Załącznik Nr 1 do Zarządzenia Nr 26/2012
Dyrektora Szkoły Podstawowej w Mieczynie
z dnia 28. 12. 2012 r.

POLITYKA BEZPIECZEŃSTWA
I
INSTRUKCJA ZARZĄDZANIA SYSTEMEM PRZETWARZANIA DANYCH OSOBOWYCH W SPOSÓB TRADYCYJNY ORAZ PRZY UŻYCIU SYSTEMU INFORMATYCZNEGO W SZKOLE PODSTAWOWEJ W MIECZYNIE

Dotyczy wszystkich komputerów i systemów informatycznych przetwarzających dane osobowe oraz dokumentacji prowadzonej w sposób tradycyjny w szkole.

Podstawa prawna

- Konstytucja RP (art. 47 i 51)
- Konwencja nr 108 Rady Europy – dotycząca osób w związku z automatycznym przetwarzaniem danych osobowych
- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Dz.U. z 2002r. Nr 101, poz. 926 z późn. zm
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. (Dz. U. z 2004 r. Nr100, poz. 1024) w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych

Podstawowe pojęcia

§ 1

- **Szkoła** – w tym dokumencie jest rozumiana jako Szkoła Podstawowa im. Prymasa Tysiąclecia w Mieczynie, zlokalizowanej pod nr 8, 29-105 Krasocin.
- **Ustawa** — rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych z dnia 29 sierpnia 1997r. (tekst jedn. Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.)
- **Administrator Danych Osobowych** – rozumie się przez to Dyrektora Szkoły Podstawowej im. Prymasa Tysiąclecia w Mieczynie .
- **Lokalny Administrator Danych Osobowych** –wychowawcy świetlicy, wychowawcy klas, bibliotekarz, nauczyciele.
- **Administrator Bezpieczeństwa Informacji** – osoba powołana zarządzeniem dyrektora, która odpowiada za bezpieczeństwo danych osobowych w systemie informatycznym szkoły, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu, w których przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń.
- **Dane osobowe** - w rozumieniu ustawy za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
- **Przetwarzanie 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.
- **Zbiór danych** - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów.
- **System informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
- **Identyfikator użytkownika (login)** - ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
- **Hasło** - ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

- **Uwierzytelnianie** — rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.
- **Integralność danych** — rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
- **Poufności danych** — rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom.
- **Użytkownik systemu** – osoba upoważniona do przetwarzania danych osobowych w systemie. Użytkownikiem może być osoba zatrudniona w szkole, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, osoba odbywająca staż w szkole.
- **Sieć lokalna –** połączenie komputerów pracujących w szkole w celu wymiany danych (informacji) dla własnych potrzeb, przy wykorzystaniu urządzeń telekomunikacyjnych
- **Sieć publiczna –** sieć telekomunikacyjna, niebędąca siecią wewnętrzną służąca do świadczenia usług telekomunikacyjnych w rozumieniu ustawy z dnia 21 lipca 2000r. – Prawo telekomunikacyjne (Dz.U. Nr 73, poz.852, z późn.zm.)
- **Sieć telekomunikacyjna –** urządzenia telekomunikacyjne zestawione i połączone w sposób umożliwiający przekaz sygnałów pomiędzy określonymi zakończeniami sieci za pomocą przewodów, fal radiowych, bądź optycznych lub innych środków wykorzystujących energię elektromagnetyczną w rozumieniu ustawy z dnia 21 lipca 2000r. – Prawo telekomunikacyjne (Dz.U.Nr 73, poz.852 z późn.zm.)
- **Teletransmisja –** przesłanie informacji za pomocą sieci telekomunikacyjnej.
- **Aplikacja –** program komputerowy wykonujący konkretne zadanie.
- **Wysoki poziom bezpieczeństwa –** musi występować wtedy, gdy przynajmniej jedno urządzenie systemu informatycznego, służące przetwarzania danych osobowych, połączone jest z siecią publiczną.

1. POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

1.1. Wykaz budynków, w których przetwarzane są dane osobowe

§ 2

L.P.	BUDYNEK - ADRES	POMIESZCZENIA
1.	SZKOŁA Podstawowa im. Prymasa Tysiąclecia w Mieczynie Mieczyn 8 29-105 Krasocin	**Gabinet dyrektora/ Sekretariat** **Biblioteka** **Pokój nauczycielski** **Sale lekcyjne**

Kopie zapasowe zawierające zbiory danych osobowych przechowywane są w sejfie w gabinecie dyrektora/sekretariacie szkoły w budynku Mieczyn 8, 29-105 Krasocin.

