
3. Z każdą aktualizacją oprogramowania i na koniec każdego roku budżetowego Administrator Systemów Informatycznych lub wyznaczony przez Administratora Danych pracownik tworzy kopie zapasowe na płytach CD wszystkich zbiorów danych przetwarza-

nych w formie elektronicznej oraz programów i narzędzi programowych, w których przetwarzane są dane osobowe.

4. Jeżeli zaistnieje taka konieczność tworzy się awaryjne kopie zapasowe, np. przed dokonaniem niezbędnych napraw systemu informatycznego bądź komputera, na którym przetwarzane są dane osobowe.
5. Procedura tworzenia kopii zapasowych obejmuje wszystkie komputery, na których przetwarzane są dane osobowe. Tworzenie kopii zapasowych polega na nagraniu na elektroniczny nośnik informacji danych podlegających procedurze tworzenia kopii zapasowych.
6. Tworzone kopie zapasowe są kopiami całościowymi.
7. Nieprzydatne już nośniki informacji pozbawia się w sposób trwały zapisanych danych osobowych.

6. OPIS SPOSOBU, MIEJSCA I OKRESU PRZECHOWYWANIA ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE ORAZ KOPII ZAPASOWYCH

1. Nośniki informatyczne zawierające dane osobowe oraz kopie zapasowe zbiorów danych osobowych, programów i narzędzi programowych służących do przetwarzania danych osobowych, przechowywane są w sposób uniemożliwiający nieuprawnione przejęcie, modyfikacje, uszkodzenie lub zniszczenie.
2. Nośnik z nagranymi kopiami zapasowymi jest umieszczany w metalowej szafie zamykanej na klucz.
3. Dostęp do nośników, o których mowa w niniejszym rozdziale ograniczony jest do Administratora Danych, Administratora Systemów Informatycznych oraz pracownika upoważnionego przez Administratora Danych.
4. Co roku Administrator Systemów Informatycznych lub osoba wskazana przez Administratora Danych dokonuje przeglądu nośników, a po ustaniu ich użyteczności usuwa zapisane dane.
5. Każdy przechowywany nośnik jest oznaczony poprzez wskazanie, jakie dane się na nim znajdują.

7. OPIS SPOSOBU ZABEZPIECZENIA SYSTEMÓW INFORMATYCZNYCH PRZED WIRUSAMI I SZKODLIWYM OPROGRAMOWANIEM

1. Z uwagi na fakt, iż komputery przetwarzające dane osobowe posiadają dostęp do sieci publicznej, Administrator Danych Osobowych wdrożył procedury oraz oprogramowanie, które chroni dane osobowe przed nieuprawnionym dostępem, zmianami, usunięciem lub uszkodzeniem. Zagrożenia te to programy zawierające złośliwy kod (wirusy), tzw. konie trojańskie oraz ataki hakerów.
2. Aby zmniejszyć to zagrożenie, zabronione jest pobieranie oraz instalowanie bez nadzoru Administratora Systemów Informatycznych jakichkolwiek programów na komputerach służących do przetwarzania danych osobowych.
3. Zabronione jest również używanie nośników informacji niepochodzących z zasobów Administratora Danych. Każda osoba przetwarzająca dane osobowe przy użyciu komputera została pouczona, aby w wypadku jakichkolwiek podejrzeń dotyczących obniżenia bezpieczeństwa danych osobowych, poinformowała o tym fakcie osobę upoważnioną przez Administratora Danych lub Administratora Systemów Informatycznych.

Typ zabezpieczenia	Nazwa programu	Częstotliwość i sposób aktualizacji oprogramowania
Program ANTYWIRUSOWY	Kaspersky Endpoint Security	Automatycznie

8. SPOSÓB REALIZACJI WYMOGÓW STAWIANYM SYSTEMOM INFORMATYCZNYM DOTYCZĄCYCH PRZETWARZANIA DANYCH

1. System informatyczny, przetwarzający dane osobowe, posiada mechanizm uwierzytelniający użytkownika, wykorzystujący identyfikator i hasło. Posiada mechanizmy, pozwalające na określenie uprawnień użytkownika do korzystania z przetwarzanych informacji (np. prawo do odczytu danych, modyfikacji istniejących danych, tworzenia nowych danych, usuwania danych).

