Zespół Szkół w Wiechlicach
ul.Brzozowa 17, 67-300 Szprotawa
tel. 68 376 75 53
NIP 924-19-05-598, REGON 361961866

Zarządzenie nr 40/2016
Dyrektora Zespołu Szkół w Wiechlicach
z dnia 22.03.2016 r.
w sprawie wprowadzenia polityki bezpieczeństwa przetwarzania danych osobowych i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Zespole Szkół w Wiechlicach

Na podstawie art. 36 ust. 1 i 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz.U. z 2015 r. poz. 2135), § 3 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) zarządzam, co następuje:

§1. Ustala się „Politykę bezpieczeństwa przetwarzania danych osobowych w Zespole Szkół w Wiechlicach", która stanowi załącznik nr 1 do niniejszego zarządzenia.

§2. Ustala się „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Zespole Szkół w Wiechlicach", która stanowi załącznik nr 2 do niniejszego zarządzenia.

§3. Zobowiązuję pracowników Zespołu Szkół w Wiechlicach do stosowania zasad określonych w powyższych dokumentach.

§4. Wykonanie niniejszego zarządzenia powierza się Administratorowi Bezpieczeństwa Informacji.

§5. Zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR
Zespołu Szkół w Wiechlicach
mgr Cecylia Brodzińska

Zespół Szkół w Wiechlicach
ul.Brzozowa 17, 67-300 Szprotawa
tel. 68 376 75 53
NIP 924-19-05-598, REGON 361961866

Załącznik nr 1
do Zarządzenia nr 40/2016
Dyrektora Zespołu Szkół w Wiechlicach
z dnia 22.03.2016 r.

Polityka bezpieczeństwa przetwarzania danych osobowych w Zespole Szkół w Wiechlicach

Wiechlice, 2016

Polityka bezpieczeństwa przetwarzania danych osobowych opisuje procedury związane z bezpieczeństwem danych osobowych, do których stosowania zobowiązani są wszyscy pracownicy Zespołu Szkół w Wiechlicach - zwanym dalej Szkołą, mający dostęp do tych danych. Dokument powstał w oparciu o ustawę z dnia 29 sierpnia 1997 o ochronie danych osobowych (Dz. U. z 2015 r. poz. 2135) - zwaną dalej ustawą oraz 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. Nr 100, poz. 1024) – zwanym dalej rozporządzeniem.

I. Zasady ogólne

Ochrona przetwarzanych w Szkole danych osobowych obowiązuje wszystkie osoby, które mają dostęp do informacji zbieranych, przetwarzanych i przechowywanych w Szkole, bez względu na zajmowane stanowisko, charakter i miejsce wykonywania pracy. Osoby te zobligowane są do podjęcia niezbędnych środków, mających na celu zapobieganiu ujawnienia tych danych osobom trzecim, jak również do zachowania w tajemnicy wszelkich informacji uzyskanych w zawiązku z wykonywanym zakresem czynności na stanowisku pracy zarówno w czasie trwania zatrudnienia jak i po jego ustaniu.

II. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe (§ 4 pkt. 1 rozporządzenia)

O przetwarzaniu danych osobowych można mówić wówczas, kiedy wykonuje się na nich jakiekolwiek operacje, czyli: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie czy usuwanie.

1. Przetwarzanie danych osobowych może odbywać się wyłącznie w obszarach do tego celu przeznaczonych, czyli w pomieszczeniach Szkoły, o jakich mowa we wstępie, w których na danych osobowych wykonywana jest przynajmniej jedna z w/w operacji. Dane osobowe mogą być przetwarzane za pomocą systemu informatycznego lub występować w formie kartotek, skorowidzów, ksiąg, wykazów czy innych zbiorów ewidencyjnych. Wykaz pomieszczeń, w których dopuszczalne jest przetwarzanie danych osobowych określa załącznik nr 1 do niniejszej Polityki Bezpieczeństwa.

2. Dostęp do pomieszczeń, gdzie przetwarzane są dane osobowe, zwłaszcza do tych, w których znajdują się serwery bądź przechowywane są kopie zapasowe mogą mieć wyłącznie osoby, posiadające dostosowane upoważnienie, zaś w biurach, w których przetwarzane są dane osobowe, a gdzie często przebywają osoby trzecie, monitory winny być skierowane, a dokumentacja w formie papierowej ułożona, w sposób uniemożliwiający wgląd w dane osobom postronnym. Wszystkie pomieszczenia, w których przetwarzane są dane osobowe powinny być zabezpieczone przed dostępem do nich osób niepowołanych.

III. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych (§ 4 pkt. 2 rozporządzenia)

Wykaz zbiorów danych osobowych przetwarzanych w Szkole wraz ze wskazaniem programów zastosowanych do ich przetwarzania określa załącznik nr 2 do niniejszej Polityki Bezpieczeństwa.

Wykaz winien być aktualizowany po wprowadzeniu do przetwarzania nowych zbiorów danych osobowych lub nowych programów, które je obsługują, w terminie 30 dni od momentu powstania zmiany.

IV. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi (§ 4 pkt. 3 rozporządzenia)

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi zawiera załącznik nr 3 do niniejszego dokumentu.

Opis powinien być aktualizowany po wprowadzeniu znaczących zmian w strukturze bazy danych, którą opisuje. w terminie 30 dni od momentu powstania zmiany.

V. Sposób przepływu danych pomiędzy poszczególnymi systemami (§ 4 pkt. 4 rozporządzenia)

Sposób współpracy pomiędzy systemami informatycznymi zastosowanymi w Zespole Szkół w Wiechlicach określa załącznik nr 4 do Polityki bezpieczeństwa.

VI. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych. (§ 4 pkt. 5 rozporządzenia)

1. Środki ochrony fizycznej.

