POLITYKA BEZPIECZEŃSTWA INFORMACJI

ZESPÓŁ SZKÓŁ SAMORZĄDOWYCH W OBJEŹDZIE

Grupa objęta: **Wszyscy współpracownicy Zespołu Szkół Samorządowych w Objeździe**

Miejsce przeznaczenia: **Zespół Szkół Samorządowych w Objeździe**

Podstawa prawna

Polityka Bezpieczeństwa Informacji uwzględnia wymagania dotyczące zarządzania bezpieczeństwem informacji zawarte w Normie PN-ISO/IEC 17799:2007 oraz w poniższych dokumentach:

1. Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997r. (Dz. U. 2002 nr 101, poz. 926 z późn. zmian.),
2. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. 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. 2004 nr 100, poz. 1024),
3. Norma PN - ISO/IEC 17799:2007 Technika informatyczna – Praktyczne zasady zarządzania bezpieczeństwem informacji.

Powyższa norma wskazuje zalecenia w zakresie zarządzania bezpieczeństwem informacji do wykorzystania przez wszystkich tych, którzy są odpowiedzialni za inicjowanie, wdrażanie oraz utrzymywanie bezpieczeństwa w organizacji. Zamiarem jest dostarczenie wszystkim użytkownikom możliwie najpełniejszej wiedzy w celu ujednolicenia norm bezpieczeństwa i efektywnej praktyki zarządzania bezpieczeństwem informacji oraz zapewnienie zaufania w stosunkach pomiędzy współpracującymi z **Zespołem Szkół Samorządowych** w Objeździe, organizacjami i klientami.

Podstawowe pojęcia

§ 1

– **Dane osobowe** - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na **numer identyfikacyjny** albo jeden z kilku specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne;

– **Zbiór danych osobowych** - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony (jego części znajdują się w różnych miejscach) lub podzielony funkcjonalnie (przetwarzany za pomocą programów realizujących różne funkcje);

– **Przetwarzanie danych osobowych** - jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, udostępnianie i usuwanie; zwłaszcza takie, które wykorzystuje się w systemach informatycznych;

– **System informatyczny** - system przetwarzania informacji realizowany w Szkole i na rzecz Szkoły, wraz ze związanymi z nimi ludźmi oraz zasobami technicznymi i finansowymi, który dostarcza i rozprowadza informacje. Ochronie podlegają nie tylko informacje osobowe, ale także użytkownicy, zasoby techniczne oraz metody ochrony informacji;

– **Bezpieczeństwo systemu informatycznego** - wdrożenie stosowanych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów informacyjnych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub nieuprawnionym pozyskaniem danych osobowych, a także ich utratą (zamierzoną lub przypadkową);

– **Administrator Danych Osobowych (ADO)** - organ, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania danych osobowych.
Administratorem Danych Osobowych jest **Dyrektor Zespołu Szkół Samorządowych w Objeździe** który ponosi pełnię odpowiedzialności wynikającej z przepisów ustawy o ochronie danych osobowych w odniesieniu do zbiorów danych osobowych znajdujących się w jego ustawowej i statutowej dyspozycji;

– **Administrator Bezpieczeństwa Informacji (ABI)** - należy przez to rozumieć osobę / podmiot (uprawnionych reprezentantów) wyznaczoną przez Administratora Danych Osobowych do nadzorowania przestrzegania zasad ochrony oraz wymagań w zakresie ochrony, wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych.

– **Administrator Systemów Informatycznych (ASI)** - należy przez to rozumieć wykonawcę (uprawnionych przedstawicieli) z zakresu informatyki odpowiedzialnego za stosowanie technicznych i organizacyjnych środków ochrony danych osobowych w systemach informatycznych;

– **Użytkownik** – osoba posiadająca upoważnienie wydane przez ADO i uprawniona do przetwarzania danych osobowych w odpowiedniej komórce organizacyjnej, w zakresie wskazanym w upoważnieniu;

– **Identyfikator użytkownika (LOGIN)** - ciąg znaków literowych i cyfrowych, lub innych, jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;

– **Hasło (Password)** - ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;

– **Zalogowanie -** uwierzytelnienie czyli działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;

– **Odbiorcy danych osobowych -** rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:

- osoby, której dane dotyczą,
- osoby, upoważnionej do przetwarzania danych,
- przedstawiciela, o którym mowa w art. 31 a ustawy o ochronie danych osobowych,
- podmiotu, o którym mowa w art. 31 ustawy o ochronie danych osobowych,
- organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.;

– **Sieć publiczna** – rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt. 22 ustawy z dnia 21 lipca 2000 r. – Prawo telekomunikacyjne (Dz.U nr 73, poz. 852 ze zm.);

– **Sieć telekomunikacyjna** – rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt. 23 ustawy z dnia 21 lipca 2000 r. – Prawo telekomunikacyjne;

– **Serwisant** – rozumie się przez to reprezentanta podmiotu zajmującego się sprzedażą, instalacją, naprawą i konserwacją sprzętu komputerowego lub oprogramowania.

CZĘŚĆ PIERWSZA

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

I.1 Wykaz miejsc, w których przetwarzane są dane osobowe

§ 2

	ADRES – BUDYNEK	**POMIESZCZENIA**	**ZABEZPIECZENIE**
1.	76-211 Objazda Objazda 95	• gabinet dyrektora • sekretariat	kluczami dysponuje dyrektor i sekretarz szkoły;
		gabinet zastępcy dyrektora	kluczami dysponuje zastępca dyrektora, dyrektor
		gabinet pedagoga szkolnego	kluczami dysponuje pedagog, klucze dostępne w sekretariacie szkoły
		gabinet pielęgniarki szkolnej	kluczami dysponuje pielęgniarka, dyrektor, klucze dostępne w sekretariacie szkoły
		Biblioteka	kluczami dysponuje bibliotekarz, klucze dostępne w pokoju nauczycielskim
		pokój nauczycielski	klucze dostępne w sekretariacie
		sale lekcyjne	klucze dostępne w pokoju nauczycielskim
		świetlica	klucze dostępne w pokoju nauczycielskim

