POLITYKA BEZPIECZEŃSTWA INFORMACJI

Administrator:

Korczakowska Szkoła Marzeń
Niepubliczna Szkoła Podstawowa

ul. Urbanistów 3
02-397 Warszawa
tel.: 603 151 843
e-mail: ksm@uczelniakorczaka.pl
NIP: 526-172-30-36
REGON: 147459919

Warszawa, 2021

Spis treści:

1. **Wstęp**.

O skuteczności działania i rozwoju każdej organizacji świadczy stopień osiągania zamierzonego celu. W procesie tym kluczowe jest stosowanie współczesnych technik i technologii, narzędzi i systemów informatycznych oraz przetwarzania i zarządzania informacją. Informacja jest jednym z najważniejszych zasobów jednostki organizacyjnej samorządu, dlatego powinna być chroniona na każdym szczeblu organizacji. Szkoła chroni zarówno informacje własne, jak i powierzone. Poufność, dostępność i integralność informacji ma kluczowe znaczenie dla utrzymania zgodności z przepisami prawa oraz wizerunku Szkoły wobec stron zainteresowanych.

Polityka Bezpieczeństwa Informacji w Korczakowskiej Szkole Marzeń - Niepublicznej Szkole Podstawowej w Warszawie stanowi zestawienie zasad, praw i reguł oraz doświadczeń i dobrych praktyk w zakresie zarządzania i ochrony danych i informacji w naszej organizacji. Polityka określa techniczne i organizacyjne środki służące do osiągnięcia celów stawianych przed systemem zarządzania bezpieczeństwem informacji, jakimi są: zapewnienie spełnienia wymagań prawnych, właściwe zabezpieczenie aktywów informacyjnych, ochrona przetwarzania danych, niezawodność funkcjonowania systemów, zmniejszenie ryzyka utraty informacji oraz systematyczna edukacja użytkowników, a w efekcie pełne zaangażowanie wszystkich pracowników w ochronę informacji.

Polityka Bezpieczeństwa Informacji została wdrożona i jest stale doskonalona w celu:

a) zapewnienia poufności, integralności i dostępności danych;
b) zapewnienia identyfikowalności czynności i zasobów podczas przetwarzania danych;
c) zapewnienia niezawodności działań;
d) podejmowania wysiłków prowadzących do poprawy poziomu bezpieczeństwa zasobów informacyjnych w Szkole.

Polityka Bezpieczeństwa Informacji jest dokumentem nadrzędnym w stosunku do wszystkich dokumentów systemowych z zakresu zarządzania bezpieczeństwem informacji.

2. Terminy, definicje i podstawy prawne.

Ilekroć w Polityce Bezpieczeństwa Informacji jest mowa o:

1) **polityce** - należy przez to rozumieć Politykę Bezpieczeństwa Informacji w Korczakowskiej Szkole Marzeń - Niepublicznej Szkole Podstawowej w Warszawie;
2) **uczelni** – należy przez to rozumieć Uczelnię Korczaka w Warszawie – Organ prowadzący Szkołę;
3) **dyrektorze –** należy przez to rozumieć Dyrektora Korczakowskiej Szkoły Marzeń - Niepublicznej Szkoły Podstawowej w Warszawie**;**
4) **szkole -** należy przez to rozumieć Korczakowską Szkołę Marzeń - Niepubliczną Szkołę Podstawową
   w Warszawie;
5) **systemie informatycznym** - należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur, narzędzi programowych zastosowanych do przetwarzania informacji i danych;
6) **SZBI** - należy przez to rozumieć System Zarządzania Bezpieczeństwem Informacji w Korczakowskiej Szkole Marzeń - Niepublicznej Szkole Podstawowej w Warszawie;
7) **użytkowniku** - należy przez to rozumieć osobę korzystającą z zasobów teleinformatycznych Szkoły.

Polityka Bezpieczeństwa Informacji w Korczakowskiej Szkole Marzeń - Niepublicznej Szkole Podstawowej w Warszawie spełnia wymagania prawne i regulacyjne, zawarte w:

1) ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych (tj.: Dz.U. z 2019 roku, poz. 1781);
2) ustawie z dnia 19 lipca 2019 r. o zapewnianiu dostępności osobom ze szczególnymi potrzebami (tj.: Dz.U. z 2020 roku, poz. 1062 z późn. zm.);
3) rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 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.2018.119.1).

Definicje:

1) **Administrator (ADO)** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania. Administratorem danych osobowych jest Korczakowska Szkoła Marzeń - Niepubliczna Szkoła Podstawowa w Warszawie.
2) **Inspektor ochrony danych (IOD)** - oznacza osobę powołaną do pełnienia funkcji Inspektora Ochrony Danych w organizacji, inspektor odgrywa kluczową rolę w zakresie wspierania „kultury ochrony danych” oraz pomaga w implementacji niezbędnych elementów RODO w codziennej działalności organizacji. Administrator oraz podmiot przetwarzający zapewniają, by inspektor był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych. Inspektor bezpośrednio podlega najwyższemu kierownictwu administratora lub podmiotu przetwarzającego. Osoby, których dane dotyczą, mogą kontaktować się z inspektorem we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem

praw przysługujących im na mocy RODO. Inspektor jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań.

