Załącznik nr 2 do Zarządzenia nr 12/2018
dyrektora Szkoły Podstawowej im. Jana Pawła II w Chwarstnicy
z dnia 03.09.2018r.

Polityka Bezpieczeństwa Informacji w zakresie bezpieczeństwa informacji i ochrony danych osobowych podczas przetwarzania dokumentacji w postaci tradycyjnej oraz elektronicznej

w Szkole Podstawowej w Chwarstnicy im. Jana Pawła II

ul. Gryfińska 19, 74-100 Gryfino

Szczegóły dokumentu:

Sporządził:	*Marta Maj* Inspektor Ochrony Danych
Data przekazania:	01.09.2018r.

Historia zmian

Data	Wersja	Utworzona przez	Opis zmiany

Spis treści

1. Cel i przeznaczenie dokumentu

Celem niniejszej dokumentacji jest przedstawienie zasad oraz procedur w zakresie budowania i stosowania systemu bezpiecznego przetwarzania danych osobowych. Dokumentacja zawiera informacje w zakresie rozwiązań technicznych umożliwiających przetwarzanie dokumentacji osobowej. Zostały przedstawione wymagania organizacyjne oraz wskazano odpowiedzialność za przetwarzanie informacji w tym danych osobowych wrażliwych zawartych w dokumentacji osobowej.

Nadrzędnym celem PBI jest:

1) Zapewnienie spełnienia wymagań prawnych.
2) Zaangażowanie wszystkich pracowników w ochronę informacji.
3) Ochrona systemów przetwarzania informacji przed nieuprawnionym dostępem bądź zniszczeniem.
4) Zmniejszenie ryzyka utraty informacji.
5) Ustanowienie Systemu Zarządzania Bezpieczeństwem Informacji.
6) Podnoszenie świadomości pracowników.
7) Właściwy dobór zabezpieczeń (środków bezpieczeństwa) oparty na rezultatach i wnioskach wynikających z procesów szacowania i postępowania z ryzykiem, wymagań prawnych, wymagań nadzoru, zobowiązań kontraktowych oraz pozostałych wymagań dotyczących bezpieczeństwa informacji.

Bezpieczeństwo informacji zapewnione jest poprzez:

1) Zarządzanie ryzykiem.
2) Klasyfikacja zasobów i ich zawartości.
3) Identyfikacja stopnia zagrożeń i ich następstw.
4) Określenie i wdrożenie działań zabezpieczających zasoby.

Zakres obowiązywania PBI.

Niniejszy dokument dotyczy wszystkich komórek organizacyjnych oraz wszystkich pracowników, a także innych osób mających dostęp do informacji chronionych (np. pracowników firm zewnętrznych realizujących prace na rzecz podmiotu).

Dokument ma zastosowanie do wszystkich informacji chronionych niezależnie od formy, w jakiej są przechowywane (papierowej, elektronicznej).

Z dokumentem są zobowiązani zapoznać się wszyscy pracownicy mający dostęp do danych osobowych oraz innych chronionych informacji.

2. Deklaracja.

Szkoła Podstawowa w Chwarstnicy deklaruje, że SZBI, w tym i niniejsza PBI została opracowana na podstawie rozporządzenia KRI, w świetle wytycznych standaryzujących obszary zabezpieczeń według Polskiej Normy PN-ISO/IEC 27001, oraz PN-ISO/IEC 27002 – w odniesieniu do ustanawiania zabezpieczeń, PN- SO/IEC 27005 – w odniesieniu do zarządzania ryzykiem, PN-ISO/IEC 24762 – w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.

SZBI w Szkole Podstawowej w Chwarstnicy to system zapewniający poufność, dostępność i integralność informacji z uwzględnieniem dodatkowo takich atrybutów, jak: autentyczność, rozliczalność, niezaprzeczalność i niezawodność, oraz ciągłość działania.