I.2 Zbiory danych przetwarzanych w systemach informatycznych

§ 3

ZBIÓR DANYCH OSOBOWYCH	**PROGRAM INFORMATYCZNY SŁUŻĄCY DO PRZETWARZANIA ZBIORU DANYCH**	**MIEJSCE PRZETWARZANIA**	**ODPOWIEDZIALNY**
Pracownicy	SIO	sekretariat	starszy referent , dyrektor, zastępca
		pomieszczenia ZOEAS przy UG Ustka	księgowa, starszy referent przy ZOEAS

Uczniowie	SIO	sekretariat	starszy referent , dyrektor szkoły, zastępca dyrektora
	HERMES	sekretariat	starszy referent, zastępca dyrektora
		gabinet dyrektora szkoły	dyrektor szkoły
	Świadectwa	pracownia komputerowa	nauczyciel informatyki; wychowawca
	MS OFFICE (WORD, EXCELL)	gabinet dyrektora szkoły	dyrektor szkoły
		gabinet zastępcy dyrektora	zastępca dyrektora
		sekretariat	starszy referent
		gabinet pedagoga	pedagog szkolny
		pokój nauczycielski	nauczyciele
	LIBRUS	gabinet dyrektora szkoły	dyrektor szkoły
		gabinet zastępcy dyrektora	zastępca dyrektora
		gabinet pedagoga	pedagog
		sale lekcyjne	nauczyciele
	E-sekretariat	sekretariat	starszy referent
	Intendentura	pokój intendentki	intendentka
	MOL	biblioteka	bibliotekarz
Rodzice	LIBRUS	gabinet dyrektora szkoły	dyrektor szkoły
		gabinet zastępcy dyrektora	zastępca dyrektora
		gabinet pedagoga	pedagog
		sale lekcyjne	nauczyciele
Klienci zewnętrzni szkoły	MS OFFICE (WORD, EXCELL- umowy cywilno - prawne), VULCAN	gabinet dyrektora szkoły, sekretariat	dyrektor szkoły, starszy referent

I.3 Zbiory danych przetwarzanych tradycyjnie

§ 4

ZBIÓR DANYCH OSOBOWYCH	DOKUMENTACJA SŁUZĄCA DO PRZETWARZANIA ZBIORU DANYCH	MIEJSCE PRZETWARZANIA /ODPOWIEDZIALNY	MIEJSCE PRZECHOWYWANIA	ZABEZPIECZENIE
Pracownicy	Orzeczenia lekarskie do celów sanitarno - epide-miologicznych	sekretariat / starszy referent	sekretariat	szafka na klucz
	Oświadczenia i wnioski do	sekretariat /starszy referent	sekretariat	szafka na klucz

	funduszu socjalnego			
	Listy obecności pracowników	sekretariat / starszy referent	sekretariat	szafka na klucz
	Zaświadczenia	sekretariat / starszy referent	sekretariat	szafka na klucz
	Protokoły powypadkowe	sekretariat / starszy referent	sekretariat	szafka na klucz
	Arkusz organizacyjny	gabinet dyrektora szkoły /dyrektor szkoły	gabinet dyrektora szkoły	szafka na klucz
	Dokumentacja nadzoru pedagogicznego	gabinet dyrektora szkoły /dyrektor szkoły	gabinet dyrektora szkoły	szafka na klucz
	Dokumentacja awansów zawodowych nauczycieli	gabinet dyrektora szkoły /dyrektor szkoły	gabinet dyrektora szkoły	szafka na klucz
	Ewidencja zwolnień lekarskich;	sekretariat / starszy referent	sekretariat	szafka na klucz
	Podania; życiorysy/CV	gabinet dyrektora szkoły /dyrektor szkoły	sekretariat	szafa na klucz
	Notatki służbowe	gabinet dyrektora szkoły /dyrektor szkoły	sekretariat	szafa na klucz
	Dokumentacja dotycząca polityki kadrowej – opiniowanie awansów, wyróżnień, odznaczeń, nagród, wnioski o odznaczenia, itp;	gabinet dyrektora szkoły /dyrektor szkoły	gabinet dyrektora szkoły	szafka na klucz
	Ewidencja osób zatrudnionych przy przetwarzaniu danych osobowych;	gabinet dyrektora szkoły /dyrektor szkoły	gabinet dyrektora szkoły	szafka na klucz
	Dokumentacja dotycząca wynagrodzeń	sekretariat,/dyrektor/ zastępca dyrektora	sekretariat, gabinet dyrektora, gabinet zastępcy	szafa na klucz
Uczniowie	Dokumentacja uczniów; Karty zapisu dziecka/ucznia	sekretariat / starszy referent	sekretariat	szafka na klucz
	Księga uczniów	sekretariat / starszy referent	sekretariat	szafa na klucz
	Arkusze ocen	pokój nauczycielski /wychowawca; sekretariat / starszy referent	sekretariat	szafa na klucz

	Dziennik wychowawcy świetlicy	świetlica/ wychowawcy świetlicy	sekretariat	szafka na klucz
	Dziennik pedagoga	gabinet pedagoga/ pedagog	gabinet pedagoga	szafka na klucz
	Dziennik bibliotekarza	biblioteka/ bibliotekarz	biblioteka	szafka na klucz
	Pomoc społeczna, stypendia, wyprawki, obiady	sekretariat / starszy referent	sekretariat	szafka na klucz
	Księga wydanych legitymacji i legitymacje	sekretariat / starszy referent	sekretariat	szafka na klucz
	Rejestr zaświadczeń i zaświadczenia	sekretariat / starszy referent	sekretariat	szafka na klucz
	Księga absolwentów	sekretariat / starszy referent	sekretariat	szafa na klucz
	Świadectwa i duplikaty	sekretariat / starszy referent	sekretariat	szafka na klucz
	Dokumentacja ubezpieczeniowa	sekretariat / starszy referent	sekretariat	szafka na klucz
	Protokoły powypadkowe	sekretariat / starszy referent	sekretariat	szafka na klucz
	Karta zdrowia ucznia	gabinet pielęgniarki szkolnej; pielęgniarka	gabinet pielęgniarki szkolnej	szafka na klucz
	Karty szczepień	pielęgniarki szkolnej; pielęgniarka	gabinet pielęgniarki szkolnej	szafka na klucz
	Karty biblioteczne	biblioteka/ nauczyciel biblioteki	biblioteka	szafka na klucz
	Dokumentacja pomocy psychologiczno - pedagogicznej (opinie, orzeczenia)	gabinet pedagoga szkolnego, pokój nauczycielski	sekretariat, gabinet pedagoga szkolnego	szafka na klucz
	Ewidencja uczniów przystępujących do egzaminów zewnętrznych	gabinet dyrektora szkoły /dyrektor szkoły	gabinet dyrektora szkoły/ sekretariat	szafka na klucz
	Dokumenty zarchiwizowane	sekretariat/ starszy referent	pomieszczenie gospodarcze	pomieszczenie na klucz, klucze w sekretariacie
	Protokóły rad pedagogicznych, księga uchwał;	gabinet dyrektora szkoły /dyrektor szkoły	gabinet dyrektora szkoły	szafka na klucz
	Umowy zawierane z osobami fizycznymi;	gabinet dyrektora szkoły, sekretariat/ dyrektor szkoły	gabinet dyrektora szkoły /sekretariat	szafka na klucz
	Ewidencja decyzji – zwolnienia z obowiązkowych zajęć, odroczenia	gabinet dyrektora szkoły, sekretariat/ /dyrektor szkoły	gabinet dyrektora szkoły/sekretariat	szafka na klucz

