POLITYKA BEZPIECZEŃSTWA W ZAKRESIE ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W SZKOLE PODSTAWOWEJ NR. 7 W SOCHACZEWIE

Podstawa prawna:

1. Ustawa z dnia 29 sierpnia 1997r. o ochronie danych osobowych(tekst jednolity: Dz. U. 2016r. poz. 922)
2. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych o organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne, służące do przetwarzania danych osobowych(Dz. U. 2004r. nr. 100 poz. 1024)

I. POSTANOWIENIA WSTĘPNE

1. „Polityka bezpieczeństwa w zakresie zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Szkole Podstawowej, jest dokumentem zwanym dalej polityką bezpieczeństwa, który określa zasady i procedury przetwarzania danych osobowych i ich zabezpieczenia przed nieuprawnionym ujawnieniem.

2. Niniejsza polityka bezpieczeństwa dotyczy zarówno danych osobowych przetwarzanych w sposób tradycyjny w księgach, aktach, wykazach i innych zbiorach ewidencyjnych, jak i w systemach informatycznych.

3. Polityka bezpieczeństwa w zakresie zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, zawiera:
   1) identyfikację zasobów systemu tradycyjnego i informatycznego;
   2) wykaz pomieszczeń, tworzący obszar, w którym przetwarzane są dane osobowe;
   3) wykaz zbiorów danych osobowych oraz programy zastosowane do przetwarzania tych danych;
   4) opis struktury zbiorów danych i sposoby ich przepływu;
   5) środki techniczne i organizacyjne, służące zapewnieniu poufności przetwarzanych danych.

4. Procedury i zasady określone w niniejszym dokumencie stosuje się do wszystkich osób upoważnionych do przetwarzania danych osobowych, zarówno zatrudnionych w szkole jak i innych, np. studentów, odbywających w nim praktyki pedagogiczne.

II. DEFINICJE

Ilekroć w instrukcji jest mowa o:

1) **administratorze danych osobowych** – rozumie się przez to osobę, decydującą o celach i środkach przetwarzania danych. W Szkole Podstawowej nr. 7 w Sochaczewie funkcję administratora danych pełni dyrektor szkoły(ADO);

2) **administratorze bezpieczeństwa informacji** – rozumie się przez to osobę, której administrator danych powierzył pełnienie obowiązków administratora bezpieczeństwa informacji(ABI);

3) **administratorze systemu** – rozumie się przez to osobę nadzorującą pracę systemu informatycznego oraz wykonującą w nim czynności wymagające specjalnych uprawnień;

4) **dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;

5) **zbiór danych** – zestaw danych osobowych posiadający określoną strukturę, prowadzony wg określonych kryteriów oraz celów;

6) **przetwarzanie danych** – wykonywanie jakichkolwiek operacji na danych osobowych, np. zbieranie, utrwalanie, opracowywanie, udostępnianie, zmienianie, usuwanie;

7) **haśle** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym,

8) **identyfikatorze użytkownika** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym (login),

9) **odbiorcy danych** – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem: osoby, której dane dotyczą; osobę upoważnioną do przetwarzania danych; osobę, której powierzono przetwarzanie danych; organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem,

10) **osobie upoważnionej do przetwarzania danych osobowych** – rozumie się przez to pracownika szkoły, który upoważniony został do przetwarzania danych osobowych przez dyrektora szkoły na piśmie;

11) **poufności danych** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom;

12) **raporcie** – rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;

13) **rozporządzeniu MSWiA** – rozumie się przez to 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.);

14) **serwisancie** – rozumie się przez to firmę lub pracownika firmy, zajmującej się instalacją, naprawą i konserwacją sprzętu komputerowego;

15) **sieci publicznej** – rozumie się przez to sieć telekomunikacyjną, wykorzystywaną głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych;

16) **systemie informatycznym** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

17) **szkole** – rozumie się przez to Szkołę Podstawową nr. 7 w Sochaczewie,

18) **teletransmisji** – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;

19) **ustawie** – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r., poz. 922. z późniejszymi zmianami);

20) **uwierzytelnianiu** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;

21) **użytkowniku** – rozumie się przez to pracownika szkoły upoważnionego do przetwarzania danych osobowych, zgodnie z zakresem obowiązków, któremu nadano identyfikator i przyznano hasło,

22) **jednostce** – rozumie się przez to Szkołę Podstawową nr. 7 w Sochaczewie,

23) **kierownictwie** – rozumie się przez to Dyrektora Szkoły Podstawowej,

24) **obszarze kontrolowanym** – rozumie się przez to obszar, znajdujący się pod ochroną, o ograniczonym dostępie osób nieautoryzowanych, w którym odbywa się przetwarzanie danych, w tym danych osobowych.

III. ORGANIZACJA PRZETWARZANIA DANYCH OSOBOWYCH

1. Administrator danych osobowych

Funkcję administratora danych osobowych sprawuje dyrektor szkoły. Administrator danych osobowych realizuje zadania w zakresie ochrony danych osobowych, w tym zwłaszcza:

1) podejmuje decyzje o celach i środkach przetwarzania danych osobowych z uwzględnieniem przede wszystkim zmian w obowiązującym prawie, organizacji administratora danych oraz technik zabezpieczenia danych osobowych,

2) upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnie zakresie, odpowiadającym zakresowi jej obowiązków, oraz odwołuje te upoważnienia lub wyrejestrowuje użytkownika z systemu informatycznego,

3) wyznacza administratora bezpieczeństwa informacji oraz administratora sieci oraz określa zakres ich zadań i czynności,

4) prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych oraz pozostałą dokumentację z zakresu ochrony danych, o ile jako właściwej do jej prowadzenia nie wskaże innej osoby,

5) zapewnia we współpracy z administratorem bezpieczeństwa informacji i systemu użytkownikom odpowiednie stanowiska i warunki pracy, umożliwiające bezpieczne przetwarzanie danych,

6) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur.

2. Administrator bezpieczeństwa informacji

Administrator bezpieczeństwa informacji realizuje zadania w zakresie nadzoru nad przestrzeganiem ochrony danych osobowych, w tym zwłaszcza:

1) sprawuje nadzór nad wdrożeniem stosowanych środków fizycznych, a także organizacyjnych i technicznych w celu zapewnienia bezpieczeństwa danych;

2) sprawuje nadzór nad funkcjonowaniem systemu zabezpieczeń, w tym także nad prowadzeniem ewidencji z zakresu ochrony danych osobowych;

2) koordynuje wewnętrzne audyty przestrzegania przepisów o ochronie danych osobowych;

4) nadzoruje udostępnianie danych osobowych odbiorcom danych i innym podmiotom;

5) zawiera wzory dokumentów (odpowiednie klauzule w dokumentach), dotyczących ochrony danych osobowych;

6) nadzoruje prowadzenie ewidencji i innej dokumentacji z zakresu ochrony danych osobowych;

7) prowadzi oraz aktualizuje dokumentację, opisującą sposób przetwarzanych danych osobowych oraz środki techniczne i organizacyjne, zapewniające ochronę przetwarzanych danych osobowych;

8) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia systemu informatycznego;

9) przygotowuje wyciągi z polityki bezpieczeństwa, dostosowane do zakresów obowiązków osób upoważnionych do przetwarzania danych osobowych;

10) przygotowuje materiały szkoleniowe z zakresu ochrony danych osobowych i prowadzi szkolenia osób upoważnionych do przetwarzania danych osobowych;

11) w porozumieniu z administratorem danych osobowych na czas nieobecności(urlop, choroba) wyznacza swojego zastępcę.