3) **Administrator systemu informatycznego (ASI)** - oznacza osobę wyznaczoną przez administratora do zarządzania systemami informatycznymi, w których przetwarza się informacje w organizacji.
4) **Najwyższym kierownictwie administratora (najwyższe kierownictwo)** – rozumie się przez to osoby, które reprezentują organizację, ustanawiają Politykę Bezpieczeństwa Informacji oraz inne polityki, a także określają role, odpowiedzialność i uprawnienia (Dyrektora KSM).
5) **Osoba upoważniona** – rozumie się przez to osobę posiadającą formalne upoważnienie do przetwarzania danych osobowych wydane przez Administratora.
6) **Podmiocie zewnętrznym** – rozumie się przez to kontrahenta Administratora.
7) **Dane osobowe** – wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"). Osoba fizyczna możliwa do zidentyfikowania 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.
8) **Zbiór danych osobowych** – rozumie się przez to uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.
9) **Informacja** – wszelkie zapisy w formie papierowej, w systemach komputerowych oraz na innych nośnikach przetwarzane w systemach tradycyjnych, elektronicznych i komunikacyjnych będących własnością Szkoły, funkcjonujących w Szkole lub tylko administrowanych przez Szkołę.
10) **Aktyw/zasób** – wszystko to, co ma wartość dla organizacji w zakresie informacji (zarówno informacje, jak i środki techniczne oraz organizacyjne do ich przetwarzania).
11) **Przetwarzanie** – rozumie się przez to operacje lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie 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.
12) **System Zarządzania Bezpieczeństwem Informacji (SZBI)** - oznacza część systemu zarządzania, który oparty jest na podejściu wynikającym z ryzyka biznesowego, odnoszący się do ustanowienia, wdrożenia, eksploatacji, monitorowania, utrzymania i doskonalenia bezpieczeństwa informacji; SZBI zawiera strukturę organizacyjną w tym polityki, zakres odpowiedzialności, zasady, procedury, procesy i zasoby wg Polskiej Normy PN-ISO/IEC 27001.
13) **Polityka Bezpieczeństwa Informacji (PBI)** – rozumie się przez to zestaw formalnych zasad, procedur oraz kodeksów dobrych praktyk odnoszących się do bezpieczeństwa przepływu informacji zbieżnych z celami istnienia organizacji.
14) **Polityka Bezpieczeństwa Danych Osobowych (PBDO)** – jest to zestaw praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji danych osobowych, wewnątrz określonej organizacji. Polityka odnosi się całościowo do problemu zabezpieczenia danych przetwarzanych tradycyjnie – w formie papierowej, jak i danych przetwarzanych w systemie informatycznym. Celem polityki

jest wskazanie działań jakie należy wykonać oraz ustanowienie zasad i reguł postępowania, które należy stosować, aby właściwie wykonywać obowiązki administratora w zakresie zabezpieczenia danych osobowych.

15) **Polityka Bezpieczeństwa Systemów Informatycznych (PBSI)** - jest to zestaw praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania systemem.
16) **Procedura Zarządzania Incydentami (PZI)** – rozumie się przez to zestaw formalnych procedur odnoszących się do postępowania z naruszeniami w zakresie bezpieczeństwa ochrony danych osobowych.
17) **Bezpieczeństwo informacji** – zachowanie poufności, integralności i dostępności informacji w wyniku stosowania procesu zarządzania ryzykiem.
18) **Incydent bezpieczeństwa informacji** – pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań Szkoły i zagrażają bezpieczeństwu informacji.
19) **Poufność** – zapewnienie dostępu do informacji tylko osobom upoważnionym.
20) **Integralność** – zapewnienie że dokument nie zostanie zmieniony w sposób nieuprawniony.
21) **Dostępność** – zapewnienie, że osoby upoważnione będą miały dostęp do informacji zawsze gdy jest to im niezbędne.
22) **Ryzyko** – prawdopodobieństwo wystąpienia zagrożenia, które wykorzystując podatność(ci) aktywu, może doprowadzić do jego uszkodzenia lub zniszczenia.
23) **Szacowanie ryzyka** – całościowy proces analizy i oceny ryzyka.
24) **Postępowanie z ryzykiem** – proces wyboru i wdrażania środków modyfikujących ryzyko.
25) **Zarządzanie ryzykiem** – proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych przy zachowaniu akceptowalnego poziomu kosztów.
26) **Analizie Ryzyka Ogólnego i Ocenie Skutków dla Przetwarzania danych (DPIA)** – rozumie się przez to dokumentację zawierającą opis metodologii, częstotliwości oraz zakresu przeprowadzanego procesu szacowanie.

3. Zakres Systemu Bezpieczeństwa Informacji SZBI w Szkole stanowi część Zintegrowanego Systemu Zarządzania, odnoszącą się do:

1) ustanawiania,
2) wdrażania,
3) eksploatacji,
4) monitorowania,
5) utrzymywania,
6) doskonalenia bezpieczeństwa informacji.

4. Polityka Bezpieczeństwa Informacji ma zastosowanie do całego systemu informacyjnego Szkoły, w szczególności do:

1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są informacje podlegające ochronie;

2) informacji będących własnością Szkoły;
3) informacji będących własnością klientów Szkoły, uzyskanych na podstawie zawartych umów;
4) wszystkich pracowników w rozumieniu przepisów kodeksu pracy, stażystów i innych osób mających dostęp do informacji podlegających ochronie.

5. Zakres Systemu Zarządzania Bezpieczeństwem Informacji

Szkoła, określając zakres Systemu Zarządzania Bezpieczeństwem Informacji, rozważała zarówno kontekst wewnętrzny jak i zewnętrzny, identyfikowała strony zainteresowane, a także określała interfejsy i zależności między działaniami wykonywanymi wewnątrz organizacji oraz przez inne organizacje.

Kontekst wewnętrzny.

