SZKOŁA PODSTAWOWA
im. Ziemi Lubelskiej
w Radawcu Dużym, gm. Konopnica
21-030 Motycz, woj. lubelskie
tel./fax 81 50-30-022
NIP: 713-24-92-400, Regon: 001180501

ZARZĄDZENIE Nr 13/03/2018

Dyrektora Szkoły Podstawowej im. Ziemi Lubelskiej w Radawcu Dużym

z dnia 10.03. 2018 r.

w sprawie wprowadzenia Procedury - Zarządzanie systemem informatycznym służącym do przetwarzania danych osobowych

Na podstawie art. 68 ust. 1 pkt 1 i ust. 5 ustawy z dnia 14 grudnia 2016 r. Prawo oświatowe (tekst jedn. Dz.U. z 2018 r. poz. 996 z późn. zm.) oraz art. 24 ust. 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.U.UE.L. z 2016 r. nr 119, s. 1) zarządzam, co następuje:

§ 1.

Wprowadzam do stosowania w Szkole Podstawowej im. Ziemi Lubelskiej w Radawcu Dużym . Procedurę - Zarządzanie systemem informatycznym służącym do przetwarzania danych osobowych stanowiącą załącznik do niniejszego Zarządzenia.

§ 2.

Wykonanie Zarządzenia powierzam pracownikom Szkoły Podstawowej im. Ziemi Lubelskiej w Radawcu Dużym : nauczycielom i pracownikom niebędącym nauczycielami.

§ 3.

Zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR SZKOŁY
mgr Hanna Szymańska

SZKOŁA PODSTAWOWA
im. Ziemi Lubelskiej
w Radawcu Dużym, gm. Konopnica
21-030 Motycz, woj. lubelskie
tel./fax 81 50-30-022
NIP: 713-24-92-400, Regon: 001180501

Załącznik
do Zarządzenia Nr 13/01/2018
Dyrektora Szkoły Podstawowej
im. Ziemi Lubelskiej w Radawcu Dużym
z dnia 10.03.2018 r.

PROCEDURA – ZARZĄDZANIE SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

ZATWIERDZAM
DYREKTOR SZKOŁY
H. Szymańska
.....mgr Hanna Szymańska
(data i podpis Administratora)

SZKOŁA PODSTAWOWA
im. Ziemi Lubelskiej
w Radawcu Dużym, gm. Konopnica
21-030 Motycz, woj. lubelskie
tel./fax 81 50-30-022
NIP: 713-24-92-400, Regon: 001180501

PROCEDURA - ZARZĄDZANIE SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

§ 1

1. Zgodnie z art. 24 ust. 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.U.UE.L. z 2016 r. nr 119, s. 1) ustanawia się Procedurę - zarządzanie systemem informatycznym służącym do przetwarzania danych osobowych (dalej także: PZSI) obowiązującą w Szkole Podstawowej im. Ziemi Lubelskiej w Radawcu Dużym.
2. Procedura - zarządzanie systemem informatycznym służącym do przetwarzania danych osobowych określa sposób zarządzania systemami informatycznymi, wykorzystywanymi do przetwarzania danych osobowych w Szkole Podstawowej im. Ziemi Lubelskiej w Radawcu Dużym., w celu zabezpieczenia danych osobowych przed zagrożeniami, w tym przed ich udostępnieniem osobom nieupoważnionym, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.
3. Procedura - zarządzanie systemem informatycznym służącym do przetwarzania danych osobowych obejmuje swoim zakresem wszystkie osoby i wszystkie systemy biorące udział w procesie przetwarzania danych osobowych.
4. Szczegółowe instrukcje dotyczące systemów informatycznych wykorzystywanych u Administratora do przetwarzania danych osobowych są opracowane przez administratorów i właścicieli tych systemów i aplikacji i mogą stanowić załączniki do niniejszej PZSI.
5. Nieprzestrzeganie postanowień zawartych w niniejszej PZSI może skutkować dla pracowników sankcjami w pełnym zakresie dopuszczonym przez stosunek pracy oraz obowiązujące przepisy prawa.
6. Wykaz systemów i kluczowych aplikacji wykorzystywanych w Szkole Podstawowej im. Ziemi Lubelskiej w Radawcu Dużym.stanowi załącznik nr 1 do niniejszej PZSI.

§ 2

Ilekroć w niniejszej PZSI jest mowa o:

a) ADO, Administratorze należy przez to rozumieć Szkole Podstawowej im. Ziemi Lubelskiej w Radawcu Dużym, z siedzibą w Radawcu Dużym , reprezentowaną przez Dyrektora Szkoły,

b) Administratorze aplikacji należy przez to rozumieć właściciela, dostawcę lub autora systemu lub aplikacji służącej do przetwarzania danych osobowych,

c) ASI, Administratorze Systemów Informatycznych należy przez to rozumieć pracownika (lub podmiot zewnętrzny) odpowiedzialnego za nadzór nad systemami informatycznymi wykorzystywanymi u Administratora,

d) czynności przetwarzania, czynności przetwarzania danych osobowych należy przez to rozumieć zespół powiązanych ze sobą operacji na danych osobowych, wykonywanych przez jedną lub kilka osób, które można określić w sposób zbiorczy, w związku z celem, w jakim te czynności są podejmowane,