1.2. Zbiory danych przetwarzanych w systemach informatycznych i opis struktury przetwarzanych danych osobowych

§ 3

ZBIÓR DANYCH OSOBOWYCH	PROGRAM INFORMATYCZNY SŁUŻĄCY DO PRZETWARZANIA ZBIORU DANYCH	STRUKTURA DANYCH
PRACOWNICY	• SIO • WORD • EXCEL	•PESEL •NIP •imię (imiona) i nazwisko •nazwisko rodowe •data i miejsce urodzenia •płeć •adres stały •numer telefonu •e-mail •**dowód osobisty (seria, numer, przez kogo wydany, data wydania)** •imię ojca •imię matki •stan cywilny i rodzinny •numer legitymacji służbowej •posiada gospodarstwo rolne •emeryt/rencista •obywatelstwo •dane osoby do kontaktu •wykształcenie •nazwa szkoły i rok ukończenia •staż pracy •historia pracy •warunki zatrudnienia •wysokość wynagrodzenia •ukończone kursy •kary i nagrody •nieobecność w pracy •informacja o karalności •informacje o stanie zdrowia

ZBIÓR DANYCH OSOBOWYCH	PROGRAM INFORMATYCZNY SŁUŻĄCY DO PRZETWARZANIA ZBIORU DANYCH	STRUKTURA DANYCH
UCZNIOWIE	•SIO •WORD •EXCEL •ŚWIADECTWA	•PESEL •imię (imiona) i nazwisko •data i miejsce urodzenia •adres stały •adres tymczasowy •imiona i nazwiska rodziców (prawnych opiekunów) •numer legitymacji szkolnej •informacje o wynikach w nauce •karty zdrowia dziecka

1.3. Zbiory danych przetwarzanych tradycyjnie.

§ 4 ZBIÓR DANYCH OSOBOWYCH	**DOKUMENTACJA SŁUŻĄCA DO PRZETWARZANIA ZBIORU DANYCH**	**STRUKTURA DANYCH**
PRACOWNICY	**AKTA OSOBOWE**	• PESEL • NIP • imię (imiona) i nazwisko •nazwisko rodowe • data i miejsce urodzenia •płeć • adres stały • numer telefonu • e-mail • dowód osobisty (seria, numer, przez kogo wydany, data wydania) • imię ojca • imię matki • stan cywilny i rodzinny • numer legitymacji służbowej •posiada gospodarstwo rolne • emeryt/rencista • obywatelstwo •dane osoby do kontaktu • wykształcenie • nazwa szkoły i rok ukończenia • staż pracy • historia pracy • warunki zatrudnienia • wysokość wynagrodzenia • ukończone kursy • kary i nagrody • nieobecność w pracy • informacja o karalności •informacje o stanie zdrowia
	ZAŚWIADCZENIA	•PESEL • NIP • Imiona/nazwisko • Nazwisko rodowe • Data i miejsce urodzenia • Adres stały •Miejsce pracy
	PROTOKOŁY POWYPADKOWE	•Imiona i nazwisko •Nazwisko rodowe •Data i miejsce urodzenia •Adres stały •Informacje o stanie zdrowia

	ARKUSZ ORGANIZACYJNY	• Imiona i nazwisko • Staż pracy • Historia pracy • Tytuł zawodowy • Ukończone szkoły, kursy • Uzyskane kwalifikacje • Zawód wyuczony i zawód wykonywany • Warunki zatrudnienia
	DOKUMENTACJA AWANSU ZAWODOWGO	• Imiona i nazwisko • Data i miejsce urodzenia • Adres zamieszkania • Wykształcenie • Historia pracy • Uzyskane kwalifikacje
UCZNIOWIE	**DOUMENTAJA UCZNIÓW**	• PESEL • imię (imiona) i nazwisko • data i miejsce urodzenia • adres stały • adres tymczasowy • imiona i nazwiska rodziców (prawnych opiekunów) • numer legitymacji szkolnej • informacje o wynikach w nauce • numer telefonu rodziców • e-mail • adresy zamieszkania rodziców
	KSIĘGA UCZNIÓW	• PESEL • imię (imiona) i nazwisko • data i miejsce urodzenia • adres stały • adres tymczasowy • imiona i nazwiska rodziców (prawnych opiekunów) • adresy rodziców (prawnych opiekunów
	ARKUSZE OCEN	• PESEL • imię (imiona) i nazwisko • data i miejsce urodzenia • adres zamieszkania • imiona i nazwiska rodziców (prawnych opiekunów)
	DZIENNIKI LEKCYJNE	• PESEL • imię (imiona) i nazwisko • data i miejsce urodzenia • adres zamieszkania • imiona i nazwiska rodziców (prawnych opiekunów) • adresy i numery telefonów rodziców (prawnych opiekunów) • nieobecności w szkole