	obowiązku szkolnego			
	Deklaracje uczęszczania na religię, sprzeciw od zajęć z wychowania do życia w rodzinie	sekretariat/ wychowawca	sekretariat	szafka na klucz

I.4 System przetwarzania danych

§ 5

1. W skład systemu wchodzą:

a) dokumentacja papierowa (korespondencja, dokumenty pracowników, uczniów i klientów zewnętrznych szkoły),

b) wydruki komputerowe,

c) urządzenia i oprogramowanie komputerowe służące do przetwarzania informacji,

d) procedury przetwarzania danych w tym systemie, w tym procedury awaryjne.

2. Przetwarzanie danych osobowych w systemie informatycznym odbywa się przy zachowaniu **wysokiego poziom bezpieczeństwa.**

I. 5 Środki techniczne i organizacyjne stosowane w przetwarzaniu danych

Cele i zasady funkcjonowania polityki bezpieczeństwa

§ 6

1. Realizując Politykę bezpieczeństwa informacji zapewnia ich:

a) poufność – informacja nie jest udostępniana lub ujawniana nieupoważnionym osobom, podmiotom i procesom,
b) integralność – dane nie zostają zmienione lub zniszczone w sposób nie autoryzowany,
c) dostępność – istnieje możliwość wykorzystania ich na żądanie, w założonym czasie, przez autoryzowany podmiot,
d) rozliczalność – możliwość jednoznacznego przypisania działań poszczególnym osobom,
e) autentyczność – zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana,
f) niezaprzeczalność – uczestnictwo w całości lub części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie jest niepodważalne,
g) niezawodność – zamierzone zachowania i skutki są spójne.

2. Polityka bezpieczeństwa informacji w Szkole ma na celu zredukowanie możliwości wystąpienia negatywnych konsekwencji naruszeń w tym zakresie, tj.:

a) naruszeń danych osobowych rozumianych jako prywatne dobro powierzone Szkole,

b) naruszeń przepisów prawa oraz innych regulacji,

c) utraty lub obniżenia reputacji Szkoły,

d) strat finansowych ponoszonych w wyniku nałożonych kar,

e) zakłóceń organizacji pracy spowodowanych nieprawidłowym działaniem systemów.

3. Realizując Politykę bezpieczeństwa w zakresie ochrony danych osobowych Szkoła dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia, aby dane te były:

a) przetwarzane zgodnie z prawem,

b) zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,

c) merytorycznie poprawne i adekwatne w stosunku do celu, w jakim są przetwarzane,

d) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

Kompetencje i odpowiedzialność w zarządzaniu bezpieczeństwem danych osobowych

§ 7

Za przetwarzanie danych osobowych niezgodnie z prawem, celami przetwarzania lub przechowywanie ich w sposób niezapewniający ochrony interesów osób, których te dane dotyczą grozi odpowiedzialność karna wynikająca z przepisów ustawy o ochronie danych osobowych lub pracownicza na zasadach określonych w kodeksie pracy.

Administrator Danych Osobowych (ADO) – Dyrektor Szkoły:

- formułuje i wdraża warunki techniczne i organizacyjne służące ochronie danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem,
- decyduje o zakresie, celach oraz metodach przetwarzania i ochrony danych osobowych,
- wydaje upoważnienie do przetwarzania danych osobowych określając w nich zakres i termin ważności – wzór upoważnienia określa **załącznik nr 1,**
- odwołuje upoważnienie **– załącznik nr 2**
- odpowiada za zgodne z prawem przetwarzanie danych osobowych w Szkole.

Administrator Bezpieczeństwa Informacji (ABI) – pracownik Szkoły wyznaczony przez Dyrektora:

- egzekwuje zgodnie z prawem przetwarzanie danych osobowych w Szkole w imieniu ADO,

- prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych – wzór rejestru określa **załącznik nr 3**,
- ewidencjonuje oświadczenia osób upoważnionych o zaznajomieniu się z zasadami zachowania bezpieczeństwa danych – wzór oświadczenia określa **załącznik nr 4**,
- określa potrzeby w zakresie stosowanych w Szkole zabezpieczeń, wnioskuje do ADO o zatwierdzenie proponowanych rozwiązań i nadzoruje prawidłowość ich wdrożenia,
- udziela wyjaśnień i interpretuje zgodność stosowanych rozwiązań w zakresie ochrony danych osobowych z przepisami prawa,
- bierze udział w podnoszeniu świadomości i kwalifikacji osób przetwarzających dane osobowe w Szkole i zapewnia odpowiedni poziom przeszkolenia w tym zakresie.