e) danych osobowych należy przez to rozumieć informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej. Dane osobowe dzieli się na dane zwykłe i szczególne kategorie danych osobowych („dane wrażliwe"). Jako przykład danych zwykłych można wskazać: numery identyfikacyjne: imię, nazwisko, adres zamieszkania, PESEL, NIP, nr i serię paszportu, nr i serię dowodu osobistego; cechy fizyczne: wygląd zewnętrzny, siatkówka oka, linie papilarne; cechy fizjologiczne: grupa krwi; cechy ekonomiczne: status majątkowy, lista zaległości finansowych; środki komunikacji elektronicznej: numer telefonu, adres e-mail. Do szczególnych kategorii danych osobowych zalicza się dane: ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne, dane dotyczące zdrowia, seksualności lub orientacji seksualnej osoby,

f) dostępności należy przez to rozumieć właściwość określająca, że zasób systemu informatycznego jest możliwy do wykorzystania na żądanie, w założonym czasie, przez podmiot uprawniony do pracy w systemie informatycznym,

g) Dyrektorze należy przez to rozumieć Dyrektora Szkole Podstawowej im. Ziemi Lubelskiej w Radawcu Dużym,

h) identyfikatorze należy przez to rozumieć ciąg znaków literowych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,

i) incydencie ochrony danych osobowych należy przez to rozumieć zdarzenie albo serię niepożądanych lub niespodziewanych zdarzeń ochrony danych osobowych stwarzających znaczne prawdopodobieństwo zakłócenia działań Szkoły i zagrożenia ochrony danych osobowych,

j) integralności danych należy przez to rozumieć właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,

k) integralność systemu należy przez to rozumieć nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej,

l) IOD należy przez to rozumieć Inspektora Ochrony Danych Osobowych,

m) haśle należy przez to rozumieć ciąg znaków alfanumerycznych, znany jedynie użytkownikowi,

n) naruszeniu ochrony danych osobowych należy przez to rozumieć naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych,

o) obszarze przetwarzania danych należy przez to rozumieć pomieszczenia określone przez Administratora, tworzące obszar, w którym przetwarzane są dane osobowe i inne informacje prawem chronione; obszar przetwarzania danych określony jest w rejestrze czynności przetwarzania danych („Lokalizacja miejsca przetwarzania"),

p) odbiorcy danych należy przez to rozumieć osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Strona trzecia to osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż osoba, której dane dotyczą, Administrator, podmiot przetwarzający czy osoby, które – z upoważnienia Administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii Europejskiej lub prawem państwa członkowskiego, nie są uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych osobowych mającymi zastosowanie stosownie do celów przetwarzania.

q) osobie upoważnionej do przetwarzania danych osobowych należy przez to rozumieć osobę, która złożyła Administratorowi oświadczenie o zachowaniu w tajemnicy przetwarzanych danych i stosowanych sposobach zabezpieczenia tych danych, posiadającą imienne upoważnienie do przetwarzania danych osobowych wydane przez Administratora,

r) podmiocie przetwarzającym (procesorze) należy przez to rozumieć osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora,

s) przetwarzaniu danych osobowych należy przez to rozumieć operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie,

t) poufności danych należy przez to rozumieć właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom,

u) rozliczalności należy przez to rozumieć właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,

v) RODO należy przez to rozumieć Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L. z 2016 r. poz. 119, s. 1),

w) serwisancie należy przez to rozumieć firmę lub pracownika firmy zajmującej się sprzedażą, instalacją, naprawą i konserwacją sprzętu informatycznego,

x) systemie, systemie informatycznym należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w Szkole w celu przetwarzania danych,

y) Szkole należy przez to rozumieć Szkole Podstawowej im. Ziemi Lubelskiej w Radawcu Dużym.

z) usuwaniu danych należy przez to rozumieć trwałe zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,

aa) ustawie, ustawie o ochronie danych osobowych należy przez to rozumieć ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000),

bb) uwierzytelnieniu należy przez to rozumieć działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu,

cc) użytkowniku należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych, której nadano identyfikator i przyznano hasło, w celu umożliwienia dostępu do systemu informatycznego,

dd) zbiorze danych należy przez to rozumieć uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

§ 3

1. Niniejsza PZSI została opracowana na podstawie aktualnie obowiązujących przepisów prawa z zakresu ochrony danych osobowych, w oparciu o dobre praktyki i normy dotyczące ochrony danych osobowych, uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania danych oraz ryzyko naruszenia praw lub wolności osób fizycznych wynikające z przetwarzania danych osobowych.
2. Za priorytet uznano zagwarantowanie zgromadzonym danym osobowym, przez cały okres ich przetwarzania w systemach informatycznych, charakteru poufnego wraz z zachowaniem ich integralności i rozliczalności.

