Zarządzenie Nr2/2016
z dnia 4.02.2016 r.
Dyrektora Medycznego Studium
Zawodowego im. Zofii Bagińskiej
w Parczewie

POLITYKA
BEZPIECZEŃSTWA INFORMACJI

w Medycznym Studium Zawodowym
im. Zofii Bagińskiej w Parczewie

I. POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

II. INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

III. INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA DANYCH

IV. KONTROLA W ZAKRESIE BEZPIECZEŃSTWA INFORMACJI

Podstawa prawna;

- Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r.

  (tekst jednolity: Dz. U. 2002 r. Nr 101 poz. 926 z późn.zm.)

- 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) – art. 39a ustawy .

- Rozporzadzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U . z 2012 r. poz. 526)

I. POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

§ 1

DEFINICJE

1) **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, jeżeli jej tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

2) **Zbiór danych** - 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).

3) **Przetwarzanie danych** - jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

4) **System informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

5) **Administrator Danych Osobowych** – organ, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania danych osobowych.

6) **Osoba upoważniona (użytkownik)** – osoba posiadająca upoważnienie wydane przez Administratora Danych Osobowych do przetwarzania danych osobowych.

7) **Zabezpieczenie danych w systemie informatycznym** - wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.

8) **Zgoda osoby, której dane dotyczą** – oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie. Zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.

9) **Hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

10) **Poufność danych** – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom.

11) **Sieć telekomunikacyjna** - urządzenia telekomunikacyjne i linie 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 (art.2 pkt 23 ustawy z dnia 21 lipca 2000r.- Prawo telekomuniacyjne, Dz.U.Nr 73,poz.852 z póż.zm).

12) **Teletransmisja** – przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej.

§2

WYKAZ BUDYNKÓW I POMIESZCZEŃ TWORZĄCYCH OBSZAR W KTÓRYM PRZETYWARZANE SĄ DANE OSOBOWE

1) Dane osobowe gromadzone i przetwarzane są w budynku Medycznego Studium Zawodowego im.Zofii Bagińskiej , mieszczącym się w Parczewie przy ul. Szpitalnej 1C.

2) Obszarami do przetwarzania danych osobowych z użyciem sprzętu komputerowego oraz sposobem tradycyjnym są:

- gabinet dyrektora ,
- sekretariat szkoły ,
- biuro księgowości
- pokój nauczycielski
- biblioteka szkolna
- archiwum szkoły
- sale lekcyjne
- pokój kierownika internatu

3)Dane osobowe w studium przetwarzane są;

- w formie papierowej (system tradycyjny)
- w formie elektronicznej (system informatyczny)

§3

ZBIORY DANYCH PRZETWARZANYCH W SYSTEMACH INFORMATYCZNYCH

ZBIÓR DANYCH OSOBOWYCH	PROGRAM DO PRZTWARZANIA DANYCH	STRUKTURA ZBIORÓW DANYCH
Pracownicy	Kadry Optivum	PESEL/ NIP/ imię(imiona) i nazwisko/ nazwisko rodowe/ data i miejsce urodzenia/ płeć/ adres/ numer telefonu/ e-mail/ dowód osobisty (seria i nr, wydany przez, data wydania)/ imiona rodziców/ stan cywilny i rodzinny/ emeryt/ rencista/ obywatelstwo/ dane osoby kontaktowej/ wykształcenie/ nazwa szkoły i rok ukończenia/ staż pracy/ historia zatrudnienia/ wysokość wynagrodzenia/ ukończone kursy/ kary i nagrody/ nieobecności w pracy/ informacja o karalności/ informacje o stanie zdrowia
	Płace Optivum	PESEL/ NIP/ imię(imiona) i nazwisko/ nazwisko rodowe/ data i miejsce urodzenia/ płeć/ adres/ numer telefonu/ e-mail/ dowód osobisty (seria i nr, wydany przez, data wydania)/ imiona rodziców/ emeryt/ rencista/ obywatelstwo/wykształcenie/ staż pracy/ wysokość wynagrodzenia/ warunki zatrudnienia/ tytuł zawodowy/ nieobecności w pracy/ numer konta bankowego
	Płatnik	PESEL/ NIP/ imiona/ nazwisko/ nazwisko rodowe/ adres/ data i miejsce urodzenia/ stan rodzinny /płeć/stopień niepełnosprawności
	SIO	PESEL/ płeć/ wykształcenie/ staż pracy/stopień awansu zawodowego/ warunki zatrudnienia/ tytuł zawodowy/ uzyskane kwalifikacje/ nieobecności w pracy
	HOME BANKING	Imię/nazwisko/adres/numer konta bankowego
	ERU-PZU	Imię/ nazwisko/ adres zamieszkania / pesel/ data urodzenia/ informacje o stanie zdrowia
Uczniowie	SMOK	Imiona/nazwisko/pesel/data urodzenia/adres zamieszkania / numer telefonu / e-mail/informacja o stanie zdrowia
	OBIEG OKE	Imiona/nazwisko/pesel/data urodzenia/adres zamieszkania / numer telefonu / e-mail/informacja o stanie zdrowia