2. System informatyczny, przetwarzający dane osobowe, posiada mechanizmy, pozwalające na odnotowanie faktu wykonania operacji na danych. W szczególności zapis ten powinien obejmować:

   a) rozpoczęcie i zakończenie pracy przez użytkownika systemu,
   b) operacje wykonywane na przetwarzanych danych, a w szczególności ich dodanie, modyfikację oraz usunięcie,
   c) przesyłanie za pośrednictwem systemu danych osobowych przetwarzanych w systemie informatycznym innym podmiotom niebędącym właścicielem ani współwłaścicielem systemu,
   d) nieudane próby dostępu do systemu informatycznego, przetwarzającego dane osobowe oraz nieudane próby wykonania operacji na danych osobowych,
   e) błędy w działaniu systemu informatycznego podczas pracy danego użytkownika.

3. Zapis działań użytkownika uwzględnia:
   a) identyfikator użytkownika,
   b) datę i czas, w którym zdarzenie miało miejsce,
   c) rodzaj zdarzenia,
   d) określenie informacji, których zdarzenie dotyczy (identyfikatory rekordów).

4. System informatyczny zapewnia zapis faktu przekazania danych osobowych z uwzględnieniem:

   a) identyfikatora osoby, której dane dotyczą,
   b) osoby przesyłającej dane,
   c) odbiorcy danych,
   d) zakresu przekazanych danych osobowych,
   e) daty operacji,
   f) sposobu przekazania danych.

9. PROCEDURY WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMÓW ORAZ NOŚNIKÓW INFORMACJI SŁUŻĄCYCH DO PRZETWARZANIA DANYCH

1. W wypadku wystąpienia takiej potrzeby, lecz nie rzadziej niż raz na rok, Administrator Systemów Informatycznych lub osoba wyznaczona przez Administratora Danych Osobowych, dokonuje przeglądu i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych.
2. Wykryte podczas przeglądu i konserwacji nieprawidłowości w działaniu sprzętu lub programów służących do przetwarzania danych osobowych, usuwa się niezwłocznie.
3. Przegląd i konserwacja mogą być zlecone podmiotowi zewnętrznemu specjalizującemu się w tego typu działaniach. W wypadku przekazania sprzętu lub nośników informacji służących do przetwarzania danych osobowych podmiotowi trzeciemu, pozbawia się je zapisanych danych osobowych w sposób, który uniemożliwi ich odtworzenie.
4. Podczas dokonywania przeglądu i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych zostaną zachowane szczególne warunki ostrożności, w celu zabezpieczenia danych osobowych przed dostępem osób nieuprawnionych.
5. Zmiana konfiguracji sprzętu komputerowego, na którym znajdują się dane osobowe lub zmiana jego lokalizacji, może być dokonana tylko za wiedzą i zgodą Administratora Danych Osobowych.
6. Administrator Systemów Informatycznych lub osoba wyznaczona przez Administratora Danych Osobowych prowadzi Dziennik systemu informatycznego, zgodnie ze wzorem określonym w niniejszej instrukcji.

10. POZIOM BEZPIECZEŃSTWA

1. Administrator Danych zastosował środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności, aby zabezpieczyć dane osobowe przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy o ochronie danych osobowych oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

10.1. Określenie stosowanego poziomu bezpieczeństwa

1. W zależności od właściwości zbioru danych Administrator Danych Osobowych stosuje następujące poziomy bezpieczeństwa: podstawowy, podwyższony lub wysoki.

1) **Poziom co najmniej podstawowy** stosuje się, gdy w systemie informatycznym nie są przetwarzane dane wrażliwe oraz żadne z urządzeń systemu informatycznego, służącego do przetwarzania danych osobowych nie jest połączone z siecią publiczną.
2) **Poziom co najmniej podwyższony** stosuje się, gdy w systemie informatycznym przetwarzane są dane wrażliwe oraz żadne z urządzeń systemu informatycznego, służącego do przetwarzania danych osobowych nie jest połączone z siecią publiczną.
3) **Poziom wysoki** stosuje się, gdy przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, połączone jest z siecią publiczną.