Administrator Systemu Informatycznego (ASI) – pracownik Szkoły wyznaczony przez Dyrektora:

- zarządza bezpieczeństwem przetwarzania danych osobowych w systemie informatycznym zgodnie z wymogami prawa i wskazówkami ABI,
- doskonali i rozwija metody zabezpieczenia danych przed zagrożeniami związanymi z ich przetwarzaniem,
- przydziela identyfikatory użytkownikom systemu informatycznego oraz zaznajamia ich z procedurami ustalania i zmiany haseł dostępu,
- nadzoruje prace związane z rozwojem, modyfikacją, serwisowaniem i konserwacją systemu,
- zapewnia bezpieczeństwo wewnętrznego i zewnętrznego obiegu informacji w sieci i zabezpieczenie łączy zewnętrznych,
- prowadzi nadzór nad archiwizacją zbiorów danych oraz zabezpiecza elektroniczne nośniki informacji zawierających dane osobowe.

Pracownik przetwarzający dane (PPD) – pracownik upoważniony przez ABI:

- chroni prawo do prywatności osób fizycznych powierzających Szkole swoje dane osobowe poprzez przetwarzanie ich zgodnie z przepisami prawa oraz zasadami określonymi w Polityce bezpieczeństwa i Instrukcji zarządzania systemem informatycznym Szkoły,
- zapoznaje się zasadami określonymi w Polityce bezpieczeństwa i Instrukcji zarządzania systemem informatycznym Szkoły i składa oświadczenie o znajomości tych przepisów.

Zasady udzielania dostępu do danych osobowych

§ 8

1. Dostęp do danych osobowych może mieć wyłącznie **osoba zaznajomiona** z przepisami ustawy o ochronie danych osobowych oraz zasadami zawartymi w obowiązującej w Szkole Polityce bezpieczeństwa i Instrukcji zarządzania systemem informatycznym. Osoba zaznajomiona z zasadami ochrony danych potwierdza to w **pisemnym oświadczeniu**.

2. Dostęp do danych osobowych może mieć wyłącznie osoba posiadająca **upoważnienie** wydane przez ADO.

3. ABI może wyznaczyć upoważnionych do przetwarzania danych osobowych pracowników Szkoły do nadzoru nad upoważnionymi pracownikami podmiotów zewnętrznych lub innymi upoważnionymi osobami przetwarzającymi dane osobowe w Szkole.

Udostępnianie i powierzanie danych osobowych

§ 9

1. Dane osobowe mogą być udostępnione osobom i podmiotom z mocy przepisów prawa lub jeżeli w sposób wiarygodny uzasadnią one potrzebę ich posiadania, a ich udostępnienie nie naruszy praw i wolności osób, których one dotyczą.

2. Udostępnienie danych może nastąpić **na pisemny wniosek** zawierający następujące elementy:

- adresat wniosku (administrator danych),
- wnioskodawca,
- podstawa prawna (wskazanie potrzeby),
- wskazanie przeznaczenia,
- zakres informacji.

3. Administrator odmawia udostępnienia danych jeżeli spowodowałoby to naruszenie dóbr osobistych osób, których dane dotyczą lub innych osób.

4. Powierzenie danych może nastąpić wyłącznie w drodze **pisemnej umowy**, w której osoba przyjmująca dane zobowiązuje się do przestrzegania obowiązujących przepisów ustawy o ochronie danych osobowych. Umowa powinna zawierać informacje o podstawia prawnej powierzenia danych, celu i sposobie ich przetwarzania.

5. Każda osoba fizyczna, której dane przetwarzane są w Szkole, ma prawo zwrócić się z **wnioskiem** o udzielenie informacji związanych z przetwarzaniem tych danych, prawo do kontroli i poprawiania swoich danych osobowych, a także w przypadkach określonych w art. 32 ust 1 pkt 7 i 8 ustawy o ochronie danych osobowych prawo wniesienia umotywowanego żądania zaprzestania przetwarzania danych oraz sprzeciwu wobec przekazywania ich innym podmiotom.

6. Sprawy związane z udzielaniem informacji w tym zakresie prowadzi ABI, udzielając informacji o zawartości zbioru danych na piśmie zgodnie ze wzorem w **załączniku nr 5**.

Bezpieczeństwo w przetwarzaniu danych osobowych w formie tradycyjnej

§ 10

1. Pomieszczenia, w których znajdują się przetwarzane zbiory danych osobowych pozostają zawsze pod bezpośrednim nadzorem upoważnionego do ich przetwarzania pracownika. Opuszczenie pomieszczenia, w których znajdują się zbiory danych osobowych musi być poprzedzone przeniesieniem zbioru danych do odpowiednio zabezpieczonego miejsca. Przy planowanej dłuższej nieobecności pracownika pomieszczenie winno być zamknięte na klucz.

2. Klucze do szaf, w których przechowywane są dane osobowe mają jedynie pracownicy upoważnieni do przetwarzania danych osobowych w zakresie zgodnym z kategorią danych.

3. Korzystanie ze zbiorów danych osobowych przez osoby niezatrudnione w Szkole powinno odbywać się po uzyskaniu **upoważnienia** lub skonsultowane z ABI w przypadku osób upoważnionych do przetwarzania tych danych na podstawie ogólnie obowiązujących przepisów.

Bezpieczeństwo w przetwarzaniu danych osobowych w systemach informatycznych

§ 11

Zasady bezpiecznego użytkowania systemu informatycznego zawarte są w ***Instrukcji zarządzania systemem informatycznym***, obligatoryjnej do zapoznania się i stosowania przez wszystkich użytkowników systemu informatycznego szkoły.

I.6 Analiza ryzyka związanego z przetwarzaniem danych osobowych

Identyfikacja zagrożeń

§ 12

FORMA PRZETWARZANIA DANYCH	ZAGROŻENIA
Dane przetwarzane w sposób tradycyjny	• oszustwo, kradzież, sabotaż; • zdarzenia losowe (powódź, pożar); • zaniedbania pracowników szkoły (niedyskrecja, udostępnienie danych osobie nieupoważnionej); • niekontrolowana obecność nieuprawnionych osób w obszarze przetwarzania; • pokonanie zabezpieczeń fizycznych; • podsłuchy, podglądy; • ataki terrorystyczne; • brak rejestrowania udostępniania danych; • niewłaściwe miejsce i sposób przechowywania dokumentacji.
Dane przetwarzane w systemach informatycznych	• nieprzydzielenie użytkownikom systemu informatycznego identyfikatorów; • niewłaściwa administracja systemem; • niewłaściwa konfiguracja systemu; • zniszczenie (sfałszowanie) kont użytkowników; • kradzież danych kont; • pokonanie zabezpieczeń programowych; • zaniedbania pracowników szkoły (niedyskrecja, udostępnienie danych osobie nieupoważnionej);

	• niekontrolowana obecność nieuprawnionych osób w obszarze przetwarzania; • zdarzenia losowe (powódź, pożar); • niekontrolowane wytwarzanie i wypływ danych poza obszar przetwarzania z pomocą nośników informacji i komputerów przenośnych; • naprawy i konserwacje systemu lub sieci teleinformatycznej wykonywane przez osoby nieuprawnione; • przypadkowe bądź celowe uszkodzenie systemów i aplikacji informatycznych lub sieci; • przypadkowe bądź celowe modyfikowanie systemów i aplikacji informatycznych lub sieci; • przypadkowe bądź celowe wprowadzenie zmian do chronionych danych osobowych • brak rejestrowania zdarzeń tworzenia lub modyfikowania danych.