§4

ZBIORY DANYCH PRZTWARZANYCH W SPOSÓB TRADYCYJNY.

ZBIÓR DANYCH OSOBOWYCH	DOKUMENTACJA DO PRZTWARZANIA DANYCH	STRUKTURA ZBIORÓW DANYCH
Pracownicy	Akta osobowe	PESEL/ NIP/ imię(imiona) i nazwisko/ nazwisko rodowe/ data i miejsce urodzenia/ płeć/ adres/ numer telefonu/ e-mail/ dowód osobisty (seria i nr, wydany przez, data wydania)/ imiona rodziców/ stan cywilny i rodzinny/ posiada gospodarstwo rolne/ emeryt/ rencista/ obywatelstwo/ dane osoby kontaktowej/ wykształcenie/ nazwa szkoły i rok ukończenia/ staż pracy/ historia zatrudnienia/ wysokość wynagrodzenia/ ukończone kursy/ kary i nagrody/ nieobecności w pracy/ informacja o karalności/ informacje o stanie zdrowia
	Informacje o zarobkach (PIT)	PESEL/ imię i nazwisko/ data urodzenia/ adres/ wysokość zarobków
	Listy płac	PESEL/ imię i nazwisko/ stanowisko/ wysokość wynagrodzenia
	Karty wynagrodzeń	imię i nazwisko/ pesel/stanowisko/ wysokość wynagrodzenia /adres zamieszkania
	Oświadczenia i wnioski do funduszu socjalnego	Imię i nazwisko/ adres/ wysokość dochodów/ stan rodzinny
	Zaświadczenia	PESEL/ NIP/ imię i nazwisko/ data urodzenia/ adres/ wysokość zarobków/ warunki pracy
	Dokumentacja ubezpieczeniowa	PESEL/ NIP/ imię i nazwisko/ nazwisko rodowe/ data i miejsce urodzenia/ adres/ wysokość zarobków/ stanowisko/ informacja o stanie zdrowia
	Protokoły powypadkowe	imię i nazwisko/ nazwisko rodowe/ data i miejsce urodzenia/ adres/ stanowisko/ informacja o stanie zdrowia
	Dokumentacja awansów zawodowych nauczycieli	Imię i nazwisko/ data i miejsce urodzenia/ adres/ wykształcenie/ historia pracy/ uzyskane kwalifikacje
	Arkusz organizacyjny	Imię i nazwisko/staż pracy