1) budynki Zespołu Szkół w Wiechlicach, tj. budynek główny oraz budynki filialne w Długiem, Siecieborzycach i Lesznie Górnym, czyli obszary, w których dokonuje się przetwarzania danych osobowych są wyposażone w system alarmowy,
2) wszystkie urządzenia służące do przetwarzania danych osobowych znajdują się w zamkniętych pomieszczeniach,
3) wszystkie dokumenty w formie papierowej przechowywane są w biurach, w zamkniętych szafach, do których osoby postronne nie mają dostępu.

2. Środki organizacyjne:

1) powołanie Administratora Bezpieczeństwa Informacji odpowiedzialnego za działania organizacyjne i środki techniczne zapewniające wymagany poziom bezpieczeństwa danych:

a) do zadań ABI należy:

- przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe,
- podejmowanie odpowiednich działań w przypadku wykrycia naruszeń zabezpieczeń lub podejrzenia naruszenia w systemie,
- nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których przetwarzane są dane osobowe oraz nadzór nad kontrolą przebywających w nich osób,
- nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe,
- zarządzanie hasłami użytkowników, systemami antywirusowymi i ich procedurami,
- nadzór nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności,
- nadzór nad obiegiem dokumentów zawierający dane osobowe,
- nadzór nad prawidłowością archiwizacji oraz usuwania danych osobowych,
- monitorowanie funkcjonowania zabezpieczeń wdrożonych w celu ochrony danych osobowych,
- nadzór nad prowadzeniem wymaganej dokumentacji,
- wdrożenie szkoleń z zakresu przepisów dotyczących ochrony danych oraz stosowanie środków technicznych i organizacyjnych przy przetwarzaniu danych w systemach informatycznych.

2) przetwarzać dane osobowe mogą tylko pracownicy Zespołu Szkół w Wiechlicach, którym Administrator Danych wydał upoważnienia do przetwarzania tych danych (wzór upoważnienia stanowi załącznik nr 1 do dokumentu Instrukcja zarządzania system informatycznym);

3) osoby, o których mowa w pkt 2, składają pisemne oświadczenie o zachowaniu w tajemnicy informacji, z jakimi mają do czynienia w trakcie wykonywania swoich obowiązków. Pracownicy są przeszkoleni w zakresie przepisów o ochronie danych osobowych, a zatem posiadają wiedzę o odpowiedzialności karnej za niezgodne z prawem przetwarzanie danych osobowych (wzór oświadczenia stanowi załącznik nr 2 do Instrukcji zarządzania system informatycznym;

4) dokumenty zawierające dane osobowe przekazywane są zgodnie z instrukcją kancelaryjną do archiwum zakładowego, zaś te, których termin przydatności upłynął są niszczone w niszczarkach;

5) opracowano instrukcję zarządzania systemem informatycznych służącym do przetwarzania danych osobowych w omawianej placówce oświatowej.

DYREKTOR
Zespołu Szkół w Wiechlicach
mgr Cecylia Błodzińska

Załącznik nr 1
do Polityki bezpieczeństwa przetwarzania danych osobowych
w Zespole Szkół w Wiechlicach

Wykaz pomieszczeń Zespołu Szkół w Wiechlicach, tworzących obszar, w którym są przetwarzane dane osobowe

Lp.	Zbiór danych osobowych	Adres	Pomieszczenie
1.	Zamówienia publiczne	Wiechlice, ul. Brzozowa 17	
2.	Pomoc materialna	Wiechlice, ul. Brzozowa 17, Długie 79, Leszno Górne ul. Szkolna 2a, Siecieborzyce 49a	
3.	Księga uczniów	Wiechlice, ul. Brzozowa 17, Długie 79, Leszno Górne ul. Szkolna 2a, Siecieborzyce 49a	
4.	Księga dzieci	Wiechlice, ul. Brzozowa 17, Długie 79, Leszno Górne ul. Szkolna 2a, Siecieborzyce 49a	
5.	Zbiory danych gromadzone w archiwum zakładowym	Wiechlice, ul. Brzozowa 17, Długie 79, Leszno Górne ul. Szkolna 2a, Siecieborzyce 49a	
6.	Ewidencja pracowników Zespołu Szkół w Wiechlicach	Wiechlice ul. Brzozowa 17	
7.	Staże i praktyki zawodowe	Wiechlice, ul. Brzozowa 17, Długie 79, Leszno Górne ul. Szkolna 2a, Siecieborzyce 49a	
8.	Rejestr korespondencji	Wiechlice, ul. Brzozowa 17, Długie 79, Leszno Górne ul. Szkolna 2a, Siecieborzyce 49a	
9.	System Informacji Oświatowej	Wiechlice, ul. Brzozowa 17, Długie 79, Leszno	

		Górne ul. Szkolna 2a, Siecieborzyce 49a	
10.	Realizacja obowiązku szkolnego – ewidencja uczniów	Wiechlice, ul. Brzozowa 17, Długie 79, Leszno Górne ul. Szkolna 2a, Siecieborzyce 49a	
11.	Płace pracowników	Wiechlice ul. Brzozowa 17	
12.	Arkusze ocen	Wiechlice, ul. Brzozowa 17, Długie 79, Leszno Górne ul. Szkolna 2a, Siecieborzyce 49a	
13.	Karty biblioteczne	Wiechlice, ul. Brzozowa 17, Długie 79, Leszno Górne ul. Szkolna 2a, Siecieborzyce 49a	
14.	Zakładowy Fundusz Świadczeń Socjalnych	Wiechlice, ul. Brzozowa 17, Długie 79, Leszno Górne ul. Szkolna 2a, Siecieborzyce 49a	
15.	Magazyn	Wiechlice, ul. Brzozowa 17, Długie 79, Leszno Górne ul. Szkolna 2a, Siecieborzyce 49a	
16.	Dokumentacja ubezpieczeniowa	Wiechlice, ul. Brzozowa 17	
17.	E-dziennik	Wiechlice, ul. Brzozowa 17, Długie 79, Leszno Górne ul. Szkolna 2a, Siecieborzyce 49a	
18.	Arkusz organizacyjny	Wiechlice, ul. Brzozowa 17,	
19.	Inwentarz	Wiechlice, ul. Brzozowa 17, Długie 79, Leszno Górne ul. Szkolna 2a, Siecieborzyce 49a	