Wdrożony SZBI, którego elementem jest niniejsza PBI, może podlegać ciągłemu doskonaleniu, zgodnie z wymaganiami normy PN-ISO/IEC 27001.

Celem wdrożonego w Szkole Podstawowej w Chwarstnicy SZBI jest osiągnięcie właściwego poziomu organizacyjnego i technicznego, który:

- maksymalnie ograniczy występowanie zagrożeń dla bezpieczeństwa informacji,

- zapewni zachowanie poufności informacji chronionych, integralności i dostępności informacji chronionych (niepublicznych) oraz jawnych (publicznych).

- zapewni poprawne i bezpieczne funkcjonowanie wszystkich systemów informatycznych przetwarzających informację.

3. Podstawowe pojęcia i skróty.

1) **Administrator Danych Osobowych (ADO)** w rozumieniu RODO jednostka organizacyjna decydująca o celach i środkach przetwarzania danych osobowych.
2) **Inspektor Ochrony Danych (IOD)** – osoba fizyczna odpowiedzialna za zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez: sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, nadzorowanie opracowania i aktualizowania dokumentacji.
3) **Akceptowanie ryzyka** - decyzja, aby zaakceptować ryzyko.
4) **Aktywa** - wszystko, co ma wartość dla organizacji.
5) **Analiza ryzyka** - systematyczne wykorzystanie informacji do zidentyfikowania źródeł i oszacowania ryzyka.
6) **Autentyczność**- właściwość polegająca na tym, że pochodzenie lub zawartość danych opisujących obiekt są takie, jak deklarowane.
7) **Bezpieczeństwo informacji** - zachowanie poufności, integralności i dostępności informacji; dodatkowo, mogą być brane pod uwagę inne własności, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.
8) **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. Za dane osobowe uważa się: nazwisko, imię, nazwisko rodowe, PESEL, NIP, data zatrudnienia, wykształcenie, data i miejsce urodzenia, imiona i nazwiska rodowe rodziców, seria i numer dowodu osobistego, książeczki wojskowej, stan cywilny, płeć, adres zamieszkania lub pobytu, informacje o stanie zdrowia, nałogach, przynależności wyznaniowej, związkowej. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.
9) **Dane szczególnych kategorii** - dane o pochodzeniu rasowym lub etnicznym, poglądach politycznych, przekonaniach religijnych lub filozoficznych, przynależności wyznaniowej, partyjnej lub związkowej, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.
10) **Dostępność** - właściwość bycia dostępnym i użytecznym na żądanie upoważnionego

podmiotu.

11) **Elektroniczne nośniki informacji – (ENI)** - zewnętrzne nośniki danych, w szczególności płyty CD, DVD, PenDrive, pamięci typu FLASH.
12) **Hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.
13) **Identyfikator użytkownika** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
14) **Incydent związany z bezpieczeństwem informacji** - jest to pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji.
15) **Integralność danych** – właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany, właściwość polegająca na zapewnieniu dokładności i kompletności aktywów.
16) **Niezaprzeczalność** - brak możliwości zanegowania swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie.
17) **Ocena ryzyka** - proces porównywania oszacowanego ryzyka z określonymi kryteriami w celu określenia znaczenia ryzyka.
18) **Postępowanie z ryzykiem** - proces wyboru i wdrażania środków modyfikujących ryzyko.
19) **Poufność danych** – właściwość polegająca na tym, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom.
20) **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.
21) **Rozliczalność** - właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
22) **Ryzyko szczątkowe** - ryzyko pozostające po procesie postępowania z ryzykiem.
23) **Sieć lokalna (intranet)** - połączenie jednostek komputerowych pracujących w celu wymiany danych (informacji) dla własnych potrzeb, przy wykorzystaniu urządzeń telekomunikacyjnych.
24) **System informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
25) **Szacowanie ryzyka** - całościowy proces analizy i oceny ryzyka.
26) **SZBI** – system zarządzania bezpieczeństwem informacji - jest to część całościowego systemu zarządzania, oparta na podejściu wynikającym z ryzyka biznesowego, odnosząca się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji. SZBI zawiera strukturę organizacyjną, planowane działania, zakresy odpowiedzialności, zasady, procedury, procesy i zasoby.
27) **Uwierzytelnianie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.
28) **Użytkownik** - osoba upoważniona przez ADO do przetwarzania danych osobowych zarówno w systemach tradycyjnych „T" jak i w systemie informatycznym – elektronicznym „E" (pracownik, osoba wykonująca pracę na podstawie umowy cywilno-prawnej, osoba odbywająca staż pracy, praktykant).
29) **Zabezpieczenie danych w systemie informatycznym** - wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.
30) **Zarządzanie ryzykiem** - skoordynowane działania kierowania i zarządzania organizacją z uwzględnieniem ryzyka.
31) **Zbiór danych** - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest

rozproszony lub podzielony funkcjonalnie.

32) **Zdarzenie związane z bezpieczeństwem informacji** - jest określonym stanem systemu, usługi lub sieci, który wskazuje na możliwe naruszenie polityki bezpieczeństwa informacji.
33) **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.

4. Organizacja bezpieczeństwa informacji.

Administrator Danych Osobowych odpowiada za:

1) Przeszkolenie instruktażowe pracowników w zakresie związanym z bezpieczeństwem informacji na stanowiskach pracy.
2) Przestrzeganie zasad bezpieczeństwa informacji przez nich samych jak i przez podległych im pracowników.
3) Identyfikowanie i dokumentowanie zagrożeń istotnych dla bezpieczeństwa informacji.
4) Przeprowadzanie audytów zgodności SZBI.
5) Zatwierdzenie warunków technicznych i organizacyjnych służących bezpieczeństwu informacji, w tym ochronie danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem obowiązujących regulacji prawnych oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
6) Cele, zakres oraz metody przetwarzania i ochrony informacji, w tym danych osobowych.
7) Właściwą realizacje praw osób, których dane przetwarza.
8) Realizację obowiązku informacyjnego.

Kompetencje i odpowiedzialność w obszarze zarządzania bezpieczeństwem informacji:

<u>Obowiązki Administratora Danych</u>

1) Administrator danych zobowiązany jest do zapewnienia, aby dane osobowe były przetwarzane zgodnie z prawem, zbierane dla oznaczonych, zgodnych z prawem celów, merytorycznie poprawne i adekwatne w stosunku do celów.
2) Wyznacza osobę, odpowiedzialną za bezpieczeństwo danych osobowych.
3) Opracowuje instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych, przeznaczoną dla osób zatrudnionych przy przetwarzaniu tych danych.
4) Określa budynki, pomieszczenia lub części pomieszczeń, tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego zestawu komputerowego.
5) Opracowuje instrukcję, określającą sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji.
6) Prowadzi ewidencję osób uprawnionych do przetwarzania danych osobowych oraz uprawnionych do dostępu w poszczególnych systemach.
7) Organizuje szkolenia mające na celu zaznajomienie każdej osoby przetwarzającej dane osobowe z przepisami dotyczącymi ich ochrony.
8) Odpowiada za to by zakres czynności osoby zatrudnionej przy przetwarzania danych osobowych określał odpowiedzialność tej osoby za ochronę danych przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem danych, nielegalnym ujawnieniem danych w stopniu odpowiednim do zadań realizowanych w procesie przetwarzania danych osobowych.

9) Zgłasza Inspektora Ochrony Danych Osobowych w ewidencji prowadzonej przez PUODO.

Obowiązki użytkownika systemu informacji.