Administrator bezpieczeństwa informacji ma prawo:

1) wyznaczania, rekomendowania i egzekwowania wykonania zadań związanych z ochroną danych osobowych w całej organizacji;

2) wstępu do pomieszczeń w których zlokalizowane są zbiory danych i przeprowadzanie niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z ustawą;

3) żądania złożenia pisemnych lub ustnych wyjaśnień w zakresie niezbędnym do ustalenia stanu faktycznego;

4) żądania okazania dokumentów i wszelkich danych mających bezpośredni związek z problematyką kontroli;

5) żądania udostępnienia do kontroli urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych.

3. Administrator systemu

Administrator systemu realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym administratora danych, w tym zwłaszcza:

1) zarządza systemem informatycznym, w którym są przetwarzane dane osobowe, posługując się hasłem dostępu do wszystkich stacji roboczych z pozycji administratora;

2) przeciwdziała dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe;

3) na wniosek dyrektora szkoły przydziela każdemu użytkownikowi identyfikator(login) oraz hasło do systemu informatycznego oraz dokonuje ewentualnych modyfikacji uprawnień, a także usuwa konta użytkowników.

4) nadzoruje działanie mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych;

5) podejmuje działania w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego;

6) wyrejestrowuje użytkowników na polecenie administratora danych;

7) zmienia w poszczególnych stacjach roboczych hasła dostępu, ujawniając je wyłącznie danemu użytkownikowi oraz, w razie potrzeby, administratorowi bezpieczeństwa informacji lub administratorowi danych;

8) w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego informuje administratora bezpieczeństwa informacji o naruszeniu i współdziała z nim przy usuwaniu skutków naruszenia;

9) prowadzi szczegółową dokumentację naruszeń bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym;

10) sprawuje nadzór nad wykonywaniem napraw, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe, nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego;

11) podejmuje działania, służące zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji.

4. Osoba upoważniona do przetwarzania danych

Osoba upoważniona do przetwarzania danych osobowych jest zobowiązana przestrzegać następujących zasad:

1) może przetwarzać dane osobowe wyłącznie w zakresie ustalonym indywidualnie przez administratora danych w upoważnieniu i tylko w celu wykonywania nałożonych

obowiązków. Rozwiązanie stosunku pracy, odwołanie z pełnionej funkcji powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych;

2) musi zachować tajemnicę danych osobowych oraz przestrzegać procedur ich bezpiecznego przetwarzania. Przestrzeganie tajemnicy danych osobowych obowiązuje przez cały okres zatrudnienia u administratora danych, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji;

3) zapoznaje się z przepisami prawa w zakresie ochrony danych osobowych oraz postanowieniami niniejszej polityki i instrukcji zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych;

4) stosuje określone przez administratora danych oraz administratora bezpieczeństwa informacji procedury oraz wytyczne mające na celu zgodne z prawem, w tym zwłaszcza adekwatne, przetwarzanie danych;

5) korzysta z systemu informatycznego administratora danych w sposób zgodny ze wskazówkami zawartymi w instrukcji obsługi urządzeń wchodzących w skład systemu informatycznego, oprogramowania i nośników;

6) zabezpiecza dane przed ich udostępnianiem osobom nieupoważnionym.

IV.IDENTYFIKACJA ZASOBÓW SYSTEMU INFORMATYCZNEGO

1. Struktura informatyczna Zespołu Szkół składa się z sieci wewnętrznej. Informacje przetwarzane w tej strukturze są jawne, ale podlegają ochronie zgodnie z przepisami ustawy.

2. Wymiana danych możliwa jest za pośrednictwem takich nośników, jak: płyty CD-ROM, przenośnej pamięci USB, oraz za pośrednictwem usług internetowych – poczty elektronicznej. Jako system operacyjny wykorzystywany jest Windows XP Microsoft.

V. WYKAZ POMIESZCZEŃ, TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE

1. Przetwarzaniem danych osobowych jest wykonywanie jakichkolwiek operacji na danych osobowych, takich jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza tych, które wykonuje się w systemie informatycznym.

2. Dane osobowe przetwarzane są tylko i wyłącznie na terenie Szkoły Podstawowej nr. 7 w Sochaczewie.

3. Ze względu na szczególne nagromadzenie danych osobowych szczególnie chronione powinny być pomieszczenia znajdujące się w budynku szkoły, zgodnie z poniższym wykazem.

Wykaz budynków lub części pomieszczeń tworzących obszar,
w którym przetwarzane są dane osobowe
(Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r.)

Lp.	Dokładny adres	Dział użytkujący pomieszczenie	Zabezpieczenie
1.	Ul. Fryderyka Chopina 99, 96-500 Sochaczew	Gabinet Dyrektora	Kluczami dysponuje Dyrektor
2.	Ul. Fryderyka Chopina 99, 96-500 Sochaczew	Sekretariat	Kluczami dysponuje Sekretarz Szkoły oraz osoba sprzątająca
3.	Ul. Fryderyka Chopina 99, 96-500 Sochaczew	Gabinet kierownika administracji i intendenta	Kluczami dysponują osoby pracujące w tym gabinecie oraz osoba sprzątająca
4.	Ul. Fryderyka Chopina 99, 96-500 Sochaczew	Biblioteka	Kluczami dysponują osoby pracujące w bibliotece oraz osoba sprzątająca
5.	Ul. Fryderyka Chopina 99, 96-500 Sochaczew	Gabinet pedagoga	Kluczami dysponuje pedagog oraz osoba sprzątająca
6.	Ul. Fryderyka Chopina 99, 96-500 Sochaczew	Gabinet psychologa	Kluczami dysponuje psycholog oraz osoba sprzątająca
7.	Ul. Fryderyka Chopina 99, 96-500 Sochaczew	Gabinet medyczny	Kluczami dysponują pielęgniarki oraz osoba sprzątająca
8.	Ul. Fryderyka Chopina 99, 96-500 Sochaczew	Pomieszczenie stanowisk do spraw kadrowych	Kluczami dysponują osoby tu pracujące oraz osoba sprzątająca
9.	Ul. Fryderyka Chopina 99, 96-500 Sochaczew	Pokój nauczycielski	Kluczami dysponują nauczyciele oraz osoba sprzątająca
10.	Ul. Fryderyka Chopina 99, 96-500 Sochaczew	Gabinet wicedyrektora	Kluczami dysponuje wicedyrektor oraz osoba sprzątająca
11.	Ul. Chodakowska 4, 96-500 Sochaczew	Gabinet wicedyrektora(klas I-III)	Kluczami dysponuje wicedyrektor oraz osoba sprzątająca

VI.STRUKTURA ZBIORÓW DANYCH, SPOSÓB PRZEPŁYWU DANYCH I ZAKRES ICH PRZETWARZANIA

Rejestr zbiorów danych osobowych ze wskazaniem programów do przetwarzania tych danych

L.p.	Nazwa zbioru	Zastosowane programy	Uwagi
1.	Dane pracownicze	Ewidencja papierowa, elektroniczna ewidencja pracownicza	Teczki akt osobowych, VULCAN, sekretariat, SIO, PEFRON
2.	Dane uczniów i związane z nimi dane rodziców/opiekunów prawnych	Ewidencja papierowa, elektroniczna ewidencja	SIO, OKE, Hermes, sekretariat, Optivum
3.	Rejestr uczniów realizujących obowiązek szkolny w innych placówkach	Ewidencja papierowa, elektroniczna ewidencja	SIO, OKE, VULCAN, sekretariat, Optivum
4.	Zamówienia publiczne	Ewidencja papierowa, elektroniczna ewidencja	Forma papierowa
5.	Archiwum	Ewidencja papierowa	Forma papierowa
6.	Upoważnienia do odbioru dzieci	Ewidencja papierowa	Znajdują się u nauczycieli
7.	Rejestr korespondencji	Ewidencja papierowa	Znajduje się w sekretariacie
8.	Dane kontrahentów	Ewidencja papierowa	Znajdują się w pokoju kierownika gospodarczego
9.	Dane serwisu internetowego szkoły	zs.sochaczew@wp.pl	

Opis struktury zbiorów danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami(Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r.)