2. Jeżeli Administrator Danych Osobowych stosuje wysoki poziom bezpieczeństwa (pkt 10.2.3 Instrukcji), to oznacza to, że realizuje on wymogi określone także przez podstawowy (pkt 10.2.1 Instrukcji) i podwyższony (pkt 10.2.2 Instrukcji) poziom bezpieczeństwa. Analogicznie, jeśli Administrator Danych Osobowych stosuje podwyższony poziom bezpieczeństwa, to oznacza to, że realizuje on wymogi określone także przez podstawowy poziom bezpieczeństwa.
3. Na wszystkich stacjach roboczych, na których przetwarzane są dane osobowe, wprowadza się, wysoki poziom zabezpieczeń.

10.2. Stosowane zabezpieczenia

10.2.1. Poziom podstawowy

Nazwa zabezpieczenia	Stosowanie z bezpieczeni
Zabezpieczenie obszaru, w którym przetwarzane są dane osobowe, przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych	Tak
Przebywanie osób nieuprawnionych, jest dopuszczalne za zgodą administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych	Tak
Stosowane są mechanizmy kontroli dostępu do danych	Tak
Jeżeli dostęp do danych posiadają co najmniej 2 osoby to w systemie rejestrowany jest dla każdego użytkownika odrębny identyfikator oraz dostęp do danych jest możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia	Tak
System jest zabezpieczony przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego	tak
System jest zabezpieczony przed utratą danych spowodowaną utratą zasilania lub zakłóceniami w sieci zasilającej	Autonomiczn zasilacze up
Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie jest przydzielany innej osobie	Tak
W przypadku gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni. Hasło składa się co najmniej z 6 znaków	Tak
Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych osobowych	Tak
Kopie zapasowe przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem oraz usuwa się niezwłocznie po ustaniu ich użyteczności	Tak
Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem, w którym przetwarzane są dane osobowe, w tym stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych	Tak
Administrator danych monitoruje wdrożone zabezpieczenia systemu informatycznego	Tak
Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do: 1. likwidacji – pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie. 2. przekazania podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie. 3. naprawy – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych	Tak

10.2.2. Poziom podwyższony

Nazwa zabezpieczenia	Stosowanie zabezpieczeni
W przypadku gdy do uwierzytelnienia użytkowników używa się haseł, składa się ono co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry i znaki specjalne.	Tak
Urządzenia i nośniki zawierające dane osobowe, zabezpiecza się w sposób zapewniający poufność i integralność tych danych	Tak

10.2.3. Poziom wysoki

Nazwa zabezpieczenia	Stosowanie z bezpieczeni
Administrator danych stosuje środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej.	Tak

Załącznik nr 1 a
do instrukcji

Upoważnienie nr .....

do przetwarzania danych osobowych
w systemie informatycznym oraz tradycyjnym

W dniu ..... nadaję uprawnienia
Pani ..... - (stanowisko) nauczyciel
Pracownika Szkoły Podstawowej nr 2 z Oddziałami Dwujęzycznymi im. Aleksandry Piłsudskiej w Suwałkach

1) do obsługi systemu informatycznego i
przetwarzania danych w sposób tradycyjny

Nazwa zbioru danych	w zakresie (P) pełnym, (WG) wglądu, (W) wprowadzania, (M) modyfikacji, (U) usuwania, (A) archiwizacji
1) dane osobowe uczniów, w tym dane osobowe uczniów z orzeczeniami o potrzebie kształcenia specjalnego, (P)	
2) dane osobowe uczniów korzystających ze świetlicy szkolnej, (P)	
3) dane rodziców uczniów (prawnych opiekunów) (P)	

Zobowiązuję Panią/a do przestrzegania przepisów dotyczących ochrony danych osobowych oraz wprowadzonych i wdrożonych do stosowania przez Administratora Danych „Polityki bezpieczeństwa -- regulamin przechowywania i ochrony danych osobowych" wraz z załącznikami.

Suwałki, ...