		•informacje o wynikach w nauce
	KSIĘGA WYDANYCH LEGITYMACJI I LEGITYMACJE SZKOLNE	•imię (imiona) i nazwisko •data i miejsce urodzenia •adres zamieszkania •numer legitymacji
	REJESTR ZAŚWIADCZEŃ I ZAŚWIADCZENIA	•imię (imiona) i nazwisko •data i miejsce urodzenia •adres zamieszkania •klasa
	ŚWIADECTWA I DUPLIKATY	•PESEL •imię (imiona) i nazwisko •data i miejsce urodzenia
	KARTY BIBLIOTECZNE	•imię (imiona) i nazwisko •data i miejsce urodzenia •adres zamieszkania

I.4. System przetwarzania danych osobowych

§ 5

W skład systemu wchodzą:

- dokumentacja papierowa (korespondencja, dokumenty pracowników i uczniów);
- wydruki komputerowe;
- urządzenia i oprogramowanie komputerowe służące do przetwarzania informacji;
- procedury przetwarzania danych w tym systemie, w tym procedury awaryjne.

I.5 Środki techniczne i organizacyjne stosowane w przetwarzaniu danych

I.5.1 Cele i zasady funkcjonowania polityki bezpieczeństwa

§ 6

Realizując Politykę Bezpieczeństwa informacji zapewnia ich:

- Poufność – informacja nie jest udostępniania lub ujawniana nieupoważnionym osobom, podmiotom i procesom,
- Integralność – dane nie zostaną zmienione lub zniszczone w sposób nieautoryzowany,
- Dostępność – istnieje możliwość wykorzystania ich na żądanie, w założonym czasie, przez autoryzowany podmiot,
- Rozliczalność – możliwość jednoznacznego przypisania działań poszczególnym osobom,
- Autentyczność – zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana,
- Niezaprzeczalność – uczestnictwo w całości lub części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie jest niepodważalne,
- Niezawodność – zamierzone zachowania i skutki są spójne.

§ 7

Polityka Bezpieczeństwa informacji w Szkole Podstawowej w Mieczynie ma na celu zredukowanie możliwości wystąpienia negatywnych konsekwencji naruszeń w tym zakresie, tj.:

1. naruszeń danych osobowych rozumianych jako prywatne dobro powierzone Szkole;
2. naruszeń przepisów prawa oraz innych regulacji;
3. utraty lub obniżenia reputacji Szkoły;
4. strat finansowych ponoszonych w wyniku nałożonych kar;
5. zakłóceń organizacji pracy spowodowanych nieprawidłowym działaniem systemów.

§ 8

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:
- przetwarzane zgodnie z prawem,
- zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnego z tymi celami,
- merytorycznie poprawne i adekwatne w stosunku do celu, w jakim są przetwarzane,
- przechowywane w postaci umożliwiającej identyfikacje osób, których dotyczą, nie dłużej jednak niż jest to niezbędne do osiągnięcia celu przetwarzania.

I. 5. 2 Kompetencje i odpowiedzialność w zarządzaniu bezpieczeństwem danych osobowych

§ 9

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.

§ 10

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,
- odpowiada za zgodne z prawem przetwarzanie danych osobowych w Szkole.

§ 11

Administrator Bezpieczeństwa Informacji (ABI) – 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 konserwacja systemu, zapewnia bezpieczeństwo zewnętrznego i wewnętrznego obiegu informacji w sieci i zabezpieczenia łączy zewnętrznych,

- prowadzi nadzór nad archiwizacją zbiorów danych oraz zabezpiecza elektroniczne nośniki informacji zawierających dane osobowe.