Lp.	Nazwa zbioru danych	Struktura zbiorów	Przepływ danych	Uwagi
1.	Dane pracownicze	Imię, imiona, nazwisko, data i miejsce urodzenia, imiona rodziców, adres zamieszkania, nr telefonu, wykształcenie, przebieg dotychczasowego zatrudnienia, PESEL, NIP, nr dowodu osobistego	Papierowa i elektroniczna ewidencja pracownicza	Składowana na potrzeby kadrowe

2.	Dane uczniów	Imię, imiona, nazwisko, data urodzenia, miejsce urodzenia, imiona rodziców, adres zamieszkania, PESEL	Papierowa i elektroniczna ewidencja	Na potrzeby szkoły
3.	Rejestr uczniów	Imię, imiona, nazwisko, data urodzenia, miejsce urodzenia, imiona rodziców, adres zamieszkania, PESEL	Papierowa i elektroniczna ewidencja	Na potrzeby szkoły
4.	Zamówienia publiczne	Nazwa firmy, adres, nr telefonu	Ewidencja papierowa	Na potrzeby szkoły
5.	Archiwum	Tak jak w pkt. 1 i 2 oraz dane księgowe	Ewidencja papierowa	Na potrzeby szkoły
6.	Upoważnienia do odbioru dzieci	Imię i nazwisko opiekunów odbierających dzieci	Ewidencja papierowa	Na potrzeby szkoły
7.	Rejestr korespondencji	Pisma przychodzące i wychodzące, nr korespondencji, nazwa	Ewidencja papierowa	Na potrzeby szkoły
8.	Dane kontrahenta	Nazwa firmy, NIP, termin płatności, nr konta, nazwa banku	Ewidencja papierowa	Na potrzeby szkoły
9.	Kopie faktur	Nazwa firmy, NIP, termin płatności, nr konta, nazwa banku	Ewidencja papierowa	Na potrzeby szkoły
10.	Dane serwisu internetowego szkoły		Ewidencja elektroniczna	Składowana na potrzeby wizerunku szkoły

VII. ŚRODKI TECHNICZNE I ORGANIZACYJNE, SŁUŻĄCE ZAPEWNIENIU POUFNOŚCI PRZETWARZANYCH DANYCH

1. Bezpieczeństwo osobowe

Zachowanie poufności

1. Dyrektor szkoły danych przeprowadza nabór na wolne stanowiska. Kandydaci na pracowników są dobierani z uwzględnieniem ich kompetencji merytorycznych, a także kwalifikacji moralnych. Zwraca się uwagę na takie cechy kandydata, jak uczciwość, odpowiedzialność, przewidywalność zachowań.

2. Ryzyko utraty bezpieczeństwa danych przetwarzanych w szkole, pojawiające się ze strony osób trzecich, które mają dostęp do danych osobowych (np. serwisanci), jest minimalizowane przez podpisanie umów powierzenia przetwarzania danych osobowych.

3. Ryzyko ze strony osób, które potencjalnie mogą w łatwiejszy sposób uzyskać dostęp do danych osobowych (np. osoby sprzątające pomieszczenia szkolne), jest minimalizowane przez zobowiązywanie ich do zachowania tajemnicy.

4. Ryzyko ze strony osób, które dokonują bieżących napraw komputera, minimalizowane jest obecnością użytkownika systemu.

Szkolenia w zakresie ochrony danych osobowych

1. Administrator bezpieczeństwa informacji uwzględnia następujący plan szkoleń:
a) szkoli się każdą osobę, która ma zostać upoważniona do przetwarzania danych osobowych,
b) szkolenia wewnętrzne wszystkich osób upoważnionych do przetwarzania danych osobowych przeprowadzane są w przypadku każdej zmiany zasad lub procedur ochrony danych osobowych,
c) przeprowadza się szkolenia dla osób innych niż upoważnione do przetwarzania danych, jeśli pełnione przez nie funkcje wiążą się z zabezpieczeniem danych osobowych.

2. Strefy bezpieczeństwa

W szkole wydzielono strefę bezpieczeństwa, tj: sekretariat z kasą pancerną, gabinet dyrektora szkoły, w których mogą przebywać inni użytkownicy danych tylko w jego obecności; to samo dotyczy uczniów, ich rodziców oraz interesantów; nikt z osób postronnych nie może przebywać sam w sekretariacie i gabinecie dyrektora; kluczem do gabinetu dyrektora i sekretariatu może dysponować na stałe dyrektor i sekretarz szkoły po złożeniu odpowiedniego oświadczenia o konsekwencjach służbowych i dyscyplinarnych, wynikających z faktu ich zagubienia.

3. Zabezpieczenie sprzętu

1. Wszystkie urządzenia systemu informacyjnego w szkole są zasilane za pośrednictwem zasilaczy awaryjnych (UPS).

2. W celu zapewnienia większego bezpieczeństwa i ochrony danych powinno wykorzystać się system operacyjny Microsoft Windows.

3. Administrator systemu jest jedyną osoba uprawnioną do instalowania i usuwania oprogramowania systemowego i narzędziowego.

4. Bieżąca konserwacja sprzętu wykorzystywanego w szkole do przetwarzania danych prowadzona jest przez jej pracowników, przede wszystkim przez administratora sieci.

5. Poważne naprawy wykonywane przez pracowników firm zewnętrznych realizowane są w budynku szkoły po zawarciu z podmiotem wykonującym naprawę umowy o powierzenie przetwarzania danych osobowych, określającej kary umowne za naruszanie bezpieczeństwa danych.

6. Wszystkie awarie, działania konserwacyjne i naprawy systemu informatycznego są opisywane w stosownych protokołach, które podpisują osoby uczestniczące w naprawie lub konserwacji.

4. Zabezpieczenia we własnym zakresie

W celu podniesienia bezpieczeństwa danych każda osoba upoważniona do przetwarzania danych lub użytkownik systemu informatycznego zobowiązani są do:

1) ustawiania ekranów komputerowych tak, aby osoby niepowołane nie mogły oglądać ich zawartości, a zwłaszcza nie naprzeciwko wejścia do pomieszczenia;

2) niepozostawienia bez kontroli dokumentów i nośników danych w klasach i innych miejscach publicznych oraz w samochodach;

3) dbania o prawidłową wentylację komputerów (nie można zasłaniać kratek wentylatorów meblami, zasłonami lub stawiać komputerów tuż przy ścianie);

4) niepodłączania do listew, podtrzymujących napięcie, przeznaczonych dla sprzętu komputerowego innych urządzeń, szczególnie tych łatwo powodujących spięcia (np. grzejniki, czajniki, wentylatory);

5) pilnego strzeżenia akt;

6) kasowania po wykorzystaniu danych na dyskach przenośnych;

7) nieużywania powtórnie dokumentów zadrukowanych jednostronnie;

8) niezapisywania hasła wymaganego do uwierzytelnienia się w systemie na papierze lub innym nośniku;

9) powstrzymywania się przez osoby upoważnione do przetwarzania danych osobowych od samodzielnej ingerencji w oprogramowanie i konfigurację powierzonego sprzętu, nawet gdy z pozoru mogłoby to usprawnić pracę lub podnieść poziom bezpieczeństwa danych;

10) przestrzegania przez osoby upoważnione do przetwarzania danych osobowych swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła oraz stosowania się do zaleceń administratora bezpieczeństwa informacji;

11) opuszczania stanowiska pracy dopiero po aktywizowaniu wygaszacza ekranu lub po zablokowaniu stacji roboczej w inny sposób;