ZBIÓR DANYCH OSOBOWYCH	DOKUMENTACJA DO PRZTWARZANIA DANYCH	STRUKTURA ZBIORÓW DANYCH
Uczniowie	Dokumentacja uczniów	PESEL/ imiona i nazwisko/ data i miejsce urodzenia/ płeć/ adres/ nr telefonu/ e-mail/ imiona, nazwiska i adres rodziców (prawnych opiekunów)/ numer legitymacji szkolnej/ obywatelstwo/ osoba kontaktowa/ wykształcenie/ historia nauki/ wyznanie/ informacje o stanie zdrowia/ orzeczenia i opinie z poradni psychologiczno-pedagogicznej
	Księga uczniów	PESEL/ imiona i nazwisko/ data i miejsce urodzenia/ płeć/ adres/ imiona, nazwiska i adres rodziców (prawnych opiekunów)/
	Arkusze ocen	PESEL/ imiona i nazwisko/ data i miejsce urodzenia/ płeć/ adres/ imiona, nazwiska i adres rodziców (prawnych opiekunów)/ wyznanie/ informacja o wynikach nauczania
	Dzienniki lekcyjne, dzienniki praktyk	PESEL/ imiona i nazwisko/ data i miejsce urodzenia/ płeć/ adres/ imiona, nazwiska i adres rodziców (prawnych opiekunów)/ numery telefonów/ obywatelstwo/ informacja o wynikach nauczania/ nieobecności w szkole
	Księga wydanych legitymacji i	Imiona i nazwisko/ data i miejsce urodzenia/ adres/ klasa/ numer legitymacji
	Rejestr zaświadczeń i zaświadczenia	Imiona i nazwisko/ data i miejsce urodzenia/ adres/ klasa
	Księga absolwentów	Imiona i nazwisko/ numer w księdze uczniów/ numer świadectwa/ data ukończenia szkoły
	Świadectwa i duplikaty	PESEL/ imiona i nazwisko/ data i miejsce urodzenia/ informacje o wynikach w nauce
	Dokumentacja ubezpieczeniowa	PESEL/ imiona i nazwisko/ data i miejsce urodzenia/ adres/
	Protokoły powypadkowe	PESEL/ imiona i nazwisko/ data i miejsce urodzenia/ adres/informacje o stanie zdrowia
	Karty zdrowia ucznia	PESEL/ imiona i nazwisko/ data i miejsce urodzenia/ adres/imiona rodziców(prawnych opiekunów)/ informacje o stanie zdrowia
	Karty szczepień	PESEL/ imiona i nazwisko/ data i miejsce urodzenia/ adres/imiona rodziców(prawnych opiekunów)/ informacje o stanie zdrowia
	Karty biblioteczne	Imiona i nazwisko/ klasa
	Księga mieszkańców internatu	Pesel/imię i nazwisko/data i miejsce urodzenia/

§5

SPOSÓB PRZEPŁYWU DANYCH MIEDZY POSZCZEGÓLNYMI SYSTEMAMI

PŁACE OPTIVUM→ PŁATNIK

- Z programu Płace Vulcan Optivum do programu Płatnik przekazywane są dane dotyczące zarejestrowania i wyrejestrowania pracowników oraz składek na ubezpieczenie społeczne i zdrowotne-dane przekazywane manualnie

§6

ŚRODKI TECHNICZNE I ORGANIZACYJNE NIEZBĘDNE DO PRZTWARZANIA DANYCH OSOBOWYCH

I.

1) Realizując Politykę bezpieczeństwa danych osobowych zapewnia się ich;
   - poufność- dane nie są udostępniane osobom i podmiotom nieupoważnionym,
   - integralność – dane nie są zmieniane lub niszczone w sposób nieautoryzowany,
   - rozliczalność – przypisanie działań poszczególnym osobom ,
2) Polityka bezpieczeństwa informacji w Medycznym Studium Zawodowym ma na celu zredukowanie możliwości wystąpienia negatywnych konsekwencji naruszeń w tym zakresie, tj.:
   - naruszeń danych osobowych rozumianych jako prywatne dobro powierzone Szkole,
   - naruszeń przepisów prawa oraz innych regulacji,
   - utraty lub obniżenia reputacji Studium,
   - strat finansowych ponoszonych w wyniku nałożonych kar,
   - zakłóceń organizacji pracy spowodowanych nieprawidłowym działaniem systemów.

