Szkoła Podstawowa z Oddziałami Integracyjnymi nr 343 w Warszawie
im. Matki Teresy z Kalkuty
ul. Kopcińskiego 7, 02-777 Warszawa
tel/fax: 22 643 84 54, e-mail: sp343@edu.um.warszawa.pl

SP343.021.12.2017.D

ZARZĄDZENIE NR 5 / 2017
DYREKTORA SZKOŁY PODSTAWOWEJ Z ODDZIAŁAMI INTEGRACYJNYMI
NR 343 W WARSZAWIE
z dnia 27 lutego 2017 roku

w sprawie: ochrony danych osobowych

Na podstawie ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r., poz. 922 ze zm.) zarządza się, co następuje:

§ 1

Wprowadza się:

1. Politykę bezpieczeństwa informacji w Szkole Podstawowej z Oddziałami Integracyjnymi nr 343 im. Matki Teresy z Kalkuty w Warszawie, stanowiącą załącznik nr 1 do niniejszego zarządzenia.
2. Instrukcję określającą sposób zarządzenia systemem informatycznym służącym do przetwarzania danych osobowych w Szkole Podstawowej z Oddziałami Integracyjnymi nr 343 im. Matki Teresy z Kalkuty w Warszawie, stanowiącą załącznik nr 2 do niniejszego zarządzenia.

§ 2

Dokumenty, o których mowa w § 1, udostępnione są w sekretariacie szkoły.

§ 3

Traci moc zarządzenie nr10/2014 z dnia 28 października 2014 r.

§ 4

Zarządzenie wchodzi w życie z dniem ogłoszenia.

DYREKTOR SZKOŁY
mgr Jolanta Kubalska

Szkoła Podstawowa
z Oddziałami Integracyjnymi nr 343
im. Matki Teresy z Kalkuty
02-777 Warszawa, ul. Kopcińskiego 7
tel./fax: 22 643-84-54
NIP: 951-13-54-011

Załącznik nr 1 do Zarządzenia nr 5 /2017
Dyrektora Szkoły Podstawowej
z Oddziałami Integracyjnymi nr 343
im. Matki Teresy z Kalkuty w Warszawie
z dnia 27.02.2017r.

POLITYKA BEZPIECZEŃSTWA

Szkoła Podstawowa z Oddziałami Integracyjnymi nr 343

im. Matki Teresy z Kalkuty

ul. Stefana Kopcińskiego 7

02-777 Warszawa

Data i miejsce sporządzenia dokumentu:	**Warszawa, 20.02.2017r.**
Data ujednolicenia dokumentu:	
Ilość stron:	**32**

SPIS TREŚCI

Polityka bezpieczeństwa przetwarzania danych osobowych w Szkole Podstawowej z Oddziałami Integracyjnymi Nr 343 im. Matki Teresy z Kalkuty w Warszawie

Dokumenty powiązane:

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Szkole Podstawowej z Oddziałami Integracyjnymi nr 343 im. Matki Teresy z Kalkuty w Warszawie.

§ 1
Postanowienia ogólne

1. Polityka bezpieczeństwa przetwarzania danych osobowych w Szkole Podstawowej z Oddziałami Integracyjnymi nr 343 im. Matki Teresy z Kalkuty zwana dalej „Polityką", została wydana na podstawie § 3 ust. 1 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).
2. Celem Polityki jest stworzenie podstaw dla właściwego wykonania obowiązków Administratora Danych w zakresie zabezpieczenia i prawidłowej ochrony przetwarzanych danych osobowych i zapewnienie zgodności jego działań z Ustawą o Ochronie Danych Osobowych oraz jej rozporządzeniami wykonawczymi.
3. Polityka określa zasady przetwarzania danych osobowych oraz ich zabezpieczania przed nieuprawnionym dostępem, jako zestaw praw, reguł i zaleceń, regulujących sposób ich zarządzania, ochrony w Szkole Podstawowej z Oddziałami Integracyjnymi nr 343 w Warszawie, zwanej dalej Szkołą.
4. Polityka zawiera informacje dotyczące rozpoznawania procesów przetwarzania danych osobowych oraz wprowadzonych zabezpieczeń technicznych i organizacyjnych, zapewniających ochronę przetwarzanych danych osobowych.
5. Niniejszą Politykę stosuje się do:
   1) Danych osobowych:
      a) przetwarzanych w systemach informatycznych,
      b) zapisanych się na zewnętrznych nośnikach informacji.
   2) Informacji dotyczących bezpieczeństwa przetwarzania danych osobowych:
      c) służących do uwierzytelnienia w systemach informatycznych, w których są przetwarzane dane osobowe,

d) dotyczących wdrożonych zabezpieczeń technicznych i organizacyjnych.

6. Bez względu na zajmowane stanowisko, miejsce wykonywanej pracy oraz charakter stosunku pracy, zasady określone w niniejszej Polityce oraz w dokumentach powiązanych powinny być znane i stosowane przez pracowników oraz w niezbędnym zakresie przez współpracowników przetwarzających dane osobowe, których administratorem jest Szkoła Podstawowa z Oddziałami Integracyjnymi nr 343 w Warszawie lub które Szkoła przetwarza na podstawie umów powierzeń, o których mowa w art. 31 Ustawy.

§ 2
Definicje

Użyte w niniejszej Polityce pojęcia są wspólne dla wszystkich dokumentów powiązanych z niniejszą Polityką oraz dla wszystkich pozostałych dokumentów, które zostały przyjęte w Szkole Podstawowej z Oddziałami Integracyjnymi nr 343 im. Matki Teresy z Kalkuty w zakresie ochrony danych osobowych w Szkole.

1. **Administrator Danych** – Szkoła Podstawowa z Oddziałami Integracyjnymi nr 343 im. Matki Teresy z Kalkuty ul. Stefana Kopcińskiego 7, 02-777 Warszawa, REGON 010288559, podmiot decydujący o środkach i celach przetwarzania danych osobowych, reprezentowany przez Dyrektora Szkoły.
2. **Administrator Bezpieczeństwa Informacji** – wyznaczona osoba odpowiedzialna za nadzorowanie stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, w tym w szczególności za przeciwdziałanie dostępowi osób trzecich

   do systemu, w którym przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie ochrony danych osobowych,
3. **Administrator Systemów Informatycznych** – wyznaczona osoba, odpowiedzialna za funkcjonowanie infrastruktury informatycznej, na którą składa się cały sprzęt informatyczny oraz systemy i aplikacje informatyczne, za ich przeglądy, konserwację oraz za stosowanie technicznych i organizacyjnych środków bezpieczeństwa w systemach informatycznych.
4. **Bezpieczeństwo przetwarzania danych osobowych** - zachowanie poufności, integralności i rozliczalności danych osobowych; dodatkowo, mogą być brane pod uwagę inne własności, takie jak dostępność, autentyczność, niezaprzeczalność i niezawodność.
5. **Dyrekcja** – dyrektor, wicedyrektor.
6. **Dane Osobowe** - każda informacja dotycząca żyjącej osoby fizycznej, która pozwala na bezpośrednią lub pośrednią identyfikację tej osoby.
7. **GIODO** – Generalny Inspektor Ochrony Danych Osobowych.
8. **Integralność danych** – właściwość zapewniająca, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany.

9. **Naruszenie ochrony danych osobowych** – zamierzone lub przypadkowe naruszenie środków technicznych i organizacyjnych zastosowanych w celu ochrony danych osobowych. W szczególności, gdy stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszanie ochrony danych osobowych.
10. **Poufność** – właściwość zapewniająca, że informacja (np. dane osobowe) jest dostępna jedynie osobom upoważnionym.
11. **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.
12. **Rozporządzenie** - Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakie powinny spełniać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).
13. **Rozporządzenie I**- Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz. U. z 2015r. poz. 719).
14. **Rozporządzenie II** - Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz. U. z 2015r. poz. 745).
15. **Rozliczalność** – właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
16. **System informatyczny** – zespół współpracujących urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
17. **Ustawa** – Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz. U. z 2016r. poz. 922 z późn. zm.).
18. **Użytkownik systemu** – osoba upoważniona do bezpośredniego dostępu do danych osobowych przetwarzanych w systemie informatycznym, która posiada ustalony identyfikator i hasło.
19. **Właściciel zasobów danych osobowych** – osoba wyznaczona przez dyrektora, odpowiedzialna za ochronę danych osobowych przetwarzanych w podległej komórce organizacyjnej. Jest ona zobowiązana zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy o ochronie danych osobowych oraz nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.

20. **Zbiór danych osobowych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony czy podzielony funkcjonalnie.
21. **Zbiór nieinformatyczny** - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony lub podzielony funkcjonalnie, prowadzony poza systemem informatycznym, w szczególności w formie kartoteki, skorowidza, księgi, wykazu lub innego zbioru ewidencyjnego.

§ 3
Deklaracja dyrekcji

1. Dyrekcja zobowiązuje się do podjęcia odpowiednich kroków, mających na celu zapewnienie prawidłowej ochrony danych osobowych, w szczególności do zapewnienia, że przez cały okres ich przetwarzania, dane będą:
   1) przetwarzane zgodnie z prawem.
   2) zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami.
   3) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane.
   4) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.
   5) zabezpieczone środkami technicznymi i organizacyjnymi, które zapewniają rozliczalność, integralność oraz poufność danych.
2. Przy przetwarzaniu danych osobowych w systemach informatycznych Szkoły należy stosować wysoki poziom bezpieczeństwa w rozumieniu § 6 ust. 4 Rozporządzenia.

§ 4
Przegląd dokumentacji z zakresu ochrony danych osobowych

1. Niniejsza Polityka oraz dokumenty z nią powiązane powinny być aktualizowane wraz ze zmieniającymi się przepisami prawnymi o ochronie danych osobowych oraz zmianami faktycznymi w ramach Szkoły oraz poza nią, które mogą powodować, że zasady ochrony danych osobowych określone w obowiązujących dokumentach będą nieaktualne lub nieadekwatne.
2. Przegląd Polityki ma na celu stwierdzenie, czy postanowienia Polityki odpowiadają aktualnej i planowanej działalności Szkoły oraz stanowi prawnemu aktualnemu w momencie dokonywania przeglądu.
3. Fakty wystąpienia poważnych naruszeń ochrony danych osobowych powinny skutkować zmianami w dokumencie niniejszej Polityki i dokumentach powiązanych.
4. Zmiany niniejszej Polityki wymagają przeglądu innych dokumentów obowiązujących w Szkole dotyczących ochrony danych osobowych.
5. Wszelkie znaczące zmiany Polityki powinny być zatwierdzane przez Dyrekcję.

§ 5
Zarządzanie ochroną danych osobowych

1. Realizację zamierzeń w celu zwiększenia skuteczności ochrony danych osobowych powinny zagwarantować następujące założenia:
   1) przeszkolenie użytkowników w zakresie bezpieczeństwa przetwarzania danych osobowych.
   2) przypisanie użytkownikom określonych atrybutów pozwalających na ich identyfikację w systemach informatycznych (np. hasła, identyfikatory), umożliwiających im dostęp do danych osobowych - stosownie do zakresu upoważnienia i indywidualnych poziomów uprawnień.
   3) okresowe sprawdzanie przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych osobowych.
   4) podejmowanie niezbędnych działań, w celu likwidacji słabych ogniw w systemie ochrony danych osobowych.
   5) śledzenie osiągnięć w dziedzinie bezpieczeństwa systemów informatycznych i - w miarę możliwości organizacyjnych i techniczno-finansowych - wdrażanie nowych narzędzi i metod pracy oraz sposobów zarządzania systemami informatycznymi, służących wzmocnieniu bezpieczeństwa przetwarzanych danych osobowych.
2. Na każdym etapie przetwarzania danych osobowych należy brać pod uwagę, w niezbędnym zakresie, integralność, poufność oraz rozliczalność dla przetwarzanych danych osobowych.
3. Dyrekcja powinna uzyskać zapewnienie, że pracownicy, wykonawcy oraz użytkownicy reprezentujący stronę trzecią:
   1) są odpowiednio wprowadzani w swoje obowiązki i odpowiedzialności związane z ochroną danych osobowych i ich przetwarzaniem przed przyznaniem im dostępu do danych osobowych.
   2) otrzymują zalecenia określające wymagania w zakresie bezpieczeństwa danych osobowych związane z ich obowiązkami w Szkole. Wypełniają zalecenia i warunki zatrudnienia, które uwzględniają zasady ochrony danych osobowych oraz właściwe metody pracy.
   3) w sposób ciągły utrzymują odpowiednie umiejętności i kwalifikacje.
4. Za bieżącą, operacyjną ochronę danych osobowych odpowiada każda osoba przetwarzająca te dane w zakresie zgodnym z zakresem upoważnienia, kompetencjami lub rolą sprawowaną w procesie przetwarzania danych.

§ 6
Odpowiedzialność Administratora Danych Osobowych

1. Administrator Danych Osobowych jest odpowiedzialny za przetwarzanie i ochronę danych osobowych zgodnie z przepisami prawa, w tym wprowadzenie do stosowania procedur postępowania zapewniających prawidłowe przetwarzanie danych osobowych, rozumiane jako ochronę danych przed ich udostępnieniem osobom nieupoważnionym, zmianą lub zabraniem

przez osobę nieuprawnioną, przetwarzaniem z naruszeniem Ustawy oraz utratą, uszkodzeniem lub zniszczeniem.

2. Do kompetencji Administratora Danych Osobowych należy w szczególności:
   1) wyznaczenie funkcji Administratora Bezpieczeństwa Informacji.
   2) wyznaczenie funkcji Administratora Systemów Informatycznych.
   3) wyznaczanie Właścicieli zasobów danych osobowych.
   4) określenie celów i strategii ochrony danych osobowych.
   5) podział zadań i obowiązków związanych z organizacją ochrony danych osobowych.
3. Do obowiązków Administratora Danych Osobowych należy:
   1) zapewnienie szkoleń dla pracowników w zakresie przepisów o ochronie danych osobowych oraz zagrożeń związanych z ich przetwarzaniem.
   2) przyjmowanie i zatwierdzanie niezbędnych, wymaganych przez przepisy prawa dokumentów regulujących ochronę danych osobowych w Szkole.
   3) zapewnienie środków finansowych na ochronę fizyczną pomieszczeń, w których przetwarzane są dane osobowe.
   4) zapewnienie środków finansowych niezbędnych do ochrony danych osobowych przetwarzanych w systemach informatycznych oraz w zbiorach nieinformatycznych.
   5) zapewnienie środków finansowych na merytoryczne przygotowanie osób odpowiedzialnych za nadzór nad ochroną danych osobowych.
   6) zapewnienie realizacji obowiązku zgłoszenia i aktualizacji zbiorów danych osobowych do rejestracji GIODO.