20.	Średnie Wynagrodzenia Nauczycieli	Wiechlice, ul. Brzozowa 17,	

Załącznik nr 2
do Polityki bezpieczeństwa przetwarzania danych osobowych
w Zespole Szkół w Wiechlicach

Wykaz zbiorów danych osobowych przetwarzanych w Zespole Szkół w Wiechlicach

Lp.	Zbiór danych osobowych	Rodzaj systemu/programu	Uwagi
1.	Zamówienia publiczne	dokumentacja papierowa	
2.	Pomoc materialna	dokumentacja papierowa	
3.	Księga uczniów	dokumentacja papierowa/program: Sekretariat, Świadectwa, Uonet +, Dziennik elektroniczny	
4.	Księga dzieci	dokumentacja papierowa/program: Sekretariat, Uonet +, Dziennik elektroniczny	
5.	Zbiory danych gromadzone w archiwum zakładowym	dokumentacja papierowa	
6.	Ewidencja pracowników Zespołu Szkół w Wiechlicach	dokumentacja papierowa/program: Kadry Optivum Vulcan, Płace Optivum Vulcan	
7.	Staże i praktyki zawodowe	dokumentacja papierowa	
8.	Rejestr korespondencji	dokumentacja papierowa	
9.	System Informacji Oświatowej	Program „System Informacji Oświatowej" („stary" oraz „modernizowany")	
10.	Realizacja obowiązku szkolnego – ewidencja uczniów	dokumentacja papierowa/program: Sekretariat, Dziennik elektroniczny	
11.	Płace pracowników	Dokumentacja papietowa/programy: Płace Optivum Vulcan, Płatnik, Księgowość	

		Optivum Vulcan, Średnie wynagrodzenie nauczycieli	
12.	Arkusze ocen	dokumentacja papierowa/program: Arkusze Optivum Vulcan	
13.	Karty biblioteczne	dokumentacja papierowa/program: MOL Optivum	
14.	Zakładowy Fundusz Świadczeń Socjalnych	dokumentacja papierowa	
15.	Magazyn	dokumentacja papierowa/program: Magazyn	
16.	Dokumentacja ubezpieczeniowa	dokumentacja papierowa/program: Kadry Optivum Vulcan, Płace Optivum Vulcan, Płatnik	
17.	E-dziennik	Program: Dziennik UONET +	
18.	Arkusz organizacyjny	Dokumentacja papierowa/program: Arkusz Sigma Vulcan	
19.	Inwentarz	Dokumentacja papierowa/program Inwentarz Optivum Vulcan	
20.	Średnie Wynagrodzenia Nauczycieli	Dokumentacja papierowa/program: SWN	

Załącznik nr 3
do Polityki bezpieczeństwa przetwarzania danych osobowych
w Zespole Szkół w Wiechlicach

Struktura zbiorów danych osobowych przetwarzanych w Zespole Szkół w Wiechlinach

Lp.	Zbiór danych osobowych	Zawartość poszczególnych pól informacyjnych i powiązania między nimi
1.	Zamówienia publiczne	Zakres: nazwa Firmy, REGON, NIP, siedziba Firmy, zakres działalności, imię i nazwisko właściciela
2.	Pomoc materialna	Zakres: nazwiska i imiona, adres zamieszkania lub pobytu, PESEL, skład rodziny, stopień pokrewieństwa, dochody, nr telefonu, adres e-mial
3.	Księga uczniów	Zakres: imię i nazwisko, adres zamieszkania, imiona rodziców, imiona rodzeństwa, data urodzenia, nr PESEL
4.	Księga dzieci	Zakres: imię i nazwisko, adres zamieszkania, imiona rodziców, imiona rodzeństwa, data urodzenia
5.	Zbiory danych gromadzone w archiwum zakładowym	Zakres: imiona i nazwisko, nazwisko rodowe, data i miejsce urodzenia, imiona rodziców, PESEL, NIP, obywatelstwo, płeć, adres zameldowania/zamieszkania/korespondencji, nr telefonu, e-mail, skład rodziny (imiona i nazwisko, data urodzenia, stopień pokrewieństwa, miejsce pracy, nazwa szkoły), wykształcenie, historia zatrudnienia, stan majątkowy, służba wojskowa, seria i nr dowodu osobistego, data wystawienia i organ wydający, nr rachunku bankowego, wynagrodzenie, stanowisko
6.	Ewidencja pracowników Zespołu Szkół w Wiechlicach	Zakres: imiona i nazwisko, nazwisko rodowe, data i miejsce urodzenia, imiona rodziców, PESEL, NIP, obywatelstwo, płeć, adres zameldowania/zamieszkania/korespondencji, nr telefonu, e-mail, skład rodziny (imiona i nazwisko, data urodzenia, stopień pokrewieństwa, miejsce pracy, nazwa szkoły), wykształcenie, historia zatrudnienia, stan majątkowy, służba wojskowa, seria i nr dowodu osobistego, data wystawienia i organ wydający, nr rachunku bankowego, wynagrodzenie, stanowisko
7.	Staże i praktyki zawodowe	Zakres: imię i nazwisko, data urodzenia, PESEL, NIP, adres zamieszkania, skład rodziny, wykształcenie, wynagrodzenie, imiona rodziców
8.	Rejestr korespondencji	Zakres: imię i nazwisko, adres, nazwa firmy, siedziba
9.	System Informacji Oświatowej	Zakres: PESEL, płeć, rok urodzenia, forma i wymiar zatrudnienia, stopień awansu