12) kopiowania tylko jednostkowych danych (pojedynczych plików). Obowiązuje zakaz robienia kopii całych zbiorów danych lub takich ich części, które nie są konieczne do wykonywania obowiązków przez pracownika. Jednostkowe dane mogą być kopiowane na nośniki magnetyczne, optyczne i inne po ich zaszyfrowaniu i przechowywane w zamkniętych na klucz szafach. Po ustaniu przydatności tych kopii dane należy trwale skasować lub fizycznie zniszczyć nośniki, na których są przechowywane;

13) udostępniania danych osobowych pocztą elektroniczną tylko w postaci zaszyfrowanej;

14) niewynoszenia na jakichkolwiek nośnikach całych zbiorów danych oraz szerokich z nich wypisów, nawet w postaci zaszyfrowanej;

15) wykonywania kopii roboczych danych, na których się właśnie pracuje, tak często, aby zapobiec ich utracie;

16) kończenia pracy stacji roboczej po wprowadzeniu danych przetwarzanych tego dnia w odpowiednie obszary serwera, a następnie prawidłowym wylogowaniu się użytkownika i wyłączeniu komputera oraz odcięciu napięcia w UPS i listwie;

17) niszczenia w niszczarce lub chowania do szaf zamykanych na klucz wszelkich wydruków zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończonym dniu pracy;

18) niepozostawianie osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe, bez obecności osoby upoważnionej do przetwarzania danych osobowych;

19) zachowania tajemnicy danych, w tym także wobec najbliższych;

20) umieszczanie kluczy do szaf w ustalonym, przeznaczonym do tego miejscu po zakończeniu dnia pracy;

21) zamykanie okien w razie opadów czy innych zjawisk atmosferycznych, które mogą zagrozić bezpieczeństwu danych osobowych;

22) zamykanie okien w razie opuszczania pomieszczenia, w tym zwłaszcza po zakończeniu dnia pracy;

23) zamykania drzwi na klucz po zakończeniu pracy w danym dniu. Jeśli niemożliwe jest umieszczenie wszystkich dokumentów, zawierających dane osobowe w zamykanych szafach, należy powiadomić o tym dyrektora szkoły.

5. Wykorzystywanie akt i dokumentów szkolnych do pracy w domu

1. Wykorzystywanie akt i dokumentów, zawierających dane osobowe (dzienniki lekcyjne, arkusze ocen), do pracy w domu jest możliwe tylko po uzyskaniu upoważnienia na piśmie, udzielanego przez dyrektora szkoły.

2. Sekretarz szkoły lub upoważniona przez niego osoba prowadzi ewidencję akt spraw i dokumentów szkolnych, wynoszonych przez uprawnionych pracowników.

3. Niedopuszczalne jest pozostawienie akt lub dokumentów bez dozoru w czasie ich przenoszenia do domu np. w samochodzie.

4. Z wynoszonych dokumentów może korzystać wyłącznie upoważniony pracownik, który powinien dołożyć wszelkich starań, aby osoby postronne, w tym domownicy, nie mogły mieć do nich dostępu. Dokumenty przechowywane w domu, w czasie, w którym nie są konieczne do wykonywania pracy, powinny być zamykane w sposób uniemożliwiający dostęp osób innych niż upoważniony pracownik.

5. Upoważniony pracownik po zakończeniu wykonywania pracy w domu powinien niezwłocznie zwrócić dokumenty dyrektorowi szkoły.

6. Pracownicy, wynoszący dokumenty i akta spraw do domu, są obowiązani do ochrony danych w nich zawartych i w razie ich udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym podlegają grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2 zgodnie z art. 51 ustawy.

6. Postępowanie z nośnikami danych i ich bezpieczeństwo

Osoby upoważnione do przetwarzania danych osobowych powinny pamiętać zwłaszcza, że:

1) dane z nośników przenośnych niebędących kopiami zapasowymi po wprowadzeniu do systemu informatycznego administratora danych powinny być trwale usuwane z tych nośników przez fizyczne zniszczenie (np. płyty CD-ROM) lub usunięcie danych programem trwale usuwającym pliki. Jeśli istnieje uzasadniona konieczność, dane pojedynczych osób (a nie całe zbiory czy szerokie wypisy ze zbiorów) mogą być przechowywane na specjalnie oznaczonych nośnikach. Nośniki te muszą być przechowywane w zamkniętych na klucz szafach, nieudostępnianych osobom postronnym. Po ustaniu przydatności tych danych nośniki powinny być trwale kasowane lub niszczone;

2) uszkodzone nośniki przed ich wyrzuceniem należy zniszczyć fizycznie w niszczarce służącej do niszczenia nośników;

3) zabrania się powtórnego używania do sporządzania brudnopisów pism jednostronnie zadrukowanych kart, jeśli zawierają one dane chronione. Zaleca się natomiast dwustronne drukowanie brudnopisów pism i sporządzanie dwustronnych dokumentów;

4) po wykorzystaniu wydruki, zawierające dane osobowe, należy codziennie przed zakończeniem pracy zniszczyć w niszczarce. O ile to możliwe, nie należy przechowywać takich wydruków w czasie dnia na biurku ani też wynosić poza siedzibę administratora danych.

7. Kontrola dostępu do systemu

1. Poszczególnym osobom upoważnionym do przetwarzania danych osobowych przydziela się konta opatrzone niepowtarzalnym identyfikatorem, umożliwiające dostęp do danych, zgodnie z zakresem upoważnienia do ich przetwarzania. Administrator bezpieczeństwa informacji po uprzednim przedłożeniu upoważnienia do przetwarzania danych osobowych, zawierającego odpowiedni wniosek dyrektora szkoły, przydziela pracownikowi upoważnionemu do przetwarzania danych konto w systemie informatycznym, dostępne po wprowadzeniu prawidłowego identyfikatora i uwierzytelnieniu hasłem. System wymusza zmianę hasła przy pierwszym logowaniu.

2. Pierwsze hasło wymagane do uwierzytelnienia się w systemie przydzielane jest przez administratora bezpieczeństwa informacji po odebraniu od osoby upoważnionej do przetwarzania danych oświadczenia, zawierającego zobowiązanie do zachowania w tajemnicy pierwszego i następnych haseł oraz potwierdzenie odbioru pierwszego hasła.

3. Do zagwarantowania poufności i integralności danych osobowych konieczne jest przestrzeganie przez użytkowników swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła oraz stosowania się do zaleceń administratora bezpieczeństwa informacji.

8. Kontrola dostępu do sieci

1. System informatyczny posiada szerokopasmowe połączenie z Internetem. Dostęp do niego jest jednak ograniczony. Na poszczególnych stacjach roboczych można przeglądać tylko wyznaczone strony www.

2. Korzystanie z zasobów sieci wewnętrznej (internet) jest możliwe tylko w zakresie uprawnień przypisanych do danego konta osoby upoważnionej do przetwarzania danych osobowych.

9. Udostępnianie danych osobowych

1. Udostępnianie danych osobowych policji, służbie miejskiej i sądom może nastąpić w związku z prowadzonym przez nie postępowaniem.

2. Udostępnianie informacji policji odbywa się według następującej procedury:

1) udostępnianie danych osobowych funkcjonariuszom policji może nastąpić tylko po przedłożeniu wniosku o przekazanie lub udostępnienie informacji. Wniosek ten powinien mieć formę pisemną i zawierać:

a) oznaczenie wnioskodawcy,
b) wskazanie przepisów uprawniających do dostępu do informacji,
c) określenie rodzaju i zakresu potrzebnych informacji oraz formy ich przekazania lub udostępnienia,
d) wskazanie imienia, nazwiska i stopnia służbowego policjanta upoważnionego do pobrania informacji lub zapoznania się z ich treścią.