§ 12

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

- 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 z zasadami określonymi w Polityce Bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym Szkoły i składa oświadczenie o znajomości tych przepisów

I. 5. 3 Zasady udzielania dostępu do danych osobowych

§ 13

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.

§ 14

Dostęp do danych osobowych może mieć wyłącznie osoba posiadająca pisemne oraz imienne upoważnienie wydane przez ADO.

I. 5. 4 Udostępnianie i powierzanie danych osobowych

§ 15

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

§ 16

Udostępnienie danych może nastąpić na pisemny wniosek zawierający następujące elementy:

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

§ 17

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

§ 18

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 podstawie prawnej powierzenia danych, celu i sposobie ich przetwarzania.

§ 19

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.

§ 20

Sprawy związane z udzielaniem informacji w tym zakresie prowadzi ADO, udzielając informacji o zawartości zbioru danych na piśmie.

I. 5. 5 Bezpieczeństwo w przetwarzaniu danych osobowych w formie tradycyjnej

§ 21

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

§ 22

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

§ 23

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

I. 5. 6 Bezpieczeństwo w przetwarzaniu danych osobowych w systemach informatycznych

§ 24

Zasady bezpiecznego użytkowania systemu informatycznego zawarte są w *Instrukcji Zarządzania Systemem Informatycznym*, obligatoryjnej dla zapoznania się i stosowania przez wszystkich użytkowników systemu informatycznego Szkoły.

I. 6 Analiza ryzyka związanego z przetwarzaniem danych osobowych
I. 6. 1 Identyfikacja zagrożeń

§ 25

FORMA PRZETWARZANIA DANYCH	ZAGROŻENIA
Dane przetwarzane w sposób tradycyjny	- oszustwo, kradzież, sabotaż; - zdarzenia losowe (powódź, pożar); - zaniedbania pracowników szkoły (niedyskrecja, udostępnianie danych osobie nieupoważnionej); - niekontrolowana obecność osób nieupoważnionych w obszarze przetwarzania danych; - pokonanie zabezpieczeń fizycznych; - podsłuchy, podglądy; - atak terrorystyczny; - brak rejestrowania udostępniania danych - niewłaściwe miejsce i sposób przechowywania dokumentacji
Dane przetwarzane w systemach informatycznych	- nie przydzielenie użytkownikom systemu identyfikatorów; - niewłaściwa administracja systemem; - niewłaściwa konfiguracja systemu; - zniszczenie (sfałszowanie) kont użytkowników; - kradzież danych kont; - pokonanie zabezpieczeń programowych; - zaniedbanie pracowników szkoły (niedyskrecja, udostępnianie danych osobom nieupoważnionym) - niekontrolowana obecność nieuprawnionych osób - zdarzenia losowe (powódź, pożar) - niekontrolowane wytwarzanie i wypływ danych poza obszar przetwarzania za pomocą nośników informacji i komputerów przenośnych; - naprawy i konserwacja systemu lub sieci teleinformatycznej wykonane przez osoby nieuprawnione; - przypadkowe lub celowe uszkodzenie systemów i aplikacji informatycznych lub sieci; - przypadkowe lub celowe wprowadzanie zmian do chronionych danych osobowych; - brak rejestrowania zdarzeń tworzenia lub modyfikowania danych;

I. 6. 2 Sposób zabezpieczenia danych

§ 26

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, które upoważnił ADO - 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; - stosowanie ochrony zasilania (ups); - systematyczne tworzenie kopii zapasowych zbiorów danych przetwarzanych w systemach informatycznych; - składowanie danych sensytywnych oraz nośników wymiennych i nośników kopii zapasowych w odpowiednio zabezpieczonych szafach; - przydzielenie pracownikom indywidualnych kont użytkowników i haseł dostępu; - stosowanie indywidualnych haseł logowania do poszczególnych programów; - właściwa budowa hasła;

I. 6. 3 Określenie wielkości ryzyka

§ 27

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.