Szkoła określa kontekst wewnętrzny uwzględniając następujące czynniki:

1) schemat organizacyjny będący odzwierciedleniem zależności pomiędzy komórkami funkcjonalnymi w kontekście przepływu danych osobowych oraz określający bezpośrednią podległość Inspektora Ochrony Danych;
2) ład organizacyjny w rozumieniu zindywidualizowanych zasad zarządzania organizacją znajdujących swoje źródło we wdrożonych procedurach i normach;
3) ustanowione przez najwyższe kierownictwo cele organizacji w rozumieniu celów strategicznych, ekonomicznych i pozaekonomicznych, taktycznych, operacyjnych (katalog otwarty);
4) określoną przez najwyższe kierownictwo misję organizacji w rozumieniu zespołu wartości podkreślających rolę organizacji na rzecz otoczenia, w którym organizacja działa;
5) aktywa organizacji w postaci zasobu ludzkiego - jego wiedzy, kompetencji, umiejętności oraz postaw;
6) procesy podejmowania decyzji uwzględniając strukturę organizacyjną;
7) kulturę organizacji;
8) relacje do wewnątrz organizacji.

Kontekst zewnętrzny

Szkoła określając kontekst zewnętrzny uwzględniła następujące czynniki:

1) relacje z zewnętrznymi podmiotami;
2) środowisko zewnętrzne mające wpływ na cele organizacji: prawne, finansowe, ekonomiczne i technologiczne.

6. Deklaracja Najwyższego Kierownictwa w zakresie bezpieczeństwa informacji w Korczakowskiej Szkole Marzeń - Niepublicznej Szkole Podstawowej w Warszawie.

1. Celem wprowadzenia Polityki Bezpieczeństwa Informacji w Korczakowskiej Szkole Marzeń - Niepublicznej Szkole Podstawowej w Warszawie jest zharmonizowanie systemu ochrony danych osobowych w taki sposób, by zapewnić realizacje podstawowych praw i wolności osób fizycznych, których dane osobowe organizacja przetwarza w związku z realizacją czynności edukacyjno-administracyjnych oraz zadań publicznych.

2. Celem wprowadzenia Polityki Bezpieczeństwa Informacji jest także ciągłe edukowanie osób zaangażowanych w proces przetwarzania danych osobowych.
3. Polityka Bezpieczeństwa Informacji ma również na celu zapewnienie poufności oraz integralności danych osobowych, względem których zachodzi proces przetwarzania poprzez przypisanie odpowiedzialności i uprawnień względem osób upoważnionych do przetwarzania tych danych oraz użytkowników systemów teleinformatycznych.
4. Dyrektor, stojąc na stanowisku, że informacja jest newralgicznym zasobem Szkoły, wdrożył w ramach Zintegrowanego Systemu Zarządzania w Korczakowskiej Szkole Marzeń - Niepublicznej Szkole Podstawowej w Warszawie system zarządzania bezpieczeństwem informacji i zobowiązuje się do podejmowania wszelkich działań prowadzących do kompleksowego zabezpieczenia informacji oraz zapewnienia środków niezbędnych do realizacji niniejszej Polityki.
5. Najwyższe kierownictwo dochowuje należytej staranności, by System Zarządzania Bezpieczeństwa Informacji był silnie zintegrowany z innymi systemami czy procesami, które warunkują osiągniecie celów strategicznych przez organizacje.
6. Najwyższe kierownictwo deklaruje, iż bezpieczeństwo informacji jest uwzględniane w ramach projektowania procesów czy systemów, które służą organizacji do osiągnięcia celów strategicznych.
7. Najwyższe kierownictwo, wdrażając Politykę Bezpieczeństwa Informacji wykazuje przywództwo i zaangażowanie w kontekście bezpieczeństwa przetwarzanych danych osobowych w związku z realizacją czynności administracyjnych poprzez zapewnienie, iż wprowadzona Polityka Bezpieczeństwa Informacji jest:
    a) zgodna z celami strategicznymi istnienia organizacji,
    b) określa cele bezpieczeństwa informacji,
    c) zobowiązuje najwyższe kierownictwo do ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji,
    d) określa spełnienie wymagań zgodnie z obowiązującymi normami prawnymi,
    e) jest zakomunikowana w organizacji,
    f) jest dostępna jako udokumentowana i formalnoprawnie wdrożona procedura,
    g) jest dostępna dla podmiotów zainteresowanych, o ile jest to uzasadnione względami formalnoprawnymi.

7. Organizacja bezpieczeństwa informacji w Korczakowskiej Szkole Marzeń - Niepublicznej Szkole Podstawowej w Warszawie.

Odpowiedzialność za realizację ochrony informacji w Szkole ponoszą wszyscy pracownicy Szkoły – proporcjonalnie do wykonywanych obowiązków i posiadanych uprawnień.

1) każdy pracownik Szkoły jest zapoznawany z zasadami bezpieczeństwa oraz z aktualnymi procedurami ochrony informacji na swoim stanowisku pracy w Szkole zawartymi w Instrukcji podstawowych zasad bezpieczeństwa dla pracowników Szkoły;
2) stażyści i praktykanci również są zapoznawani z tymi zasadami;
3) właściciel aktywu odpowiada za bieżące nadzorowanie oraz zarządzanie aktywem.

Zakres odpowiedzialności ADO

Administrator Danych Osobowych zapewnia, aby odpowiedzialność i uprawnienia osób pełniących istotną rolę w procesie ochrony informacji w Szkole zostały odpowiednio przydzielone i bezpośrednio zakomunikowane.