§ 4

1. W celu zapewnienia właściwego nadzoru nad systemami informatycznymi wykorzystywanymi przez Administratora wyznacza on Administratora Systemu Informatycznego (ASI) oraz określa zakres jego zadań i czynności w zakresie ochrony danych osobowych.
2. Administrator Systemu Informatycznego powinien posiadać stosowne uprawnienia w nadzorowanych systemach informatycznych, gwarantujące skuteczne wykonywanie zadań z zakresu nadzoru wszędzie tam, gdzie jest to możliwe. Nie oznacza to jednak automatycznego prawa dostępu do danych osobowych przetwarzanych w tych systemach.
3. Do obowiązków ASI w zakresie ochrony danych osobowych przetwarzanych w systemach informatycznych należy w szczególności:
   a) operacyjne zarządzanie systemami informatycznymi w sposób zapewniający ochronę

danych osobowych w nich przetwarzanych,

b) przestrzeganie opracowanych dla systemów informatycznych procedur operacyjnych i bezpieczeństwa,

c) zarządzanie stosowanymi w systemach informatycznym środkami uwierzytelnienia, w tym rejestrowanie i wyrejestrowywanie użytkowników oraz dokonywanie zmiany uprawnień,

d) utrzymanie systemów informatycznych w należytej sprawności technicznej,

e) regularne tworzenie kopii zapasowych zasobów danych osobowych oraz programów służących do ich przetwarzania oraz okresowe sprawdzanie poprawności wykonania kopii zapasowych,

f) wykonywanie lub nadzór nad wykonywaniem okresowych przeglądów i konserwacji, zgodnie z odrębnymi procedurami, sprzętu informatycznego, systemów informatycznych, aplikacji oraz elektronicznych nośników informacji, na których zapisane są dane osobowe,

g) zapewnienie niezbędnego przeszkolenia użytkowników systemów informatycznych.

§ 5

1. Do obowiązków użytkowników systemu informatycznego w zakresie ochrony danych osobowych w systemach informatycznych należy w szczególności:

a) przestrzeganie obowiązujących dla systemu zasad przetwarzania danych osobowych,

b) przestrzeganie obowiązujących dla systemu procedur operacyjnych i bezpieczeństwa,

c) udostępnianie danych osobowych wyłącznie osobom upoważnionym lub uprawnionym do ich uzyskania,

d) uniemożliwienie dostępu do danych osobowych w systemie lub ich podglądu przez osoby nieupoważnione,

e) informowanie ADO i IOD o wszelkich naruszeniach, podejrzeniach naruszenia i nieprawidłowościach w sposobie przetwarzania i ochrony danych osobowych z uwzględnieniem Procedury - postępowanie w przypadku naruszenia danych osobowych i dokumentowanie naruszeń ochrony danych osobowych,

f) wykonywanie bez zbędnej zwłoki poleceń IOD w zakresie ochrony danych osobowych, jeśli są one zgodne z przepisami powszechnie obowiązującego prawa,

g) podejmowanie współpracy przy ustaleniu przyczyn naruszenia ochrony danych osobowych oraz usuwania skutków tych naruszeń, w tym zapobieganie ich

ewentualnemu ponownemu wystąpieniu,

h) przetwarzanie danych osobowych wyłącznie w celach określonych przez swoich przełożonych i wynikających z zakresu obowiązków.

2. Użytkownicy przed przystąpieniem do przetwarzania danych osobowych w systemie informatycznym, zobowiązani są zapoznać się z Polityką Bezpieczeństwa Informacji Szkoły Podstawowej im. Ziemi Lubelskiej w Radawcu Dużym oraz niniejszą PZSI.
3. Użytkownicy podlegają szkoleniom w zakresie zasad bezpieczeństwa i środków podjętych dla ochrony danych przetwarzanych w systemach informatycznych oraz stosownie do potrzeb wynikających ze zmian w systemach informatycznych (wymiana sprzętu na nowszej generacji, zmiana oprogramowania) - prowadzonym przez ASI oraz w związku ze zmianą przepisów o ochronie danych osobowych w tym zmianą wewnętrznych regulacji w zakresie ochrony danych osobowych - prowadzonym przez IOD.

§ 6

1. Uwzględniając kategorie danych osobowych oraz konieczność zachowania bezpieczeństwa ich przetwarzania w systemie informatycznym połączonym z siecią publiczną, wprowadza się wysoki poziom bezpieczeństwa.
2. Środki bezpieczeństwa na poziomie wysokim:
   a) pomieszczenia tworzące obszar przetwarzania danych osobowych zabezpiecza się przed dostępem osób nieupoważnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych,
   b) przebywanie osób nieupoważnionych w obszarze przetwarzania danych jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych osobowych,
   c) w systemie informatycznym służącym do przetwarzania danych osobowych stosuje się mechanizmy kontroli dostępu do tych danych,
   d) jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas zapewnia się, aby w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator, a dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia,
   e) system informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego oraz utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej,

f) identyfikator użytkownikowi nadaje ASI lub Administrator aplikacji,

g) identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie,

h) jeśli do uwierzytelniania użytkowników używa się hasła, jest ono tworzone zgodnie z zasadami określonymi w § 8 PZSI,

i) dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych,

j) kopie zapasowe przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem,

k) kopie zapasowe usuwa się niezwłocznie po ustaniu ich użyteczności,

l) osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych, w tym stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych,

m) urządzenia, dyski lub inne elektroniczne nośniki zawierające dane osobowe, przeznaczone do:

   1) likwidacji - pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,

   2) przekazania podmiotowi nieuprawnionemu do przetwarzania danych — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie,

   3) naprawy - pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem Administratora lub osoby upoważnionej przez Administratora,

n) urządzenia dyski lub inne elektroniczne nośniki zawierające dane osobowe przekazywane poza obszar przetwarzania danych, zabezpiecza się w sposób zapewniający poufność i integralność tych danych,

o) system informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem,

p) w przypadku zastosowania logicznych zabezpieczeń obejmują one:

   1) kontrolę przepływu informacji pomiędzy systemem informatycznym Administratora a siecią publiczną,

   2) kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego

Administratora,

q) wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej stosuje się środki kryptograficznej ochrony.