1) Użytkownik zobowiązany jest dbać o bezpieczeństwo powierzonych mu do przetwarzania, archiwizowania lub przechowywania danych zgodnie z obowiązującą Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji, regulaminami i instrukcjami wewnętrznymi.
2) Ochrona danych przed dostępem osób nieupoważnionych.
3) Ochrona danych przed przypadkowym lub nieumyślnym zniszczeniem, utratą lub modyfikacją.
4) Ochrona nośników magnetycznych i optycznych oraz wydruków komputerowych przed dostępem osób nieupoważnionych oraz przed przypadkowym zniszczeniem.
5) Utrzymywanie w tajemnicy powierzonych identyfikatorów, haseł, częstotliwość ich zmiany oraz szczegóły technologiczne systemów także po ustaniu zatrudnienia.
6) Archiwizowanie danych zgodnie z instrukcją.
7) Użytkownik obsługujący system informatyczny w obszarze przyznanego mu dostępu do systemu zobowiązany jest do sprawdzania czy nie wprowadzono nieautoryzowanych aplikacji oraz zmian w zainstalowanych aplikacjach.
8) Zabrania się pod rygorem odpowiedzialności służbowej i karnej ujawniania danych, kopiowania baz danych lub ich części poza przewidzianymi kopiami zapasowymi.
9) Zabrania się wykorzystywania sprzętu komputerowego i sieci komputerowej do celów prywatnych.
10) Zabrania się używania prywatnych komunikatorów.
11) Zabrania się ściągania i wysyłania plików (filmów, muzyki itp..).
12) Zabrania się korzystania z nośników nieznanego pochodzenia.
13) Zabrania się instalowania jakiegokolwiek oprogramowania
14) Zaleca się robienie kopii zapasowych ważnych plików i baz danych, jeśli nie są realizowane centralnie. Kopie należy wykonywać na udziałach sieciowych.
15) Użytkownik jest zobowiązany do zachowanie porządku na biurku w trakcie pracy oraz schowanie wszystkich dokumentów po jej zakończeniu.
16) Użytkownik jest zobowiązany do stosowania zasady „czystego pulpitu" polegającej na blokowaniu stacji poprzez wciśnięcie równocześnie klawisza „Windows" + „l".
17) Wszelkie niepotrzebne dokumenty/brudnopisy należy zniszczyć najpierw ręcznie, a następnie w niszczarce jeśli zawierają dane osobowe, pieczątki firmowe, podpisy itp.; zabrania się wyrzucania całych dokumentów do śmietnika.

5. *Kontrola dostępu do informacji.*

Dostęp do informacji podlega ciągłej kontroli, która polega na:

1) Wydzielaniu obszarów przeznaczonych do przechowywania oraz przetwarzania zbiorów danych.
2) Zarządzaniu uprawnieniami poszczególnych użytkowników.
3) Nadzorowaniu działalności stron trzecich, mogących wpłynąć na bezpieczeństwo informacji
4) Bieżącym informowaniu pracowników o wszelkich zmianach w zakresie regulacji dotyczących przechowywania, przetwarzania i udostępniania informacji.
5) Wszystkie osoby posiadające dostęp do informacji podlegają przeszkoleniu w zakresie obowiązujących przepisów prawa.

6. Zarządzanie aktywami i ryzykiem.

Ważnym elementem zarządzania aktywami i bezpieczeństwem informacji jest przeprowadzanie okresowego szacowania ryzyka i opracowanie planów postępowania z ryzykiem. Analiza uzyskanych wyników stanowi podstawę do podejmowania działań w zakresie doskonalenia ochrony aktywów.

Identyfikowanie ryzyk polega na możliwym rozpoznaniu zagrożeń, które mogą wpływać na bezpieczeństwo informacji.

Na szacowanie ryzyka składają się :

1) Analiza ryzyka.
2) Ocena ryzyka.

W szacowaniu ryzyka określa się wartość aktywów informacyjnych, identyfikuje się mające zastosowanie zagrożenia oraz istniejące (lub mogące zaistnieć) podatności, identyfikuje się istniejące zabezpieczenia i ich wpływ na zidentyfikowane ryzyko, określa się możliwe następstwa oraz na końcu wskazuje się priorytety uzyskanych ryzyk i ustala ich kolejność zgodnie z kryteriami oceny ryzyka wyznaczonymi podczas ustanawiania kontekstu.