Sposób zabezpieczenia danych

§ 13

FORMA PRZETWARZANIA DANYCH	STOSOWANE ŚRODKI OCHRONY
Dane przetwarzane w sposób tradycyjny	• przechowywanie danych w pomieszczeniach zamykanych na zamki patentowe; • przechowywanie danych osobowych w szafach zamykanych na klucz; • przetwarzanie danych wyłącznie przez osoby posiadające upoważnienie nadane przez ABI; • zapoznanie pracowników z zasadami przetwarzania danych osobowych oraz obsługą systemu służącego do ich przetwarzania.
Dane przetwarzane w systemach informatycznych	• kontrola dostępu do systemów; • zastosowanie programów antywirusowych i innych regularnie aktualizowanych narzędzi ochrony; • systematyczne tworzenie kopii zapasowych zbiorów danych przetwarzanych w systemach informatycznych; • składowanie nośników wymiennych i nośników kopii zapasowych w odpowiednio zabezpieczonych szafach; • przydzielenie pracownikom indywidualnych kont użytkowników i haseł; • stosowanie indywidualnych haseł logowania do poszczególnych programów; • właściwa budowa hasła.

Określenie wielkości ryzyka

§ 14

Poziom ryzyka naruszenia bezpieczeństwa danych jest niski. Zastosowane techniczne i organizacyjne środki ochrony są adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych osobowych.

Identyfikacja obszarów wymagających szczególnych zabezpieczeń

§ 15

Uwzględniając kategorie przetwarzanych danych oraz zagrożenia zidentyfikowane w wyniku przeprowadzonej analizy ryzyka dla systemów informatycznych, stosuje się wysoki poziom bezpieczeństwa. Administrator Bezpieczeństwa Informacji i Administrator Systemów Informatycznych przeprowadzają okresową analizę ryzyka dla poszczególnych systemów i na tej podstawie przedstawiają Administratorowi Danych Osobowych propozycje dotyczące zastosowania środków technicznych i organizacyjnych, celem zapewnienia właściwej ochrony przetwarzanym danym.

CZĘŚC DRUGA

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

II.1 Cel instrukcji

§ 16

1. Instrukcja określa sposób zarządzania systemem informatycznym, wykorzystywanym do przetwarzania danych osobowych, przez administratora danych tj. w celu zabezpieczenia danych osobowych przed zagrożeniami, w tym zwłaszcza przed ich udostępnieniem osobom nieupoważnionym, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.

2. 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.

a) Administrator Systemu Informatycznego prowadzi elektroniczny system ewidencji:

- sprzętu komputerowego,
- osób pracujących w systemie,
- nadanych uprawnień pracownikom do właściwych systemów informatycznych,
- miejsc przetwarzania danych osobowych,
- kopii bezpieczeństwa.

b) Ewidencje sprzętu komputerowego mogą być prowadzone również w formie papierowej.

II.2 Nadawanie i rejestrowanie uprawnień

§ 17

1. Przetwarzać dane osobowe w systemach informatycznych może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych w Szkole.

2. Za tworzenie, modyfikację i nadawanie uprawnień kontom użytkowników odpowiada ASI.

3. ASI nadaje uprawnienia w systemie informatycznym na podstawie upoważnienia nadanego pracownikowi przez ABI.

4. Usuwanie kont stosowane jest wyłącznie w uzasadnionych przypadkach, standardowo, przy ustaniu potrzeby utrzymywania konta danego użytkownika ulega ono dezaktywacji w celu zachowania historii jego aktywności.

5. Osoby dopuszczone do przetwarzania danych osobowych zobowiązane są do zachowania tajemnicy w zakresie tych danych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje również po ustaniu stosunku pracy, co jest równoznaczne z cofnięciem uprawnień do przetwarzania danych osobowych.

II.3 Wyrejestrowywanie uprawnień

§ 18

1. Wyrejestrowania użytkownika z systemu informatycznego dokonuje Administrator Systemu Informatycznego.

2. Wyrejestrowanie, o którym mowa w ust. 1, może mieć charakter czasowy lub trwały.

3. Wyrejestrowanie następuje poprzez:

- zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe),
- usunięcie danych użytkownika z bazy systemu (wyrejestrowanie trwałe).

4. Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy.

II.4 Zabezpieczenie danych w systemie informatycznym

§ 19

1. Oprogramowanie wykorzystywane do przetwarzania danych posiada własny system kont (zabezpieczonych hasłami) i uprawnień. Zmiana hasła jest wymuszona automatycznie przez system.

2. Administrator Bezpieczeństwa Informacji może, w uzasadnionych sytuacjach, polecić dokonanie zmiany hasła przez użytkownika.

3. Hasło 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.

4. Identyfikator składa się z imienia oraz nazwiska użytkownika. W identyfikatorze pomija się polskie znaki diakrytyczne. Taki sposób nadawania identyfikatorów gwarantuje ich unikalność.