3. ASI monitoruje wdrożone zabezpieczenia systemu informatycznego.

§ 7

1. Przetwarzanie danych w systemie informatycznym może być prowadzone wyłącznie w pomieszczeniach odpowiednio zabezpieczonych przed nieuprawnionym dostępem, uszkodzeniem bądź zniszczeniem sprzętu i danych.
2. Zabezpieczenia w pomieszczeniach pracowniczych muszą spełniać następujące minimalne wymagania:
   a) drzwi do pomieszczenia zwykłe – nie przeciwpożarowe, nie antywłamaniowe,
   b) zamki w drzwiach do pomieszczenia zwykłe – nie antywłamaniowe,
   c) pomieszczenia zabezpieczone są przed skutkami pożaru za pomocą wolnostojącej gaśnicy zgodnie z obowiązującymi przepisami p.poż.,
   d) szafki przeznaczone na nośniki z danymi niemetalowe, zamykane na zamki zwykłe.
3. Szafki przeznaczone na nośniki z danymi osobowymi o solidnej konstrukcji zamykane na klucz lub szafy metalowe bądź sejfy, w przypadku, gdy wskazuje na to wynik szacowania ryzyka.

§ 8

1. Hasła użytkowników do systemu tworzone są z uwzględnieniem poniższych zasad:
   a) hasło składa się z minimum 8 znaków,
   b) hasło musi spełniać warunek złożoności polegający na występowaniu w nim: wielkiej i małej litery, oraz cyfry lub znaku specjalnego (np. !@#),
   c) hasło musi być zmieniane co najmniej raz na 30 dni,
   d) kolejne hasła muszą być różne,
   e) hasła należy przechowywać w sposób gwarantujący ich poufność.
2. Zabrania się udostępniania haseł innym osobom.
3. Zabrania się tworzenia haseł na podstawie:
   a) cech i numerów osobistych (np. dat urodzenia, imion itp.),
   b) sekwencji klawiszy klawiatury (np. qwerty, 12qwaszx),
   c) identyfikatora użytkownika.
4. Zabrania się tworzenia haseł łatwych do odgadnięcia.
5. Logowanie anonimowe do systemu informatycznego jest zabronione dla użytkowników.

6. Uwierzytelnienie następuje wyłącznie po podaniu zgodnego hasła i powiązanego z nim identyfikatora.
7. W przypadku logowania do systemu informatycznego odbywającego się po raz pierwszy, użytkownik ma obowiązek zmiany hasła tymczasowego na właściwe, znane tylko użytkownikowi.
8. W przypadku systemów, które nie wymuszają automatycznie cyklicznej zmiany hasła oraz nie kontrolują jego znaków obowiązkiem użytkownika jest samodzielna cykliczna zmiana hasła zgodnie z wyżej określonymi zasadami.
9. Użytkownik ponosi pełną odpowiedzialność za utworzenie hasła i jego bezpieczne przechowywanie.
10. Hasła nie mogą być ujawniane w sposób celowy lub przypadkowy i powinny być znane wyłącznie użytkownikowi.
11. Hasła nie mogą być przechowywane w formie dostępnej dla osób nieupoważnionych:
    a) w plikach,
    b) na kartkach papieru w miejscach dostępnych dla osób trzecich,
    c) w skryptach,
    d) w innych zapisach elektronicznych i papierowych, które byłyby dostępne dla osób trzecich.
12. W przypadku podejrzenia ujawnienia haseł osobie nieupoważnionej, użytkownik niezwłocznie zmienia hasło lub zgłasza wniosek o zmianę hasła do ASI.
13. Użytkownik utrzymuje hasło w tajemnicy również po upływie jego ważności.
14. Zabrania się przekazywania hasła za pomocą telefonu, przesyłania z pomocą faksu i poczty e-mail w formie jawnej (niezaszyfrowanej).
15. Zabrania się udostępniania innym osobom indywidualnych identyfikatorów, w tym w szczególności nazwy użytkownika i innych danych umożliwiających uwierzytelnienie, w tym haseł.
16. Hasła użytkowników uprzywilejowanych (tzn. użytkowników posiadających uprawnienia na poziomie ASI) są zabezpieczone u Administratora na wypadek sytuacji awaryjnych, szczególnie w przypadku nieobecności ASI.

§ 9

Przy eksploatacji systemów informatycznych przetwarzających dane osobowe należy przestrzegać następujących zasad:

1. zabrania się użytkownikom, bez zgody ASI, wprowadzania zmian do oprogramowania lub sprzętu informatycznego poprzez jego samodzielne konfigurowanie lub wyposażanie,
2. zabrania się użytkownikom umożliwiania osobom trzecim uzyskiwania nieupoważnionego dostępu do systemów informatycznych,
3. zabrania się użytkownikom korzystanie z systemów informatycznych w sposób zagrażający integralności systemów i integralności danych,
4. zabrania się użytkownikom podejmowania prób testowania, modyfikacji i naruszenia zabezpieczeń systemów informatycznych lub jakichkolwiek działań noszących takie znamiona,
5. zabrania się użytkownikom, bez zgody ASI lub IOD, przenoszenia aplikacji oraz zasobów zlokalizowanych na zasobach sieciowych na dyski lokalne oraz przenośne nośniki danych,
6. zabrania się użytkownikom, bez zgody ASI lub IOD, podłączanie prywatnego lub osoby trzeciej urządzenia informatycznego do systemu informatycznego.