Do najważniejszych obowiązków Administratora Danych Osobowych należą:

1) sprawowanie nadzoru nad bezpieczeństwem oraz przetwarzaniem informacji w Szkole;
2) zapewnienie środków technicznych i organizacyjnych przetwarzania informacji z uwzględnieniem przede wszystkim zmian w obowiązującym prawie, organizacji administratora oraz technik zabezpieczenia informacji, w tym danych osobowych;
3) wprowadzenie w Szkole procedur zapewniających wysoki poziom zabezpieczenia ochrony przetwarzanych informacji;
4) upoważnianie oraz odwoływanie upoważnień poszczególnych osób do przetwarzania danych osobowych w określonym indywidualnie zakresie, odpowiadającym zakresowi obowiązków;
5) powoływanie Inspektora Ochrony Danych i zawiadamianie Prezesa Urzędu Ochrony Danych Osobowych o wyznaczeniu IOD oraz zapewnienie by inspektor ochrony danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych;
6) wyznaczanie Administratora Systemu Informatycznego oraz określenie zakresu jego zadań i czynności;
7) wyznaczanie osoby odpowiedzialnej za prowadzenie rejestru osób upoważnionych: do przetwarzania danych osobowych, posiadających dostęp do zasobów sieci informatycznej Szkoły;
8) wyznaczanie osoby odpowiedzialnej za prowadzenie rejestru umów powierzenia danych osobowych, rejestru czynności przetwarzania danych osobowych, rejestru kategorii czynności przetwarzania, rejestru incydentów;
9) wyznaczanie osoby odpowiedzialnej za prowadzenie rejestru realizacji praw osób, których dane dotyczą;
10) podejmowanie odpowiednich działań w przypadku naruszenia lub podejrzenia naruszenia procedur bezpiecznego przetwarzania danych osobowych, w tym m.in. zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu oraz zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych;
11) zapewnianie prowadzenia szkoleń w Szkole lub podejmowanie innych działań w celu podnoszenia kwalifikacji swoich pracowników w zakresie ochrony danych i bezpiecznego przetwarzania informacji;
12) zapewnienie możliwości zapoznania się pracowników Szkoły z obowiązującymi w przepisami oraz przyjętymi w organizacji procedurami dotyczącymi bezpiecznego przetwarzania danych osobowych oraz bezpieczeństwa informacji;
13) zlecanie okresowego szacowania ryzyka zagrożeń dla procesów przetwarzania informacji;
14) zlecanie okresowej oceny skutków dla ochrony danych osobowych;
15) dokonywanie przeglądu oraz uaktualniania środków organizacyjnych i technicznych zastosowanych w organizacji w tym zapewnienie okresowych audytów wewnętrznych SZBI;
16) wdrożenie, utrzymanie i ciągłe doskonalenie Systemu Zarządzania Bezpieczeństwem Informacji oraz ochrony danych osobowych i ewentualne podejmowanie działań korygujących;
17) zapewnienie bieżącego nadzoru nad realizacją regulacji przyjętej w dokumentacji wchodzącej w skład SZBI;
18) planowanie prac dotyczących aktualizacji Systemu Zarządzania Bezpieczeństwem Informacji;
19) komunikowanie SZBI w Szkole;
20) wprowadzenie i uaktualnianie procedury reagowania na incydenty, określającej zasady i formy zgłaszania wystąpienia incydentu przez pracowników;

21) zapewnienie ciągłości bezpieczeństwa informacji;
22) archiwizacja i bieżący nadzór nad wdrożonymi, zmienianymi i zarchiwizowanymi wersjami dokumentacji SZBI;
23) ocena wyników działań na rzecz bezpieczeństwa informacji oraz skuteczności systemu zarządzania informacji;
24) zlecanie i nadzorowanie corocznego audytu SZBI;
25) zapewnienie pracownikom niezbędnych uprawnień, do przetwarzania informacji w tym danych osobowych;
26) zapewnienie złożenia przez pracowników oświadczenia o znajomości przepisów o ochronie danych osobowych oraz zobowiązania do zachowania w tajemnicy danych osobowych i informacji na temat zabezpieczenia tych danych;
27) zapewnienie aktualności, adekwatności oraz merytorycznej poprawności informacji zbieranych i przetwarzanych w określonym przez nich celu;
28) realizacja obowiązku informacyjnego o przetwarzaniu danych osobowych wobec osób, których dane są pozyskiwane zgodnie z opracowaną procedurą;
29) zapewnienie, na żądanie uprawnionych osób, udostępnienia informacji o przetwarzanych danych osobowych oraz podmiotach, którym zostały one udostępnione.

Zakres odpowiedzialności IOD

Inspektor Ochrony Danych realizuje zadania w zakresie nadzoru nad przestrzeganiem zasad ochrony danych osobowych obowiązujących w Korczakowskiej Szkole Marzeń - Niepublicznej Szkole Podstawowej w Warszawie.