§ 7
Odpowiedzialność Administratora Bezpieczeństwa Informacji

1. Funkcję Administratora Bezpieczeństwa Informacji pełni pracownik wyznaczony przez Dyrektora Szkoły. Administrator Bezpieczeństwa Informacji nadzoruje przestrzeganie zasad ochrony danych osobowych zarówno w systemach informatycznych, jak również w zbiorach danych osobowych prowadzonych w formie papierowej i elektronicznej.
2. Do kompetencji Administratora Bezpieczeństwa Informacji należy:
   1) określenie zasad ochrony danych osobowych.
   2) wnioskowanie o ukaranie osób winnych naruszenia przepisów i zasad dotyczących ochrony danych osobowych.
3. Do obowiązków Administratora Bezpieczeństwa Informacji należy:
   1) zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:
      a) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych,
      b) nadzorowanie opracowania i aktualizowania dokumentacji, o której mowa w art. 36 ust. 2, oraz przestrzegania zasad w niej określonych,

c) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych;

2) prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów, o których mowa w art. 43 ust. 1, zawierającego nazwę zbioru oraz informacje, o których mowa w art. 41 ust. 1 pkt 2-4a i 7,
3) nadzór nad wdrożeniem stosownych środków organizacyjnych, technicznych i fizycznych w celu ochrony przetwarzanych danych osobowych,
4) nadawanie, zmienianie oraz cofanie uprawnień do przetwarzania danych osobowych w tym systemach informatycznych,
5) nadzór nad zapewnieniem przez Właścicieli zasobów danych osobowych dostosowania funkcjonalności systemów przetwarzających dane osobowe do wymagań określonych w Rozporządzeniu,
6) reprezentowanie Szkoły w kontaktach z Biurem GIODO w tym udział w kontrolach przeprowadzanych przez Inspektorów GIODO,
7) przygotowywanie zgłoszeń zbiorów danych osobowych do rejestracji w Biurze GIODO,
8) reagowanie na zgłaszane incydenty związane z naruszeniem ochrony danych osobowych oraz analizowanie ich przyczyn i kierowanie wniosków dotyczących ukarania winnych naruszeń,
9) sprawowanie nadzoru nad przestrzeganiem zastosowanych środków technicznych i organizacyjnych zapewniających ochronę przetwarzanym danym osobowym odpowiednią do zagrożeń oraz kategorii danych objętych ochroną powinno być głównym zadaniem Administratora Bezpieczeństwa Informacji,
10) prowadzenie pełnej dokumentacji związanej z ochroną danych osobowych, zawierającej:
    a) ewidencję zbiorów danych osobowych,
    b) ewidencję osób upoważnionych do przetwarzania danych osobowych we wszystkich zbiorach oraz nadzór nad prowadzeniem rejestru nadanych upoważnień do przetwarzania danych w systemach informatycznych
    c) wykaz obszarów przetwarzania danych osobowych,
    d) dokumenty z audytów i przeglądów bezpieczeństwa,
    e) oryginały i kopie dokumentów dotyczących ochrony danych osobowych, w szczególności polityka bezpieczeństwa, instrukcje, regulaminy, procedury,
    f) kopie wniosków o rejestrację zbiorów,
11) udzielanie odpowiedzi na zapytania kierowane do Administratora Danych Osobowych przez podmioty zewnętrzne dotyczące administrowanych zbiorów danych osobowych.

4. Sprawozdanie ABI powinno zawierać:
    1) oznaczenie administratora danych i adres jego siedziby lub miejsca zamieszkania,
    2) imię i nazwisko administratora bezpieczeństwa informacji,

3) wykaz czynności podjętych przez administratora bezpieczeństwa informacji w toku sprawdzenia oraz imiona, nazwiska i stanowiska osób biorących udział w tych czynnościach,
4) datę rozpoczęcia i zakończenia sprawdzenia,
5) określenie przedmiotu i zakresu sprawdzenia,
6) opis stanu faktycznego stwierdzonego w toku sprawdzenia oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych,
7) stwierdzone przypadki naruszenia przepisów o ochronie danych osobowych w zakresie objętym sprawdzeniem wraz z planowanymi lub podjętymi działaniami przywracającymi stan zgodny z prawem,
8) wyszczególnienie załączników stanowiących składową część sprawozdania,
9) podpis administratora bezpieczeństwa informacji, a w przypadku sprawozdania w postaci papierowej - dodatkowo parafy administratora bezpieczeństwa informacji na każdej stronie sprawozdania,
10) datę i miejsce podpisania sprawozdania przez administratora bezpieczeństwa informacji.

5. Administrator Bezpieczeństwa Informacji w zakresie realizacji swoich obowiązków, ma prawo żądania od pozostałych osób, bez względu na rangę ich stanowiska, udzielania natychmiastowej pomocy w razie stwierdzenia, że doszło do naruszenia przepisów o ochronie danych osobowych.

§8
Odpowiedzialność Administratora Systemów Informatycznych

1. Funkcję Administratora Systemów Informatycznych pełni pracownik – administrator sieci w szkole.
2. Do obowiązków Administratora Systemów Informatycznych należy:
   1) nadzór nad nadawaniem uprawnień do przetwarzania danych osobowych w systemach informatycznych,
   2) nadzór nad stosowaniem środków zapewniających bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych, a w szczególności przeciwdziałających dostępowi osób niepowołanych do tych systemów,
   3) podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń,
   4) identyfikacja i analiza zagrożeń oraz ocena ryzyka, na które może być narażone przetwarzanie danych osobowych w systemach informatycznych i tradycyjnych,
   5) sprawowanie nadzoru nad przechowywanymi kopiami zapasowymi opisanymi w Instrukcji zarządzania systemem informatycznym.

§ 9
Odpowiedzialność Właścicieli zasobów danych osobowych

1. Dyrekcja wyznacza Właścicieli zasobów danych osobowych, którzy są odpowiedzialni za ochronę przypisanych i przetwarzanych zbiorów danych osobowych w podległej komórce organizacyjnej.
2. Do kompetencji Właścicieli zasobów danych osobowych należy:
   1) określanie celów w jakich mają być przetwarzane dane osobowe, zakresu oraz czasu trwania przetwarzania danych osobowych,
   2) określenie sposobu przetwarzania danych osobowych (czy w systemach informatycznych, czy w zbiorach nieinformatycznych),
   3) ustalenie, czy dane przetwarzane dla określonego celu mają mieć charakter poufny.
3. Do obowiązków Właścicieli zasobów danych osobowych należy:
   1) zapewnienie podstaw prawnych do przetwarzania danych osobowych od chwili zebrania danych osobowych do chwili ich usunięcia,
   2) zapewnienie aktualności, adekwatności oraz merytorycznej poprawności danych osobowych przetwarzanych w określonym przez nich celu,
   3) zapewnienie dostosowania funkcjonalności systemów przetwarzających dane osobowe do wymagań określonych w Rozporządzeniu,
   4) realizację obowiązku informowania o przetwarzaniu danych osobowych, osób, których dane osobowe są pozyskiwane,
   5) zapewnienie na żądanie uprawnionych osób, udostępniania informacji o przetwarzanych danych osobowych oraz podmiotach, którym zostały one udostępnione,
   6) zapewnienie złożenia przez pracowników oświadczenia o znajomości przepisów o ochronie danych osobowych oraz zobowiązania do zachowania w tajemnicy danych osobowych oraz informacji na temat zabezpieczania danych osobowych,
   7) zapewnienie uzyskania przez pracowników przetwarzających dane osobowe, formalnego upoważnienia do przetwarzania danych osobowych,
   8) w przypadku utworzenia nowego zbioru danych osobowych ustalenie, kogo dotyczą dane osobowe, jaki jest ich zakres (np. imię i nazwisko, adres zamieszkania, NIP, PESEL itp.), cel przetwarzania oraz komu dane osobowe mają być udostępniane. Wszystkie te informacje powinny zostać przekazane do Administratora Bezpieczeństwa Informacji.

§ 10
Odpowiedzialność pracowników i użytkowników systemu

1. W celu osiągnięcia i utrzymania wysokiego poziomu bezpieczeństwa przetwarzania danych osobowych konieczne jest zaangażowanie ze strony każdego pracownika w zakresie ochrony danych osobowych.
2. Pracownicy Szkoły są zobowiązani do postępowania zgodnie z Polityką Bezpieczeństwa.

3. Za bezpieczeństwo przetwarzania danych osobowych w określonym zbiorze, indywidualną odpowiedzialność ponosi przede wszystkim każdy pracownik mający dostęp do danych.
4. Pracownicy mający dostęp do danych osobowych nie mogą ich ujawniać zarówno w miejscu pracy, jak i poza nim, w sposób wykraczający poza czynności związane z ich przetwarzaniem w zakresie obowiązków służbowych, w ramach udzielonego upoważnienia do przetwarzania danych.
5. W miejscu przetwarzania danych osobowych utrwalonych w formie papierowej pracownicy zobowiązani są do stosowania zasady tzw. „czystego biurka". Zasada ta oznacza nie pozostawianie materiałów zawierających dane osobowe w miejscu umożliwiającym fizyczny dostęp do nich osobom nieuprawnionym. Za realizację powyższej zasady odpowiedzialny jest na swym stanowisku każdy z pracowników.
6. Niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe musi odbywać się w sposób uniemożliwiający odczytanie zawartej w nich treści, np. z wykorzystaniem niszczarek.
7. Niedopuszczalne jest wynoszenie materiałów zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych. Za bezpieczeństwo i zwrot materiałów zawierających dane osobowe odpowiada w tym przypadku osoba dokonująca ich wyniesienia oraz jej bezpośredni przełożony.
8. Przebywanie osób nieuprawnionych w pomieszczeniu, w którym przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych osobowych, chyba że dane te są w odpowiedni sposób zabezpieczone przed dostępem.
9. Pracownicy zobowiązani są do zamykania na klucz wszelkich pomieszczeń lub budynków wchodzących w skład obszarów, w których przetwarzane są dane osobowe w czasie ich chwilowej nieobecności w pomieszczeniu pracy, jak i po jej zakończeniu, a klucze nie mogą być pozostawione w zamku w drzwiach. Pracownicy zobowiązani są do dołożenia należytej staranności w celu zabezpieczenia posiadanych kluczy przed nieuprawnionym dostępem.
10. Pracownicy Szkoły są zobowiązani do informowania o wszelkich podejrzeniach naruszenia lub zauważonych naruszeniach oraz słabościach systemu przetwarzającego dane osobowe bezpośrednio do Administratora Bezpieczeństwa Informacji.
11. Pracownicy powinni na podstawie dokonanej identyfikacji ewentualnych zagrożeń, przedkładać Administratorowi Bezpieczeństwa Informacji projekty i propozycje nowych rozwiązań, których celem jest zwiększenie poziomu ochrony danych osobowych.

§ 11
Kontrola przetwarzania i stanu zabezpieczenia danych osobowych

1. Nadzór i kontrolę nad ochroną danych osobowych przetwarzanych w Szkole Podstawowej z Oddziałami Integracyjnymi nr 343 im. Matki Teresy z Kalkuty w Warszawie sprawuje

Administrator Bezpieczeństwa Informacji oraz Administrator Systemów Informatycznych - w odniesieniu do danych osobowych przetwarzanych w systemach informatycznych służących do przetwarzania danych osobowych.

2. Czynności kontrolne przeprowadzane są raz do roku.
3. Z czynności kontrolnych sporządzany jest protokół, w którym dokonuje się dokładnego opisu zakresu kontroli i przeprowadzonych czynności.
4. Protokół podpisywany jest przez osoby wykonujące czynności kontrolne. Dołącza się go do dokumentacji przechowywanej u Administratora Bezpieczeństwa Informacji.
5. Wzór protokołu z kontroli lub czynności sprawdzających, o których mowa w niniejszym Rozdziale /**załącznik nr 11** do niniejszej Polityki/.

§ 12
Sankcje za naruszenie zasad ochrony danych osobowych

1. Naruszenie zasad ochrony danych osobowych przez pracownika, może skutkować postawieniem mu zarzutu popełnienia, jednego z przestępstw określonych w Rozdziale 8 Ustawy lub przestępstwa określonego w art 266 Kodeksu Karnego. W takim przypadku zgodnie z przepisem art 66 Kodeksu Pracy umowa o pracę z pracownikiem tymczasowo aresztowanym wygasa z upływem 3 miesięcy nieobecności pracownika w pracy z powodu tymczasowego aresztowania, chyba że pracodawca rozwiąże wcześniej bez wypowiedzenia umowę o pracę z winy pracownika.
2. Zgodnie z art. 100 § 2 pkt 5 Kodeksu Pracy, pracownik jest obowiązany przestrzegać tajemnicy określonej w odrębnych przepisach. Dane osobowe, którym Szkoła nadaje charakter poufny mają charakter takiej tajemnicy, a jej ujawnienie w zależności od zakresu ujawnionych danych osobowych oraz nastawienia pracownika dopuszczającego się nieuprawnionego ujawnienia danych, może mieć charakter naruszenia lub ciężkiego naruszenia obowiązków pracowniczych.
3. Pracownik dopuszczający się nieuprawnionego ujawnienia lub wykorzystania danych osobowych w sposób sprzecznych z ich przeznaczeniem (np. wykorzystania danych osobowych do celów prywatnych) czy też ich przetwarzania w sposób niezgodny z przyjętymi w Szkole procedurami może zostać ukarany karą upomnienia lub karą nagany.
4. W razie ciężkiego naruszenia obowiązku zachowania danych osobowych w tajemnicy lub przetwarzania ich w sposób rażąco sprzeczny z przyjętymi zasadami i procedurami, dyrektor może rozwiązać bez wypowiedzenia umowę o pracę z winy pracownika.
5. Sankcje dotyczące ujawnienia poufnych danych osobowych stosuje się analogicznie do ujawnienia przez pracownika informacji dotyczących zabezpieczenia danych osobowych w Szkole.