§ 10

Praca na poszczególnych stacjach roboczych powinna odbywać się z uwzględnieniem następujących zasad:

1. rozpoczęcie pracy na stacji roboczej następuje po włączeniu komputera, a następnie wprowadzeniu indywidualnego, znanego tylko użytkownikowi identyfikatora i hasła,
2. każda stacja robocza musi posiadać zaktualizowany system operacyjny,
3. każda stacja robocza musi posiadać zaktualizowany program antywirusowy,
4. każda stacja robocza musi posiadać włączoną zaporę ogniową (Firewall),
5. należy chronić ekrany komputerów (ustawienie monitora powinno uniemożliwiać podgląd), wydruki leżące na biurkach oraz w otwartych szafach przed osobami trzecimi,
6. monitory komputerów powinny być wyposażone w wygaszacze ekranu,
7. powinna być zastosowana blokada komputerów - wznowienie wyświetlenia powinno następować po wprowadzeniu hasła,
8. w przypadku opuszczenia stanowiska pracy, użytkownik ma obowiązek wylogowania się z systemu lub w inny sposób zablokowania stacji roboczej, stanowisko pracy nie może pozostać z uruchomionym i dostępnym systemem bez nadzoru pracującego na nim użytkownika,
9. zabrania się uruchamiania i instalowania na stacjach roboczych jakiegokolwiek oprogramowania, w tym aplikacji przenośnych niewymagających instalacji (ang. portable),
10. instalacji wszelkiego oprogramowania dokonuje wyłącznie ASI,

11. zabrania się przechowywania na stacjach roboczych gier oraz plików multimedialnych, np. filmów, zdjęć, obrazów, dźwięków niezwiązanych z zadaniami służbowymi,
12. przed użyciem zewnętrznego nośnika danych na stacji roboczej użytkownik musi każdorazowo wykonać skanowanie programem antywirusowym wszystkich danych na nośniku,
13. zabrania się wykonywania kopii całych zbiorów danych; całe zbiory danych mogą być kopiowane tylko przez ASI lub automatycznie przez system, z zachowaniem procedur ochrony danych osobowych,
14. jednostkowe dane mogą być kopiowane na nośniki magnetyczne, optyczne i inne, po ich zaszyfrowaniu i przechowywane w zamkniętych na klucz szafach, po ustaniu przydatności tych kopii, dane należy trwale skasować lub fizycznie zniszczyć nośniki, na których są przechowywane,
15. jednostkowe dane mogą być przekazywane pocztą elektroniczną pomiędzy komputerami tylko po ich zabezpieczeniu,
16. przesyłanie danych osobowych pocztą elektroniczną może odbywać się tylko w postaci zaszyfrowanej,
17. zabrania się wynoszenia poza obszar przetwarzania danych na jakichkolwiek nośnikach całych zbiorów danych oraz szerokich z nich wypisów, nawet w postaci zaszyfrowanej,
18. przetwarzając dane osobowe, należy odpowiednio często robić kopie robocze danych, na których się pracuje, tak by zapobiec ich utracie,
19. zakończenie pracy na stacji roboczej następuje po wprowadzeniu danych tego dnia przetwarzanych w odpowiednie obszary zasobów sieciowych, a następnie prawidłowym wylogowaniu się przez użytkownika i wyłączeniu komputera,
20. przed opuszczeniem pomieszczenia należy:
    a) zniszczyć w niszczarce lub schować do zamykanych na klucz szaf wszelkie wykonane wydruki zawierające dane osobowe,
    b) schować do zamykanych na klucz szaf wszelkie dokumenty zawierające dane osobowe,
    c) umieścić klucze do szaf w ustalonym, przeznaczonym do tego miejscu,
    d) zamknąć okna,
21. opuszczając pomieszczenie należy zamknąć za sobą drzwi na klucz.

§ 11

1. Praca na komputerach przenośnych powinna odbywać się z uwzględnieniem następujących zasad:

a) użytkownicy, którym zostały powierzone komputery przenośne, powinni chronić je przed uszkodzeniem, kradzieżą i dostępem osób postronnych, szczególną ostrożność należy zachować podczas transportu. Przekazanie pracownikom służbowych komputerów przenośnych odbywa się na podstawie protokołu zdawczo-odbiorczego,

b) zabrania się używania komputerów przenośnych przez osoby inne niż użytkownicy, którym zostały one powierzone,

c) praca na komputerze przenośnym powinna być możliwa dopiero po wprowadzeniu hasła i indywidualnego identyfikatora użytkownika,

d) pliki zawierające dane osobowe przechowywane na komputerach przenośnych powinny być zaszyfrowane i opatrzone hasłem dostępu,

e) zabrania się wykonywania nieautoryzowanych kopii całych zbiorów danych lub szerokich z nich wypisów przez osoby do tego nieupoważnione,

f) użytkownicy przetwarzający dane osobowe na komputerach przenośnych obowiązani są do systematycznego wprowadzania tych danych w określone miejsca na zasobach sieciowych Administratora, a następnie do trwałego usuwania ich z pamięci powierzonych komputerów przenośnych,

g) zabrania się samodzielnej modernizacji oprogramowania i sprzętu w powierzonych komputerach przenośnych, wszelkie zmiany mogą być dokonywane tylko przez ASI,

h) razie wystąpienia usterek w pracy komputerów przenośnych lub w razie wystąpienia konieczności aktualizacji ich oprogramowania należy zgłosić to ASI,