II.

1) Administratorem Danych Osobowych(ADO) w Medycznym Studium Zawodowym w Parczewie jest Dyrektor Szkoły.

- Administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, 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 celów, w jakich są przetwarzane,
  d) przechowywane w postaci umożliwiającej identyfikacje osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

- Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmiana, utrata, uszkodzeniem lub zniszczeniem.
- Administrator danych jest obowiązany zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.
- Administrator danych prowadzi ewidencję osób upoważnionych do ich przetwarzania, która powinna zawierać:
  a) imię i nazwisko osoby upoważnionej,
  b) datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych,
  c) identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.

  Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych stanowi **Załącznik nr 1.**

2) Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych osobowych . Wzór upoważnienia stanowi **Załącznik nr 2.**

3) Upoważnienia udzielane są w formie pisemnej na czas określony lub na czas nieokreślony - do odwołania udzielonego upoważnienia. **Załącznik nr 3.**

4) Osoby upoważnione(użytkownicy) :

- chronią prawo do prywatności osób fizycznych powierzających szkole swoje dane osobowe poprzez przetwarzanie ich zgodnie z przepisami prawa oraz zasadami określonymi w Polityce Bezpieczeństwa Danych Osobowych.

- zapoznają się zasadami określonymi w Polityce Bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym Studium i składają oświadczenie o znajomości tych przepisów. Wzór oświadczenia stanowi **Załącznik nr 4.**

III.

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 podstawie 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.

IV.

1) Pomieszczenia, w których znajdują się przetwarzane zbiory danych osobowych pozostają zawsze pod bezpośrednim nadzorem upoważnionego do ich przetwarzania pracownika.

2)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.

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

V.

Sposób zabezpieczenia danych

Forma przetwarzania danych	Zagrożenia	Środki ochrony
Dane przetwarzane w sposób tradycyjny	• oszustwo, kradzież, sabotaż; • zdarzenia losowe (powódź, pożar); • zaniedbania pracowników szkoły (niedyskrecja, udostępnienie danych osobie nieupoważnionej); • niekontrolowana obecność nieuprawnionych osób wobszarze przetwarzania; • pokonanie zabezpieczeń fizycznych; • podsłuchy, podglądy; • brak rejestrowania udostępniania danych; • niewłaściwe miejsce i sposób przechowywania dokumentacji.	•przechowywanie danych w pomieszczeniach zamykanych na klucz •przechowywanie danych osobowych w szafach zamykanych na klucz •przetwarzanie danych wyłącznie przez osoby posiadające upoważnienie nadane przez ADO •zapoznanie pracowników z zasadami przetwarzania danych osobowych oraz obsługą systemu służącego do ich przetwarzania
Dane przetwarzane w systemach informatycznych	• niewłaściwa administracja systemem; • niewłaściwa konfiguracja systemu; • 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 obszarprzetwarzaniaz pomocą nośników informacji i komputerów przenośnych; •naprawy i konserwacje systemu wykonywane przez osoby nieuprawnione; • przypadkowe bądź celowe uszkodzenie systemów i aplikacji informatycznych •przypadkowe bądź celowe modyfikowanie systemów i aplikacji informatycznych lub sieci; •przypadkowe bądź celowe wprowadzenie zmian do chronionych danych osobowych;	• kontrola dostępu do systemów •zastosowanie programów antywirusowych •systematyczne tworzenie kopii zapasowych zbiorów danych przetwarzanych w systemach informatycznych; •składowanie nośników wymiennych i nośników kopii zapasowych w odpowiednio zabezpieczonych szafach; •stosowanie indywidualnych haseł logowania do poszczególnych programów; •właściwa budowa hasła

II.INSTRUKCJA ZARZADZANIA SYSTEMEM INFORMATYCZNYM w Medycznym Studium Zawodowym im. Z. Bagińskiej w PARCZEWIE

Przetwarzanie danych osobowych odbywa się na trzech komputerach w sekretariacie szkoły , księgowości i pokoju nauczycielskim. W/w. komputery są jednostkami samodzielnymi, które nie są podłączone do serwera pracowni komputerowej szkoły.