I. 6. 4 Identyfikacja obszarów wymagających szczególnych zabezpieczeń

§ 28

Uwzględniając kategorie przetwarzanych danych oraz zagrożenia zidentyfikowane w wyniku przeprowadzonej analizy ryzyka dla systemów informatycznych stosuje się wysoki poziom bezpieczeństwa. ABI przeprowadza okresową analizę ryzyka dla poszczególnych systemów i na tej podstawie przedstawia ADO propozycje dotyczące zastosowania środków technicznych i organizacyjnych, celem zapewnienia właściwej ochrony przetwarzanym danym.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

II. 1 Nadawanie i rejestrowanie uprawnień do przetwarzania danych w systemie informatycznym

§ 29

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

§ 30

Za tworzenie, modyfikację i nadawanie uprawnień kontom użytkowników odpowiada ABI.

§ 31

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

§ 32

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

§ 33

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

II. 2 Zabezpieczenie danych w systemie informatycznym

§ 34

Ochronę przed awariami zasilania oraz zakłóceniami w energii elektrycznej stacji roboczych, na których przetwarzane są dane osobowe zapewniają zasilacze UPS.

§ 35

Oprogramowanie wykorzystywane do przetwarzania danych posiada własny system kont (zabezpieczonych hasłami) i uprawnień.

§ 36

Hasła do systemu stacji roboczych mają długość przynajmniej 8 znaków (duże i małe litery oraz znaki cyfry lub znaki specjalne) i okres ważności ustawiony na nie dłużej niż 1 miesiąc. Hasło nie może być zapisywane i przechowywane w miejscu dostępnym dla osób nieuprawnionych.

§ 37

W przypadku utraty hasła użytkownik ma obowiązek skontaktować się z ABI celem uzyskania nowego hasła.

§ 38

Hasła użytkowników uprzywilejowanych, posiadających uprawnienia na poziomie administratorów systemów informatycznych objęte są takimi samymi restrykcjami dotyczącymi ich poufności jak pozostałe hasła.

§ 39

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 właścicielami ani współwłaścicielami 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.

§ 40

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.

§ 41

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. Za dokonywanie skanowania systemu w poszukiwaniu złośliwego oprogramowania (w przypadku braku ochrony rezydentnej) i aktualizację bazy wirusów odpowiada użytkownik stacji roboczej.

II. 3 Zasady bezpieczeństwa podczas pracy w systemie informatycznym

§ 42

W celu rozpoczęcia pracy w systemie informatycznym użytkownik:

1) loguje się do systemu operacyjnego przy pomocy identyfikatora i hasła (aktualizacja użytkownika w bazie usług katalogowych),

2) loguje się do programów i systemów wymagających dodatkowego wprowadzania unikalnego identyfikatora i hasła.

§ 43

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

§ 44

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

§ 45

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

§ 46

Zawieszenie korzystania z systemu informatycznego może nastąpić losowo wskutek awarii lub planowo (np. w celu konserwacji sprzętu). Planowe zawieszenie prac jest poprzedzone poinformowaniem pracowników Szkoły przez ABI na co najmniej 30 minut przed planowanym zawieszeniem.

§ 47

Pracownik korzystający z systemu informatycznego zobowiązany jest do powiadomienia ABI 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.

Na fakt naruszenia zabezpieczeń systemów mogą wskazywać:

- nietypowy stan stacji roboczej (np. brak zasilania, problemy z uruchamianiem)
- 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.

II. 4 Tworzenie kopii zapasowych

§ 48

Dane systemów kopiowane są w trybie semestralnym (kopie baz danych). Kopie awaryjne danych zapisywanych w programach wykonane są semestralnie (15 stycznia, 30 czerwca).

§ 49

Odpowiedzialnym za wykonanie kopii danych i kopii awaryjnych jest pracownik obsługujący dany program przetwarzające dane.

§ 50

Dodatkowe kopie wynikające np. ze zmiany platformy sprzętowej i kopie awaryjne przechowywane są w sejfie w sekretariacie/gabinecie dyrektora. Osobą odpowiedzialną za wymianę kopii awaryjnych na aktualne jest ABI.

§ 51

Okresową weryfikację kopii bezpieczeństwa pod kątem ich przydatności do odtworzenia danych przeprowadza ABI.

§ 52

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

II. 5 Udostępnienie danych

§ 53

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

II. 6 Przeglądy i konserwacje systemów

§ 54

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

§ 55

Prace wymienione w § 54 powinny uwzględniać wymagany poziom zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych.

§ 56

Przed rozpoczęciem prac wymienionych w § 54 przez osoby nie będące pracownikami Szkoły należy dokonać potwierdzenia tożsamości tychże osób.