i) komputery przenośne muszą być wyposażone w odpowiednie programy ochrony antywirusowej, których aktualizację sugeruje automatycznie system,

j) w przypadku podłączenia komputera przenośnego do sieci Internet poza siecią Szkoły należy zastosować firewall zainstalowany bezpośrednio na komputerze, system antywirusowy oraz system wykrywania włamań IPS/IDS,

k) każdy użytkownik musi zachować szczególną ostrożność podczas korzystania z zasobów sieci publicznej,

l) komputer przenośny nie może być pozostawiany w miejscu narażającym go na kradzież (np. w otwartym pomieszczeniu, w samochodzie),

m) przypadku pozostawienia komputerów przenośnych w miejscu pracy zaleca się po zakończeniu pracy umieszczanie ich w zamkniętych na klucz szafach lub w pomieszczeniach objętych kontrolą dostępu.

2. W zakresie nieuregulowanym powyższymi zasadami przy przetwarzaniu danych osobowych na komputerach przenośnych obowiązują zasady dotyczące pracy na stacjach

roboczych.

§ 12

Korzystanie przez pracowników z Internetu i poczty służbowej powinno odbywać się z uwzględnieniem następujących zasad:

1. praca w sieci Internet nie może zagrażać bezpieczeństwu danych i systemów informatycznych,
2. pracownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie pobrane z Internetu i przez niego zainstalowane,
3. zabrania się w szczególności:
   a) wykorzystywania sieci Internet w sposób, który mógłby narazić Szkołę na utratę dobrego imienia, np. otwieranie stron WWW o złej reputacji, udostępnianie chronionych informacji na portalach społecznościowych, przesyłanie pocztą elektroniczną wrażliwych danych osobowych bez zabezpieczeń,
   b) udostępniania łącza internetowego dostarczonego przez Szkołę osobom nieupoważnionym,
   c) obciążania sieci poprzez pobieranie filmów, plików muzycznych, gier, aplikacji i plików graficznych niezwiązanych z obowiązkami pracowniczymi,
4. korzystając z poczty elektronicznej Szkoły należy stosować w szczególności następujące zasady:
   a) po odebraniu wiadomości elektronicznej upewnić się, że adres nadawcy jest prawidłowy,
   b) nie otwierać załączników z poczty e-mail, której nadawcy nie znamy,
   c) nie uruchamiać linków w poczcie e-mail, przesłanych przez nieznanych lub niezaufanych nadawców,
   d) przesyłać wiadomości wyłącznie po upewnieniu się, że adres odbiorcy jest prawidłowy, np. poprzez potwierdzenie elektroniczne otrzymania wiadomości,
5. przesyłanie danych osobowych w innym celu, niż wykonywanie obowiązków, jest zabronione,
6. korzystanie z prywatnej poczty elektronicznej do realizacji celów służbowych jest zabronione,
7. korzystanie ze służbowej poczty elektronicznej do celów prywatnych jest zabronione,
8. konfigurację oprogramowania, za pomocą którego realizuje się dostęp do zasobów Internetu, wykonuje ASI.

§ 13

1. Dostęp zdalny do zasobów Administratora, możliwy jest tylko po spełnieniu zasad określonych w niniejszej PZSI.
2. Dostęp zdalny do zasobów Administratora udziela ASI na podstawie pisemnej zgody Dyrektora.
3. Do dostępu zdalnego należy wykorzystywać poniższy standard bezpieczeństwa:
   a) Virtual Private Network,
   b) kanał SSL lub IPSec,
   c) algorytm szyfrujący AES z długością klucza min. 128 bit,
   d) długość klucza wstępnego: min. 20 znaków,
   e) hasła użytkownika muszą spełniać wymagania niniejszej PZSI.
4. ASI prowadzi pisemny wykaz osób posiadających dostęp zdalny do zasobów Administratora (wraz z danymi historycznymi).
5. Zabrania się podejmowania czynności zmierzających do penetrowania zasobów sieci.
6. Zabrania się wykorzystywania dostępu zdalnego:
   a) z komputerów innych niż służbowe, należące do Szkoły,
   b) z sieci publicznie dostępnych np. kafejki internetowe, dworce PKP, restauracje, bezprzewodowe sieci otwarte (hotspoty).

§ 14

Tworzenie, testowanie i przechowywanie kopii zapasowych danych powinno odbywać się z uwzględnieniem następujących zasad:

1. za tryb i częstotliwość tworzenia kopii zapasowych odpowiada ASI oraz Administrator aplikacji,
2. ASI oraz Administratorzy aplikacji odpowiadają za opracowanie procedur tworzenia i testowania kopii bezpieczeństwa, przy czym kopie zapasowe są wykonywane według następującego harmonogramu:
   a) codziennie – kopie różnicowe lub przyrostowe baz danych oraz innych istotnych danych znajdujących się na serwerach, niezbędnych do sprawnego funkcjonowania Szkoły, po zakończeniu godzin pracy,
   b) przed każdym serwisem baz danych lub aktualizacją oprogramowania obsługujących bazy danych i systemów operacyjnych na serwerach,
   c) w cyklu miesięcznym – kopia całościowa systemów operacyjnych na serwerach oraz baz danych aplikacji,