5. W przypadku utracenia hasła użytkownik ma obowiązek skontaktować się z ASI celem uzyskania nowego hasła.

6. System informatyczny przetwarzający dane osobowe musi posiadać mechanizmy pozwalające na odnotowanie faktu wykonania operacji na danych. W szczególności zapis ten powinien obejmować:

- rozpoczęcie i zakończenie pracy przez użytkownika systemu,
- operacje wykonywane na przetwarzanych danych,
- przesyłanie za pośrednictwem systemu danych osobowych przetwarzanych w systemie informatycznym innym podmiotom nie będącym właścicielem ani współwłaścicielem systemu,
- nieudane próby dostępu do systemu informatycznego przetwarzającego dane osobowe oraz nieudane próby wykonania operacji na danych osobowych,
- błędy w działaniu systemu informatycznego podczas pracy danego użytkownika.
- nieudane próby dostępu do systemu informatycznego przetwarzającego dane osobowe oraz nieudane próby wykonania operacji na danych osobowych,
- błędy w działaniu systemu informatycznego podczas pracy danego użytkownika.

7. System informatyczny powinien zapewnić zapis faktu przekazania danych osobowych z uwzględnieniem:

- identyfikatora osoby, której dane dotyczą,
- osoby przesyłającej dane,
- odbiorcy danych,
- zakresu przekazanych danych osobowych,
- daty operacji,
- sposobu przekazania danych.

8. Stosuje się aktywną ochronę antywirusową lub w przypadku braku takiej możliwości przynajmniej raz w tygodniu skanowanie całego systemu (w poszukiwaniu „złośliwego oprogramowania”) na każdym komputerze, na którym przetwarzane są dane osobowe.

9. Za dokonywanie skanowania systemu w poszukiwaniu złośliwego oprogramowania na stacjach roboczych (w przypadku braku ochrony rezydentnej) i aktualizację bazy wirusów odpowiada administrator systemu.

10. **Użytkownik jest zobowiązany** zawiadomić administratora systemu o pojawiających się komunikatach, wskazujących na wystąpienie zagrożenia wywołanego szkodliwym oprogramowaniem.

11. Użytkownicy mogą korzystać z zewnętrznych nośników danych tylko po uprzednim sprawdzeniu zawartości nośnika oprogramowaniem antywirusowym.

II.3 Zasady bezpieczeństwa podczas pracy w systemie informatycznym

§ 20

1. W celu rozpoczęcia pracy w systemie informatycznym użytkownik:

- loguje się do systemu operacyjnego przy pomocy identyfikatora i hasła;
- loguje się do programów i systemów wymagających dodatkowego wprowadzenia unikalnego identyfikatora i hasła.

2. W sytuacji tymczasowego zaprzestania pracy na skutek nieobecności przy stanowisku komputerowym należy uniemożliwić osobom postronnym korzystanie z systemu informatycznego poprzez wylogowanie się z sytemu lub uruchomienie wygaszacza ekranu.

3. W sytuacji gdy wgląd w wyświetlane na monitorze dane może mieć nieuprawniona osoba należy tymczasowo zmienić widok wyświetlany na monitorze lub obrócić monitor (przymknąć ekran laptopa) w sposób uniemożliwiający wgląd w wyświetlaną treść.

4. Użytkownik wyrejestrowuje się z systemu informatycznego przed wyłączeniem stacji komputerowej poprzez zamknięcie programu przetwarzającego dane oraz wylogowanie się z systemu operacyjnego.

5. Pracownik korzystający z systemu informatycznego zobowiązany jest do powiadomienia ASI w razie:

- podejrzenia naruszenia bezpieczeństwa systemu;
- braku możliwości zalogowania się użytkownika na jego konto;
- stwierdzenia fizycznej ingerencji w przetwarzane dane;
- stwierdzenia użytkowania narzędzia programowego lub sprzętowego.

6. Na fakt naruszenia zabezpieczeń systemu mogą wskazywać:

- nietypowy stan stacji roboczej (np. brak zasilania, problemy z uruchomieniem);
- wszelkiego rodzaju różnice w funkcjonowaniu systemu (np. komunikaty informujące o błędach, brak dostępu do funkcji systemu, nieprawidłowości w wykonywanych operacjach);
- różnice w zawartości zbioru danych osobowych (np. brak lub nadmiar danych);
- inne nadzwyczajne sytuacje.

Postanowienia dotyczące opisu zabezpieczenia systemu przed działaniem złośliwego oprogramowania

1. Z uwagi na fakt, iż komputery przetwarzające dane osobowe posiadają dostęp do sieci publicznej, Administrator Danych wdrożył procedury oraz oprogramowanie, które chroni dane osobowe przed nieuprawnionym dostępem, zmianą, usunięciem lub uszkodzeniem. Zagrożenia te to programy zawierające złośliwy kod (wirusy), tzw. konie trojańskie, oraz ataki hakerów.

2. Aby zmniejszyć to zagrożenie, zabronione jest pobieranie oraz instalowanie jakichkolwiek programów na komputerach służących do przetwarzania danych osobowych**. Programy instaluje Administrator Systemów Informatycznych**.
3. Zabronione jest również używanie nośników informacji niepochodzących z zasobów Administratora Danych. Każda osoba przetwarzająca dane osobowe przy użyciu komputera została pouczona, aby w wypadku jakichkolwiek podejrzeń dotyczących obniżenia bezpieczeństwa danych osobowych, poinformowała o tym fakcie osobę upoważnioną przez Administratora Danych lub Administratora Systemów Informatycznych.
4. Zabronione jest korzystanie na komputerach służących do przetwarzania danych osobowych z serwisów społecznościowych.

II.4 Tryb pracy na komputerach przenośnych

§ 21

1. Przy przetwarzaniu danych osobowych na komputerach przenośnych obowiązują procedury określone w niniejszej instrukcji.
2. Użytkownicy, którym zostały powierzone komputery przenośne, powinni chronić je przed uszkodzeniem lub utratą.
3. Obowiązuje zakaz używania komputerów przenośnych przez osoby inne niż użytkownicy, którym zostały one powierzone.
4. Praca na komputerze przenośnym możliwa jest po wprowadzeniu hasła i indywidualnego identyfikatora użytkownika.
5. Użytkownicy są zobowiązani zmieniać hasła w komputerach przenośnych nie rzadziej niż co 30 dni.

6. Obowiązuje zakaz samodzielnej modernizacji oprogramowania i sprzętu w powierzonych komputerach przenośnych. Wszelkie zmiany mogą być dokonywane tylko pod nadzorem administratora systemu, stosownie do wymagań niniejszej instrukcji. W razie wystąpienia usterek w pracy komputerów przenośnych lub w razie wystąpienia konieczności aktualizacji ich oprogramowania należy zgłosić to Administratorowi Systemu Informatycznego.