§ 13
Obowiązek informacyjny

1. W przypadku zbierania danych osobowych na formularzach, umowach, drukach (zarówno papierowych jak i elektronicznych) należy umieszczać na nich odpowiednią klauzulę informacyjną. Klauzula taka powinna informować osobę, której dane zbieramy o:
   1) adresie siedziby i pełnej nazwie Szkoły,
   2) celu zbierania danych,
   3) prawie dostępu do treści swoich danych oraz ich poprawiania,
   4) dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.
2. Przepisu określonego w ust. 1 nie stosuje się, jeżeli:
   1) przepis innej ustawy zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania,
   2) osoba, której dane dotyczą, posiada informacje, o których mowa w ust. 1.
3. W przypadku zbierania danych osobowych nie od osoby, której one dotyczą, pracownicy Szkoły są zobowiązani poinformować tę osobę, bezpośrednio po utrwaleniu zebranych danych, o:
   1) adresie siedziby i pełnej nazwie szkoły,
   2) celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych,
   3) źródle danych,
   4) prawie dostępu do treści swoich danych oraz ich poprawiania,
   5) uprawnieniach wynikających z art. 32 ust. 1 pkt 7 i 8 Ustawy.
4. Przepisu określonego w ust. 1 nie stosuje się w przypadkach określonych w art. 25 ust. 2 pkt 1, 3 i 5 Ustawy.

§ 14
Szkolenia w zakresie ochrony danych osobowych

1. Przed rozpoczęciem przetwarzania danych osobowych pracownik powinien zostać przeszkolony przez Administratora Bezpieczeństwa Informacji. Szkolenie powinno obejmować następujące zagadnienia:
   1) przepisy o ochronie danych osobowych,
   2) zasady przetwarzania danych osobowych,
   3) procedury dotyczące bezpiecznego przetwarzania danych osobowych w systemach informatycznych,
   4) zasady użytkowania urządzeń i systemów informatycznych służących do przetwarzania danych osobowych,
   5) zagrożenia na jakie może być narażone przetwarzanie danych osobowych, a w szczególności te związane z przetwarzaniem danych osobowych w systemach informatycznych,

6) zasady dostępu do pomieszczeń, w których przetwarzane są dane osobowe,

7) sposób postępowania w przypadku naruszenia ochrony danych osobowych lub systemu informatycznego,

8) odpowiedzialność z tytułu naruszenia ochrony danych osobowych.

2. Szkolenia powinny być powtarzane, gdy zaistnieje taka potrzeba.

§ 15
Wymiana informacji dotyczących danych osobowych

1. Pracownicy Szkoły w celu ochrony wymienianych informacji dotyczących danych osobowych powinni podczas przetwarzania uwzględniać następujące zasady:

   1) wykorzystywanie technik kryptograficznych do ochrony poufności, integralności i rozliczalności danych osobowych przesyłanych publicznymi sieciami telekomunikacyjnymi,

   2) ochrona wymienianych danych osobowych przed przechwyceniem, kopiowaniem, modyfikacją, błędnym wyborem drogi komunikacji i zniszczeniem,

   3) zabezpieczenia i ograniczenia związane z możliwościami przekazywania wiadomości za pomocą środków komunikacji, np. automatyczne przekazywania poczty elektronicznej na zewnątrz,

   4) zakaz pozostawiania informacji zawierających dane osobowe przy urządzeniach drukujących, np. kopiarkach, drukarkach, faksach, do których mogą mieć dostęp osoby nieupoważnione,

   5) upewnienie się przed przekazaniem danych osobowych, czy rozmówca jest osobą upoważnioną do uzyskania określonych danych osobowych,

   6) zachowania szczególnej ostrożności w trakcie rozmów telefonicznych, unikając podsłuchania danych osobowych przez osoby nieupoważnione,

   7) niepozostawianie wiadomości zawierających dane osobowe w automatycznych sekretarkach,

   8) właściwe postępowanie z faksami i fotokopiarkami, ponieważ mają one podręczną pamięć i przechowują w niej strony zawierające np. dane osobowe na wypadek błędów transmisji.

2. Transport danych osobowych w formie elektronicznej i papierowej pomiędzy obszarami, w których są przetwarzane dane osobowe powinien być prowadzony przez osoby upoważnione w sposób ograniczający możliwość ich pozyskania i odczyt przez osoby nieupoważnione.

§ 16
Przetwarzanie danych osobowych w obszarach bezpiecznych

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

2. Na pomieszczenia przetwarzania danych osobowych składają się pomieszczenia biurowe oraz części pomieszczeń, gdzie Szkoła prowadzi działalność.

3. Do pomieszczeń przetwarzania danych osobowych zalicza się:
   1) pomieszczenia biurowe, w których zlokalizowane są stacje robocze,
   2) pomieszczenia, w których przechowywane są sprawne oraz uszkodzone elektroniczne nośniki informacji, kopie zapasowe,
   3) pomieszczenia, w których przechowuje się dokumenty źródłowe oraz wydruki z systemu informatycznego,
   4) pomieszczenia, w których zlokalizowane są zbiory nieinformatyczne.
4. Przebywanie wewnątrz obszarów, o których mowa w ust. 3, osób nieuprawnionych do przetwarzania danych osobowych jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania tych danych lub za zgodą Właściciela zasobów danych osobowych.
5. Wykaz pomieszczeń i stref do przetwarzania danych osobowych prowadzi Administrator Bezpieczeństwa Informacji **/wzór stanowi załącznik nr 10 do niniejszej Polityki/**
6. Budynki lub pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane podczas nieobecności osób upoważnionych do przetwarzania danych osobowych, w sposób ograniczający możliwość dostęp do nich osobom nieupoważnionym.
7. W celu ograniczenia dostępu osób nieupoważnionych do pomieszczeń, w których zlokalizowano przetwarzanie danych osobowych, należy zapewnić:
   1) jasne określenie granic obszaru przetwarzania danych osobowych,
   2) drzwi zewnętrzne odpowiednio zabezpieczone przed dostępem osób niepowołanych,
   3) zamykanie drzwi i okien w pomieszczeniach pozostawianych bez dozoru,
   4) system wykrywania włamań oraz regularne jego testowanie.
8. Ochrona obszarów bezpiecznych powinna być zapewniona poprzez odpowiednie fizyczne zabezpieczenia wejścia zapewniające, że tylko osoby upoważnione mogą uzyskać dostęp, w tym celu należy zapewnić:
   1) nadzorowanie pobytu osób nie będących pracownikami Szkoły w obszarach bezpiecznych, chyba że ich dostęp został wcześniej zaakceptowany,
   2) kontrolowanie i ograniczenie dostępu do obszarów, gdzie są przetwarzane dane osobowe tylko dla uprawnionego personelu.
9. Nośniki elektroniczne zawierające dane osobowe należy przechowywać w zamykanych szafach , które znajdują się w obszarach przetwarzania danych osobowych.
10. Każdorazowe uchybienie zabezpieczeń fizycznych chroniących dane osobowe powinno być zgłaszane do Administratora Bezpieczeństwa Informacji.

§ 17
Dopuszczenie osób do przetwarzania danych osobowych

1.Dyrekcja upoważniona jest do przetwarzania danych osobowych, których Administratorem Danych jest Szkoła oraz danych osobowych, które są przetwarzane na podstawie art. 31 Ustawy.

2. Każda osoba po wejściu w skład Dyrekcji zobowiązana jest zapoznać się z Ustawą oraz niniejszą Polityką i dokumentami powiązanymi.

3.Przetwarzanie danych osobowych przez pracownika jest możliwe wyłącznie po uzyskaniu formalnego upoważnienia do przetwarzania danych osobowych wystawianego przez Dyrektora Szkoły lub Administratora Bezpieczeństwa Informacji /wzór upoważnienia stanowi **załącznik nr 1 i nr 2** do niniejszej Polityki/.

4. Każdy pracownik upoważniony do przetwarzania danych osobowych przed podjęciem pracy w tym zakresie ma obowiązek:

1) zapoznać się z przepisami dotyczącymi ochrony danych osobowych oraz uregulowaniami wewnętrznymi obowiązującymi w tym zakresie w Szkole,
2) złożyć pisemne oświadczenie o zachowaniu danych osobowych i sposobów ich zabezpieczania w tajemnicy, przetwarzania danych osobowych zgodnie z przepisami oraz oświadczenia o znajomości niniejszego dokumentu a także o znajomości „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Szkole." / wzór oświadczenia stanowi **załącznik nr 3** do niniejszej Polityki/.

5.Oświadczenia i upoważnienia, o których mowa wyżej przechowuje się w aktach osobowych pracownika.

§ 18
Ewidencja osób upoważnionych do przetwarzania danych osobowych

1. Osoby upoważnione do przetwarzania danych osobowych powinny być wpisywane do ewidencji. Ewidencja osób upoważnionych do przetwarzania danych osobowych /wzór stanowi **załącznik nr 4** do niniejszej Polityki/ powinna być prowadzona przez Administratora Bezpieczeństwa Informacji i powinna zawierać:
   1) imię i nazwisko osoby upoważnionej do przetwarzania danych osobowych,
   2) zakres upoważnienia do przetwarzania danych osobowych,
   3) wskazanie komórki organizacyjnej, w której osoba upoważniona pracuje,
   4) identyfikator, jeśli osoba upoważniona została zarejestrowana w systemie informatycznym, służącym do przetwarzania danych osobowych,
   5) datę nadania i odebrania uprawnień.
2. Jakakolwiek zmiana w zakresie informacji zawartych w ewidencji powinna podlegać natychmiastowemu odnotowaniu.

§ 19
Dostęp zdalny

1. Zastosowane przez Szkołę rozwiązania techniczne umożliwiające dostęp zdalny do danych osobowych powinny zapewniać integralność, poufność i rozliczalność przetwarzanych danych osobowych oraz ochronę kryptograficzną wobec danych służących do uwierzytelniania przesyłanych publicznymi łączami telekomunikacyjnymi.

2. Nadawanie uprawnień w celu dostępu zdalnego do systemów informatycznych przetwarzających dane osobowe realizowane jest przez Administratora Systemów Informatycznych po spełnieniu wymagań określonych w ust. 1 oraz po uzyskaniu akceptacji Administratora Bezpieczeństwa Informacji.
3. Dostęp do systemów informatycznych dla użytkowników zewnętrznych powinien być monitorowany pod kątem bezpieczeństwa przez Administratora Systemów Informatycznych w celu zapewnienia poufności, rozliczalności i integralności danych osobowych.

§ 20
Rejestracja i aktualizacja zbiorów danych osobowych

1. Upoważnieni pracownicy są zobowiązani do wnioskowania Administratorowi Bezpieczeństwa Informacji zamiaru utworzenia nowego zbioru danych osobowych wraz ze wskazaniem podstawy przetwarzania danych, uzasadnieniem celowości, zakresu i sposobu zbierania danych osobowych.
2. Administrator bezpieczeństwa informacji w ramach prowadzenia rejestru:
   1) wpisuje zbiór danych do rejestru przed rozpoczęciem przetwarzania w zbiorze danych,
   2) aktualizuje informacje dotyczące zbioru danych w rejestrze – w przypadku zmiany informacji objętych wpisem,
   3) wykreśla zbiór danych z rejestru – w przypadku zaprzestania przetwarzania w nim danych osobowych,
   4) udostępnia rejestr do przeglądania.
3. Czynności, o których mowa w ust. 2 pkt 2 i 3, dokonuje się niezwłocznie po zaistnieniu zdarzenia powodującego obowiązek ich dokonania.
4. W sytuacji, jeżeli rejestracja nowopowstałego zbioru danych osobowych jest ustawowo wymagana, Administrator Bezpieczeństwa Informacji przygotowuje projekt zgłoszenia zbioru danych osobowych do rejestracji w GIODO .

§ 21
Udostępnianie danych osobowych

1. Dane osobowe mogą być udostępniane podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa, osobom, których dotyczą oraz w szczególnych przypadkach na podstawie art. 29 ust. 2 Ustawy.
2. Udostępnianie danych osobowych osobie nieupoważnionej do przetwarzania danych osobowych może nastąpić wyłącznie za zgodą Właściciela zasobów danych osobowych. Zgoda może dotyczyć również udostępniania danych osobowych w przyszłości. Zarówno wniosek jak i zgoda powinny być wystosowane z zachowaniem formy pisemnej
3. Udostępniając dane osobowe należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
4. Na pisemny wniosek pochodzący od osoby, której dane dotyczą, informacje o osobie powinny być udzielone w terminie 30 dni od daty złożenia wniosku.

5. Za przygotowanie danych osobowych do udostępnienia w zakresie wskazanym we wniosku jest odpowiedzialny Właściciel zasobów danych osobowych.
6. Odpowiedź na wniosek o udostępnienie danych osobowych przed wysłaniem jest akceptowana i parafowana przez Właściciela zasobów danych osobowych oraz Administratora Bezpieczeństwa Informacji a następnie podpisywana przez Administratora lub upoważnioną osobę z Dyrekcji.
7. W przypadku odpowiedzi na wniosek, o którym mowa w ust. 2, nie od osoby, której dane dotyczą, Właściciel zasobów danych osobowych przekazuje kopię odpowiedzi do Administratora Bezpieczeństwa Informacji.
8. Informacje zawierające dane osobowe są przekazywane uprawnionym podmiotom lub osobom za potwierdzeniem odbioru, np. w następujący sposób:
   1) listem poleconym za pokwitowaniem odbioru,
   2) teletransmisji danych zgodnie z zasadami wymiany informacji opisanymi w § 13 niniejszej Polityki,
   3) innym bezpiecznym, określonym wymogiem prawnym lub umową.
9. Informacja o udostępnieniu danych osobowych podlega odnotowaniu jeśli dane osobowe udostępniane są ze zbioru danych osobowych. W takim przypadku, odnotowaniu podlega informacja o zakresie danych podlegających udostępnieniu, dacie udostępnienia odbiorcy, celu udostępnienia oraz danych osób, które ze strony Szkoły udostępniły dane osobowe. Nie dotyczy to sytuacji, gdy przepisy prawa zezwalają na zbieranie danych osobowych bez konieczności ujawniania adresata danych.