3. w celu zapewnienia poprawności wykonywania kopii bezpieczeństwa należy regularnie poddawać testowi wybraną kopię. Próba polega na odtworzeniu danych w warunkach testowych i sprawdzeniu, czy jest możliwość odczytania danych,
4. kopie zapasowe przechowuje się w odrębnym pomieszczeniu,
5. zabrania się przechowywania kopii zapasowych w pomieszczeniach przeznaczonych do przechowywania zbiorów danych pozostających w bieżącym użytkowaniu,
6. w miarę możliwości zbiorcze kopie zapasowe przechowywane są w innej lokalizacji,
7. za bezpieczne przechowywanie kopii, ich oznakowanie oraz regularne sprawdzanie przydatności odpowiada ASI,
8. nośniki zawierające nieaktualne kopie zapasowe likwiduje się. W przypadku nośników jednorazowych, takich jak płyty CD-R, DVD-R, likwidacja polega na ich fizycznym zniszczeniu w taki sposób, by nie można było odczytać ich zawartości. Nośniki wielorazowego użytku, takie jak dyski twarde, płyty CD-RW, DVD-RW, można wykorzystać ponownie do celów przechowywania kopii zapasowych po uprzednim usunięciu ich zawartości. Nośniki wielorazowego użytku nienadające się do ponownego użycia, niszczy się fizycznie np. w niszczarce.

§ 15

Zabezpieczenie systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego powinno odbywać się z uwzględnieniem następujących zasad:

1. sprawdzanie obecności wirusów komputerowych w systemie informatycznym oraz ich usuwanie powinno odbywać się przy wykorzystaniu oprogramowania zainstalowanego na serwerach, stacjach roboczych oraz komputerach przenośnych automatycznie,
2. oprogramowanie, o którym mowa w pkt 1, powinno sprawować ciągły nadzór (ciągła praca w tle) nad pracą systemu i jego zasobami oraz serwerami i stacjami roboczymi,
3. monitorowanie aktualizacji oprogramowania antywirusowego oraz określenie częstotliwości automatycznych aktualizacji definicji wirusów, dokonywanych przez to oprogramowanie należy do obowiązków ASI,
4. użytkownik niezwłocznie powiadamia ASI o pojawiających się komunikatach, wskazujących na wystąpienie zagrożenia wywołanego szkodliwym oprogramowaniem,
5. dostęp do Internetu możliwy jest na wszystkich stacjach roboczych oraz komputerach przenośnych, sieć wewnętrzna jest chroniona centralnym urządzeniem sprzętowym z wbudowanym Firewall.

§ 16

Kontrola nad wprowadzaniem, dalszym przetwarzaniem i udostępnianiem danych osobowych powinna odbywać się z uwzględnieniem następujących zasad:

1. system informatyczny służący do przetwarzania danych osobowych powinien zapewniać dla każdej osoby, której dane osobowe są przetwarzane w tym systemie automatyczne odnotowywanie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych, informacji o dacie pierwszego wprowadzenia danych do systemu oraz o identyfikatorze osoby wprowadzającej dane,
2. w przypadku zbierania danych osobowych od osoby, której dane nie dotyczą należy zapewnić w systemie informatycznym odnotowywanie informacji o źródle pochodzenia danych (proces ten nie musi odbywać się automatycznie), dla każdego systemu służącego do przetwarzania danych osobowych, z którego udostępniane są dane osobowe odbiorcom danych, należy zapewnić odnotowanie w bazie danych tego systemu informacji, komu, kiedy i w jakim zakresie dane zostały udostępnione,
3. w przypadku zgłoszenia sprzeciwu wobec przetwarzania danych osobowych system powinien zapewniać odnotowywanie tej informacji,
4. należy zapewnić rozliczalność w systemie informatycznym polegającą na dokumentowaniu w postaci elektronicznych zapisów w dziennikach systemów (logach),
5. w dziennikach systemów powinny być odnotowane działania użytkowników lub obiektów systemowych polegające na dostępie do:
   a) systemu z uprawnieniami administracyjnymi,
   b) konfiguracji systemu, w tym konfiguracji zabezpieczeń,
   c) przetwarzanych w systemach danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa,
6. informacje w dziennikach systemów przechowywane są przez co najmniej 6 miesięcy, chyba że przepisy szczególne stanowią inaczej.

§ 17

Przetwarzanie, udostępniane i likwidacja danych osobowych powinno odbywać się z uwzględnieniem następujących zasad:

1. w przypadku przekazywania lub wynoszenia urządzeń lub nośników zawierających dane osobowe, poza obszar przetwarzania danych osobowych, zabezpiecza się je w sposób zapewniający poufność, integralność i rozliczalność tych danych, przez co rozumie się:
   a) ograniczenie dostępu do danych osobowych hasłem zabezpieczającym dane przed

osobami nieupoważnionymi,

b) stosowanie metod kryptograficznych,

c) stosowanie odpowiednich zabezpieczeń fizycznych,

d) stosowanie odpowiednich zabezpieczeń organizacyjnych,

2 w zależności od stopnia zagrożenia zalecane jest stosowanie kombinacji wyżej wymienionych zabezpieczeń,

3 decyzję o likwidacji zbiorów danych osobowych, przetwarzanych w systemach informatycznych podejmuje Administrator,

4 w przypadku likwidacji elektronicznych nośników danych, należy dokonać wcześniej skutecznego usunięcia danych z tych nośników. W przypadku gdy usunięcie danych nie jest możliwe, należy uszkodzić nośniki w sposób uniemożliwiający odczyt tych danych,

5 przed przekazaniem elektronicznego nośnika danych osobie nieuprawnionej, należy usunąć z nośnika dane osobowe.