		zawodowego, wykształcenie, przygotowanie pedagogicznego, sprawowane funkcje i zajmowane stanowiska, rodzaje prowadzonych zajęć, staż pracy, wysokość wynagrodzenia, miejsce pracy, zawód
10.	Realizacja obowiązku szkolnego – ewidencja uczniów	Zakres: imię i nazwisko, adres zamieszkania, imiona rodziców, data urodzenia
11.	Płace pracowników	Zakres: imię i nazwisko, nazwisko rodowe, NIP, PESEL, imiona rodziców, seria i nr dowodu osobistego, data wystawienia i organ wydający, data i miejsce urodzenia, imiona i nazwiska oraz nr PESEL i adres członków rodziny zgłaszanych do ubezpieczenia, adres zamieszkania, informacje o dochodach, nr rachunku bankowego
12.	Arkusze ocen	Zakres: imię i nazwisko, data i miejsce urodzenia, nr PESEL, obowiązek szkolny, dane rodziców bądź opiekunów prawnych (imię i nazwisko, adres zamieszkania), informacje o uczniu, informacje o wynikach w nauce
13.	Karty biblioteczne	Zakres: imię i nazwisko, klasa
14.	Zakładowy Fundusz Świadczeń Socjalnych	Zakres: imię i nazwisko, adres, seria i nr dowodu osobistego, członkowie rodziny (imię i nazwisko, data urodzenia, stopień pokrewieństwa, miejsce pracy, nazwa szkoły, dochód brutto, dochód netto, nr rachunku bankowego
15.	Magazyn	Zakres: imię i nazwisko, nr PESEL
16.	Dokumentacja ubezpieczeniowa	Zakres: imię i nazwisko, nazwisko rodowe, adres, nr PESEL, nr NIP, seria i nr dokumentu tożsamości, data urodzenia, obywatelstwo, płeć, dane członka rodziny (PESEL, NIP, nazwisko, imię data urodzenia)
17.	E-dziennik	Zakres: imię i nazwisko ucznia, adres, nr PESEL, data urodzenia, obywatelstwo, płeć, imiona i nazwiska rodziców, nr telefonu, adres e-mail
18.	Arkusz organizacyjny	Zakres: imiona i nazwisko, data urodzenia, PESEL, płeć, wykształcenie, wynagrodzenie, rodzaje prowadzonych zajęć
19.	Inwentarz	Zakres: imiona i nazwisko, data urodzenia, PESEL, NIP, data urodzenia i miejsce, imiona rodziców, adres
20.	Średnie Wynagrodzenia Nauczycieli	Zakres: NIP, nazwisko, imię, wykształcenie, wynagrodzenie

Załącznik nr 4
do Polityki bezpieczeństwa przetwarzania danych osobowych
w Zespole Szkół w Wiechlicach

Sposób współpracy pomiędzy różnymi systemami informatycznymi, stosowanymi w Zespole Szkół w Wiechlicach

KADRY → PŁACE

Z aplikacji **Kadry Optivum Vulcan** do programu **Płace Optivum Vulcan** przekazywane są dane dotyczące zatrudnienia pracowników.

Sposób przekazywania danych: manualny

KADRY → SIO

Z aplikacji **Kadry Optivum Vulcan** do programu **SIO** przekazywane są dane dotyczące zatrudnienia pracowników.

Sposób przekazywania danych: manualny

PŁACE → PŁATNIK

Z aplikacji **Płace Optivum Vulcan** do programu **Płatnik** przekazywane są dane dotyczące zarejestrowania i wyrejestrowania pracowników oraz składek na ubezpieczenia.

Sposób przekazywania danych: manualny

PŁACE → BANK PKO BP

Z programu **Płace Optivum Vulcan** do **Bank PKO BP w Szprotawie** przekazywane są dane dotyczące należnych kwot przelewanych na konto pracowników.

Sposób przekazywania danych: manualny

KSIĘGOWOŚĆ → BANK PKO BP

Z programu **Księgowość Optivum Vulcan** do **Bank PKO BP w Szprotawie** przekazywane są dane dotyczące należnych kwot przelewanych na konto kontrahentów.

Sposób przekazywania danych: manualny

Pozostałe programy są niezależne i posiadają samodzielne bazy danych.

Zespół Szkół w Wiechlicach
ul.Brzozowa 17, 67-300 Szprotawa
tel. 68 376 75 53
NIP 924-19-05-598, REGON 361961866

Załącznik nr 2 do Zarządzenia nr 40/2016
Dyrektora Zespołu Szkól w Wiechlicach
z dnia 22.03.2016 r.

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Zespole Szkół w Wiechlicach

Wiechlice, 2016

I. Wstęp

Niniejszy dokument powstał w wyniku realizacji obowiązku nałożonego przez:

1. Ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2015 r. poz. 2135)
2. 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).

II. Definicje

Ilekroć w niniejszym dokumencie jest mowa o:

1) szkole – należy przez to rozumieć Zespół Szkół w Wiechlicach, w skład którego wchodzą: Szkoła Podstawowa im. Kornela Makuszyńskiego w Wiechlicach, Szkoła Podstawowa im. Kornela Makuszyńskiego w Wiechlicach Filia W Długiem, Szkoła Podstawowa im. Kornela Makuszyńskiego w Wiechlicach Filia w Lesznie Górnym, Szkoła Podstawowa im. Kornela Makuszyńskiego w Wiechlicach Filia w Siecieborzycach Gimnazjum nr 3 w Wiechlicach,;
2) Administratorze Danych (AD) – należy przez to rozumieć Dyrektora Zespołu Szkół;
3) Administratorze Bezpieczeństwa Informacji (ABI) – należy przez to rozumieć pracownika szkoły wyznaczonego przez Administratora Danych, odpowiedzialnego za bezpieczeństwo danych osobowych przetwarzanych w Zespole Szkół w Wiechlicach;
4) użytkowniku systemu – należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym szkoły. Użytkownikiem może być pracownik szkoły, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, osoba odbywająca w szkole staż lub praktykę. Ewidencję osób upoważnionych do przetwarzania danych osobowych prowadzi ABI;
5) loginie użytkownika – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych w systemie informatycznym;
6) haśle – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie upoważnionej do pracy w systemie informatycznym;