Wewnętrzne i zewnętrzne obowiązki IOD:

1) monitorowanie przestrzegania przepisów prawa o ochronie danych oraz polityk i procedur przyjętych przez administratora w dziedzinie ochrony danych osobowych;
2) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o spoczywających na nich obowiązkach;
3) bieżący nadzór nad dokumentacją wprowadzoną w Szkole w tym, między innymi nad:
    a) dokumentacją opisującą sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych,
    b) dokumentacją pracowniczą związaną z przetwarzaniem danych osobowych (upoważnienie do przetwarzania danych osobowych oraz rejestry osób upoważnionych do przetwarzania danych osobowych),
    c) oświadczeniami pracowników o zapoznaniu się z obowiązującymi procedurami i zachowaniu poufności;
4) zatwierdzanie wzorów dokumentów, w szczególności projektów umów powierzenia danych osobowych przygotowywanych przez pracowników administratora oraz otrzymanych bezpośrednio od kontrahentów;
5) nadzorowanie prowadzenia rejestrów upoważnień do przetwarzania danych osobowych, umów powierzenia, incydentów, czynności oraz kategorii czynności przetwarzania, a także realizacji praw osób, których dane dotyczą;
6) prowadzenie działań, na wniosek Administratora, zwiększających świadomość pracowników Szkoły poprzez prowadzenie szkoleń personelu uczestniczącego w operacjach przetwarzania;
7) udzielanie odpowiedzi na bieżące pytania i wątpliwości z zakresu ochrony danych osobowych kierowane na dedykowany adres poczty elektronicznej przez pracowników Szkoły;
8) przeprowadzanie, na wniosek Administratora, audytów w zakresie przestrzegania przepisów dotyczących ochrony danych osobowych i przyjętych przez administratora procedur;

9) nadzorowanie oraz podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń lub podejrzenia naruszenia;
10) udzielanie na żądanie Administratora zaleceń co do oceny skutków dla ochrony danych;
11) współpraca z organem nadzorczym;
12) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami;
13) w stosownych przypadkach prowadzenie konsultacji z organem nadzorczym we wszelkich innych sprawach niż wynikające z art. 36 RODO;
14) zapewnienie kontaktu dla osób, których dane dotyczą.

Zakres odpowiedzialności ASI

Administrator Systemów Informatycznych nadzoruje cały system informatyczny, zainstalowane oprogramowanie, aktualność zabezpieczeń oprogramowania służącego do przetwarzania informacji w tym danych osobowych.

Do zakresu obowiązków ASI należy:

1) zarządzanie systemami informatycznymi oraz przeciwdziałanie dostępowi osób niepowołanych do systemów informatycznych;
2) nadawanie pracownikom uprawnień dostępu do danych w systemach informatycznych wprowadzonych w Szkole poprzez:
    a) tworzenie kont użytkowników w systemach informatycznych,
    b) przypisywanie do kont startowych haseł uwierzytelniających użytkowników tych kont,
    c) resetowanie utraconych haseł i nadawanie nowych;
3) podejmowanie niezwłocznych działań w sytuacji utraty uprawnień do systemu poprzez usuwanie kont i uprawnień dla kont osób, które utraciły uprawnienia;
4) zarządzanie hasłami użytkowników i nadzór nad przestrzeganiem procedur określających częstotliwość ich zmiany;
5) wprowadzenie procedury awaryjnego odtwarzania systemu informatycznego i sprawowanie nadzoru nad hasłem administratora;
6) prowadzenie i bieżąca aktualizacja rejestru/ewidencji stosowanych programów oraz sprzętu komputerowego wraz z ich konfiguracją;
7) zabezpieczenie systemów przetwarzania danych osobowych, poprzez instalację programów antywirusowych;
8) planowanie i wykonywanie zadań związanych z tworzeniem kopii bezpieczeństwa systemów i danych;
9) wprowadzenie procedury testowania wykonanych kopii zapasowych pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego w środowisku neutralnym;
10) prowadzenie działań konserwacyjnych w systemie oraz systematyczne aktualizowanie oprogramowania systemowego, aplikacyjnego i ochronnego;
11) monitorowanie stanu środowiska IT, stanu sprzętu IT i wykorzystywanego oprogramowania oraz aktywności sieciowej użytkowników;
12) kontrola przepływu informacji pomiędzy systemami informatycznym a siecią publiczną oraz kontrola działań inicjowanych z sieci publicznej a systemem informatycznym;
13) sprawowanie nadzoru nad wykonywaniem napraw, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe;

14) zapewnienie bezawaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych osobowych;
15) zapewnienie okresowej analizy logów systemowych;
16) prowadzenie szkoleń dla użytkowników systemu informatycznego dotyczących bezpiecznej pracy w systemie;
17) planowanie inwestycji oraz dostaw i usług niezbędnych dla utrzymania i rozwoju środowiska IT w Szkole.

Zakres odpowiedzialności pracowników

Każdy Pracownik Szkoły zobowiązany jest do:

1) zapoznania się z wprowadzonymi przez Administratora procedurami w tym zwłaszcza PBI, PBDO, PBSI, instrukcją postępowania w sytuacji naruszenia bezpieczeństwa ochrony danych osobowych oraz procedurą realizacji praw osób, których dane dotyczą oraz innych procedur wprowadzonych u Administratora i postępowania zgodnie z nimi;
2) przetwarzania danych osobowych wyłącznie w zakresie ustalonym indywidualnie przez administratora w upoważnieniu i tylko w celu wykonywania nałożonych na niego obowiązków;
3) brania czynnego udziału w szkoleniach dotyczących bezpieczeństwa informacji, ochrony danych osobowych oraz bezpiecznej pracy w systemie IT;
4) w razie pojawiających się wątpliwości dotyczących bezpieczeństwa przetwarzanych informacji w tym danych osobowych, korzystania z rad i opinii IOD powołanego w Szkoły;
5) w sytuacji pobierania danych osobowych od rodziców dzieci uczęszczających do Szkoły zapewniania możliwości zapoznania się osoby, której dane dotyczą z klauzulą informacyjną;
6) stosowania określonych przez ADO procedur i środków mających na celu zabezpieczenie informacji przed ich udostępnieniem osobom nieupoważnionym;
7) zachowania w tajemnicy informacji w tym danych osobowych oraz informacji o sposobach ich zabezpieczania, przy czym przestrzeganie tajemnicy obowiązuje przez cały okres zatrudnienia u ADO, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji;
8) ochrony informacji oraz danych osobowych przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem.