§1

Nadawanie i rejestrowanie uprawnień do przetwarzania danych w systemie informatycznym.

1) Przetwarzać dane osobowe w systemie informatycznym może wyłącznie osoba upoważniona przez ADO do przetwarzania danych osobowych .

2) 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.

§2

Zabezpieczenie danych w systemie informatycznym.

1) Do systemu stacji roboczych stosuje się hasło składające się z co najmniej z 8 znaków, które zawiera wielkie i małe litery , cyfry i znaki specjalne. Hasło nie może być zapisywane lub przechowywane w miejscu dostępnym dla osób nieuprawnionych.

2) Programy do przetwarzania danych osobowych posiadają własny system kont ,zabezpieczony hasłem.

3) 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.

4) 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.

5) Ochronę przed awariami zasilania oraz zakłóceniami w sieci energetycznej serwera i stacji roboczych, na których przetwarzane są dane osobowe zapewnia zasilacz UPS.

§3

Procedury rozpoczęcia, zawieszenia i zakończenia pracy użytkownika .

1) W celu rozpoczęcia pracy w systemie informatycznym użytkownik:
   - loguje się do systemu operacyjnego przy pomocy hasła,
   - loguje się do programu i systemów wymagających dodatkowego wprowadzania unikalnego identyfikatora i hasła.

2) W sytuacji 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.

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 wygląd 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) Zawieszenie korzystania z systemu informatycznego może nastąpić losowo wskutek awarii lub planowo (np.; w celu konserwacji sprzętu) Planowane zawieszanie prac jest poprzedzone poinformowaniem pracowników studium.

6) Pracownik korzystający z systemu informatycznego zobowiązany jest do powiadomienia dyrektora szkoły w razie:
   - podejrzenia naruszenia bezpieczeństwa systemu;
   - stwierdzenia fizycznej ingerencji w przetwarzane dane;
   - stwierdzenia użytkowania narzędzia programowego lub sprzętowego.

7) 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.

§ 4

Procedura tworzenia kopii zapasowych.

1) Kopie zapasowe programu płacowo- kadrowego wykonywane są po każdorazowym sporządzeniu wypłaty.

2) Kopie zapasowe awaryjne danych zapisywanych w programach wykonywane są raz w miesiącu (w ostatni dzień roboczy miesiąca po zakończeniu pracy).

3) Odpowiedzialnym za wykonywanie kopii danych i kopii awaryjnych jest pracownik obsługujący dany program przetwarzający dane. Kopie zbiorów umieszczonych w komputerze wykonywane są automatyczne dedykowanym oprogramowaniem wytwarzanym we własnym zakresie.

4) Kopie zapasowe wykonywane sa na nośnikach danych typu płyta CD , Pendrive

5) Usuwanie kopii danych z programu następuje poprzez bezpieczne kasowanie.

§5

Miejsce przechowywania kopii zapasowych

1)Kopie zapasowe zapisane na nośnikach danych przechowywane są w zamkniętych szafach , w pomieszczeniach zamykanych na klucz .

2)Wszelkie wydruki z systemów informatycznych zawierające dane osobowe przechowywane są w miejscu uniemożliwiającym ich odczyt przez osoby nieuprawnione, w zamkniętych szafach lub pomieszczeniach

§6

Udostępnianie danych.

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

§7

Przeglądy i konserwacja systemów.

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.

§8

Niszczenie wydruków i nośników danych.

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.

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

III.INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA DANYCH

§1

Istota naruszenia danych osobowych.

1) Naruszeniem danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych osobowych, udostępniania 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 ujawnianie danych,
- pozyskiwanie danych z nielegalnych źródeł.

§2

Postępowanie w przypadku naruszenia danych osobowych.

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 do dyrektora.