§ 22
Powierzanie przetwarzania danych osobowych

1. Powierzenie przetwarzania danych osobowych występuje wówczas, gdy podmioty zewnętrzne współpracujące ze Szkołą mają dostęp do danych osobowych przetwarzanych przez Szkołę.
2. Wskazane w ust. 1 powierzenie przetwarzania danych osobowych może się odbywać wyłącznie w trybie przewidzianym w art. 31 Ustawy poprzez zawarcie na piśmie umowy powierzenia przetwarzania danych osobowych, pomiędzy Szkołą, a danym podmiotem, któremu zleca się czynności związane z przetwarzaniem danych osobowych.
3. W sytuacji powierzenia przetwarzania danych osobowych podmiotowi zewnętrznemu, w umowie powierzenia przetwarzania danych osobowych określa się przede wszystkim:
   1) zbiór, który zostanie przekazany,
   2) cel i zakres przetwarzania danych osobowych,
   3) obowiązek zachowania w tajemnicy danych osobowych oraz informacji o zabezpieczeniach tych danych,
   4) konsekwencje prawne i kary finansowe wynikające z niestosowania się do warunków umowy (z punktu widzenia ochrony danych osobowych),
   5) wymagania bezpieczeństwa dla procesu przetwarzania danych osobowych.

4. Zalecane jest aby w umowach powierzenia przetwarzania danych osobowych oraz w umowach, na podstawie których dochodzi do wymiany informacji uwzględnić następujące elementy:
   1) definicję informacji, która ma być chroniona,
   2) spodziewany czas trwania umowy, włączając w to przypadki, w których obowiązek zachowania poufności może być bezterminowy,
   3) wymagane działania w momencie zakończenia umowy,
   4) odpowiedzialność i działania obydwu stron podejmowane w celu uniknięcia nieupoważnionego ujawnienia informacji,
   5) zasady zwrotu lub niszczenia danych osobowych przy zakończeniu umowy,
   6) działania podejmowane w przypadku naruszenia warunków umowy.
5. Wykaz podmiotów, którym Administrator Danych Osobowych powierzył przetwarzanie danych osobowych prowadzi Administrator Bezpieczeństwa Informacji /wzór stanowi **załącznik nr 5** do niniejszej polityki/.

§ 23
Postępowanie w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych

1. Poniższe postanowienia mają zastosowanie zarówno w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych przetwarzanych w systemach informatycznych, jak i w zbiorach nieinformatycznych.
2. Przed przystąpieniem do pracy pracownicy zobowiązani są dokonać sprawdzenia stanu urządzeń informatycznych oraz oględzin swojego stanowiska pracy, w tym zwrócić szczególną uwagę, czy nie zaszły okoliczności wskazujące na naruszenie lub próby naruszenia ochrony danych osobowych.
3. Za okoliczności, które uznaje się za naruszenie lub podejrzenie naruszenia ochrony systemu przetwarzającego dane osobowe, uważa się w szczególności:
   1) nieuprawniony dostęp lub próbę dostępu do danych osobowych lub pomieszczeń, w których się one znajdują,
   2) nieuprawnione naruszenie lub próby naruszenia poufności, integralności i rozliczalności danych i systemu,
   3) niezamierzoną zmianę lub utratę danych zapisanych na kopiach zapasowych,
   4) nieuprawniony dostęp do danych osobowych (sygnał o nielegalnym logowaniu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu),
   5) udostępnienie osobom nieupoważnionym danych osobowych lub ich części,
   6) inny stan systemu informatycznego lub pomieszczeń, niż pozostawiony przez użytkownika po zakończeniu pracy,
   7) wydarzenia losowe, obniżające poziom ochrony systemu (np. brak zasilania lub pożar),

8) kradzież sprzętu informatycznego lub nośników zewnętrznych zawierających dane osobowe (np. wydruków komputerowych, dyskietek, płyt CD-ROM, dysków twardych, pamięci zewnętrznych, itp.).

4. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych pracownicy zobowiązani są do bezzwłocznego powiadomienia o tym fakcie Administratora Bezpieczeństwa Informacji.
5. Do czasu przybycia Administratora Bezpieczeństwa Informacji, zgłaszający:
   1) powstrzymuje się od rozpoczęcia lub kontynuowania pracy, jak również od podejmowania jakichkolwiek czynności, mogących spowodować zatarcie śladów naruszenia bądź innych dowodów,
   2) zabezpiecza elementy systemu informatycznego lub kartotek, przede wszystkim poprzez uniemożliwienie dostępu do nich osobom nieupoważnionym,
   3) podejmuje, stosownie do zaistniałej sytuacji, wszelkie niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych,
   4) udokumentuje wstępnie zaistniałe naruszenie,
   5) nie opuszcza bez uzasadnionej potrzeby miejsca zdarzenia do przybycia Administratora Bezpieczeństwa Informacji lub osoby upoważnionej przez Administratora Bezpieczeństwa Informacji,
   6) wykonuje polecenia Administratora Bezpieczeństwa Informacji.
6. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych Administrator Bezpieczeństwa Informacji, po przybyciu na miejsce:
   1) ocenia zastałą sytuację, biorąc pod uwagę w szczególności stan pomieszczeń, w których przetwarzane są dane osobowe oraz stan urządzeń, a także szacuje wielkość negatywnych następstw incydentu,
   2) wysłuchuje relacji osoby, która dokonała powiadomienia oraz innych osób związanych z incydentem,
   3) podejmuje decyzje o toku dalszego postępowania, stosownie do zakresu naruszenia lub zasadności podejrzenia naruszenia ochrony danych osobowych.
7. Administrator Bezpieczeństwa Informacji sporządza raport z przebiegu zdarzenia, w którym powinny się znaleźć w szczególności informacje o:
   1) dacie i godzinie powiadomienia,
   2) godzinie pojawienia się w pomieszczeniach, w których przetwarzane są dane,
   3) sytuacji, jaką zastał,
   4) podjętych działaniach i ich uzasadnieniu,
   5) stanie systemu po podjęciu działań naprawczych,
   6) wnioskach w sprawie ograniczenia możliwości ponownego wystąpienia naruszenia ochrony danych osobowych.

8. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych, użytkownik może kontynuować pracę dopiero po otrzymaniu pozwolenia od Administratora Bezpieczeństwa Informacji.
9. W przypadku, gdy naruszenie ochrony danych osobowych jest wynikiem uchybienia obowiązującej w Szkole dyscypliny pracy, Administrator Bezpieczeństwa Informacji wyjaśnia wszystkie okoliczności incydentu i podejmuje stosowne działania wobec osób, które dopuściły się wskazanego naruszenia.
10. Po zakończeniu czynności naprawczych system powinien utrzymać poziom ochrony nie niższy niż przed wystąpieniem incydentu związanego z naruszeniem ochrony danych osobowych.

§ 24
Wykaz zbiorów danych osobowych wraz z opisem ich struktury

1. Wykaz zbiorów danych osobowych wraz z opisem ich struktury prowadzony i aktualizowany jest przez Administratora Bezpieczeństwa Informacji /wzór stanowi **załącznik nr 6** do niniejszej polityki/.
2. Dane osobowe gromadzone we wskazanych zbiorach są przetwarzane w systemach informatycznych oraz w kartotekach ewidencyjnych, które są zlokalizowane w pomieszczeniach lub części pomieszczeń przetwarzania danych osobowych.
3. Wskazane w rejestrze zakresy danych osobowych przetwarzanych w poszczególnych zbiorach danych osobowych są ustalone w oparciu o strukturę zbiorów danych osobowych prowadzonych w systemach informatycznych.
4. Aktualny opis struktury w/w zbiorów danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi powinien być prowadzony przez Administratora Bezpieczeństwa Informacji.
5. Administrator Bezpieczeństwa Informacji w oparciu o informacje uzyskane od Administratora Systemu, prowadzi wykaz systemów zastosowanych do przetwarzania danych osobowych.

§ 25
Sposób przepływu danych pomiędzy poszczególnymi systemami

1. Administrator Bezpieczeństwa Informacji, w oparciu o informacje uzyskane od Administratora Systemów Informatycznych, prowadzi dokumentację systemów informatycznych zawierającą opis współpracy pomiędzy różnymi systemami informatycznymi oraz sposób przepływu danych pomiędzy systemami w których te dane są przetwarzane /wzór stanowi **załącznik nr 7** do niniejszej polityki/.
2. Administrator Bezpieczeństwa Informacji, w oparciu o informacje uzyskane od Administratora Systemów Informatycznych, prowadzi i systematycznie aktualizuje wykaz aplikacji funkcjonujących w placówce /wzór stanowi **załącznik nr 8** do niniejszej polityki/.

§ 26
Zasady ochrony danych osobowych w zbiorach nieinformatycznych

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

2. Dokumenty i wydruki, zawierające dane osobowe, należy przechowywać w zamykanych pomieszczeniach, do których dostęp mają jedynie uprawnione osoby.
3. Na czas nie użytkowania, dokumenty i wydruki zawierające dane osobowe powinny być zamykane w szafach biurowych lub zamykanych szufladach.
4. Wydruki robocze, błędne lub zdezaktualizowane powinny być niezwłocznie niszczone przy użyciu niszczarki do papieru lub w inny sposób zapewniający skuteczne ich usunięcie.
5. Dla udokumentowania czynności dokonywanych w celu likwidacji zbiorów archiwalnych, powinny być stosowane odpowiednie przepisy dot. zasad archiwizacji i brakowania dokumentacji.

§ 27
Środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych

1. Administrator Bezpieczeństwa Informacji prowadzi wykaz środków technicznych i organizacyjnych, które zostały zastosowane przez Administratora Danych w celu zapewnienia odpowiedniego poziomu bezpieczeństwa przetwarzania danych, a także dla zagwarantowania poufności, integralności i rozliczalności przetwarzanych danych osobowych /**załącznik nr 9** do niniejszej polityki/.

§ 28
Postanowienia końcowe

1. Niezależnie od odpowiedzialności określonej w przepisach prawa powszechnie obowiązującego, naruszenie zasad określonych w niniejszej Polityce może być podstawą rozwiązania stosunku pracy bez wypowiedzenia z osobą, która dopuściła się naruszenia.
2. W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r., o ochronie danych osobowych (Dz. U. z 2016 r, poz. 922 z późn. zm.) oraz przepisy wykonawcze do tej Ustawy.

Wykaz załączników:

Załącznik nr 1	wzór upoważnienia do przetwarzania danych osobowych dla osób zatrudnionych na podstawie umowy o pracę
Załącznik nr 2	wzór upoważnienia do przetwarzania danych osobowych dla osób zatrudnionych na podstawie umowy innej niż umowa o pracę
Załącznik nr 3	wzór oświadczenia o zobowiązaniu się do zachowania poufności
Załącznik nr 4	wzór ewidencji osób upoważnionych do przetwarzania danych osobowych
Załącznik nr 5	wzór wykazu podmiotów, którym Administrator Danych powierzył przetwarzanie danych osobowych
Załącznik nr 6	wzór wykazu zbiorów wraz z opisem ich struktury
Załącznik nr 7	wzór opisu przepływu danych osobowych
Załącznik nr 8	wzór wykazu aplikacji funkcjonujących w placówce
Załącznik nr 9	opis środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych
Załącznik nr 10	Wykaz pomieszczeń i stref do przetwarzania danych osobowych
Załącznik nr 11	protokół z kontroli przetwarzania i stanu zabezpieczenia danych osobowych/czynności sprawdzających

Dokument ujednolicono:	**pieczęć i podpis Administratora Danych:**	**Pieczęć placówki**

DYREKTOR SZKOŁY
mgr Jolanta Kubalska

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Niniejszym, jako Administrator Danych Osobowych/ Administrator Bezpieczeństwa Informacji w Szkole Podstawowej z Oddziałami Integracyjnymi nr 343 im. Matki Teresy z Kalkuty w Warszawie, na podstawie art. 37 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2016 r., poz. 922 ze zm.), **upoważniam:**

Imię i nazwisko upoważnionego pracownika	
Zbiory danych objęte zakresem upoważnienia	

Osoba upoważniona obowiązana jest przetwarzać dane osobowe zawarte w ww. zbiorach danych osobowych w zakresie i w sposób wymagany do wypełnienia obowiązków służbowych względem Administratora Danych.

Osoba upoważniona zobowiązuje się do przetwarzania danych osobowych zgodnie z udzielonym upoważnieniem oraz z przepisami Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2016 r., poz. 922 ze zm.), wydanymi na jej podstawie aktami wykonawczymi i obowiązującymi w Szkole Podstawowej z Oddziałami Integracyjnymi nr 343 im. Matki Teresy z Kalkuty w Warszawie wewnętrznymi regulacjami w sprawie ochrony danych osobowych.

Naruszenie ww. obowiązków może skutkować poniesieniem odpowiedzialności karnej na podstawie przepisów określonych w Ustawie o ochronie danych osobowych oraz stanowi ciężkie naruszenie obowiązków pracowniczych, które może być podstawą rozwiązania umowy o pracę w trybie art. 52 Kodeksu Pracy.

Upoważnienie jest ważne do odwołania.

.....
data i podpis upoważniającego

.....
data i podpis osoby upoważnionej

Oświadczenie

Oświadczam, że zapoznałam/em się z obowiązującymi w zakresie ochrony danych osobowych przepisami prawa i regulacjami wewnętrznymi obowiązującymi w Szkole Podstawowej z Oddziałami Integracyjnymi nr 343 im. Matki Teresy z Kalkuty w Warszawie (w szczególności z Polityką Bezpieczeństwa oraz Instrukcją zarządzania systemem informatycznym). Przyjmuję do wiadomości zawarte w nich obowiązki w zakresie ochrony danych osobowych i zobowiązuję się do ich stosowania.

Świadoma/y jestem obowiązku ochrony danych osobowych na zajmowanym stanowisku i w zakresie udzielonego mi upoważnienia do przetwarzania danych osobowych, a w szczególności obowiązku zachowania w tajemnicy danych osobowych i sposobów ich zabezpieczenia, również po odwołaniu upoważnienia, a także po ustaniu zatrudnienia.