8. Dokumentacja systemu zarządzania bezpieczeństwem informacji

Dokumentacja SZBI składa się z następujących głównych elementów. Są nimi:

1. Polityka bezpieczeństwa informacji.
2. Polityka bezpieczeństwa danych osobowych.
3. Polityka bezpieczeństwa systemów informatycznych.
4. Procedura realizacji obowiązku informacyjnego.
5. Procedura realizacji praw osób, których dane dotyczą.
6. Procedura postępowania w sytuacji naruszenia ochrony danych osobowych.
7. Regulamin monitoringu wizyjnego.
8. Rejestry (wersja elektroniczna - exel):
    a) rejestr czynności i kategorii przetwarzania danych,
    b) rejestr upoważnień,
    c) rejestr umów powierzenia,

d) rejestr naruszeń,
e) rejestr realizacji praw osób, których dane dotyczą,
f) rejestr szkoleń,
g) rejestr zgód;

9. Procedura monitoringu wizyjnego
10. Procedura analizy ryzyka
11. Procedura nadawania uprawnień
12. Procedura zarządzania incydentami
13. Procedura retencji danych.

9. Zasady współpracy ze stronami zainteresowanymi.

W Korczakowskiej Szkole Marzeń - Niepublicznej Szkole Podstawowej w Warszawie wdrożono standard bezpieczeństwa fizycznego w odniesieniu do klientów i podmiotów wykonujących prace zlecone na terenie Szkoły. Ponadto instrukcja ogólna w zakresie wymagań dla umów przygotowywanych w Szkole określa klauzule poufności różnego stopnia szczegółowości, niezbędne przy zawieraniu umów. Celem takiego postępowania jest zapewnienie bezpieczeństwa informacji przed dostępem osób niepowołanych, uszkodzeniem lub innymi zakłóceniami w obiektach oraz systemach Szkoły.

Wyodrębnione zostały również obszary niedostępne dla klientów, uczniów i ich rodziców oraz osób trzecich z uwagi na przetwarzane informacje bądź funkcje techniczne. Pomieszczenia komórek organizacyjnych przetwarzających dane osobowe wyposażono w fizyczne bariery biurka umożliwiające obsługę klientów przy jednoczesnym odseparowaniu ich od zasobów informacyjnych. Ciągi komunikacyjne pozostają pod stałą obserwacją systemu monitoringu.

10. Polityka kontroli dostępu do informacji.

Dostęp do informacji przechowywanych i przetwarzanych w Korczakowskiej Szkole Marzeń - Niepublicznej Szkole Podstawowej w Warszawie jest poddany kontroli. Kontrola polega na:

1) wydzieleniu obszarów przeznaczonych do przechowywania oraz przetwarzania poszczególnych zbiorów danych i zapewnieniu odpowiednich barier fizycznych przeciwdziałających nieuprawnionemu dostępowi;
2) zarządzaniu uprawnieniami poszczególnych użytkowników w sposób zapewniający dostęp wyłącznie do danych wymaganych do wykonywania obowiązków służbowych, jeśli dane te podlegają ochronie z jakiejkolwiek przyczyny;
3) stosowaniu bezpiecznych systemów przetwarzania informacji;
4) nadzorowaniu działalności stron trzecich, mogących wpłynąć na bezpieczeństwo informacji;
5) bieżącym informowaniu pracowników o wszelkich zmianach w zakresie regulacji dotyczących przechowywania, przetwarzania i udostępniania informacji.

Adekwatność i skuteczność stosowanych w Korczakowskiej Szkole Marzeń - Niepublicznej Szkole Podstawowej w Warszawie środków kontroli dostępu do informacji podlega bieżącej weryfikacji w ramach audytów wewnętrznych.

11. Klasyfikacja informacji.

Klasyfikacja została wprowadzona w celu uporządkowania w Korczakowskiej Szkole Marzeń - Niepublicznej Szkole Podstawowej w Warszawie postępowania z różnymi rodzajami informacji, które są głównym zasobem naszej organizacji. W szczególny sposób potraktowano informację, której ujawnienie może narazić pracodawcę na szkodę. Podstawowym elementem klasyfikacji są grupy informacji.

W grupach informacji zebrane zostały dokumenty logicznie ze sobą powiązane o podobnych wymaganiach związanych z bezpieczeństwem. Do określenia poziomu bezpieczeństwa danej grupy informacji przyjęto wskaźniki definiujące :

1) Przez **poufność** rozumiemy zapewnienie, iż dostęp do informacji mają tylko i wyłącznie osoby uprawnione.
2) Przez **integralność** rozumiemy zapewnienie, iż informacje nie zostały zmienione lub zniszczone w nieautoryzowany sposób (niezgodny z wewnętrznymi regulacjami Szkoły).
3) Przez **dostępność** rozumiemy możliwość dostępu do informacji w takim czasie, jaki jest oczekiwany przez użytkownika.
   Zdefiniowano trzy poziomy dla każdego z powyższych wskaźników po to, aby możliwe było powiązanie danej grupy informacji z określonym poziomem zdefiniowanego wskaźnika w skali 1-3.