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

3) Dyrektor dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych osobowych sporządzając raport. Wzór raportu z naruszenia bezpieczeństwa danych osobowych stanowi **Załącznik nr 5.**

§3

Sankcje karne.

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 dyscyplinarna.

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

V. KONTROLA W ZAKRESIE BEZPIECZEŃSTWA INFORMACJI

§1

Obowiązki dyrektora

1) Dyrektor szkoły prowadzi nie rzadziej niż raz na rok okresową kontrolę w zakresie bezpieczeństwa informacji i sporządza stosowną ankietę. Wzór ankiety z przeprowadzonej kontroli bezpieczeństwa informacji stanowi **Załącznik Nr 6**

……

ZATWIERDZAM

Załącznik nr 1

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

L.p.	Imię i nazwisko*	Identyfikator użytkownika	Data nadania uprawnień	Data ustania uprawnień	Zakres upoważnienia do przetwarzania danych osobowych	Stanowisko	Nr upoważnienia

*uzupełnić jeżeli dane przetwarzane są w systemie informatycznym

Załącznik nr 2

.....
(pieczęć szkoły)

Parczew dn,.....

Upoważnienie nr ...../20.....r.
do przetwarzania danych osobowych

Na podstawie art.37 ustawy z dnia 29 sierpnia 1997 o ochronie danych osobowych
(Dz.U. z 2002 r. Nr10 poz. 926 z póż.zm)
upoważniam Panią/ Pana.....

.....
(stanowisko pracy)

zatrudnioną(ego) w Medycznym Studium Zawodowym im. Zofii Bagińskiej w Parczewie do przetwarzania danych osobowych , zgromadzonych w formie tradycyjnej / w systemach informatycznych* obejmujących następujący zakres.....
.....

Upoważnienie jest ważne od dnia ..... do dnia ustania zatrudnienia w Medycznym Studium Zawodowym , lub do odwołania upoważnienia.

.....
(podpis Administratora Danych Osobowych)

**niepotrzebne skreślić*

Załącznik nr 3

.....
(pieczęć szkoły)

Parczew dn,.....

ODWOŁANIE UPOWAŻNIENIA
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.)
odwołuję z dniem …….. upoważnienie do przetwarzania danych osobowych wystawione dla Pani/Pana ……

Administrator Danych Osobowych

……..……
(pieczątka i podpis)

Załącznik nr 4

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 zapoznałam/em się z obowiązującymi w Medycznym Studium Zawodowym im. Zofii Bagińskiej w Parczewie zasadami dotyczącymi przetwarzania danych osobowych, określonych w „Polityce bezpieczeństwa informacji „ i zobowiązuję się ich przestrzegania. W szczególności oświadczam, że bez upoważnienia nie będę wykorzystywał/a danych osobowych ze zbiorów znajdujących się w Szkole.

Oświadczam że zapoznałam/em się z przepisami Ustawy o ochronie danych osobowych (Dz. U. 2002 r. Nr 101 poz. 926 z późn. zm.) oraz Rozporządzeniem 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).

Zostałem poinformowany o odpowiedzialności karnej, stosownie do przepisów rozdziału 8 Ustawy o ochronie danych osobowych . Niezależnie od odpowiedzialności przewidzianej w wymienionych przepisach, mam świadomość, ze złamanie zasad ochrony danych osobowych, obowiązujących w Medycznym Studium Zawodowym w Parczewie może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną.

.....

(podpis pracownika)

Załącznik nr 5

R A P O R T Z N A R U S Z E N I A
B E Z P I E C Z E Ń S T W A D A N Y C H
O S O B O W Y C H
w Medycznym Studium Zawodowym w Parczewie

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

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

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

3.Lokalizacja zdarzenia:

.....
(nr pokoju, nazwa pomieszczenia)

4.Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

.....

.....

5.Podjęte działania:

.....

.....

6.Przyczyny wystąpienia zdarzenia:

.....

.....

7.Postępowanie wyjaśniające:

.....

.....

.....

(*data, podpis Administratora Bezpieczeństwa Danych*)