7. Deklaracja ochrony własności intelektualnej.

W Szkole Podstawowej w Chwarstnicy zostały wdrożone mechanizmy zapobiegające naruszeniom prawa powszechnego związanego z ochroną własności intelektualnej. Stacje robocze zostały zabezpieczone przed możliwością instalowania oprogramowania z naruszeniem licencji.

Prowadzona jest bieżąca ewidencja sprzętu komputerowego i licencji oprogramowania.

Nadzorowana jest także własność intelektualna powierzona lub przekazana przez osoby trzecie.

8. Bezpieczeństwo zasobów ludzkich.

Szkoła Podstawowa w Chwarstnicy zatrudnia kompetentną kadrę pracowniczą do realizacji wyznaczonych zadań. Celem takiego postępowania jest ograniczenie ryzyka błędu ludzkiego, kradzieży, nadużycia lub niewłaściwego użytkowania zasobów. Realizacja postawionego celu możliwa jest dzięki wdrożonym zasadom rekrutacji pracowników.

Prowadzone są szkolenia dla pracowników z zakresu wdrożonych zasad i procedur bezpieczeństwa informacji, które zakończone jest złożeniem oświadczenia o zachowaniu poufności podczas współpracy oraz po jej zakończeniu.

Do przetwarzania informacji dopuszczone są tylko osoby posiadające stosowne upoważnienie.

9. Bezpieczeństwo fizyczne i środowiskowe.

Celem bezpieczeństwa fizycznego jest zapewnienie ochrony przed nieautoryzowanym dostępem fizycznym, uszkodzeniami lub zakłóceniami w siedzibie organizacji poprzez wprowadzenie technicznych zabezpieczeń.

10. Utrzymanie ciągłości działania.

Zastosowanie odpowiednich środków organizacyjnych i technicznych umożliwi utrzymanie ciągłości działania, odtworzenie procesów oraz wznowienie działania systemów w sytuacji kryzysowej.

Na utrzymanie ciągłości działania składają się następujące zasady:

1) Zastosowanie działań naprawczych.
2) Ustalenie reguł współpracy z innymi podmiotami.
3) Opracowanie planu awaryjnego.
4) Ciągłe doskonalenie opracowanych procedur, planów oraz środków organizacyjnych i technicznych.

11. Naruszenie bezpieczeństwa informacji.

W celu utrzymania wysokiego poziomu bezpieczeństwa informacji podejmuje się odpowiednie działania wobec sytuacji, które są związane z jego naruszeniem.

Każdy przypadek naruszenia dostępności, poufności i integralności informacji jest rejestrowany i poddawany odpowiedniej procedurze postępowania. W systemie zarządzania bezpieczeństwem informacji konieczne jest zaangażowanie wszystkich pracowników, w tym niezwłoczna interwencja na różne niepokojące sygnały i zdarzenia.

12. Podstawy prawne i organizacyjne.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016r. w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii (Dz. U. RPUE.L.2016.194.1),

Rozporządzenie Parlamentu Europejskiego i Rady(UE) 2016/679 z dnia 27 kwietnia 2016r. 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.2016.119.1),

Norma PN-ISO/IEC 27005:2014-01 Technika informatyczna - Techniki bezpieczeństwa - Zarządzanie ryzykiem w bezpieczeństwie informacji,

Norma PN-ISO/IEC 27001:2014-12 Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji –Wymagania,

Norma PN-ISO/IEC 27002:2014-12 Technika informatyczna -- Techniki bezpieczeństwa -- Praktyczne zasady zabezpieczania informacji.

13. Postanowienia końcowe.

W sprawach nieuregulowanych niniejszą PBI odpowiednie zastosowanie mają reguły i procedury zawarte w dokumentach powiązanych.

Polityka Bezpieczeństwa Informacji wchodzi w życie z dniem podpisania.

……..

(podpis Administratora Danych