Struktura klasyfikacji informacji w Korczakowskiej Szkole Marzeń - Niepublicznej Szkole Podstawowej w Warszawie opiera się na założeniu istnienia trzech poziomów postrzegania informacji:

1) **informacje jawne** – informacje publicznie dostępne,
2) **informacje wewnętrzne** – informacje, których przetwarzanie i udostępnianie podlega restrykcjom z uwagi na szczególne znaczenie dla pracodawcy (właściciela informacji):
   a) informacje **wewnętrzne dostępne** – informacje dostępne dla wszystkich pracowników Szkoły,
   b) informacje **wewnętrzne wrażliwe** – informacje dostępne dla grupy pracowników upoważnionych z uwagi na realizowane zadania regulaminowe,
3) **informacje ustawowo chronione** – tajemnice określone w odrębnych przepisach.

12. Zarządzanie aktywami i ryzykami.

Korczakowska Szkoła Marzeń - Niepubliczna Szkoła Podstawowa w Warszawie zarządza swoimi aktywami informacyjnymi poprzez zapewnienie im wymaganego poziomu bezpieczeństwa. Identyfikowane są aktywa informacyjne i klasyfikowane zgodnie ze stawianymi im wymaganiami w zakresie ochrony. Ważnym elementem zarządzania aktywami i bezpieczeństwem informacji jest przeprowadzanie okresowej analizy ryzyka i opracowywanie planów postępowania z ryzykiem. Analiza wyników stanowi podstawę podejmowania wszelkich działań w zakresie doskonalenia ochrony zasobów Szkoły. Na podstawie wyników analizy ryzyka opracowywane są plany postępowania z ryzykiem dla aktywów o ryzykach większych niż ustalony poziom ryzyka akceptowalnego. Ryzyka są przeglądane na przeglądach kierownictwa oraz po zmianach mających wpływ na system bezpieczeństwa informacji.

13. Autoryzacja nowych urządzeń.

Każde nowe lub zmienione urządzenie służące do przetwarzania informacji lub mogące w jakikolwiek inny sposób wpływać na bezpieczeństwo informacji jest weryfikowane na zgodność z wymaganiami systemu bezpieczeństwa informacji i zaakceptowane przez uprawnioną osobę. Szczegółowy opis postępowania zawiera właściwa instrukcja.

Urządzenia służące do przetwarzania informacji nie będące własnością Korczakowskiej Szkole Marzeń - Niepublicznej Szkole Podstawowej w Warszawie mogą być używane (po sprawdzeniu sprzętu pod względem kryteriów bezpieczeństwa) wyłącznie za zgodą osoby upoważnionej.

14. Zarządzanie systemami i sieciami.

Korczakowska Szkoła Marzeń - Niepubliczna Szkoła Podstawowa w Warszawie dba o przestrzeganie zasad związanych z utrzymywaniem i użytkowaniem systemów informatycznych i sieci. Celem takiego postępowania jest zapewnienie poufności, integralności i dostępności przetwarzanej przez nie informacji własnych.

Skuteczna realizacja postawionego celu możliwa jest dzięki:

1) kompetencjom i świadomości pracowników oraz podpisanym umowom ze specjalistycznymi firmami administrującymi zasobami informatycznymi;
2) opracowanym zasadom konserwacji urządzeń w celu zapewnienia ich ciągłej pracy;
3) kontrolowaniu wprowadzania wszelkich zmian do infrastruktury technicznej,
4) prowadzeniu prac rozwojowych i testowych na oddzielnych urządzeniach lub środowiskach w celu zapewnienia bezpieczeństwa systemów produkcyjnych;
5) nadzorowaniu usług dostarczanych przez strony trzecie, w szczególności odbieraniu ich i akceptowaniu w sposób świadomy uwzględniający jego wpływ na istniejący system bezpieczeństwa;
6) wdrożeniu zabezpieczeń chroniących przed oprogramowaniem złośliwym i mobilnym;
7) systematycznemu tworzeniu i testowaniu kopii bezpieczeństwa;
8) przestrzeganiu opracowanych zasad postępowania z nośnikami;
9) bieżącemu monitorowaniu aktywów informacyjnych.

Korczakowska Szkoła Marzeń - Niepubliczna Szkoła Podstawowa w Warszawie monitoruje możliwość wystąpienia incydentów bezpieczeństwa i posiada mechanizmy reagowania w przypadkach ich wystąpienia. Szczegółowy sposób postępowania zawiera właściwa instrukcja.

15. Bezpieczeństwo zasobów ludzkich.

Korczakowska Szkoła Marzeń - Niepubliczna Szkoła Podstawowa w Warszawie zapewnia 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 ustanowionym praktykom i podziałowi odpowiedzialności związanemu z weryfikacją kandydatów do pracy podczas naboru, zasadom zatrudniania pracowników oraz ustalonej procedurze rozwiązywania umów o pracę.

16. Bezpieczeństwo fizyczne, sprzętu i infrastruktury technicznej

W Korczakowskiej Szkole Marzeń - Niepublicznej Szkole Podstawowej w Warszawie określono następujące kierunkowe standardy:

a) standard bezpieczeństwa fizycznego;
b) standard bezpieczeństwa sprzętu i okablowania;
c) standard konfiguracji i eksploatacji sieci.

Z uwagi na to, że standardy zawierają informacje, których ujawnienie nieuprawnionym stronom trzecim mogłoby w istotnym stopniu obniżyć poziom bezpieczeństwa informacji, są udostępnione tylko pracownikom Korczakowskiej Szkole Marzeń - Niepublicznej Szkole Podstawowej w Warszawie wykonującym zadania określone w standardach.