7) stacji roboczej – stacjonarny lub przenośny komputer wchodzący w skład systemu informatycznego umożliwiający użytkownikom systemu dostęp do danych osobowych znajdujących się w systemie;
8) sieci lokalnej – należy przez to rozumieć połączenie systemów informatycznych szkoły wyłącznie dla własnych potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych, znajdujących się wyłącznie na terenie szkoły;
9) sieci rozległej – należy przez to rozumieć sieć publiczną w rozumieniu ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800 ze zm.);
10) danych osobowych – rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
11) zbiorze danych – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów;
12) wykazie zbiorów danych osobowych – rozumie się przez to wykaz zarejestrowanych oraz niepodlegających rejestracji zbiorów danych osobowych;
13) przetwarzaniu danych – rozumie się przez to 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;
14) systemie informatycznym – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
15) rozporządzeniu – należy przez to rozumieć rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznychi organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych;
16) ustawie – należy przez to rozumieć ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

III. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności (§ 5 pkt 1 rozporządzenia)

1. Informacje ogólne

1.1. Zarządzanie systemem informatycznym w Zespole Szkół w Wiechlicach należy do Administratora Bezpieczeństwa Informacji oraz do pracownika zajmującego stanowisko informatyka, którzy nadzorują przestrzeganie zasad ochrony przetwarzanych danych

osobowych określonych ustawą z 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r. Nr 101, poz. 926 z późn. zm.). Osoby te mają za zadanie dbać o bezpieczeństwo i prawidłowość w przebiegu procesów przetwarzania danych osobowych. Szczegółowy zakres obowiązków Administratora Bezpieczeństwa Informacji określa rozdział VI pkt. 2 Polityki bezpieczeństwa przetwarzania danych osobowych w Zespole Szkół w Wiechlicach.

1.2. Zbiory danych w szkole znajdują się na serwerach i stacjach roboczych oraz w postaci kartotek lub dokumentacji, przechowywanych w zamkniętych szafach.

2. Procedura nadawania i zmiany uprawnień

2.1. Przetwarzać dane osobowe w systemach informatycznych ma prawo jedynie osoba, która otrzymała od Administratora Danych pisemne upoważnienie do przetwarzania danych osobowych (wzór upoważnienia stanowi załącznik nr 1 do niniejszej instrukcji).

Oryginał upoważnienia przechowywany jest w aktach osobowych pracownika. Każdy pracownik, który otrzymał upoważnienie, podpisuje oświadczenie zobowiązujące go do zachowania w tajemnicy informacji nabytych podczas wykonywania swoich obowiązków zarówno podczas zatrudnienia, jak również po jego ustaniu. Wzór oświadczenia stanowi załącznik nr 2 do niniejszej instrukcji.

Obsługa szkoły (sprzątaczki, woźny), z uwagi na fakt, iż mogą mieć styczność z danymi osobowymi podpisują tylko oświadczenie. Osoby odbywające staż lub praktykę mogą mieć dostęp do danych osobowych na podstawie upoważnienia nadanego przez Administratora Danych oraz oświadczenia.

2.2. Login (identyfikator) i hasło do systemu informatycznego przetwarzającego dane osobowe są przydzielane pracownikowi tylko wówczas, kiedy posiada upoważnienie do przetwarzania danych osobowych. Za przydzielenie i wygenerowanie loginu i hasła użytkownikowi odpowiada informatyk zatrudniony w Szkole, zaś wyrejestrowanie użytkownika z systemu informatycznego dokonuje się na wniosek Administratora Danych lub przełożonego użytkownika złożony Administratorowi Bezpieczeństwa Informacji.

2.3. Administrator Bezpieczeństwa Informacji zobowiązany jest do sporządzenia i regularnego aktualizowania ewidencji pracowników upoważnionych do przetwarzania danych osobowych w Szkole. Ewidencja powinna zawierać:

1) imię i nazwisko osoby upoważnionej,
2) datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych,
3) nazwa systemu informatycznego,
4) identyfikator nadany w systemie.

Wzór ewidencji stanowi załącznik nr 3 do niniejszej instrukcji.

IV. Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem (§ 5 pkt 2 rozporządzania)

1. Najważniejszą zasadą przy wyborze metod i środków uwierzytelniania jest zapewnienie bezpieczeństwa systemu i sieci informatycznych oraz ochrona informacji przed ich ujawnieniem, zniszczeniem lub dostępem do nich osób nieuprawnionych. W tym celu w Szkole stosuje się środki bezpieczeństwa:

   1) na poziomie podwyższonym, tj.:
      a) do uwierzytelnienia użytkowników używa się hasła, składającego się min. z 8 znaków zawierających małe i wielkie litery oraz cyfry i znaki specjalne,
      b) urządzenia i nośniki zawierające dane osobowe przekazywane poza obszar zabezpiecza się w sposób zapewniający poufność i integralność tych danych;
   2) oraz na poziomie wysokim, tj.:
      a) 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,
      b) logiczne zabezpieczenia o których mowa w ppkt. a) obejmują:
         - kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych a siecią publiczną,
         - kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora danych.

2. Dostęp do danych osobowych przetwarzanych w systemie informatycznym następuje po podaniu właściwego loginu i hasła.

3. Każdy login jest inny i jest on przypisany tylko jednemu użytkownikowi. Za wszystkie czynności wykonane przy użyciu danego loginu odpowiedzialność ponosi jego użytkownik. Prawidłowy login składa się minimalnie z czterech znaków, które nie są rozdzielone spacjami ani znakami interpunkcyjnymi, nie zawiera również znaków charakterystycznych dla języka polskiego. Wszystkie loginy wpisuje się do bazy użytkowników znajdującej się

na serwerze głównym wraz z imieniem i nazwiskiem użytkownika oraz hasłem dostępu. Do bazy dostęp posiada jedynie informatyk sprawujący piecze nad prawidłowym działaniem systemu informatycznego. Następnie dane te są wprowadzane do właściwych systemów. Login użytkownika jest stały i nie powinien być zmieniany. Niedopuszczalne jest, po wyrejestrowaniu użytkownika z systemu informatycznego, przydzielenie tego samego loginu innej osobie.