§ 18

Przeglądy i konserwacja systemów oraz nośników danych służących do przetwarzania danych powinny odbywać się z uwzględnieniem następujących zasad:

1. przeglądy i konserwacje systemów oraz nośników służących do przetwarzania danych osobowych, a także wstępne czynności serwisowe dokonywane są w siedzibie Administratora na bieżąco przez ASI lub wyspecjalizowany podmiot zewnętrzny (firmę informatyczną) na podstawie zawartej z Administratorem umowy,
2. w wypadku przekazania sprzętu lub nośników służących do przetwarzania danych osobowych podmiotowi trzeciemu, pozbawia się je zapisanych danych osobowych w sposób, który uniemożliwi ich odtworzenie,
3. wykryte podczas przeglądu i konserwacji nieprawidłowości w działaniu sprzętu lub programów służących do przetwarzania danych osobowych, usuwa się niezwłocznie,
4. za prawidłowość przeprowadzenia przeglądów i konserwacji systemu informatycznego odpowiada ASI.

§ 19

Naprawy urządzeń komputerowych z chronionymi danymi osobowymi powinny odbywać się z uwzględnieniem następujących zasad:

1. naprawy urządzeń komputerowych oraz zmiany w systemie informatycznym Administratora przeprowadzane są - o ile to możliwe - przez ASI,

2. naprawy i zmiany w systemie informatycznym Administratora przeprowadzane przez serwisanta prowadzone są pod nadzorem ASI w siedzibie Administratora (jeśli to możliwe) lub poza siedzibą Administratora, po uprzednim nieodwracalnym usunięciu danych w nich przetwarzanych, a jeśli wiązałoby się to z nadmiernymi utrudnieniami, to po podpisaniu umowy powierzenia przetwarzania danych osobowych,
3. jeśli nośnik danych (dysk, płyta lub inne) zostanie uszkodzony i nie można go odczytać ani usunąć z niego danych, należy go zniszczyć mechanicznie.

§ 20

Użytkownik zobowiązany jest poinformować niezwłocznie IOD i Dyrektora o każdym naruszeniu lub podejrzeniu naruszenia bezpieczeństwa systemu informatycznego. Szczegółowy opis postępowania znajduje się w Procedurze - postępowanie w przypadku naruszenia danych osobowych i dokumentowanie naruszeń ochrony danych osobowych stanowiącej załącznik nr 5 do Polityki Bezpieczeństwa Informacji Szkoły Podstawowej im. Ziemi Lubelskiej w Radawcu Dużym.

§ 21

1. Programy zainstalowane na stacjach roboczych i na komputerach przenośnych obsługujących przetwarzanie danych osobowych muszą być użytkowane z zachowaniem praw autorskich, zgodnie z posiadanymi licencjami.
2. Oprogramowanie może być używane tylko zgodnie z prawami licencji. Oprogramowanie typu Freeware, Shareware lub inne oprogramowanie dostarczane bez opłat jest uznawane jako nieautoryzowane, jeżeli nie otrzyma stosownej aprobaty ASI.
3. Przed zainstalowaniem nowego oprogramowania ASI zobowiązany jest sprawdzić jego działanie pod kątem bezpieczeństwa całego systemu.
4. Sieć informatyczna wykorzystywana do przetwarzania danych osobowych powinna mieć zapewnione prawidłowe zasilanie energetyczne gwarantujące właściwe i zgodne z wymaganiami producenta działanie sprzętu informatycznego. Należy zastosować urządzenia typu UPS, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania.
5. Infrastruktura techniczna związana z siecią informatyczną i jej zasilaniem (rozdzielnie elektryczne, skrzynki z bezpiecznikami) powinna być zabezpieczona przed dostępem osób nieupoważnionych.

6. Wdrażanie aplikacji i oprogramowania eksploatowanych systemów powinno być poprzedzone wyczerpującymi, pozytywnymi i udokumentowanymi testami.
7. Należy zapewnić synchronizację zegarów wszystkich stosowanych systemów służących do przetwarzania danych osobowych z uzgodnionym, dokładnym źródłem czasu.
8. Należy zapewnić, aby usługi, które nie są wykorzystywane były zablokowane.

§ 22

W sprawach nieokreślonych niniejszą PZSI należy stosować instrukcje obsługi i zalecenia producentów aktualnie wykorzystywanych urządzeń i programów.

DYREKTOR SZKOŁY
mgr Hanna Szymańska

SZKOŁA PODSTAWOWA
im. Ziemi Lubelskiej
w Radawcu Dużym, gm. Konopnica
21-030 Motycz, woj. lubelskie
tel./fax 81 50-30-022
NIP: 713-24-92-400, Regon: 001180501

Załącznik nr 1

Wykaz systemów i kluczowych aplikacji wykorzystywanych w Szkole Podstawowej im. Ziemi Lubelskiej w Radawcu Dużym.

1.Microsoft Office (word, ecxel)

2.Dziennik elektroniczny Librus Synergia

3.Aplikacja e-sekretariat Librus

4.Płatnik

5.Kadry Optivum Vulcan

6.Aplikacja Systemu Informacji Oświatowej

7.Aplikacja iArkusz - program informatyczny firmy Wolters Kluwer do sporządzania arkusza organizacyjnego szkoły

DYREKTOR SZKOŁY
mgr Hanna Szymańska