2) udostępnianie danych osobowych na podstawie ustnego wniosku, zawierającego wszystkie powyższe cztery elementy wniosku pisemnego, może nastąpić tylko wtedy, gdy zachodzi konieczność niezwłocznego działania, np. w trakcie pościgu za osobą podejrzaną o popełnienie czynu zabronionego albo podczas wykonywania czynności mających na celu ratowanie życia i zdrowia ludzkiego lub mienia.
3) osoba udostępniająca dane osobowe, jest obowiązana zażądać od policjanta pokwitowania pobrania dokumentów zawierających informacje przekazane na podstawie pisemnego wniosku albo potwierdzenia faktu uzyskania wglądu w treść informacji. Policjant jest obowiązany do pokwitowania lub potwierdzenia.
4) jeśli informacje są przekazywane na podstawie ustnego wniosku, należy stosownie do okoliczności zwrócić się z prośbą o pokwitowanie albo potwierdzenie. Jeśli pokwitowanie albo potwierdzenie ze względu na okoliczności udostępniania nie są możliwe, osoba udostępniająca informacje sporządza na tę okoliczność notatkę służbową.
5) jeśli policjant pouczył osobę udostępniającą informacje o konieczności zachowania tajemnicy faktu i okoliczności przekazania informacji, to okoliczność ta jest odnotowywana w rejestrze udostępnień niezależnie od odnotowania faktu udostępniania informacji.

3. Innym podmiotom dane osobowe, dotyczące pracowników i uczniów szkoły, nie mogą być udostępniane.

10. Odpowiedzialność osób upoważnionych do przetwarzania danych osobowych

Niezastosowanie się do prowadzonej przez administratora danych polityki bezpieczeństwa przetwarzania danych osobowych, której założenia określa niniejszy dokument i naruszenie 18 procedur ochrony danych przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52 Kodeksu pracy. Niezależnie od rozwiązania stosunku pracy osoby popełniające przestępstwo, będą pociągane do odpowiedzialności karnej, zwłaszcza na podstawie art. 51 i 52. ustawy oraz art. 266. Kodeksu karnego. Przykładowo przestępstwo można popełnić wskutek:

1) stworzenia możliwości dostępu do danych osobowych osobom nieupoważnionym albo osobie nieupoważnionej,
2) niezabezpieczenia nośnika lub komputera przenośnego,
3) zapoznania się z hasłem innego pracownika wskutek wykonania nieuprawnionych operacji w systemie informatycznym administratora danych.

VIII. PRZEGLĄDY POLITYKI BEZPIECZEŃSTWA I AUDYTY SYSTEMU

Polityka bezpieczeństwa powinna być poddawana przeglądowi przynajmniej raz na rok. W razie istotnych zmian dotyczących przetwarzania danych osobowych administrator bezpieczeństwa informacji może zarządzić przegląd polityki bezpieczeństwa stosownie do potrzeb.
Administrator bezpieczeństwa informacji analizuje, czy polityka bezpieczeństwa i pozostała dokumentacja z zakresu ochrony danych osobowych jest adekwatna do:

1) zmian w budowie systemu informatycznego,
a) zmian organizacyjnych administratora danych, w tym również zmian statusu osób upoważnionych do przetwarzania danych osobowych,
b) zmian w obowiązującym prawie.

Administrator bezpieczeństwa informacji może, stosownie do potrzeb, przeprowadzić wewnętrzny audyt zgodności przetwarzania danych z przepisami o ochronie danych osobowych. Przeprowadzenie audytu wymaga uzgodnienia jego zakresu z administratorem systemu. Zakres, przebieg i rezultaty audytu dokumentowane są na piśmie w protokole podpisywanym zarówno przez administratora bezpieczeństwa informacji jak i administratora systemu.

Dyrektor szkoły, biorąc pod uwagę wyniki audytu wewnętrznego, może zlecić przeprowadzenie audytu zewnętrznego przez wyspecjalizowany podmiot.

IX.POSTANOWIENIA KOŃCOWE

1. Każda osoba, upoważniona do przetwarzania danych osobowych, zobowiązania jest do zapoznania się przed dopuszczeniem do przetwarzania danych z niniejszym dokumentem oraz złożyć stosowne oświadczenie, potwierdzające znajomość jego treści.

2. Niezastosowanie się do postanowień niniejszego dokumentu i naruszenie procedur ochrony danych jest traktowane jako ciężkie naruszenie obowiązków służbowych, skutkujące poważnymi konsekwencjami prawnymi, włącznie z rozwiązaniem stosunku pracy na podstawie art. 52 Kodeksu pracy.

3. Polityka bezpieczeństwa, wchodzi w życie z dniem 11 września 2017r.

Załączniki:

1. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Szkole Podstawowej nr. 7 w Sochaczewie

2. Oświadczenie o znajomości Polityki Bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym

3. Upoważnienie do przetwarzania danych osobowych

4. Odwołanie upoważnienia do przetwarzania danych osobowych

5. Ewidencja osób posiadających upoważnienie do przetwarzania danych osobowych

6. Wykaz jednostek komputerowych

7. Wykaz oprogramowania

8. Raport z naruszenia bezpieczeństwa danych osobowych

Załącznik 1

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W SZKOLE PODSTAWOWEJ NR. 7 W SOCHACZEWIE

I. CELE WPROWADZENIA I ZAKRES ZASTOSOWANIA INSTRUKCJI ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

1. „Instrukcja zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Szkole Podstawowej nr. 7 w Sochaczewie, zwana dalej instrukcją, została wprowadzona w celu spełnienia wymagań, o których jest mowa w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2016 r., poz. 922. z późniejszymi zmianami) oraz 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. 2004r.,nr 100, poz. 1024), tj. zabezpieczenia danych osobowych przed zagrożeniami, w tym zwłaszcza przed ich udostępnieniem osobom nieupoważnionym, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.
2. Instrukcja jest dokumentem powiązanym z „Polityką bezpieczeństwa w zakresie zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Szkole Podstawowej nr. 7 w Sochaczewie i wraz z nim składa się na dokumentację wymaganą przez art. 36. ust. 2. ustawy o ochronie danych osobowych.
3. Niniejsza instrukcja znajduje zastosowanie do systemów informatycznych, stosowanych w szkole, w których są przetwarzane dane osobowe.
4. Instrukcja podlega monitorowaniu i w razie potrzeby uaktualnianiu każdego roku, do końca stycznia, przez administratora danych osobowych lub upoważnioną przez niego osobę, w ramach sprawowania kontroli zarządczej.
5. Dokument instrukcji przechowywany jest w wersji papierowej i elektronicznej.

II. NADAWANIE I REJESTROWANIE (WYREJESTROWANIE) UPRAWNIEŃ DO PRZETWARZANIA DANYCH W SYSTEMIE INFORMATYCZNYM

1. Nadawanie i rejestrowanie uprawnień.

1) Dostęp do systemu informatycznego, służącego do przetwarzania danych osobowych, może uzyskać wyłącznie osoba upoważniona do przetwarzania danych osobowych, zarejestrowana jako użytkownik w tym systemie przez dyrektora szkoły lub uprawnioną przez niego osobę.
2) Rejestracja użytkownika, o którym jest mowa w punkcie 1 polega na nadaniu identyfikatora i przydzieleniu hasła oraz wprowadzeniu tych danych do bazy użytkowników systemu.

2. Wyrejestrowanie uprawnień.

1) wyrejestrowanie użytkownika systemu informatycznego dokonuje dyrektor szkoły lub upoważniona przez niego osoba,
2) wyrejestrowanie, o którym jest mowa w punkcie 1 może mieć charakter czasowy lub trwały,
3) wyrejestrowanie następuje przez:
a) zablokowanie konta użytkownika do czasu ustania przyczyny, uzasadniającej blokadę (wyrejestrowanie czasowe),
b) usunięcie danych użytkownika z bazy użytkowników systemu (wyrejestrowanie trwałe).
4) czasowe wyrejestrowanie użytkownika z systemu musi nastąpić w razie:
a) nieobecności użytkownika w pracy, trwającej dłużej niż 21 dni kalendarzowych,
b) zawieszenia w pełnieniu obowiązków służbowych,
5) przyczyną czasowego wyrejestrowania użytkownika z systemu informatycznego może być:
a) wypowiedzenie umowy o pracę,
b) wszczęcie postępowania dyscyplinarnego,
6) przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy lub innego stosunku prawnego, w ramach którego zatrudniony był użytkownik.