4. Dla bezpieczeństwa danych osobowych, system informatyczny przetwarzający te dane wymusza na użytkownikach zmianę hasła co 30 dni od momentu jej ostatniej zmiany.

V. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu (§ 5 pkt 3 rozporządzania)

Przed rozpoczęciem każdy pracownik powinien upewnić się, czy nie wystąpiły przesłanki świadczące o naruszeniu ochrony danych osobowych. Oznaki, o których mowa to np.:

1) brak możliwości uruchomienia przez użytkownika aplikacji pozwalającej na dostęp do danych osobowych, brak możliwości zalogowania się do tej aplikacji,
2) inny zakres danych niż normalnie dostępny dla użytkownika - dużo więcej lub dużo mniej danych,
3) kradzież sprzętu informatycznego, w którym przechowywane są dane osobowe lub ślady włamania lub prób włamania do obszaru, w którym przetwarzane są dane osobowe;
4) pojawienie się niestandardowych komunikatów generowanych przez system informatyczny;
5) wygląd aplikacji inny niż normalnie
6) sytuacje losowe niekorzystnie wpływające na zasoby systemu jak np. wybuch gazu, pożar, zalania pomieszczeń, katastrofa budowlana, niepożądana ingerencja ekipy remontowej itp.;
5) naruszenie dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (np. niewylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie wydrukowanych danych osobowych w drukarce czy w kserokopiarce, niewykonanie w określonym terminie kopii bezpieczeństwa, itp.);

W przypadku stwierdzenia naruszenia ochrony danych osobowych każdy pracownik zatrudniony przy przetwarzaniu danych osobowych ma obowiązek natychmiast zgłosić ten

fakt Administratorowi Bezpieczeństwa Informacji, który po zapoznaniu się z zaistniałą sytuacją, wybiera właściwą opcję do dalszego postępowania mając na uwadze politykę bezpieczeństwa w tym zakresie. Administrator Bezpieczeństwa Informacji w formie protokołu szczegółowo opisuje przypadek naruszenia oraz sporządza raport, którego wzór stanowi załącznik nr 4 do niniejszej dokumentacji.

1. Procedura rozpoczęcia pracy

1) rozpoczęcie pracy w systemie informatycznym obejmuje wprowadzenie przez użytkownika loginu i hasła dostępu w taki sposób, aby możliwie najlepiej udaremnić osobom niepowołanym ich podejrzenie oraz ogólne stwierdzenie poprawności działania systemu,
2) Po przekroczeniu trzech prób nieprawidłowego logowania, system automatycznie zamyka aplikację. Zalogowanie się wymaga wówczas ponownego włączenia aplikacji.

2. Procedura zawieszenia pracy

1) w przypadku pozostawienia przez użytkownika stacji roboczej w bezruchu po 15 minutach uruchamia się wygaszasz ekranu, który automatycznie blokuje dostęp do systemu. Aby go odblokować należy ponownie się zalogować.
2) W biurach, w których przetwarzane są dane, a w których jednocześnie mogą przebywać osoby trzecie, monitory stanowisk dostępu do danych powinny być ustawione w taki sposób, aby osobom tym udaremnić wgląd w dane.
3) Przy każdorazowym opuszczaniu stanowiska pracy przy stacji roboczej, pracownik powinien dopilnować, aby na ekranie komputera nie były wyświetlane dane osobowe. W celu zwiększenia bezpieczeństwa powinno się zablokować komputer używając do tego jednocześnie klawiszy Carl+Alt+Delete i wybrać opcję – ZABLOKUJ KOMPUTER.

3. Procedura zakończenia pracy

Warunkiem koniecznym przy zakończeniu pracy w systemie informatycznym jest prawidłowe wylogowanie się z aplikacji przez użytkownika, tzn. należy:

1) zamknąć aplikację;
2) zamknąć system;
3) wyłączyć monitor.

VI. Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania (§ 5 pkt 4 rozporządzania)

Dane osobowe przetwarzane w systemie informatycznym zabezpieczane są kopiami zapasowymi tworzonymi przez informatyka.

1. W momencie lokalnego przetwarzania danych osobowych na stacjach roboczych informatyk zobowiązany jest do centralnego przechowywania kopii danych, w taki sposób, aby możliwe było zabezpieczenie ich dostępności poprzez wykonanie kopii zapasowych. Pod sformułowaniem centralnego przechowywania kopii danych należy rozumieć comiesięczne przegranie zbioru danych na celowo wydzielony ku temu obszar dysku na serwerze. W przypadku, gdy z przyczyn technicznych jest to niewykonalne wówczas kopie zapasowych baz danych sporządzane są na nośniku wymiennym i przechowywane w miejscu niedostępnym dla osób trzecich.

2. Do tworzenia kopii zapasowych służą specjalnie przeznaczone do tego celu urządzania będące częścią systemu informatycznego na nośnikach wymiennych adekwatnych do rodzaju urządzenia.

3. W razie przechowywania kopii zapasowych przez okres dłuższy niż 6 m-cy, 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) kontrolowane odnośnie ich dalszej przydatności.

VII. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych, o których mowa w § 5 pkt 4 rozporządzenia

1. Nośniki danych tak w postaci elektronicznej, jak i papierowej winny być zabezpieczone przed dostępem osób nieupoważnionych, nieautoryzowaną modyfikacją i zniszczeniem. Dane osobowe mogą być zapisywane na nośnikach przenośnych w przypadku tworzenia kopii zapasowych lub, gdy istnieje taka potrzeba, przeniesienia tych danych w postaci elektronicznej, a wykorzystanie do tego celu sieci informatycznej może okazać się ryzykowne.

2. Nośniki danych osobowych oraz wydruki powinny być przechowywane w zamkniętych szafach wewnątrz pomieszczeń, w których dokonuje się przetwarzania danych osobowych i pod żadnym pozorem nie powinny być bezzasadnie wynoszone poza ten obszar. Przekazywanie nośników danych osobowych i wydruków poza budynki należące do Szkoły powinno odbywać się za wiedzą Administratora Bezpieczeństwa Informacji.