..... **.....**
podpis administratora systemu informatycznego **podpis pracownika**

Wypełnia Administrator Systemu Informatycznego

Hasło dostępu do komputera w sali lekcyjnej .....

Identyfikator użytkownika .....

Data zarejestrowania w systemie .....

Data wyrejestrowania użytkownika (zablokowania dostępu) do systemu .....

.....
podpis Administratora Systemu Informatycznego

Załącznik nr 1 b
do instrukcji

Upoważnienie nr .....
do przetwarzania danych osobowych
w systemie informatycznym oraz tradycyjnym

W dniu ..... nadaję uprawnienia
Pani ..... - (stanowisko) pracownika administracyjno - obsługowego Szkoły Podstawowej nr 2 z Oddziałami Dwujęzycznymi im. Aleksandry Piłsudskiej w Suwałkach

1) do obsługi systemu informatycznego i
przetwarzania danych w sposób tradycyjny

Nazwa zbioru danych — w zakresie
(P) pełnym, (WG) wglądu, (W) wprowadzania,
(M) modyfikacji, (U) usuwania, (A) archiwizacji

1, ...
2. .....
3. .....
4. .....
5. .....
6. .....
7. .....

Zobowiązuję Panią/a do przestrzegania przepisów dotyczących ochrony danych osobowych oraz wprowadzonych i wdrożonych do stosowania przez Administratora Danych „Polityki bezpieczeństwa - regulamin przechowywania i ochrony danych osobowych" wraz z załącznikami.

Suwałki, ...

....

podpis administratora systemu informatycznego — **podpis pracownika**

Wypełnia Administrator Systemu Informatycznego

Identyfikator użytkownika .....

hasło tymczasowe .....

Data zarejestrowania w systemie .....

Data wyrejestrowania użytkownika
(zablokowania dostępu) do systemu .....

.....
podpis Administratora
Systemu Informatycznego

Załącznik nr 1 c
do instrukcji

Anuluję/cofam Upoważnienie nr .....

do przetwarzania danych osobowych
w systemie informatycznym oraz tradycyjnym

W dniu ..... anuluję/cofam uprawnienia
Pani ..... - (stanowisko) nauczyciel
Pracownika Szkoły Podstawowej nr 2 z Oddziałami Dwujęzycznymi im. Aleksandry Piłsudskiej w Suwałkach

1) do obsługi systemu informatycznego i
przetwarzania danych w sposób tradycyjny

Nazwa zbioru danych	w zakresie (P) pełnym, (WG) wglądu, (W) wprowadzania, (M) modyfikacji, (U) usuwania, (A) archiwizacji
1) dane osobowe uczniów, w tym dane osobowe uczniów z orzeczeniami o potrzebie kształcenia specjalnego, (P) 2) dane osobowe uczniów korzystających ze świetlicy szkolnej, (P) 3) dane rodziców uczniów (prawnych opiekunów) (P)	

Zobowiązuję Panią/a do przestrzegania przepisów dotyczących ochrony danych osobowych oraz wprowadzonych i wdrożonych do stosowania przez Administratora Danych „Polityki bezpieczeństwa -- regulamin przechowywania i ochrony danych osobowych" wraz z załącznikami.

Suwałki, ...

....

podpis administratora systemu informatycznego **podpis pracownika**

Wypełnia Administrator Systemu Informatycznego

Hasło dostępu do komputera w sali lekcyjnej .....

Identyfikator użytkownika .....

Data zarejestrowania w systemie .....

Data wyrejestrowania użytkownika (zablokowania dostępu) do systemu .....

.....
podpis Administratora Systemu Informatycznego

Załącznik nr 1 d
do instrukcji

Anulowanie/ cofnięcie Upoważnienia nr .....
do przetwarzania danych osobowych
w systemie informatycznym oraz tradycyjnym

W dniu ..... anuluję/cofam uprawnienia
Pani ..... - (stanowisko) pracownika administracyjno - obsługowego Szkoły Podstawowej nr 2 z Oddziałami Dwujęzycznymi im. Aleksandry Piłsudskiej w Suwałkach

1) do obsługi systemu informatycznego i
przetwarzania danych w sposób tradycyjny

Nazwa zbioru danych — w zakresie
(P) pełnym, (WG) wglądu, (W) wprowadzania,
(M) modyfikacji, (U) usuwania, (A) archiwizacji

1. .....
2. .....
3. .....
4. .....
5. .....
6. .....
7. .....