.....
data i podpis osoby upoważnionej

Rozdzielnik 2 egz. w oryginale:

1 x oryginał dokumentacja kadrowa

1 x oryginał osoba upoważniona

Załącznik nr 2 - wzór upoważnienia do przetwarzania danych osobowych dla osób zatrudnionych na podstawie umowy innej niż umowa o pracę

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Niniejszym, jako Administrator Danych Osobowych/ Administrator Bezpieczeństwa Informacji w Szkole Podstawowej z Oddziałami Integracyjnymi nr 343 im. Matki Teresy z Kalkuty w Warszawie, na podstawie

art. 37 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2016 r., poz. 922 ze zm.), **upoważniam:**

Imię i nazwisko upoważnionego	
Zbiory danych objęte zakresem upoważnienia	

Osoba upoważniona obowiązana jest przetwarzać dane osobowe zawarte w ww. zbiorach danych osobowych w zakresie i w sposób wymagany do wypełnienia obowiązków służbowych względem Administratora Danych.

Osoba upoważniona zobowiązuje się do przetwarzania danych osobowych zgodnie z udzielonym upoważnieniem oraz z przepisami Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2016 r., poz. 922 ze zm.), wydanymi na jej podstawie aktami wykonawczymi i obowiązującymi w Szkole Podstawowej z Oddziałami Integracyjnymi nr 343 im. Matki Teresy z Kalkuty w Warszawie wewnętrznymi regulacjami w sprawie ochrony danych osobowych.

Naruszenie ww. obowiązków może skutkować poniesieniem odpowiedzialności karnej na podstawie przepisów określonych w Ustawie o ochronie danych osobowych oraz odpowiedzialności cywilnej.

Upoważnienie jest ważne do odwołania.

.....
data i podpis upoważniającego

.....
data i podpis osoby upoważnionej

Oświadczenie

Oświadczam, że zapoznałam/em się z obowiązującymi w zakresie ochrony danych osobowych przepisami prawa i regulacjami wewnętrznymi obowiązującymi w Szkole Podstawowej z Oddziałami Integracyjnymi nr 343 im. Matki Teresy z Kalkuty w Warszawie (w szczególności z Polityką Bezpieczeństwa oraz Instrukcją zarządzania systemem informatycznym). Przyjmuję do wiadomości zawarte w nich obowiązki w zakresie ochrony danych osobowych i zobowiązuję się do ich stosowania.

Świadoma/y jestem obowiązku ochrony danych osobowych w związku z pełnioną przeze mnie funkcją i w zakresie udzielonego mi upoważnienia do przetwarzania danych osobowych, a w szczególności obowiązku zachowania w tajemnicy danych osobowych i sposobów ich zabezpieczenia, również po odwołaniu upoważnienia, a także po ustaniu stosunku prawnego łączącego mnie z Administratorem Danych.

.....
data i podpis osoby upoważnionej

Rozdzielnik 2 egz. w oryginale:
1 x oryginał dokumentacja kadrowa
1 x oryginał osoba upoważniona

Szkoła Podstawowa
z Oddziałami Integracyjnymi nr 343
im. Matki Teresy z Kalkuty
02-777 Warszawa, ul. Kopcińskiego 7
tel./fax: 22 643-84-54
NIP: 951-13-54-011

Warszawa, dnia .....

OŚWIADCZENIE O ZOBOWIĄZANIU SIĘ DO ZACHOWANIA POUFNOŚCI

Ja niżej podpisana/y . . . . . .

zamieszkała/y w . . . . . .

zatrudniona/y na stanowisku . . . . . .

zobowiązuję się zachować w tajemnicy informacje uzyskane w związku z dopuszczeniem do dostępu do informacji, w stosunku do których istnieje obowiązek zachowania poufności.

Uzyskane informacje zachowam w poufności zarówno w trakcie zatrudnienia, jak i po jego ustaniu.

.....

podpis pracownika

Szkoła Podstawowa
z Oddziałami Integracyjnymi nr 343
im. Matki Teresy z Kalkuty
02-777 Warszawa, ul. Kopcińskiego 7
tel./fax: 22 643-84-54
NIP: 951-13-54-011

Załącznik nr 4 - wzór ewidencji osób upoważnionych do przetwarzania danych osobowych

Nr	Imię i nazwisko osoby upoważnionej	Data nadania upoważnienia	Data ustania upoważnienia	Indywidualny identyfikator w systemie informatycznym	Nazwy zbiorów objętych zakresem upoważnienia
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
11.					
12.					
13.					
14.					

Szkoła Podstawowa
z Oddziałami Integracyjnymi nr 343
im. Matki Teresy z Kalkuty
02-777 Warszawa, ul. Kopcińskiego 7
tel./fax: 22 643-84-54
NIP 951-13-54-011

Załącznik nr 5 - wzór wykazu podmiotów, którym Administrator Danych powierzył przetwarzanie danych osobowych

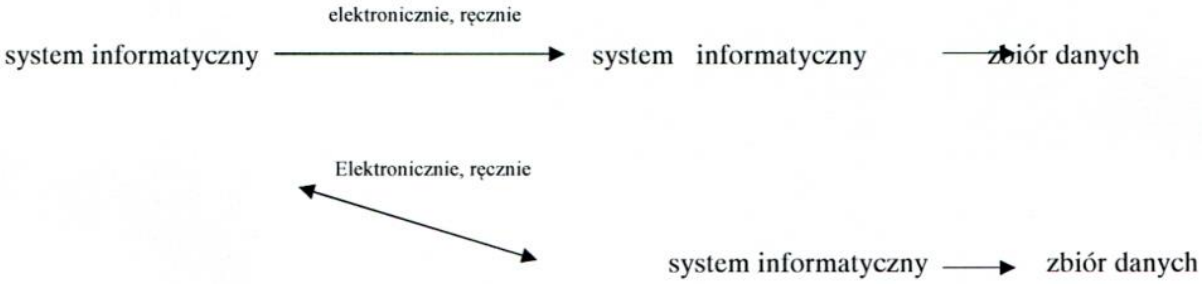
	Adres / lokalizacja	Uwagi
Podmioty, którym Administrator Danych powierzył przetwarzanie danych osobowych		

Szkoła Podstawowa
z Oddziałami Integracyjnymi nr 343
im. Matki Teresy z Kalkuty
02-777 Warszawa, ul. Kopcińskiego 7
tel./fax: 22 643-84-54
NIP: 951-13-54-011

Załącznik nr 6 - wzór wykazu zbiorów wraz z opisem ich struktury

Nr	Nazwa	Systemy informatyczne	Cel przetwarzania	Zakres przetwarzanych danych	Uwagi
1.					
2.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					

Załącznik nr 7 - wzór opisu przepływu danych osobowych



Szkoła Podstawowa
z Oddziałami Integracyjnymi nr 343
im. Matki Teresy z Kalkuty
02-777 Warszawa, ul. Kopcińskiego 7
tel./fax: 22 643-84-54
NIP: 951-13-54-011

Załącznik nr 8 - wzór wykazu aplikacji funkcjonujących w placówce

Lp.	Aplikacja	Wykaz zbioru	Uwagi
1			
2			
3			

Szkoła Podstawowa
z Oddziałami Integracyjnymi nr 343
im. Matki Teresy z Kalkuty
02-777 Warszawa, ul. Kopcińskiego 7
tel./fax: 22 643-84-54

Załącznik nr 9 - opis środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych

ŚRODKI TECHNICZNE

Środek ochrony technicznej i fizycznej	Zastosowano (TAK / NIE)	Uwagi
1. Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym **drzwiami zwykłymi** (niewzmacnianymi, nie przeciwpożarowymi).	**TAK**	
2. Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności na włamanie – drzwi klasy C	**TAK**	
3. Zbiór danych osobowych przechowywany jest w pomieszczeniu, w którym okna zabezpieczone są za **pomocą krat, rolet lub folii antywłamaniowej.**	**TAK**	
4. Pomieszczenia, w którym przetwarzany jest zbiór danych osobowych wyposażone są w **system alarmowy przeciwwłamaniowy.**	**TAK**	
5. Dostęp do pomieszczeń, w których przetwarzany jest zbiory danych osobowych objęte są **systemem kontroli dostępu.**	**TAK**	
6. Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych kontrolowany jest przez **system monitoringu z zastosowaniem kamer przemysłowych.**	**TAK**	
7. Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych jest w czasie **nieobecności zatrudnionych** tam pracowników **nadzorowany przez służbę ochrony.**	**TAK**	
8. Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej **niemetalowej szafie.**	**TAK**	
9. Zbiór danych osobowych w formie papierowej przechowywany jest w **zamkniętej metalowej szafie.**	**TAK**	
10. Zbiór danych osobowych w formie papierowej przechowywany jest **w zamkniętym sejfie lub kasie pancernej.**	**TAK**	
11. **Kopie zapasowe/archiwalne** zbioru danych osobowych przechowywane są w **zamkniętej niemetalowej szafie.**	**NIE**	
12. **Kopie zapasowe/archiwalne** zbioru danych osobowych przechowywane są **w zamkniętej metalowej szafie.**	**NIE**	

13.**Kopie zapasowe/archiwalne** zbioru danych osobowych przechowywane są **w zamkniętym sejfie lub kasie pancernej.**	**TAK**	
14. Pomieszczenie, w którym przetwarzane są zbiory danych osobowych zabezpieczone jest przed skutkami pożaru za pomocą **systemu przeciwpożarowego** i/lub **wolnostojącej gaśnicy.**	**TAK**	
15. Dokumenty zawierające dane osobowe **po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.**	**TAK**	

ŚRODKI ORGANIZACYJNE

Środek organizacyjny	Zastosowano (TAK / NIE)	Uwagi
1.Do przetwarzania danych osobowych dopuszczono wyłącznie osoby posiadające upoważnienie nadane przez administratora danych	**TAK**	
2.Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych	**TAK**	
3.Wyznaczono Administratora Bezpieczeństwa Informacji	**TAK**	
4.Opracowano i wdrożono Politykę Bezpieczeństwa o której mowa w ustawie o ochronie danych osobowych	**TAK**	
5.Opracowano i wdrożono Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych	**TAK**	
6.Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych	**TAK**	
7.Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego	**TAK**	
8.Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy	**TAK**	
9.Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym	**TAK**	
10.Kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco	**TAK**	

Szkoła Podstawowa
z Oddziałami Integracyjnymi nr 343
im. Matki Teresy z Kalkuty
02-777 Warszawa, ul. Kopcińskiego 7
tel./fax: 22 643-84-54
NIP: 951-13-54-011

Warszawa, ...

Wykaz pomieszczeń i stref do przetwarzania danych osobowych

1.	Wykaz pomieszczeń, w których przewarzane są dane osobowe.	
2.	Wykaz pomieszczeń, w których znajdują się komputery stanowiące element systemu informatycznego	
3.	Wykaz pomieszczeń, gdzie przechowuje się wszelkie nośniki informacji zawierające dane osobowe (szafy z dokumentacją papierową, szafy zawierające komputerowe nośniki informacji z kopiami zapasowymi danych, stacje komputerowe, serwery i inne urządzenia komputerowe)	
4.	Wykaz pomieszczeń, w których składowane są uszkodzone komputerowe nośniki danych (taśmy, dyski, płyty CD, dyski przenośne, uszkodzone komputery)	
5.	Wykaz pomieszczeń składnicy akt	
6.	Wykaz pomieszczeń, w których znajdują się klucze do poszczególnych sal (zamykane szafki z kluczami)	

Warszawa, ...

PROTOKÓŁ
Z KONTROLI / CZYNNOŚCI SPRAWDZAJĄCYCH*
w zakresie ochrony danych osobowych

1. Nazwa kontrolowanej jednostki organizacyjnej: .....
2. Zbiory danych osobowych, których przetwarzanie podlega kontroli: .....
3. Data wykonania czynności kontrolnych: .....
4. Imię i nazwisko oraz stanowisko osoby wykonującej czynności kontrolne: .....
5. Imiona i nazwiska osób udzielających informacji dotyczących ochrony danych osobowych w kontrolowanej komórce organizacyjnej: .....
6. Ustalenia dokonane w trakcie czynności kontrolnych:

   .....

   .....

   .....

   .....

   .....

   .....

   Wnioski i zalecenia pokontrolne:

   .....

   .....

   .....

   .....

   .....

   ....

   (data i podpis osoby wykonującej czynności kontrolne) (data i podpis kierownika kontrolowanej kom. organizacyjnej)

Otrzymują:

1 x Administrator Danych Osobowych kontrolowanej placówki

1 x Administrator Bezpieczeństwa Informacji

---

* niepotrzebne skreślić

SZKOŁA PODSTAWOWA Z ODDZIAŁAMI INTEGRACYJNYMI NR 343 im. Matki Teresy z Kalkuty w Warszawie

Al. Stefana Kopcińskiego 7, 02-777 Warszawa. tel./fax: 22 643 84 54; e -mail: sp343@edu.um.warszawa.pl

Załącznik nr 2 do zarządzenia nr 5/2017
Dyrektora Szkoły Podstawowej
z Oddziałami Integracyjnymi nr 343 w Warszawie
z dnia 27 lutego 2017 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W SZKOLE PODSTAWOWEJ Z ODDZIAŁAMI INTEGRACYJNYMI NR 343 IM. MATKI TERESY Z KALKUTY W WARSZAWIE

SPIS TREŚCI

Zawartość

Dokumenty powiązane:

Polityka Bezpieczeństwa przetwarzania danych osobowych w Szkole Podstawowej z Oddziałami Integracyjnymi nr 343 im. Matki Teresy z Kalkuty w Warszawie

§ 1 Postanowienia ogólne

1. Głównym celem wprowadzenia Instrukcji zarządzania systemami informatycznymi jest zapewnienie zgodności działania Szkoły Podstawowej z Oddziałami Integracyjnymi nr 343 im. Matki Teresy z Kalkuty w Warszawie z Ustawą o ochronie danych osobowych oraz jej rozporządzeniami wykonawczymi.
2. Dokument Instrukcji zarządzania systemem informatycznym został opracowany w oparciu o wytyczne zawarte w następujących aktach prawnych:
   1) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024 z późn. zm.),
   2) Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2016 r., poz. 922 z późn. zm.).
3. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Szkole Podstawowej z Oddziałami Integracyjnymi nr 343 im. Matki Teresy z Kalkuty w Warszawie określa zasady, tryb postępowania i zalecenia Administratora Danych, które muszą być stosowane przez osoby przez niego upoważnione do przetwarzania danych osobowych w systemach informatycznych.
4. Podstawowymi celami zabezpieczeń systemów informatycznych służących do przetwarzania danych osobowych jest zapewnienie jak najwyższego poziomu bezpieczeństwa przetwarzanych danych osobowych w systemach informatycznych.
5. Za priorytet uznano zagwarantowanie zgromadzonym danym osobowym, przez cały okres ich przetwarzania w systemach, charakteru poufnego wraz z zachowaniem ich integralności i rozliczalności.
6. Administrator Bezpieczeństwa Informacji powinien posiadać stosowne uprawnienia w nadzorowanych systemach informatycznych, gwarantujące skuteczne wykonywanie zadań z zakresu nadzoru wszędzie tam, gdzie jest to możliwe.