III.METODY I ŚRODKI UWIERZYTELNIENIA

1. Każdy użytkownik systemu informatycznego otrzymuje od administratora bezpieczeństwa informacji identyfikator i hasło.
2. Hasło użytkownika powinno składać się z unikalnego zestawu co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne. Hasło nie może być identyczne z identyfikatorem użytkownika ani jego imieniem lub nazwiskiem.
3. Zabrania się użytkownikom systemu udostępniania swojego identyfikatora i hasła innym osobom oraz korzystania przez osoby upoważnione do przetwarzania danych osobowych z identyfikatora lub hasła innego użytkownika.
4. Zmiana haseł w systemie następuje nie rzadziej niż raz w miesiącu.

IV. PROCEDURY ZWIĄZANE Z GROMADZENIEM, PRZECHOWYWANIEM, PRZETWARZANIEM, USUWANIEM DANYCH OSOBOWYCH

1. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informacyjnym oraz wskazanie osoby odpowiedzialnej za te czynności.

1) Przetwarzać dane osobowe w systemie informatycznym może wyłącznie osoba posiadająca upoważnienie do przetwarzania danych osobowych (wzór tego upoważnienia stanowi załącznik nr. 3 do niniejszej instrukcji). Wydanie upoważnienia oraz rejestracja

użytkownika systemu informatycznego, przetwarzającego dane osobowe, następuje na wniosek dyrektora szkoły.
2) Oryginał upoważnienia zostaje przekazany pracownikowi za potwierdzeniem odbioru, kopia upoważnienia zostaje dołączona do akt osobowych pracownika.
3) Identyfikator i hasło do systemu informatycznego, przetwarzającego dane osobowe, są przydzielone użytkownikowi tylko w przypadku, gdy posiada on pisemne upoważnienie do przetwarzania danych osobowych. Za przydzielenie i wygenerowanie identyfikatora i hasła użytkownikowi, który pierwszy raz będzie korzystał z systemu informatycznego, odpowiada administrator bezpieczeństwa informatycznego. Wyrejestrowanie użytkownika z systemu informatycznego następuje na wniosek administratora danych osobowych.
4) Administrator jest zobowiązany do przeprowadzenia ewidencji pracowników upoważnionych do przetwarzania danych osobowych w Szkole Podstawowej nr. 7 w Sochaczewie

2. Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

1) Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.
2) Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi. Użytkownik odpowiada za wszystkie czynności wykonane przy użyciu identyfikatora, którym się posługuje.
3) Identyfikator i hasło użytkownika powinny odpowiadać wymaganiom, określonym w rozdziale III.
4) Nazwy i hasła użytkowników, posiadających uprawnienia do informatycznego przetwarzania danych osobowych, powinny być przechowywane w szafie metalowej, w archiwum szkoły, do której dostęp jest w pełni kontrolowany, przy czym dostęp do niej mają wyłącznie osoby uprawnione. Nazwy i hasła użytkowników powinny być przechowywane w opieczętowanej i opatrzonej pieczęcią szkoły i podpisem administratora kopercie.
5) W przypadku konieczności użycia nazw i haseł tych użytkowników konieczny jest wpis, ilustrujący zaistniałą sytuację w „Dzienniku haseł", który jest przechowywany w szafie metalowej wraz z kopertą, w której znajdują się hasła. Wpis powinien zawierać następujące informacje:
a) imię i nazwisko oraz stanowisko osoby upoważnionej, udostępniającej dostęp do szafy metalowej, w której znajdują się hasła,
b) imię i nazwisko oraz stanowisko osoby, która pobiera nazwy użytkowników i hasła,
c) krótki opis sytuacji, która zmusiła do awaryjnego wykorzystania haseł.
6) O konieczności i okolicznościach awaryjnego użycia nazw i haseł musi niezwłocznie zostać powiadomiony administrator bezpieczeństwa informacyjnego.

3. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu

1) Przed rozpoczęciem pracy, w trakcie rozpoczynania pracy z systemem informatycznym oraz w trakcie pracy każdy pracownik jest obowiązany do zwrócenia bacznej uwagi, czy nie wystąpiły symptomy, mogące świadczyć o naruszeniu ochrony danych osobowych.

2) Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione oraz ogólne stwierdzenie poprawności działania systemu.
3) Maksymalna liczba prób wprowadzenia hasła przy logowaniu się do systemu wynosi dziesięć. Po przekroczeniu tej liczby prób logowania system blokuje dostęp do zbioru danych na poziomie danego użytkownika. Odblokowania konta może dokonać administrator systemu informatycznego w porozumieniu z administratorem bezpieczeństwa informacji. Użytkownik informuje administratora bezpieczeństwa informacji o zablokowaniu dostępu do zbioru danych.
4) W przypadku bezczynności użytkownika na stacji roboczej przez okres dłuższy niż 30 minut automatycznie włączony jest wygaszasz ekranu. Wygaszacze ekranu powinny być zaopatrzone w hasła zbudowane analogicznie do haseł używanych przez użytkownika przy logowaniu.
5) Zmianę użytkownika stacji roboczej każdorazowo musi poprzedzać wylogowanie się poprzedniego użytkownika. Niedopuszczalne jest, aby dwóch lub większa liczba użytkowników wykorzystywała wspólne konto użytkownika.
6) W przypadku, gdy przerwa w pracy na stacji roboczej trwa dłużej niż 60 minut, użytkownik obowiązany jest wylogować się z aplikacji i systemu stacji roboczej, na której pracuje oraz sprawdzić, czy nie zostały pozostawione bez zamknięcia nośniki informacji, zawierające dane osobowe. W pomieszczeniach, w których przetwarzane są dane i w których jednocześnie mogą przebywać osoby postronne, monitory stanowisk dostępu do danych powinny być ustawione w taki sposób, żeby uniemożliwić tym osobom wgląd w dane.
7) Zakończenie pracy użytkownika w systemie informatycznym obejmuje wylogowanie się użytkownika z aplikacji.

4. Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych, służących do ich przetwarzania

1) Dane osobowe, przetwarzane w systemie informatycznym, podlegają zabezpieczeniu poprzez tworzenie kopii zapasowych. Za proces tworzenia kopii zapasowych odpowiada administrator systemu informatycznego lub osoba specjalnie w tym celu wyznaczona.
2) Kopie zapasowe informacji przechowywanych w systemie informatycznym, przetwarzającym dane osobowe, tworzone są w następujący sposób:
a) kopia zapasowa aplikacji przetwarzającej dane osobowe – pełna kopia wykonywana przez użytkownika każdego dnia, po zakończeniu pracy z aplikacją, kopie umieszczone są na nośnikach wymiennych, kopia przechowywana jest w zamkniętej szafie,
b) zbiorcze (miesięczne) kopie wykonywane są przez administratora sieci i przechowywane są przez okres dwóch tygodni, po tym terminie stare kopie są niszczone poprzez nadpisywanie ich przez bardziej aktualne.
3) W przypadku przechowywania kopii zapasowych przez okres dłuższy niż pół roku, wszystkie kopie zapasowe zbiorów danych osobowych, aplikacji przetwarzających dane osobowe oraz danych konfiguracyjnych systemu informatycznego, przetwarzającego dane osobowe, których to dotyczy, muszą być okresowo (co najmniej raz na pół roku) sprawdzane pod względem ich dalszej przydatności. Czynności te wykonuje administrator systemu informatycznego lub osoba przez niego upoważniona.
4) Nośniki kopii zapasowych, które zostały wycofane z użycia, jeżeli jest to możliwe, należy pozbawić zapisanych danych za pomocą specjalnego oprogramowania do bezpiecznego usuwania zapisanych danych. W przeciwnym wypadku podlegają

fizycznemu zniszczeniu z wykorzystaniem metod adekwatnych do typu nośnika, w sposób uniemożliwiający odczytanie zapisanych danych.

5. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych

1) Nośniki danych zarówno w postaci elektronicznej, jak i papierowej powinny być zabezpieczone przed dostępem osób nieuprawnionych, nieautoryzowaną modyfikacją i zniszczeniem. Dane osobowe mogą być zapisywane na nośnikach przenośnych w przypadku tworzenia kopii zapasowych lub gdy istnieje konieczność przeniesienia tych danych w postaci elektronicznej, a wykorzystanie do tego celu sieci informatycznej jest nieuzasadnione, niemożliwe lub zbyt niebezpieczne.
2) Nośniki danych osobowych oraz wydruki powinny być przechowywane w zamkniętych szafach i nie powinny być bez uzasadnionej przyczyny wynoszone poza ten obszar. Przekazywanie nośników danych osobowych i wydruków poza budynek szkoły powinno odbywać się za wiedzą administratora danych osobowych.
3) Kopie miesięczne przechowuje się przez okres 6 miesięcy.
4) W przypadku, gdy nośnik danych osobowych nie jest dłużej potrzebny, należy przeprowadzić zniszczenie nośnika lub usunięcie danych z nośnika zgodnie ze wskazówkami umieszczonymi w punkcie 4. Jeżeli wydruk danych osobowych nie jest dłużej potrzebny, należy przeprowadzić zniszczenie wydruku przy użyciu niszczarki dokumentów.
5) W przypadku, gdy kopia zapasowa nie jest dłużej potrzebna, należy przeprowadzić jej zniszczenie lub usunięcie danych z nośnika, na którym się ona znajduje.
6) W przypadku kopii zapasowych sporządzanych indywidualnie przez użytkownika – odpowiedzialny za ich zniszczenie jest użytkownik(w obecności administratora bezpieczeństwa informacji).

6. Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

1) W związku z tym, że system informatyczny narażony jest na działanie oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do tego systemu, konieczne jest podjęcie odpowiednich środków ochronnych.
2) Można wyróżnić następujące rodzaje występujących tu zagrożeń:

a) nieuprawniony dostęp bezpośrednio do bazy danych,
b) uszkodzenie kodu aplikacji, umożliwiającej dostęp do bazy danych w taki sposób, że przetwarzane dane osobowe ulegną zafałszowaniu lub zniszczeniu,
c) przechwycenie danych podczas transmisji w przypadku rozproszonego przetwarzania danych z wykorzystaniem ogólnodostępnej sieci internet,
d) przechwycenie danych z aplikacji, umożliwiającej dostęp do bazy danych na stacji roboczej wykorzystywanej do przetwarzania danych osobowych przez wyspecjalizowany program szpiegowski i nielegalne przesłanie tych danych poza miejsce przetwarzania danych,
e) uszkodzenie lub zafałszowanie danych osobowych przez wirus komputerowy, zakłócający pracę aplikacji, umożliwiającej dostęp do bazy danych na stacji roboczej wykorzystywanej do przetwarzania danych osobowych.

3) W celu przeciwdziałania wymienionym zagrożeniom system informatyczny musi posiadać następujące zabezpieczenia:

a) autoryzację użytkowników przy zachowaniu odpowiedniego poziomu komplikacji haseł dostępu,
b) stosowanie szyfrowanej transmisji danych przy zastosowaniu odpowiedniej długości klucza szyfrującego,
c) stosowanie odpowiedniej ochrony antywirusowej na stacjach roboczych wykorzystywanych do przetwarzania danych osobowych.

4) Potencjalnymi źródłami przedostawania się programów szpiegowskich oraz wirusów komputerowych na stacje robocze są:
a) załączniki do poczty elektronicznej,
b) przeglądane strony internetowe,
c) pliki i aplikacje, pochodzące z nośników wymiennych, uruchamiane i odczytywane na stacji roboczej.

5) W celu zapewnienia ochrony antywirusowej administrator systemu informatycznego, przetwarzający dane osobowe lub osoba specjalnie do tego celu wyznaczona, jest odpowiedzialny za zarządzanie systemem wykrywającym i usuwającym wirusy. System antywirusowy powinien być skonfigurowany w następujący sposób:
a) rezydentny monitor antywirusowy (uruchomiony w pamięci operacyjnej stacji roboczej) powinien być stale włączony,
b) antywirusowy skaner ruchu internetowego powinien być stale włączony,
c) monitor zapewniający ochronę przed wirusami w dokumentach MS Office, powinien być stale włączony,
d) skaner poczty elektronicznej powinien być stale włączony.

6) Systemy antywirusowe, zainstalowane na stacjach roboczych, powinny być skonfigurowane w sposób następujący:
a) zablokowanie możliwości ingerencji użytkownika w ustawienia oprogramowania antywirusowego,
b) możliwość centralnego uaktualnienia wzorców wirusów.

7) System antywirusowy powinien być aktualizowany na podstawie materiałów publikowanych przez producenta oprogramowania.

8) Użytkownicy systemu informatycznego zobowiązani są do następujących działań:
a) skanowania zawartości dysków stacji roboczej, pracującej w systemie informatycznym pod względem potencjalnie niebezpiecznych kodów – przynajmniej 2 razy w tygodniu,
b) skanowania zawartości nośników wymiennych odczytywanych na stacji roboczej, pracującej w systemie informatycznym, pod względem potencjalnie niebezpiecznych kodów – przy każdym odczycie,
c) skanowanie informacji przesyłanych do systemu informatycznego pod kątem pojawienia się niebezpiecznych kodów – na bieżąco.

9) W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy administrator systemu informatycznego lub inny wyznaczony pracownik powinien podjąć działania, zmierzające do usunięcia zagrożenia. W szczególności działania te mogą obejmować:
a) usunięcie zainfekowanych plików, o ile jest to akceptowalne ze względu na prawidłowe funkcjonowanie systemu informatycznego,
b) odtworzenie plików z kopii zapasowych po uprzednim sprawdzeniu, czy dane zapisane na kopiach nie są zainfekowane,
c) samodzielną ingerencję w zawartość pliku – w zależności od posiadanych kwalifikacji lub skonsultowanie się z zewnętrznymi ekspertami.

10) System informatyczny, przetwarzający dane osobowe, powinien posiadać mechanizmy pozwalające na zabezpieczenie ich przed utratą lub wystąpieniem zafałszowania w wyniku awarii zasilania lub zakłóceń w sieci zasilającej. W związku z tym system

informatyczny powinien być wyposażony w co najmniej filtry zabezpieczające stacje robocze przed skutkami przepięcia.