7. Komputery przenośne wyposażone są w odpowiednie programy ochrony antywirusowej, których aktualizację wykazuje automatycznie system.

8. Bezwzględnie zakazuje się wynoszenia komputerów przenośnych poza teren Szkoły.

9. Użytkownik zalogowany zobowiązany jest do przechowywania swoich plików w miejscu wskazanym przez ASI. Zabrania się usuwania nie swoich plików.

10. Zabronione jest przetwarzanie plików niezgodne z obowiązującym prawem autorskim.

II.5 Tworzenie kopii zapasowych

§ 22

1. Użytkowników obowiązuje zakaz tworzenia kopii zbiorów danych; całe zbiory danych mogą być

kopiowane wyłącznie przez administratora systemu (odpowiednie nośniki) lub automatycznie przez system, z zachowaniem przyjętych procedur ochrony danych osobowych.

2. Odpowiedzialnym za wykonanie kopii danych i kopii awaryjnych jest Administrator Sytemu Informatycznego.

3. Kopie przechowywane są w szafie w sekretariacie (pokój nr 31) Szkoły.

4. Kopie zapasowe zbiorów danych należy okresowo sprawdzać pod kątem ich przydatności do odtworzenia w przypadku awarii systemu. Okresową weryfikację kopii bezpieczeństwa pod kątem ich przydatności do odtworzenia danych przeprowadza ASI.

5. Usuwanie kopii danych następuje poprzez bezpieczne kasowanie. Nośniki danych, na których zapisywane są kopie bezpieczeństwa niszczy się trwale w sposób mechaniczny.

II.6 Udostępnienie danych

§ 23

1. Dane osobowe przetwarzane w systemach informatycznych mogą być udostępnione osobom i podmiotom z mocy przepisów prawa.

2. Do podmiotów, dla których dopuszczalne jest udostępnianie danych przez szkołę należą:

- Organ Nadzorujący (w związku z awansem zawodowym, wyniki badań psychologiczno-pedagogicznych dzieci i młodzieży, ewaluacji zewnętrznej, zadań wynikających z organizacji pracy szkoły);
- Organ Prowadzący (wykaz z czasem pracy pracowników, udostępnianie dzienników zajęć, wykazy wygenerowane z SIO);
- Dzienniki lekcyjne (dane rodziców w zakresie opisanym w Rozporządzeniu MEN z dnia 19 lutego 2002r. w sprawie sposobu prowadzenia dokumentacji);
- Strona www (dane osobowe ucznia i np. jego osiągnięcia, publikowanie list z wynikami, ocenami, zdjęciem – tylko za zgodą);
- Szkolna tablica ogłoszeń (publikowanie list z wynikami, ocenami, zdjęciem – tylko za zgodą)
- Formularz zgłoszeniowy do szkoły (dane osobowe: nr telefonu, PESEL dziecka, itp. – tylko za zgodą);
- Podmioty świadczące usługi w zakresie oświaty, np. PZU (w zależności od celu);
- Podmioty nadzorujące realizację projektu EFS (dane osobowe uczestników projektu, w zależności od celu).

II.7 Przeglądy i konserwacje systemów

§ 24

1. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe mogą być wykonywane wyłącznie przez pracowników Szkoły lub przez upoważnionych przedstawicieli wykonawców.

2. Prace wymienione w § 24 powinny uwzględniać wymagany poziom zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych.

3. Przed rozpoczęciem prac wymienionych w § 24 przez osoby niebędące pracownikami Szkoły należy dokonać potwierdzenia tożsamości tychże osób.

II.8 Niszczenie wydruków i nośników danych

§ 25

1. Wszelkie wydruki z systemów informatycznych zawierające dane osobowe przechowywane są w miejscu uniemożliwiającym ich odczyt przez osoby nieuprawnione, w zamkniętych szafach lub pomieszczeniach i po upływie ich przydatności są niszczone przy użyciu niszczarek / w sposób uniemożliwiający ich odczytanie (pocięte w poprzeczne paski)

2. Niszczenie zapisów na nośnikach danych powinno odbywać się poprzez wymazywanie informacji oraz formatowanie nośnika.

3. Uszkodzone nośniki danych przed ich wyrzuceniem należy fizycznie zniszczyć w niszczarce.

CZĘŚĆ TRZECIA

INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA DANYCH

III.1 Istota naruszenia danych osobowych

§ 26

1. Naruszeniem danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych osobowych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego, a w szczególności:

- nieautoryzowany dostęp do danych,
- nieautoryzowane modyfikacje lub zniszczenie danych,
- udostępnienie danych nieautoryzowanym podmiotom,
- nielegalne ujawnienie danych,
- pozyskiwanie danych z nielegalnych źródeł.

III.2 Postępowanie w przypadku naruszenia danych osobowych

§ 27

1. Każdy pracownik Szkoły, który stwierdzi fakt naruszenia bezpieczeństwa danych przez osobę przetwarzającą dane osobowe, bądź posiada informację mogącą mieć wpływ na bezpieczeństwo danych osobowych jest zobowiązany niezwłocznie zgłosić to ABI lub ADO.

2. Każdy pracownik Szkoły, który stwierdzi fakt naruszenia bezpieczeństwa danych ma obowiązek podjąć czynności niezbędne do powstrzymania skutków naruszenie ochrony oraz ustalić przyczynę i sprawcę naruszenia ochrony.

3. W przypadku stwierdzenia naruszenia bezpieczeństwa danych należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia oraz nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia ABI.

4. ABI podejmuje następujące kroki:

- zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając zagrożenie w prawidłowości pracy Szkoły,

- może zażądać dokładnej relacji z zaistniałego naruszenia bezpieczeństwa danych osobowych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje w związku z zaistniałym naruszeniem,
- rozważa celowość i potrzebę powiadamiania o zaistniałym naruszeniu ADO,
- nawiązuje kontakt ze specjalistami spoza urzędu (jeśli zachodzi taka potrzeba).

§ 28

1. ABI dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych osobowych sporządzając raport wg wzoru stanowiącego **załącznik nr 6** i przekazuje go ADO.