§ 2 Definicje

Użyte w niniejszej Instrukcji pojęcia są wspólne dla wszystkich dokumentów powiązanych z niniejszą Instrukcją oraz dla wszystkich pozostałych dokumentów, które zostały przyjęte w Szkole Podstawowej z Oddziałami Integracyjnymi nr 343 im. Matki Teresy z Kalkuty w zakresie ochrony danych osobowych w Szkole:

1. **ustawa** – ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz. U. 2016 r., poz. 922 z późn. zm.), zwana dalej „Ustawą",
2. **dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
3. **przetwarzanie danych** – 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,
4. **poufność danych** – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom.
5. **Instrukcja**- Instrukcja Zarządzania Systemami Informatycznymi służącym do przetwarzania danych osobowych w Szkole Podstawowej z Oddziałami Integracyjnymi nr 343 im. Matki Teresy z Kalkuty w Warszawie.
6. **Szkoła**- Szkoła Podstawowa z Oddziałami Integracyjnymi nr 343 im. Matki Teresy z Kalkuty w Warszawie.

§ 3 Obowiązki w zakresie ochrony danych osobowych

1. Do obowiązków osób zaangażowanych w przetwarzanie danych osobowych w systemach informatycznych należy:
   1) Podejmowanie współpracy przy ustaleniu przyczyn naruszenia ochrony danych osobowych oraz usuwania skutków tych naruszeń, w tym zapobieganie ich ewentualnemu ponownemu wystąpieniu.
   2) Przetwarzanie danych osobowych wyłącznie w celach określonych przez swoich przełożonych.
2. Do kompetencji osób zarządzających pracownikami należy w szczególności wystawianie dla bezpośrednio podległych pracowników wniosków o nadanie, zmianę lub cofnięcie uprawnień do systemów informatycznych, w których są przetwarzane dane osobowe.
3. Użytkownicy powinni podlegać okresowym szkoleniom, stosownie do potrzeb wynikających ze zmian w systemie informatycznym (wymiana sprzętu na nowszej generacji, zmiana oprogramowania) oraz w związku ze zmianą przepisów o ochronie danych osobowych lub zmianą wewnętrznych regulacji.

§ 4 Obowiązki Administratora Bezpieczeństwa Informacji

Do obowiązków Administratora Bezpieczeństwa Informacji w zakresie ochrony danych osobowych przetwarzanych w systemach informatycznych należy w szczególności:

1) Nadzór nad stosowaniem środków ochrony.
2) Nadzór nad przestrzeganiem przez Administratora Systemów Informatycznych i użytkowników systemu procedur bezpieczeństwa, w szczególności przestrzegania Polityki Bezpieczeństwa obowiązującej w Szkole.
3) Wskazywanie zagrożeń oraz reagowanie na naruszenia ochrony danych osobowych i usuwanie ich skutków.

4) Prowadzenie ewidencji użytkowników systemów informatycznych, w których przetwarzane są dane osobowe, stanowiącej część ewidencji osób upoważnionych do przetwarzania danych osobowych oraz wszelkiej dokumentacji opisującej sposób realizacji i stopień ochrony danych osobowych w Szkole.
5) Kontrolowanie nadanych w systemach informatycznych uprawnień do przetwarzania danych osobowych pod kątem ich zgodności z wpisami umieszczonymi w ewidencji osób upoważnionych do przetwarzania danych osobowych.
6) Prowadzenie szkoleń dla użytkowników w zakresie stosowanych w systemach informatycznych środków ochrony danych osobowych.
7) Uzgadnianie z Administratorem Systemów Informatycznych procedur regulujących wykonywanie czynności w systemach lub aplikacjach służących do przetwarzania danych osobowych.

§ 5 Obowiązki Administratora Systemów Informatycznych

Do obowiązków Administratora Systemów Informatycznych w zakresie ochrony danych osobowych przetwarzanych w systemach informatycznych należy w szczególności:

1) Operacyjne zarządzanie systemami informatycznymi w sposób zapewniający ochronę danych osobowych w nich przetwarzanych.
2) Przestrzeganie opracowanych dla systemu procedur operacyjnych i bezpieczeństwa.
3) Kontrola przepływu informacji pomiędzy systemem informatycznym a siecią publiczną oraz kontrola działań inicjowanych z sieci publicznej a systemem informatycznym.
4) Zarządzanie stosowanymi w systemach informatycznym środkami uwierzytelnienia, w tym rejestrowanie i wyrejestrowywanie użytkowników oraz dokonywanie zmiany uprawnień na podstawie zaakceptowanych wniosków przez osobę do tego upoważnioną.
5) Utrzymanie systemu w należytej sprawności technicznej.
6) Regularne tworzenie kopii zapasowych zasobów danych osobowych oraz programów służących do ich przetwarzania oraz okresowe sprawdzanie poprawności wykonania kopii zapasowych.
7) Wykonywanie lub nadzór nad wykonywaniem okresowych przeglądów i konserwacji, zgodnie z odrębnymi procedurami, sprzętu IT, systemów informatycznych, aplikacji oraz elektronicznych nośników informacji, na których zapisane są dane osobowe.
8) Prowadzenie i systematyczne aktualizowanie Rejestru nadanych uprawnień /wzór stanowi **załącznik nr 1** do niniejszej Instrukcji/

§ 6 Obowiązki Właścicieli zasobów danych osobowych

1. Do obowiązków Właścicieli zasobów danych osobowych w zakresie ochrony danych osobowych przetwarzanych w systemach informatycznych należy w szczególności:
   1) Zapewnienie właściwego poziomu ochrony danych osobowych w systemach, dla danych za które są odpowiedzialni.

2) Informowanie Administratora Bezpieczeństwa Informacji o zmianie celu przetwarzania danych osobowych w systemie lub poszerzeniu zakresu zbieranych danych osobowych.

2. Wykaz zabezpieczeń stosowanych w Szkole stanowi **załącznik nr 2** do niniejszej Instrukcji.

§ 7 Obowiązki użytkowników

Do obowiązków użytkowników systemu informatycznego w zakresie ochrony danych osobowych w systemach informatycznych należy w szczególności

1) Przestrzeganie opracowanych dla systemu zasad przetwarzania danych osobowych.
2) Przestrzeganie opracowanych dla systemu procedur operacyjnych i bezpieczeństwa.
3) Udostępnianie danych osobowych wyłącznie osobom upoważnionym lub uprawnionym do ich uzyskania.
4) Uniemożliwienie dostępu lub podglądu danych osobowych w systemie dla osób nieupoważnionych.
5) Informowanie Administratora Bezpieczeństwa Informacji o wszelkich naruszeniach, podejrzeniach naruszenia i nieprawidłowościach w sposobie przetwarzania i ochrony danych osobowych.
6) Wykonywania poleceń Administratora Bezpieczeństwa Informacji w zakresie ochrony danych osobowych jeśli są one zgodne z przepisami prawa powszechnie obowiązującego.

§ 8 Bezpieczna eksploatacja systemów informatycznych

Bezpieczna eksploatacja systemów informatycznych przetwarzających dane osobowe zostaje zapewniona poprzez przestrzeganie następujących zasad:

1) Użytkownikom zabrania się wprowadzania zmian do oprogramowania, sprzętu informatycznego poprzez jego samodzielne konfigurowanie i wyposażanie.
2) Użytkownikom zabrania się umożliwiania stronom trzecim uzyskiwania nieupoważnionego dostępu do systemów informatycznych.
3) Użytkownikom nie wolno instalować nowego lub aktualizować już zainstalowanego oprogramowania.
4) Użytkownikom nie wolno korzystać z systemów informatycznych dla celów innych niż związane z wykonywaniem obowiązków służbowych.
5) Użytkownikom nie wolno podejmować prób testowania, modyfikacji i naruszenia zabezpieczeń systemów informatycznych lub jakichkolwiek działań noszących takie znamiona.
6) Informacje przetwarzane przy użyciu współdzielonych aplikacji sieciowych na stacjach roboczych muszą być zapisywane na dyskach serwera.
7) Wszystkie aplikacje sieciowe, współdzielone zasoby użytkowe muszą być ulokowane na przeznaczonych do tego celu serwerach.

8) Nieautoryzowane podłączenie własnego lub strony trzeciej urządzenia teleinformatycznego do systemu informatycznego Szkoły jest zabronione.

§9 Nadawanie uprawnień do przetwarzania danych osobowych

1. Użytkownicy systemu przetwarzającego dane osobowe przed przystąpieniem do przetwarzania danych osobowych w tym systemie informatycznym, zobowiązani są zapoznać się z:
   1) Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r., poz. 922 z późn. zm.).
   2) Polityką bezpieczeństwa przetwarzania danych osobowych w Szkole.
2. Użytkownicy przed dopuszczeniem do obsługi systemu informatycznego, w którym przetwarzane są dane osobowe powinni podlegać przeszkoleniu w zakresie obsługi sprzętu informatycznego, oprogramowania systemowego oraz oprogramowania do obsługi aplikacji, którą będą wykorzystywali.
3. Pierwsze zarejestrowanie użytkownika w systemie i nadanie odpowiednich uprawnień do systemu przetwarzającego dane osobowe musi być poprzedzone złożeniem przez użytkownika oświadczenia o:
   1) Zachowaniu w tajemnicy danych osobowych i sposobów ich zabezpieczania oraz przetwarzaniu danych osobowych zgodnie z przepisami.
   2) Uzyskanie formalnego upoważnienia do przetwarzania danych osobowych.
4. Wzory oświadczenia oraz upoważnienia stanowią załączniki nr 1, 2 i 3 do „Polityki bezpieczeństwa przetwarzania danych osobowych w Szkole.
5. Po spełnieniu wymagań określonych w ust. 3, przełożony pracownika albo ABI, w przypadku, gdy dostęp do danych osobowych przetwarzanych w systemie ma uzyskać Dyrekcja, zgłasza wniosek do Administratora Systemów Informatycznych (ASI) o zarejestrowanie użytkownika w systemie (założenie mu konta). Wniosek przekazany do ASI może być przekazany w postaci elektronicznej, ale w takim wypadku konieczna jest jego archiwizacja na odpowiednich nośnikach gwarantujących trwałość i niezmienność zapisu
6. Identyfikator oraz zakres dostępu użytkownika powinien być rejestrowany w rejestrze nadanych uprawnień oraz w ewidencji osób upoważnionych do przetwarzania danych osobowych, określonej w„Polityce bezpieczeństwa przetwarzania danych osobowych w Szkole".
7. Administratorzy Systemów Informatycznych powinni przekazywać użytkownikom tymczasowe hasła dostępowe w sposób bezpieczny. W tym celu powinni unikać pośrednictwa osób trzecich lub korzystania do tego celu z niechronionych wiadomości poczty elektronicznej.
8. Procedurę nadawania uprawnień do przetwarzania danych osobowych w systemach należy stosować odpowiednio, w przypadku zmiany uprawnień w systemach lub w przypadku odebrania uprawnień w systemach.
9. Zmiany dotyczące użytkownika, takie jak rozwiązanie umowy o pracę lub utrata upoważnienia, są przesłanką do natychmiastowego wyrejestrowania użytkownika z systemu oraz unieważnienia

hasła i odnotowanie tego faktu w ewidencji osób upoważnionych do przetwarzania danych osobowych, o której mowa w ust. 6.

10. Prawa dostępu przyznane użytkownikom, którzy nie są pracownikami etatowymi Szkoły powinny mieć charakter czasowy i mogą być przyznawane na okres odpowiadający wykonywanemu zadaniu.
11. Dostęp do systemu informatycznego a także do poszczególnych aplikacji i baz danych przetwarzających dane osobowe powinien być możliwy tylko po podaniu identyfikatora odrębnego dla każdego użytkownika i poufnego hasła.

§ 10 Metody i środki uwierzytelniania w systemie

1. Identyfikatory i hasła są sposobem zagwarantowania rozliczalności, poufności i integralności danych osobowych przetwarzanych w systemach informatycznych. Służą do weryfikowania tożsamości użytkownika, uzyskania dostępu do określonych zasobów.
2. Mając na uwadze zagwarantowanie wysokiego poziomu bezpieczeństwa przetwarzania danych osobowych oraz zagwarantowania użytkownikom pełnej rozliczalności wykonywanych przez nich operacji w systemach informatycznych, wszyscy użytkownicy przy uwierzytelnianiu do systemów informatycznych powinni stosować się do poniższych zasad:
   1) Użytkownik systemu powinien posiadać unikalny identyfikator do swojego osobistego i wyłącznego użytku.
   2) Hasła dostępu do systemów informatycznych powinny być tworzone przez użytkownika i stanowią tajemnicę służbową, znaną wyłącznie temu użytkownikowi z zastrzeżeniem § 8 ust. 7
   3) Użytkownik ponosi pełną odpowiedzialność za utworzenie hasła dostępu oraz jego przechowywanie.
   4) Hasła nie mogą być ujawniane lub przekazywane komukolwiek, bez względu na okoliczności.
   5) Użytkownik nie powinien przechowywać haseł w widocznych miejscach, nie powinien umieszczać haseł w żadnych automatycznych procesach logowania.
3. Użytkownicy są odpowiedzialni za wszelkie działania w systemach informatycznych prowadzone z użyciem ich identyfikatora i hasła.
4. Administrator Systemów Informatycznych jest odpowiedzialny za okresowe sprawdzanie, usuwanie lub blokowanie zbędnych identyfikatorów użytkowników oraz kont w systemach za które są odpowiedzialni.
5. Administrator Systemów Informatycznych powinien przeprowadzać przegląd autoryzacji i uprawnień nie rzadziej niż co 6 miesięcy dla standardowych użytkowników.