II. 7 Niszczenie wydruków i nośników danych

§ 57

Wszystkie 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.

§ 58

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

§ 59

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

INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA DANYCH

III. 1 Istota naruszenia danych osobowych

§ 60

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 przypadkach naruszenia danych osobowych

§ 61

Każdy pracownik Szkoły, który stwierdzi fakt naruszenia bezpieczeństwa danych przez osobę przetwarzająca dane osobowe, bądź posiada informacje mogąca mieć wpływ na bezpieczeństwo danych osobowych jest zobowiązany zgłosić to niezwłocznie do ABI lub ADO.

§ 62

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

§ 63

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

§ 64

ABI podejmuje następujące kroki:

- zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania dokładnej relacji z zaistniałego naruszenia 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 powiadomienia o zaistniałym naruszeniu ADO,
- nawiązuje kontakt ze specjalistami spoza Szkoły (jeśli zachodzi taka potrzeba)

§ 65

ABI dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych osobowych sporządzając raport i przekazuje go ADO.

§ 66

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

§ 67

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.

§ 68

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 – Rejestr osób upoważnionych do przetwarzania danych osobowych
Załącznik nr 3 – Oświadczenie pracownika o zapoznaniu się z zasadami zachowania bezpieczeństwa danych osobowych
Załącznik nr 4 – Informacja o zawartości zbioru danych
Załącznik nr 5 – Raport z naruszenia bezpieczeństwa danych osobowych

Załącznik nr 1
do Polityki Bezpieczeństwa Informacji
w Szkole Podstawowej w Mieczynie

Mieczyn, dnia ……. 20…r.

……
(pieczęć szkoły)

UPOWAŻNIENIE nr …../20….
do przetwarzania danych osobowych
w Szkole Podstawowej im. Prymasa Tysiąclecia w Mieczynie

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

……

Zatrudnioną/zatrudnionego w Szkole Podstawowej im. Prymasa Tysiąclecia w Mieczynie na stanowisku …… do przetwarzania danych osobowych zgromadzonych w formie tradycyjnej oraz w systemach informatycznych w okresie od dnia 2012r. na czas trwania umowy o pracę w zakresie określonym w obowiązkach służbowych.

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

……..
(podpis Administratora Danych Osobowych)

Załącznik nr 2
do Polityki Bezpieczeństwa Informacji
w Szkole Podstawowej w Mieczynie

REJESTR WYDANYCH UPOWAŻNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH

L.p.	**Imię i nazwisko**	**stanowisko**	**Data nadania**	**Data ustania**	**Identyfikator** (jeżeli dane są przetwarzane w systemie informatycznym)
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
11.					
12.					
13.					
14.					
15.					
16.					

Załącznik nr 3
do Polityki Bezpieczeństwa Informacji
w Szkole Podstawowej w Mieczynie

Mieczyn, dnia …… 20…….r.

…….
(imię i nazwisko)
……
(stanowisko)

OŚWIADCZENIE O ZACHOWANIU POUFNOŚCI I ZAPOZNANIU SIĘ Z PRZEPISAMI PBI OBOWIĄZUJĄCYMI
W SZKOLE PODSTAWOWEJ W MIECZYNIE

Ja niżej podpisany/a oświadczam, że 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 Szkoły Podstawowej im. Prymasa Tysiąclecia w Mieczynie* i zobowiązuję się ich przestrzegać.

Zostałem/am zapoznany/a z przepisami Ustawy o ochronie danych osobowych (Dz.U. 2002r. Nr 101 poz.926 z późn.zm.) oraz Rozporządzenia MSWiA w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004r. 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 Szkole Podstawowej w Mieczynie może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną.

…….
(podpis pracownika)

Załącznik nr 4
do Polityki Bezpieczeństwa Informacji
w Szkole Podstawowej w Mieczynie

Mieczyn, dn…..20…..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 Szkole Podstawowej w Mieczynie 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 Szkole Podstawowej w Mieczynie w Zespole Obsługi Placówek Oświatowych w Krasocinie dla celów: ……. 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 5
do Polityki Bezpieczeństwa Informacji
w Szkole Podstawowej w Mieczynie

Mieczyn, dn……20…..r.

……
/pieczęć szkoły/

RAPORT Z NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH w S Z K O L E P O D S T A W O W E J w M I E C Z Y N I E

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)