Zobowiązuję Panią/a do przestrzegania przepisów dotyczących ochrony danych osobowych oraz wprowadzonych i wdrożonych do stosowania przez Administratora Danych „Polityki bezpieczeństwa - regulamin przechowywania i ochrony danych osobowych" wraz z załącznikami.

Suwałki,.....

..... **.....**

podpis administratora systemu informatycznego — **podpis pracownika**

Wypełnia Administrator Systemu Informatycznego

Identyfikator użytkownika .....

Hasło tymczasowe .....

Data zarejestrowania w systemie .....

Data wyrejestrowania użytkownika
(zablokowania dostępu) do systemu .....

.....
podpis Administratora
Systemu Informatycznego

Załącznik 2

do instrukcji

..... Suwałki, dnia.....

(imię i nazwisko)

.....

(stanowisko)

OŚWIADCZENIE

Niniejszym zobowiązuję się do zachowania poufności, nieujawniania osobom nieupoważnionym i zachowania w tajemnicy wszelkich danych: osobowych, technicznych, technologicznych, finansowych, handlowych, prawnych i wszelkich informacji powierzonych od innych stron zainteresowanych, do których mam, lub będę miał(a) dostęp z tytułu wykonywania swoich zadań służbowych i obowiązków pracowniczych w Szkole Podstawowej nr 2 z Oddziałami Dwujęzycznymi im. Aleksandry Piłsudskiej w Suwałkach, a nie przeznaczonych do publicznego rozpowszechniania.

Potwierdzam, że zapoznałem/am się z:

- definicją danych osobowych w rozumieniu art. 4 pkt 1 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,
- regulaminami, instrukcjami i procedurami obowiązującymi w Szkole Podstawowej nr 2 z Oddziałami Dwujęzycznymi im. Aleksandry Piłsudskiej w Suwałkach wiążącymi się z ochroną danych osobowych i zobowiązuję się do ich przestrzegania.

Jednocześnie jestem świadomy/a, że osoby upoważnione do przetwarzania danych zobowiązane są zachować w tajemnicy przetwarzane dane osobowe oraz sposoby ich zabezpieczenia, także po ustaniu stosunku pracy lub po upływie ważności upoważnienia. Ponadto podlegają odpowiedzialności karnej wynikającej z art. 266 kodeksu karnego.

Zobowiązanie się do nierozpowszechniania i niewykorzystywania informacji zdobytych w trakcie wykonywania obowiązków pracowniczych, a także po ustaniu zatrudnienia. Z chwilą ustania zatrudnienia zobowiązuję się do niezwłocznego zwrócenia pracodawcy wszelkich dokumentów oraz innych materiałów dotyczących informacji chronionych

w Szkole Podstawowej nr 2 z Oddziałami Dwujęzycznymi im. Aleksandry Piłsudskiej w Suwałkach. Przyjmuję do wiadomości i akceptuję, iż postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych w rozumieniu przepisów Kodeksu Pracy, że Szkoła Podstawowa nr 2 z Oddziałami Dwujęzycznymi im. Aleksandry Piłsudskiej w Suwałkach jako strona poszkodowana ma prawo do dochodzenia na zasadach ogólnych odszkodowania odpowiadającego wysokości poniesionej szkody.

.....

(podpis pracownika)

Załącznik nr 3

do instrukcji

Dziennik zawiera opisy wszelkich zdarzeń istotnych dla działania systemu informatycznego, a w szczególności:
1) w przypadku awarii - opis awarii, przyczyna awarii, szkody wynikłe na skutek awarii, sposób usunięcia awarii, opis systemu po awarii, wnioski;
2) w przypadku konserwacji systemu – opis podjętych działań, wnioski

DZIENNIK SYSTEMU INFORMATYCZNEGO

Lp.	Data i godzina	Opis zdarzenia	Podjęte działania / wnioski	Podpis