7. Sposób realizacji wymogów, o których mowa w § 7 ust. 1. pkt. 4. rozporządzenia MSWiA

1) System informatyczny, przetwarzający dane osobowe, musi posiadać mechanizm uwierzytelniający użytkownika, wykorzystujący identyfikator i hasło. Powinien także posiadać mechanizmy, pozwalające na określenie uprawnień użytkownika do korzystania z przetwarzanych informacji (np. prawo do odczytu danych, modyfikacji istniejących danych, tworzenia nowych danych, usuwania danych).
2) System informatyczny, przetwarzający dane osobowe, musi posiadać mechanizmy, pozwalające na odnotowanie faktu wykonania operacji na danych. W szczególności zapis ten powinien obejmować:

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

3) Zapis działań użytkownika uwzględnia:

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

4) Ponadto system informatyczny powinien zapewnić zapis faktu przekazania danych osobowych z uwzględnieniem:

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

8. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych

1) Wszelkie prace związane z naprawami i konserwacją systemu informatycznego, przetwarzającego dane osobowe, muszą uwzględniać wymagany poziom zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych.
2) Prace serwisowe na terenie szkoły, prowadzone w tym zakresie, mogą być wykonywane wyłącznie przez jego pracowników lub przez upoważnionych przedstawicieli wykonawców zewnętrznych, znajdujących się w towarzystwie pracowników szkoły.
3) Przed rozpoczęciem prac serwisowych przez osoby spoza szkoły konieczne jest potwierdzenie tożsamości serwisantów.
4) Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:

a) likwidacji — pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
b) przekazania podmiotowi nieuprawnionemu do przetwarzania danych — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
c) naprawy — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

V. POZIOM BEZPIECZEŃSTWA

Uwzględniając kategorie danych osobowych oraz konieczność zachowania bezpieczeństwa ich przetwarzania w systemie informatycznym, połączonym z siecią publiczną, wprowadza się „poziom wysoki" bezpieczeństwa w rozumieniu § 6 rozporządzenia.

VI. STOSOWANE ŚRODKI BEZPIECZEŃSTWA

1. Zgodnie z treścią § 6, ust. 4 rozporządzenia, o którym jest mowa w pkt. 1.1. niniejszej instrukcji stosuje się w szkole środki bezpieczeństwa na poziomie wysokim.
2. W szkole stosuje się następujące środki bezpieczeństwa:

1) Zabezpieczenie obszaru, w którym przetwarzane są dane osobowe, przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.
2) Przebywanie osób nieuprawnionych, jest dopuszczalne za zgodą administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.
3) Stosowane są mechanizmy kontroli dostępu do danych.
4) Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie jest przydzielany innej osobie.
5) W przypadku, gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż dwa razy w roku.
6) Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów, służących do przetwarzania danych osobowych.
7) Administrator danych monitoruje wdrożone zabezpieczenia systemu informatycznego.
8) Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:

a) likwidacji – pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,
b) przekazania podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie,
c) naprawy – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

9) Urządzenia i nośniki, zawierające dane osobowe, zabezpiecza się w sposób zapewniający poufność i integralność tych danych.
10) Administrator danych stosuje środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej.

VII. POSTANOWIENIA KOŃCOWE

1. Osobą odpowiedzialną za przegląd przestrzegania instrukcji, przegląd jej aktualności oraz aktualizację, a także nadawanie praw dostępu do systemu informatycznego jest administrator bezpieczeństwa informacji lub inna osoba upoważniona przez administratora danych.
2. W sprawach nieokreślonych niniejszą instrukcją należy stosować instrukcje obsługi i zalecenia producentów aktualnie wykorzystywanych urządzeń i programów.
3. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się przed dopuszczeniem do przetwarzania danych z niniejszą instrukcją.
4. Niezastosowanie się do procedur określonych w niniejszej instrukcji przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52 kodeksu pracy.
5. Niniejsza instrukcja wchodzi w życie z dniem 21 listopada 2016r.

…..……
(Administrator danych osobowych)

Załącznik 2

……., dn……..

…….
(imię i nazwisko pracownika)

OŚWIADCZENIE

1. Oświadczam, że znana mi jest treść:

a) Dokumentacji ochrony danych osobowych obowiązującej w Szkole Podstawowej nr. 7 w Sochaczewie, zawartej w Polityce Bezpieczeństwa i Instrukcji Przetwarzania Danych Osobowych,
b) Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (tekst jednolity: Dz. U. 2002 r. Nr 101 poz. 926 ze zmianami),
c) 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. z 2004 r. Nr 100, poz. 1024).

2. Jednocześnie zobowiązuję się nie ujawniać informacji, z którymi zapoznałam się w związku z wykonywaną pracą, a w szczególności nie będę:

a) ujawniać danych zawartych w zbiorach danych, do których uzyskałam dostęp za upoważnieniem administratora danych,
b) ujawniać szczegółów technologicznych używanych w systemach informatycznych oraz oprogramowania,
c) udostępniać osobom nieupoważnionym nośników magnetycznych i optycznych oraz wydruków komputerowych,
d) kopiować lub przetwarzać danych w sposób inny niż dopuszczony obowiązującą dokumentacją.

……..……. ……
(data, miejscowość) *(podpis pracownika)*

Załącznik 3

……., dn……..

UPOWAŻNIENIE
do przetwarzania danych osobowych

Działając na podstawie art. 37 Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz. U. z 2002 r. nr 101, poz. 926 z późn. zm.)

- udziela się Pani/Panu[1]:

……
(imię i nazwisko pracownika)

……
(stanowisko służbowe)

upoważnienia do przetwarzania danych osobowych, których Administratorem jest Szkoła Podstawowa nr. 7 w Sochaczewie oraz do przetwarzania danych osobowych powierzonych szkole przez podmioty trzecie.

Jest Pan/Pani[1] upoważniony/upoważniona[1] do przetwarzania danych osobowych wyłącznie w zakresie wynikającym z Pana/Pani[1] zadań oraz polecenia służbowego.

Upoważnienie traci moc z chwilą ustania stosunku pracy.

……
(data i podpis Administratora Bezpieczeństwa Informacji)

[1] Niepotrzebne skreślić

Załącznik 4

……., dn……..

ODWOŁANIE UPOWAŻNIENIA
do przetwarzania danych osobowych

Działając na podstawie art. 37 Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz. U. z 2002 r. nr 101, poz. 926 z późn. zm.)

- odwołuje się z dniem ……. ……

upoważnienie do przetwarzania danych osobowych, których Administratorem jest Szkoła Podstawowa nr. 7 w Sochaczewie oraz do przetwarzania danych osobowych powierzonych szkole przez podmioty trzecie wystawione dla Pani/Pana:

……
(imię i nazwisko pracownika)

……
(stanowisko służbowe)

……
(data i podpis Administratora Bezpieczeństwa Informacji)

Załącznik 5

Ewidencja osób posiadających upoważnienie do przetwarzania danych osobowych

Lp.	Imię i nazwisko	Stanowisko służbowe	Okres upoważnienia	Wykaz zbiorów danych wynikających z upoważnienia	Identyfikator(Nazwa programu przetwarzanych danych osobowych w systemie informatycznym)

Załącznik 6

Wykaz jednostek komputerowych

Lp.	Oznaczenie zestawu komputerowego	Opis techniczny	Adres IP nazwa sieciowa	Ozn	Wykaz uprawnionego oprogramowa-nia	Rodzaj licencji	Dokument	Zainsta-lowano	Osoba odpowie-dzialna	Porozumie-nie

Załącznik 7

Wykaz oprogramowania

Lp.	Wewnętrzne oznaczenie licencji	Nazwa nabytego programu	Rodzaj licencji	Faktura	Umowa	Ważna do…	Odnowienie do…	Ilość	Atrybut licencji	Oznaczenie licencji wg producenta

Załącznik 8

……., dn……..

RAPORT
z naruszenia bezpieczeństwa danych osobowych

1. Data……. Godzina……
2. Osoba powiadamiająca o zaistniałym zdarzeniu:

   ……...
   (Imię i nazwisko, stanowisko służbowe)
3. Lokalizacja zdarzenia ……...

   ……..
4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące ……..

   ……..
   ……
   ……
5. Przyczyny wystąpienia zdarzenia ……..

   ……

   ……
6. Podjęte działania ……..

   ……..

   ……..
7. Postępowanie wyjaśniające …….

……

……

……
(data i podpis Administratora Bezpieczeństwa Informacji)