3. W przypadku, gdy nośnik danych osobowych lub kopia zapasowa staną się nieprzydatne i nie podlegają archiwizacji, należy dokonać ich zniszczenia, bądź też usunięcia danych za pomocą specjalnego oprogramowania do bezpiecznego usuwania zapisanych danych. W przeciwnym wypadku podlegają one fizycznemu skasowaniu z wykorzystaniem metod należytych do typu nośnika, w sposób zapobiegający odczytaniu zapisanych na nich danych. Aby skasować nośniki typu USB, dysk twardy, pendrive należy je przekazać informatykowi. Jeżeli natomiast wydruk danych osobowych nie jest już dłużej potrzebny, należy przeprowadzić zniszczenie wydruku przy użyciu niszczarki dokumentów.

VIII. Sposób zabezpieczenia systemu informatycznego przez działalnością oprogramowania, o którym mowa w pkt III ppkt. 1 załącznika do rozporządzenia (§ 5 pkt 6 rozporządzenia)

Biorąc pod uwagę, iż system informatyczny wystawiony jest na działanie oprogramowania, celem którego jest uzyskanie nielegalnego dostępu do tego systemu konieczne jest podjęcie stosownych środków zapobiegawczych.

1. Wyróżnia się następujące rodzaje zagrożeń,:
   1) nieuprawniony dostęp bezpośrednio do bazy danych;
   2) uszkodzenie kodu aplikacji umożliwiającej dostęp do bazy danych w taki sposób, że przetwarzane dane osobowe ulegną zafałszowaniu lub zniszczeniu;
   3) przechwycenie danych podczas transmisji w przypadku rozproszonego przetwarzania danych z wykorzystaniem ogólnodostępnej sieci Internet;
   4) 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;
   5) uszkodzenie lub zafałszowanie danych osobowych przez wirus komputerowy zakłócający pracę aplikacji umożliwiającej dostęp do bazy danych na stacji roboczej wykorzystywanej do przetwarzania danych osobowych.

2. Aby przeciwdziałać zagrożeniom system informatyczny powinien być wyposażony w następujące zabezpieczenia:
   1) fizyczne odseparowanie serwera bazy danych od sieci zewnętrznej;
   2) autoryzacja użytkowników przy zachowaniu odpowiedniego poziomu komplikacji haseł dostępu;
   3) stosowanie odpowiedniej ochrony antywirusowej na stacjach roboczych wykorzystywanych do przetwarzania danych osobowych.

3. Najczęstszymi przyczynami wdzierania się programów szpiegowskich oraz wirusów komputerowych na stacje robocze są:
   1) załączniki do poczty elektronicznej;
   2) przeglądane strony internetowe;
   3) pliki i aplikacje pochodzące z nośników wymiennych uruchomiane i odczytywane na stacji roboczej.

4. Aby zapewnić ochronę antywirusową system antywirusowy powinien być skonfigurowany w następujący sposób:
   1) rezydentny monitor antywirusowy (uruchomiony w pamięci operacyjnej stacji roboczej) powinien być stale włączony;
   2) antywirusowy skaner ruchu internetowego powinien być stale włączony;
   3) monitor zapewniający ochronę przed wirusami makr w dokumentach MS Office powinien być stale włączony;
   4) skaner poczty elektronicznej powinien być stale włączony.

5. Systemy antywirusowe zainstalowane na stacjach roboczych natomiast powinny być skonfigurowane w sposób następujący:
   1) zablokowanie możliwości ingerencji użytkownika w ustawienia oprogramowania antywirusowego,
   2) możliwość centralnego uaktualniania wzorców wirusów.

6. Użytkownicy systemu informatycznego zobowiązani są do:
   1) skanowania zawartości nośników wymiennych odczytywanych na stacji roboczej pracującej w systemie informatycznym pod względem potencjalnie niebezpiecznych kodów – przy każdym odczycie.
   2) skanowanie informacji przesyłanych do systemu informatycznego pod kątem pojawienia się niebezpiecznych kodów – na bieżąco.

7. W sytuacji wystąpienia infekcji i niemożności automatycznego usunięcia wirusów przez system antywirusowy osoba zatrudniona na stanowisku informatyka powinna podjąć działania mające na celu usunięcie tegoż zagrożenia. Działania te mogą obejmować m.in.:
   1) usuniecie zainfekowanych plików, o ile jest to akceptowalne ze względu na prawidłowe funkcjonowanie systemu informatycznego;
   2) odtworzenie plików z kopii zapasowych po uprzednim sprawdzeniu, czy dane zapisane na kopiach nie są zainfekowane;
   3) samodzielną ingerencję w zawartość pliku – w zależności od posiadanych kwalifikacji lub skonsultowanie się z zewnętrznymi ekspertami.

8. System informatyczny przetwarzający dane osobowe powinien posiadać mechanizmy zabezpieczające te dane przed utratą lub wystąpieniem zafałszowania w wyniku niepoprawnego funkcjonowania lub zakłóceń w sieci zasilającej. Z uwagi na to system informatyczny powinien być zaopatrzony przynajmniej w:
   1) filtry zabezpieczające stacje robocze skutkami przepięcia,
   2) zasilacze awaryjne serwerów baz danych, serwerów aplikacji oraz urządzeń pamięci masowej pozwalające na bezpieczne zamkniecie aplikacji przetwarzających dane osobowe w sposób umożliwiający poprawne zapisanie przetwarzanych danych.

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

1. System informatyczny przetwarzający dane osobowe musi posiadać mechanizm uwierzytelniający użytkownika, wykorzystujący login 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:
   1) rozpoczęcie i zakończenie pracy przez użytkownika systemu;
   2) operacje wykonywane na przetwarzanych danych, a w szczególności ich dodanie, modyfikację oraz usunięcie;

3) przesyłanie za pośrednictwem systemu danych osobowych przetwarzanych w systemie informatycznym innym podmiotom nie będącym właścicielem ani współwłaścicielem systemu;
4) nieudane próby dostępu do systemu informatycznego przetwarzającego dane osobowe oraz nieudane próby wykonania operacji na danych osobowych;
5) błędy w działaniu systemu informatycznego podczas pracy danego użytkownika.