§ 11 Wymogi dotyczące uwierzytelniania

1. Wszystkie konta dostępowe (identyfikatory) do systemów informatycznych powinny być chronione hasłem lub innym bezpiecznym, zaakceptowanym przez Administratora Bezpieczeństwa Informacji sposobem uwierzytelniania.

2. Identyfikator oraz nadane uprawnienia powinny umożliwiać wykonywanie czynności wyłącznie zgodnych z zakresem powierzonych obowiązków.
3. Identyfikator użytkownika powinien być niepowtarzalny a po wyrejestrowaniu się z systemu informatycznego nie powinien być przydzielany innej osobie.
4. Identyfikator, który utracił ważność nie może być ponownie przydzielony innemu użytkownikowi.
5. Hasło początkowe, które jest przydzielane przez Administratora Systemów Informatycznych, powinno umożliwiać użytkownikowi zarejestrowanie się w systemie tylko jeden raz i powinno być natychmiast zmienione przez użytkownika.
6. Użytkownicy powinny wybierać hasła dobrej jakości:
   1) Długości co najmniej 8 znaków.
   2) Które są łatwe do zapamiętania, a trudne do odgadnięcia.
   3) Nie są oparte na prostych skojarzeniach, łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących właściciela konta (np. imię, nazwisko, numer telefonu, data urodzenia itp.).
   4) W których występuje przynajmniej jedna duża litera, jedna mała litera, jedna cyfra lub znak specjalny.
   5) W których nie występują kolejne znaki, które nie są topologiczne (tzn. wynikające z układu klawiszy na klawiaturze, typu „qwer6", „zaq1xsw2CDE#" itp.).
7. Hasła nie mogą być takie same jak identyfikator użytkownika oraz nie mogą być zapisywane w systemach w postaci jawnej.
8. Hasła powinny być utrzymywane w tajemnicy również po upływie ich ważności.
9. Należy unikać ponownego lub cyklicznego używania starych haseł.
10. Hasła dla użytkowników o wysokich uprawnieniach (np. administrator) mogą być wykorzystywane tylko w uzasadnionych przypadkach i fakt ten powinien być udokumentowany.
11. Hasła użytkowników o wysokich uprawnieniach powinny być przechowywane w miejscu zabezpieczonym przed dostępem osób nieupoważnionych.
12. Udostępnienie hasła osobie postronnej należy traktować jako poważny incydent naruszenia ochrony danych osobowych.

§ 12 Wymogi dotyczące zmiany haseł

1. Użytkownik jest zobowiązany zmieniać hasło, w którego posiadaniu się znajduje:
   1) Okresowo, zgodnie z wymaganiami dla danego systemu informatycznego (przed upływem terminu ważności hasła).
   2) W przypadku ujawnienia lub podejrzenia ujawnienia hasła.
2. W przypadku braku dostępu do konta chronionego hasłem, w którego posiadaniu się znajduje, użytkownik zobowiązany jest wystąpić o zmianę hasła do właściwego Administratora Systemów Informatycznych, w sytuacji:
   1) Zapomnienia/zgubienia hasła.

2) Wygaśnięcia ważności hasła.

3) Zablokowania konta spowodowanego nieprawidłowym wprowadzeniem hasła.

4) Braku uprawnień/interfejsu umożliwiających samodzielną zmianę hasła.

3. Zmiana haseł użytkowników powinna być wymuszana przez system co 30 dni, w przypadku braku wymuszenia przez system, użytkownik sam jest zobowiązany do zmiany hasła co 30 dni.

§ 13 Procedura bezpiecznego uwierzytelniania

1. Procedura bezpiecznego uwierzytelniania w systemie informatycznym zapewnia minimalizowanie możliwości nieautoryzowanego dostępu do systemu. Procedura powinna ujawniać minimum informacji o systemie informatycznym tak, aby nie pozwolić nieuprawnionemu użytkownikowi na uzyskanie dodatkowych wskazówek w celu ich wykorzystania w sposób niedozwolony. W tym celu należy zapewnić:

   1) Wyświetlanie ogólnego ostrzeżenia, że dostęp do stacji roboczej dozwolony jedynie dla uprawnionych użytkowników.

   2) Zatwierdzanie jedynie kompletnych informacji wejściowych, niezbędnych przy logowaniu jeżeli wystąpi błąd, system nie powinien wskazywać, która część danych jest poprawna, a która niepoprawna.

   3) Ograniczenie liczby nieudanych prób logowania się do systemu, np. do trzech prób, oraz uwzględnić:

      a. wykonywanie zapisu nieudanych i udanych prób,

      b. wymuszanie odstępu czasowego przed każdą kolejną próbą logowania się lub odrzucanie wszelkich dalszych prób, jeśli nie mają specjalnej autoryzacji,

      c. rozłączenie połączeń,

      d. wysłanie wiadomości alarmowej na konsolę systemową w przypadku, gdy maksymalna liczba prób została osiągnięta,

      e. ustawienia maksymalnej liczby prób logowania się w połączeniu z minimalną długością hasła oraz wartością chronionego systemu,

      f. ograniczenie maksymalnego i minimalnego czasu trwania logowania; jeśli zostanie on przekroczony, system powinien przerwać procedurę logowania,

   4) Blokowanie wyświetlania hasła w trakcie wprowadzania lub ukrywanie wprowadzanych znaków pod symbolami.

   5) Blokowanie przesyłania haseł przez sieć jawnym tekstem.

§ 14 Wymagania dotyczące sprzętu i oprogramowania

1. Wygaszacz stacji roboczej powinien być skonfigurowany w taki sposób, aby aktywował się automatycznie po upływie 10 minut od ostatniego użycia stacji roboczej, uruchamiając blokadę stacji roboczej, wymuszającą ponowne zalogowanie.

2. Ekrany monitorów należy ustawić w taki sposób, by uniemożliwić osobom postronnym wgląd lub spisanie informacji aktualnie wyświetlanej na ekranie monitora.

3. Programy zainstalowane na stacjach roboczych stacjonarnych i na komputerach przenośnych obsługujących przetwarzanie danych osobowych muszą być użytkowane z zachowaniem praw autorskich i posiadać licencje.
4. Oprogramowanie może być używane tylko zgodnie z prawami licencji. Oprogramowanie typu Freewere, Shareware lub inne oprogramowanie dostarczane bez opłat jest uznawane jako nieautoryzowane, jeżeli nie otrzyma stosownej aprobaty Administratora Systemów Informatycznych.
5. Przed zainstalowaniem nowego oprogramowania właściwy Administrator Systemów Informatycznych lub inna upoważniona osoba, zobowiązana jest sprawdzić jego działanie pod kątem bezpieczeństwa całego systemu.
6. Sieć teleinformatyczna wykorzystywana do przetwarzania danych osobowych powinna mieć zapewnione prawidłowe zasilanie energetyczne gwarantujące właściwe i zgodne z wymaganiami producenta działanie sprzętu informatycznego.
7. Serwer systemu przetwarzającego dane osobowe powinien być zasilany przez UPS o odpowiednich parametrach, pozwalających na podtrzymanie zasilania przez co najmniej 15 minut oraz na wykonanie, bezpiecznego wyłączenia serwera, tak aby przed ostatecznym zanikiem zasilania zostały prawidłowo zakończone operacje rozpoczęte na zbiorze danych osobowych.
8. Infrastruktura techniczna związana z siecią teleinformatyczną i jej zasilaniem (rozdzielnie elektryczne, skrzynki z bezpiecznikami) powinna być zabezpieczona przed dostępem osób nieupoważnionych.
9. Gniazda zasilania sieci teleinformatycznej powinny być odpowiednio oznakowane, zabezpieczone przed włączeniem do nich innych odbiorników.
10. Wdrażanie aplikacji i oprogramowania eksploatowanych systemów powinno być poprzedzone pozytywnymi testami.
11. Powinna zostać opracowana metoda przywracania poprzedniej wersji, zanim zmiany zostaną wdrożone.

§ 15 Funkcjonalność systemu informatycznego

1. System informatyczny służący do przetwarzania danych osobowych powinien zapewniać dla każdej osoby, której dane osobowe są przetwarzane w tym systemie — z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie — automatyczne odnotowywanie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych, informacji o dacie pierwszego wprowadzenia danych do systemu oraz o identyfikatorze osoby wprowadzającej dane, chyba, że dostęp do systemów informatycznych i przetwarzanych w nim danych posiada wyłącznie jedna osoba, a także o źródle danych, w przypadku zbierania danych nie od osoby, której one dotyczą.
2. Dla każdego systemu służącego do przetwarzania danych osobowych, z którego udostępniane są dane osobowe odbiorcom danych, należy zapewnić odnotowanie w bazie danych tego systemu

informacji, komu, kiedy i w jakim zakresie dane zostały udostępnione, chyba, że dane pochodzą z jawnego zbioru danych osobowych.

3. W przypadku zgłoszenia sprzeciwu o którym mowa w art. 32 ust 1 pkt. 8 Ustawy, wobec przetwarzania danych osobowych system powinien zapewniać odnotowywanie tej informacji.
4. Należy zapewnić dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym sporządzenie i wydrukowanie:
   1) Zestawień zakresu i treści przetwarzanych na jej temat danych osobowych.
   2) Zestawienia zawierającego informacje wymagane w § 7 ust. 1 Rozporządzenia.
5. Zabronione jest nadawanie ukrytych znaczeń elementom numerów porządkowych w aplikacjach ewidencjonujących osoby fizyczne

§ 16 Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie

1. Przed przystąpieniem do pracy z systemem, użytkownik obowiązany jest dokonać sprawdzenia stanu urządzeń informatycznych oraz oględzin swojego stanowiska pracy, ze zwróceniem szczególnej uwagi, czy nie zaszły okoliczności wskazujące na naruszenie ochrony danych osobowych.
2. W przypadku stwierdzenia bądź podejrzenia, iż miało miejsce naruszenie ochrony danych osobowych, użytkownik systemu zobowiązany jest postępować zgodnie z procedurą opisaną w §23 „Polityki bezpieczeństwa przetwarzania danych osobowych w Szkole"
3. 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.
4. 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".
5. Kończąc pracę, użytkownik obowiązany jest do wylogowania się z systemu informatycznego. Zaleca się zamknięcie wszystkich programów i zapisanie wszystkich otwartych plików. Użytkownik powinien zaczekać przy komputerze do chwili jego wyłączenia. Należy zabezpieczyć stanowisko pracy, w szczególności wszelkiej dokumentacji, wydruków oraz wymiennych nośników informacji, na których znajdują się dane osobowe i umieszczenia ich zamykanych szafkach.

§ 17 Przetwarzanie, udostępnianie i likwidacja danych osobowych

1. W przypadku przekazywania urządzeń lub nośników zawierających dane osobowe, poza obszar przetwarzania danych osobowych, zabezpiecza się je w sposób zapewniający poufność, integralność i rozliczalność tych danych, przez co rozumie się:
   1) Ograniczenie dostępu do danych osobowych hasłem zabezpieczającym dane przed osobami nieupoważnionymi.
   2) Stosowanie metod kryptograficznych.
   3) Stosowanie odpowiednich zabezpieczeń fizycznych.
   4) Stosowanie odpowiednich zabezpieczeń organizacyjnych.

   W zależności od stopnia zagrożenia zalecane jest stosowanie kombinacji wyżej wymienionych zabezpieczeń.
2. Nieuzasadnione kopiowanie przez użytkowników plików z serwerów na stacje robocze użytkowników i na elektroniczne nośniki informacji jest zabronione bez akceptacji ze strony Administratora Bezpieczeństwa Informacji.
3. W przypadku udostępniania danych osobowych odbiorcy danych w rozumieniu art. 7 pkt 6 Ustawy, użytkownik ma obowiązek odnotować komu i kiedy udostępniono poszczególne dane.
4. Jeżeli dane osobowe nie są pozyskane od osoby, której dotyczą, użytkownik zobowiązany jest odnotować w systemie informatycznym źródło pochodzenia danych.
5. W przypadku zgłoszenia sprzeciwu o którym mowa w art. 32 ust 1 pkt. 8 Ustawy, wobec przetwarzania danych osobowych użytkownik usuwa z systemu dane osoby zgłaszającej sprzeciw pozostawiając jedynie imię, nazwisko i nr PESEL. W przypadkach wątpliwych użytkownik konsultuje się z Administratorem Bezpieczeństwa Informacji.
6. Dla udokumentowania czynności dokonywanych w celu likwidacji zbiorów danych osobowych nie podlegających archiwizacji w odrębnym trybie dla którego cel przetwarzania ustał, Administrator Bezpieczeństwa Informacji lub osoby upoważnione sporządzają protokół, w którym zamieszczają następujące informacje:
   1) Datę dokonania likwidacji.
   2) Przedmiot likwidacji (aplikacja, baza).
   3) Podpisy osób dokonujących i obecnych przy likwidacji zbiorów danych osobowych.
7. Decyzję o likwidacji zbiorów danych osobowych, przetwarzanych w systemach informatycznych podejmują Właściciele zasobów danych osobowych.
8. W przypadku likwidacji elektronicznych nośników informacji, należy dokonać wcześniej skutecznego usunięcia danych z tych nośników. W przypadku gdy usunięcie danych nie jest możliwe, należy uszkodzić nośniki w sposób uniemożliwiający odczyt tych danych.
9. Przed przekazaniem elektronicznego nośnika informacji osobie nieuprawnionej, należy usunąć z nośnika dane osobowe.