2. ABI zasięga potrzebnych mu opinii i proponuje działania naprawcze (w tym także ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych osobowych).

III.3 Sankcje karne

§ 29

1. Wobec osoby, która w przypadku naruszenia ochrony danych osobowych nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami wszczyna się postępowanie dyscyplinarne.

2. Kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia o naruszeniu danych osobowych nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą o ochronie danych osobowych.

Załączniki

Załącznik nr 1 – Upoważnienie do przetwarzania danych osobowych
Załącznik nr 2 – Odwołanie upoważnienia
Załącznik nr 3 – Rejestr osób upoważnionych do przetwarzania danych osobowych
Załącznik nr 4 – Oświadczenie pracownika o zapoznaniu się z zasadami zachowania bezpieczeństwa danych osobowych
Załącznik nr 5 – Informacja o zawartości zbioru danych
Załącznik nr 6 – Raportu z naruszenia bezpieczeństwa danych osobowych

ZAŁĄCZNIK NR 1
do „Polityki bezpieczeństwa
w Zespole Szkół Samorządowych w Objeździe”

Objazda, dnia ……..... r.

.....
(pieczęć Szkoły)

UPOWAŻNIENIE nr ……/20……..

do przetwarzania danych osobowych

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 10 poz. 926 z późn. zm.)
upoważniam Panią/Pana ..... zatrudnioną (ego) w Zespole Szkół Samorządowych w Objeździe na stanowisku ..... do przetwarzania danych osobowych zgromadzonych w formie tradycyjnej oraz w systemach informatycznych w zakresie wynikającym z zajmowanego stanowiska pracy, w okresie od dnia ..... 20…. r. do ……

Wyżej wymieniona osoba została wpisana do ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych w Szkole.

.....
(podpis Administratora Danych Osobowych)

Przyjmuję do wiadomości i stosowania.

…….....
(Podpis osoby upoważnionej)

ZAŁĄCZNIK NR 2
do „Polityki bezpieczeństwa
w Zespole Szkół Samorządowych w Objeździe”

Objazda, dnia ……..... r.

.....
(pieczęć Szkoły)

ODWOŁANIE UPOWAŻNIENIA nr ……

do przetwarzania danych osobowych

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 10 poz. 926 z późn. zm.)

odwołuję z dniem …….. upoważnienie do przetwarzania danych

osobowych wystawione dla Pani/Pana …….

Administrator Danych Osobowych

……..……
(pieczątka i podpis)

ZAŁĄCZNIK NR 3
do „Polityki bezpieczeństwa
w Zespole Szkół Samorządowych w Objeździe”

Objazda, dnia ……..... r.

.....
(pieczęć Szkoły)

REJESTR OSÓB UPOWAŻNIONYCH

do przetwarzania danych osobowych

Nr upoważnienia	Imię i nazwisko	Identyfikator użytkownika *	Zakres upoważnienia do przetwarzania danych osobowych	Data nadania uprawnień i podpis ABI	Data odebrania uprawnień i podpis ABI	Uwagi

* Wypełnia się tylko dla osób upoważnionych do przetwarzania danych osobowych, które zostały dopuszczone do przetwarzania danych osobowych w systemie

ZAŁĄCZNIK NR 4
do „Polityki bezpieczeństwa
w Zespole Szkół Samorządowych w Objeździe”

..... Objazda, dnia ……..... 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 Szkole zasadach dotyczących przetwarzania danych osobowych, określonych w „Polityce bezpieczeństwa informacji Zespołu Szkół Samorządowych w Objeździe” 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. 2002 r. Nr 101 poz. 926 z późn. zm.) 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, ze złamanie zasad ochrony danych osobowych, obowiązujących w Zespole Szkół Samorządowych w Objeździe może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną.

.....
(podpis pracownika)

ZAŁĄCZNIK NR 5
do „Polityki bezpieczeństwa
w Zespole Szkół Samorządowych w Objeździe”

Objazda, dnia ……..... r.

.....
(pieczęć Szkoły)

.....
(imię i nazwisko)

.....

.....
(adres)

INFORMACJA

o zawartości zbioru danych osobowych

W związku z Pani/Pana wnioskiem z dnia …… r. o udzielenie informacji związanych z przetwarzaniem danych osobowych w Zespole Szkół Samorządowych w Objeździe, działając na podstawie art. 33 ust. 1 Ustawy o ochronie danych osobowych informuję, że zbiór danych zawiera następujące Pani/Pana dane osobowe: ……..
…….....
.....

Powyższe dane przetwarzane są w Zespole Szkół Samorządowych w Objeździe w celu …… z zachowaniem wymaganych zabezpieczeń i zostały uzyskane ……..……..…. (podać sposób).

Powyższe dane nie były / były udostępniane …….. (podać komu) w celu …… (podać cel przekazania danych).

Zgodnie z rozdziałem 4 Ustawy o ochronie danych osobowych przysługuje Pani/Panu prawo do kontroli danych osobowych, prawo ich poprawiania, a także w przypadkach określonych w art. 32 ust. 1 pkt 7 i 8 Ustawy, prawo wniesienia umotywowanego żądania zaprzestania przetwarzania danych oraz prawo sprzeciwu wobec przetwarzania danych w celach marketingowych lub wobec przekazywania danych innemu administratorowi danych osobowych.

…….....
(podpis Administratora Bezpieczeństwa Informacji)

ZAŁĄCZNIK NR 6
do „Polityki bezpieczeństwa
Zespole Szkół Samorządowych w Objeździe”

Objazda, dnia ……..... r.

.....
(pieczęć Szkoły)

RAPORT Z NARUSZENIA BEZPIECZEŃSTWA

DANYCH OSOBOWYCH

w Zespole Szkół Samorządowych w Objeździe

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

2. Osoba powiadamiająca o zaistniałym zdarzeniu: .....

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

3. Lokalizacja zdarzenia:
.....
.....
(np. nr pokoju, nazwa pomieszczenia)

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

.....
.....
.....

5. Przyczyny wystąpienia zdarzenia:

.....
.....

6. Podjęte działania:

.....
.....

7. Postępowanie wyjaśniające:

.....
.....

.....
(podpis Administratora Bezpieczeństwa Informacji)