3. Zapis działań użytkownika uwzględnia:
1) login użytkownika;
2) datę i czas, w którym zdarzenia miało miejsce;
3) rodzaj zdarzenia;
4) określenie informacji, których zdarzenie dotyczy (identyfikatory rekordów).

4. W zakresie możliwości technicznych system informatyczny powinien posiadać mechanizmy pozwalające na samoczynne poinformowanie Administratora Bezpieczeństwa Informacji o zaistnieniu zdarzenia krytycznego, mogącego mieć znaczenie dla bezpieczeństwa przetwarzanych danych osobowych.

5. Dodatkowo system informatyczny powinien zapewnić zapis faktu przekazania danych osobowych z uwzględnieniem:
1) loginu osoby, której dane dotyczą;
2) osoby przesyłającej dane;
3) odbiorcy danych;
4) zakresu przekazanych danych osobowych;
5) daty operacji;
6) sposobu przekazania danych.

IX. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych (§ 5 pkt 8 rozporządzania)

1. Wszystkie prace przeglądowe i konserwacyjne urządzeń, które wchodzą w skład systemu informatycznego powinny być przeprowadzane w terminach podanych przez producenta systemu. Jeżeli termin nie został jednoznacznie określony, wówczas o czynnościach tych decyduje informatyk Szkoły.

2. Ogół prac związanych z naprawą i konserwacją systemu informatycznego przetwarzającego dane osobowe winien uwzględniać wymagany poziom zabezpieczenia danych przed dostępem osób nieuprawnionych. Prace serwisowe w obrębie Szkoły mogą być wykonywane wyłącznie przez informatyka lub przez upoważnionych przedstawicieli wykonawców zewnętrznych w obecności informatyka.

3. Ujawnione nieprawidłowości w trakcie przeglądów lub konserwacji winny być niezwłocznie usunięte, a przyczyny przeanalizowane. O ujawnieniu nieprawidłowości należy zawiadomić Administratora Danych oraz Administratora Bezpieczeństwa Informacji.

4. Za terminowość przeprowadzanych przeglądów, konserwacji i ich prawidłowy przebieg odpowiada informatyk.

5. 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.

DYREKTOR
Zespołu Szkół w Wrechlicach
mgr Cecylia Brodzińska

Załącznik nr 1
do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

.....
/miejscowość, data/

Wzór

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH
nr ...../20.....

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2015 r. poz. 2135) upoważniam:

.....

zatrudnioną na stanowisku .....
w *Zespole Szkół w Wiechlicach*

do przetwarzania danych osobowych w funkcjonujących systemach informatycznych, kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych, w związku z realizacją przydzielonych obowiązków pracowniczych tj. .....
..... .

Jednocześnie zobowiązuję w/w do zachowania w tajemnicy przetwarzanych danych osobowych oraz sposobu ich zabezpieczenia.

Upoważnienie ważne jest od ..... do .....
Traci moc upoważnienie nr .....

.....
Administrator Danych

Załącznik nr 2
do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

Wzór

..... Wiechlice, ... r.
(imię i nazwisko)

.....
(stanowisko)

Oświadczenie
o zachowaniu poufności i zapoznaniu się z przepisami

Ja niżej podpisany/a oświadczam, iż zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których mam lub będę miał/a dostęp w związku z wykonywaniem zadań i obowiązków służbowych wynikających ze stosunku pracy, zarówno w czasie trwania umowy, jak i po jej ustaniu.

Oświadczam, że zostałem/am poinformowany/a o obowiązujących w Zespole Szkół w Wiechlicach zasadach dotyczących przetwarzania danych osobowych, określonych w „Polityce bezpieczeństwa przetwarzania danych osobowych w Zespole Szkół w Wiechlicach" oraz w „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Zespole Szkół w Wiechlicach" i zobowiązuję się ich przestrzegać. W szczególności oświadczam, że bez upoważnienia nie będę wykorzystywał/a danych osobowych ze zbiorów znajdujących się w Szkole. Zostałem/am zapoznany/a z przepisami Ustawy o ochronie danych osobowych (Dz. U. z 2015 r. poz. 2135) oraz Rozporządzenia MSWiA 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). Poinformowano mnie również o grożącej, stosownie do przepisów rozdziału 8 Ustawy o ochronie danych osobowych odpowiedzialności karnej. Niezależnie od odpowiedzialności przewidzianej w wymienionych przepisach, mam świadomość, że złamanie zasad ochrony danych osobowych, obowiązujących w Zespole Szkół w Wiechlicach może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną.

.....
(podpis pracownika)

Załącznik nr 3
do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

Wzór

Ewidencja osób upoważnionych do przetwarzania danych osobowych w Zespole Szkół w Wiechlicach

L.p.	Numer upoważnienia	Imię i nazwisko	Zbiór danych osobowych	Nazwa systemu	Data nadania i ustania upoważnienia	Login	Uwagi
1.							
2.							
3.							
4.							
5.							
...							

Wzór

Raport z naruszenia ochrony danych osobowych
w Zespołem Szkół w Wiechlicach

1. Osoba powiadamiająca o zaistniałym zdarzeniu oraz osoby odpytane w związku ze sprawą:

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

.....

2. Data ..... Godzina.....

3. Lokalizacja zdarzania;

.....
(np. nr biura, nazwa pomieszczenia)

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

.....

5. Opis podjętych działań i metod postępowania:

.....

.....

6. Ocena przyczyn wystąpienia naruszenia:

.....

.....

7. Ocena przeprowadzonego postępowanie wyjaśniającego i naprawczego:

.....

.....

.....
data i podpis Administratora
Bezpieczeństwa Informacji