§ 18 Kopie zapasowe

1. Kopie zapasowe zbiorów danych osobowych oraz programów i narzędzi programowych służących do ich przetwarzania powinny być wykonywane na bieżąco przez Administratorów Systemów Informatycznych.
2. Kopie zapasowe powinny być tworzone na nośnikach magnetycznych, odpowiednio opisanych, oznakowanych i ewidencjonowanych.
3. Kopie zapasowe należy opisywać w sposób umożliwiający szybką i jednoznaczną identyfikację zawartych w nich danych.
4. Tworzenie, przechowywanie i likwidację kopii zapasowych powinny regulować szczegółowe instrukcje operacyjne dla poszczególnych systemów informatycznych, opracowywane przez Administratora Systemów Informatycznych, z uwzględnieniem niniejszych postanowień.
5. Administrator Systemów Informatycznych odpowiedzialni za tworzenie kopi zapasowych zobowiązani są przestrzegać terminów sporządzania kopii zapasowych oraz okresowo dokonywać kontroli możliwości odtworzenia danych zapisanych na tych kopiach pod kątem ewentualnej przydatności w sytuacji awarii systemu.
6. Kopie zapasowe powinny być tworzone w bezpiecznym systemie archiwizacji, który powinien zapewniać ograniczony dostęp fizyczny do nośników oraz przyznanie uprawnień dostępu tylko wyznaczonemu imiennie Administratorowi Systemów Informatycznych oraz Administratorowi Bezpieczeństwa Informacji.
7. Dane z kopii zapasowych powinny być odtwarzane wyłącznie przez Administratora Systemów Informatycznych.
8. Kopie zapasowe, które uległy uszkodzeniu powinny podlegać natychmiastowemu zniszczeniu.
9. Niszczenia kopii zapasowych, na nośnikach magnetycznych dokonuje Administrator Systemów Informatycznych lub inna upoważniona przez Dyrekcję osoba.
10. Proces niszczenia kopii zapasowych powinien odbywać się komisyjnie i powinien być dokumentowany.

§ 19 Przechowywanie nośników elektronicznych zawierających dane osobowe

1. Dane osobowe mogą być przechowywane:
   1) Na serwerach zlokalizowanych w obszarach wyznaczonych do przetwarzania danych osobowych.
   2) Na wymiennych nośnikach elektronicznych.
2. Po wykorzystaniu dane osobowe w postaci elektronicznej należy niezwłocznie usunąć z nośnika elektronicznego w sposób uniemożliwiający ich ponowne odtworzenie.
3. Wykorzystanie wymiennych nośników elektronicznych (CD/DVD, pamięć USB, wymienna karta pamięci, dyskietka) powinno być ściśle kontrolowane i dozwolone wyłącznie dla upoważnionych użytkowników.
4. Wymienne nośniki elektroniczne, o ile nie są użytkowane, powinny być przechowywane w zamykanych szafkach.

5. Nośniki zawierające kopie zapasowe powinny być przechowywane w innym pomieszczeniu niż to, w którym umieszczony jest serwer przetwarzający dane osobowe.
6. Kopie zapasowe powinny być przechowywane w odpowiednio zabezpieczonej, ognioodpornej szafie/ sejfie, do której dostęp mogą mieć wyłącznie osoby upoważnione.
7. Nośniki magnetyczne z danymi osobowymi powinny być:
   1) Oznaczane i przechowywane w zamykanych szafach lub sejfach.
   2) Przechowywane maksymalnie przez okres wskazany dla danego rodzaju danych osobowych przez Administratora Bezpieczeństwa Informacji.

§ 20 Ochrona systemu informatycznego przed działaniem szkodliwego oprogramowania

1. Na każdej stacji roboczej w sieci oraz serwerze przetwarzającym dane osobowe powinno być zainstalowane oprogramowanie antywirusowe skanujące na bieżąco system informatyczny.
2. Oprogramowanie antywirusowe powinno być zainstalowane tak aby użytkownik nie był w stanie wyłączyć lub pominąć etapu skanowania.
3. Kontrola antywirusowa powinna być przeprowadzana na wszystkich nośnikach magnetycznych i optycznych, służących zarówno do przetwarzania danych osobowych w systemie, jak i do celów instalacyjnych.
4. Należy stosować wersje programów antywirusowych z aktualną bazą sygnatur wirusów.
5. Nowe wersje oprogramowania antywirusowego oraz uaktualnienia bazy sygnatur wirusów instaluje Administrator Systemów Informatycznych niezwłocznie po ich otrzymaniu lub ściągnięciu, uprzednio weryfikując pochodzenie oprogramowania.
6. W razie zainfekowania systemu Administrator Systemów Informatycznych odpowiada za usunięcie wirusa.
7. Administrator Systemów Informatycznych ma prawo odłączyć od sieci stację roboczą, na której zostanie zlokalizowany wirus, jeśli uzna, że dalsze pozostawienie go w sieci zagraża innym stacjom roboczym.
8. Wykaz zabezpieczenia antywirusowego stanowi **załącznik nr 3** do niniejszej Instrukcji. Wykaz prowadzony jest i systematycznie aktualizowany przez Administratora Systemów Informatycznych.

§ 21 Zasady komunikacji w sieci teleinformatycznej

1. Przesyłanie danych osobowych drogą teletransmisji powinno odbywać się wyłącznie przy wykorzystaniu wymaganych zabezpieczeń logicznych chroniących przed nieuprawnionym dostępem, w szczególności takich jak ochrona kryptograficzna.
2. Pliki zawierające dane osobowe mogą się znajdować jedynie na serwerach, gdzie podlegają ochronie zapewnianej przez mechanizmy bezpieczeństwa systemu operacyjnego.
3. Wyłącznie w sytuacjach wyjątkowych dopuszcza się przetwarzanie danych osobowych w plikach (MS Word, MS Excel) na stacjach roboczych użytkowników, poza bazą danych, znajdującą się w określonym systemie informatycznym.

4. Zgodę na przetwarzanie danych w sytuacjach określonych w ust. 3 wydają Właściciele zasobów danych osobowych.
5. Inne technologie sieciowe takie jak sieci lokalne oparte na falach radiowych nie mogą być wykorzystywane do przekazu informacji, o ile połączenie nie jest szyfrowane. Takie połączenia mogą być używane jedynie dla wymiany poczty elektronicznej o ile wiadomo, że nie zawiera ona danych osobowych.
6. Wszystkie połączenia zewnętrzne do systemu informatycznego powinny być monitorowane.
7. System informatyczny służący do przetwarzania danych osobowych, Administrator Systemów Informatycznych powinien chronić przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.
8. Zabezpieczenia logiczne, o których mowa w ust. 7 powyżej, obejmują:
   1) Kontrolę przepływu informacji pomiędzy systemem informatycznym a siecią publiczną.
   2) Kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego.
9. Kontrola powinna być nadzorowana przez Administratora Systemów Informatycznych.

§ 22 Zasady monitorowania, przeglądu i konserwacji systemu informatycznego

1. Przeglądy, naprawy i konserwacje systemu informatycznego, które będą przeprowadzane w miejscu użytkowania tego systemu wymagają obecności Administratora Systemów Informatycznych lub innej wyznaczonej przez niego osoby.
2. Za prawidłowość przeprowadzenia przeglądów, zapewnienia jakości, konserwację i dokumentowanie zmian w systemach odpowiada Administrator Systemów Informatycznych.
3. W przypadku gdy konieczne jest dokonanie przeglądu, naprawy lub konserwacji systemu informatycznego poza miejscem jego użytkowania, z urządzenia należy wymontować element, na którym zapisane są dane osobowe, o ile jest to możliwe. W przeciwnym wypadku należy zawrzeć z podmiotem dokonującym naprawy umowę powierzenia w rozumieniu art. 31 ustawy o ochronie danych osobowych.
4. Przegląd programów i narzędzi programowych powinien być przeprowadzany w przypadku zmiany wersji oprogramowania aplikacji, zmiany wersji oprogramowania bazy danych lub wykonania zmian w projekcie systemu spowodowanych koniecznością naprawy, konserwacji lub modyfikacji systemu.
5. Przed dokonaniem zmian w systemie informatycznym należy dokonać przeglądu działania systemu w zmienionej konfiguracji w warunkach testowych na testowej bazie danych. Sprawdzenie powinno obejmować: poprawność działania wszystkich elementów aplikacji, poprawność funkcjonalną systemu.
6. Raz do roku należy przeprowadzać weryfikację całego oprogramowania użytkowego eksploatowanego na wszystkich stacjach roboczych podłączonych do systemu informatycznego pod kątem spełnienia wymogów bezpieczeństwa. .

§ 23 Zasady postępowania z komputerami przenośnymi

1. Osoba używająca komputer przenośny zawierający dane osobowe zobowiązana jest zachować szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych osobowych.
2. Osoba używająca komputer przenośny zawierający dane osobowe w szczególności powinna:
   1) Stosować ochronę kryptograficzną wobec danych osobowych przetwarzanych na komputerze przenośnym.
   2) Zabezpieczyć dostęp do komputera na poziomie systemu operacyjnego - identyfikator i hasło.
   3) Nie zezwalać na używanie komputera osobom nieupoważnionym do dostępu do danych osobowych.
   4) Nie wykorzystywać komputera przenośnego do przetwarzania danych osobowych w obszarach użyteczności publicznej.
   5) Zachować szczególną ostrożność przy podłączaniu do sieci publicznych poza obszarem przetwarzania danych osobowych.
3. Użytkownik powinien zachować wyjątkową ostrożność podczas korzystania z zasobów sieci publicznej.
4. Za wszelkie działania wykonywane na komputerze przenośnym odpowiada jego formalny użytkownik.

§ 24 Postepowanie w przypadku stwierdzenia naruszenia ochrony danych

1. Każda osoba, która poweźmie wiadomość w zakresie naruszenia bezpieczeństwa danych przez osobę przetwarzającą dane osobowe bądź posiada informacje mogące mieć wpływ na bezpieczeństwo danych osobowych, jest zobowiązana fakt ten niezwłocznie zgłosić Administratorowi Systemów Informatycznych.
2. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych Administratora Systemów Informatycznych lub upoważnionej przez niego osoby, osoba powiadamiająca powinna:
   1) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków, a następnie ustalić przyczyny, lub sprawców zaistniałego zdarzenia, jeżeli jest to możliwe,
   2) zaniechać dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić jego udokumentowanie i analizę,
   3) udokumentować wstępnie zaistniałe naruszenie,
   4) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora Systemów Informatycznych lub osoby upoważnionej.

3. Po przybyciu na miejsce naruszenia ochrony danych osobowych, Administrator Systemów Informatycznych lub osoba go zastępująca:
   1) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metod dalszego postępowania
   2) wysłuchuje relacji osoby zgłaszającej z zaistniałego naruszenia, jak również relacji każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
4. Administrator Systemów Informatycznych dokumentuje zaistniały przypadek naruszenia oraz sporządza raport według wzoru stanowiącego **Załącznik nr 4** do niniejszej Instrukcji. Raport, o którym mowa powyżej Administrator Systemów Informatycznych niezwłocznie przekazuje Administratorowi Bezpieczeństwa Informacji, a w przypadku jego nieobecności osobie wyznaczonej.
5. Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu, Administrator Systemów Informatycznych zasięga niezbędnych opinii i proponuje postępowanie naprawcze (w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń) i zarządza termin wznowienia przetwarzania danych.

§ 25 Postanowienia końcowe

1. Administrator Bezpieczeństwa Informacji zobowiązany jest zapoznać z treścią Instrukcji każdego użytkownika systemu informatycznego służącego do przetwarzania danych osobowych.
2. W sprawach nieuregulowanych w Instrukcji mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r., o ochronie danych osobowych (t.j. Dz. U. z 2016 r., poz. 922 z późn. zm.) oraz przepisów wykonawczych do tej Ustawy.

Dokument sporządzono:	**pieczęć i podpis Administratora Danych:**	**Pieczęć placówki**
Warszawa, 20.02.2017 r.		

DYREKTOR SZKOŁY
mgr Jolanta Kubalska

Załącznik nr 1

Rejestr nadanych uprawnień

Nr	Nazwa systemu informatycznego	Imię i nazwisko osoby uprawnionej	Data nadania uprawnienia	Data ustania uprawnienia
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				

Załącznik nr 2

Wykaz zabezpieczeń stosowanych w

Szkole Podstawowej z Oddziałami Integracyjnymi nr 343 im. Matki Teresy z Kalkuty w Warszawie

Poziom podstawowy

Nazwa zabezpieczenia	Stosowanie zabezpieczenia
Zabezpieczenie obszaru, w którym przetwarzane są dane osobowe, przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.	
Przebywanie osób nieuprawnionych, jest dopuszczalne za zgodą administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.	
Stosowane są mechanizmy kontroli dostępu do danych.	
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.	
System jest zabezpieczony przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego.	
System jest zabezpieczony przed utratą danych spowodowaną utratą zasilania lub zakłóceniami w sieci zasilającej.	
Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie jest przydzielany innej osobie.	
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.	
Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych osobowych.	
Kopie zapasowe przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem oraz usuwa się niezwłocznie po ustaniu ich użyteczności.	
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.	
Administrator danych monitoruje wdrożone zabezpieczenia systemu informatycznego.	
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.	

Poziom podwyższony

Nazwa zabezpieczenia	Stosowanie zabezpieczenia
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.	
Urządzenia i nośniki zawierające dane osobowe, zabezpiecza się w sposób zapewniający poufność i integralność tych danych.	

Poziom wysoki

Nazwa zabezpieczenia	Stosowanie zabezpieczenia
Administrator danych stosuje środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej.	
System informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.	

Załącznik nr 3

Wykaz oprogramowania antywirusowego zainstalowanego w

Szkole Podstawowej z Oddziałami Integracyjnymi nr 343 im. Matki Teresy z Kalkuty w Warszawie

Typ zabezpieczenia	Nazwa programu	Częstotliwość i sposób aktualizacji oprogramowania
Program/ sprzęt typu FIREWALL		
Program Antywirusowy		

RAPORT

Z NARUSZENIA BEZPIECZEŃSTWA SYSTEMU INFORMATYCZNEGO W STRUKTURZE ORGANIZACYJNEJ ADMINISTRATORA DANYCH

1. Data: ..... Godzina: .....

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

.....

(imię, nazwisko, stanowisko służbowe, nazwa użytkownika (jeśli występuje)

3. Lokalizacja zdarzenia:

.....

(np. nr pokoju, nazwa pomieszczenia)

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

.....

.....

.....

.....

.....

.....

5. Przyczyny wystąpienia zdarzenia:

.....

.....

.....

.....

6. Podjęte działania:

.....

.....

.....

.....

.....

.....

7. Postępowanie wyjaśniające:

.....

.....

.....

....

(data, podpis Administratora Systemów Informatycznych)