Przedmiot poszczególnych standardów:

1) **standard bezpieczeństwa fizycznego**: parametr bezpieczeństwa fizycznego, kontrola fizycznych wejść, zabezpieczenie biur, pokoi i urządzeń, ochrona przed zagrożeniami zewnętrznymi i środowiskowymi, praca w obszarach zabezpieczonych, obszary ogólnie dostępne, obszary dostaw i załadunku;
2) **standard bezpieczeństwa sprzętu i okablowania:** rozmieszczenie i ochrona sprzętu, urządzenia wspomagające, bezpieczeństwo okablowania, utrzymanie sprzętu, bezpieczeństwo sprzętu znajdującego się poza terenem organizacji, bezpieczne usuwanie sprzętu, wynoszenie majątku;
3) **standard konfiguracji i eksploatacji sieci:** środki kontroli przeciwko kodowi złośliwemu i mobilnemu, środki kontroli sieci, bezpieczeństwo usług sieciowych, polityki i procedury dotyczące wymiany informacji, przesyłanie wiadomości drogą elektroniczną, korzystanie z usług sieciowych, identyfikacja sprzętu w sieciach, ochrona portu służącego do zdalnego diagnozowania i konfiguracji, segregacja w sieciach, kontrola połączeń sieci, routing, nadzorowanie słabości technicznych.

17. Zarządzanie ciągłością działania.

Korczakowska Szkoła Marzeń - Niepubliczna Szkoła Podstawowa w Warszawie dba o zapewnienie ciągłości funkcjonowania usług związanych z przetwarzaniem danych. Celem takiego postępowania jest przeciwdziałanie przerwom w działalności oraz ochrona krytycznych procesów przed rozległymi awariami lub katastrofami. Realizacja postawionego celu możliwa jest dzięki ustanowionym praktykom i podziałowi odpowiedzialności związanemu z zarządzeniem ciągłością działania tak, aby ograniczyć do akceptowalnego poziomu skutki wypadków i awarii. Plany awaryjne podlegają systematycznemu testowaniu.

18. Zarządzanie zmianami.

Korczakowska Szkoła Marzeń - Niepubliczna Szkoła Podstawowa w Warszawie, mając na uwadze konieczność szybkiego dostosowywania się do wymagań stron zainteresowanych, ciągłe zmiany przepisów prawnych oraz dążenie do wzrostu efektywności i wydajności pracy, zapewnia metody postępowania dla skutecznej i terminowej obsługi zmian w infrastrukturze teleinformatycznej przy utrzymaniu pożądanego poziomu bezpieczeństwa przetwarzanych danych i ograniczeniu ryzyka negatywnego wpływu zmiany na obsługę teleinformatyczną organizacji.

Proces zarządzania zmianą w Korczakowskiej Szkole Marzeń - Niepublicznej Szkole Podstawowej w Warszawie przebiega w następujących etapach:

1) ustalenie celu zmiany;
2) rozważenie wielkości i ważności zmiany dla organizacji;
3) określenie momentów krytycznych we wdrożeniu zmiany;
4) zainicjowanie zmiany, przeprowadzenie testów, wdrożenie w systemie produkcyjnym;
5) aktywne włączenie pracowników Szkoły w proces zmiany;
6) monitorowanie i raportowanie kolejnych kroków wdrożenia zmiany.

19. Zgodność z wymaganiami prawnymi i regulacyjnymi

Korczakowska Szkoła Marzeń - Niepubliczna Szkoła Podstawowa w Warszawie dba o zapewnienie zgodności postępowania z przepisami obowiązującego prawa, przyjętych uwarunkowań umownych i normatywnych oraz wypracowanych własnych standardów. Celem takiego postępowania jest unikanie naruszania jakichkolwiek przepisów prawnych, zobowiązań wynikających z ustaw, zarządzeń lub umów oraz wymagań bezpieczeństwa. Realizacja postawionego celu możliwa jest dzięki ustanowionym praktykom i podziałowi odpowiedzialności związanemu z identyfikacją wymagań prawnych w zakresie bezpieczeństwa informacji. Prowadzone są audyty wewnętrzne i zewnętrzne funkcjonowania systemu.

20. Deklaracja ochrony własności intelektualnej.

W Korczakowskiej Szkole Marzeń - Niepublicznej Szkole Podstawowej w Warszawie zostały wdrożone mechanizmy zapobiegające naruszeniom przepisów prawa powszechnego związanych z ochroną własności intelektualnej. Przede wszystkim zabezpieczono stacje robocze przed możliwością instalacji oprogramowania z naruszeniem właściwej licencji. Sieć podlega ciągłemu monitorowaniu, a dostęp do stron oraz usług internetowych, co do których zachodzi podejrzenie naruszania własności intelektualnej lub ryzyko infekcji systemu złośliwym oprogramowaniem, może zostać zablokowany.

W ramach usług domeny wprowadzono filtrowanie plików użytkownika, blokując te z formatów, które nie będąc z założenia wynikającego z funkcjonalności przydatnymi w pracy zawodowej, mogłyby zarazem być nośnikami treści naruszających prawa autorskie i pokrewne. Prowadzona jest bieżąca ewidencja licencji oprogramowania, co zapewnia, że pracownicy upoważnieni do instalacji oprogramowania działają w granicach praw nabytych przez Uczelnię Korczaka - Korczakowska Szkołę Marzeń - Niepubliczną Szkoła Podstawowa w Warszawie. Nadzorowana jest także własność intelektualna powierzona lub przekazana przez osoby trzecie, zarówno klientów, jak i kontrahentów.

21. Postanowienia końcowe.

Najwyższe kierownictwo Korczakowskiej Szkoły Marzeń - Niepublicznej Szkoły Podstawowej w Warszawie zapoznaje pracowników Szkoły, stażystów i praktykantów z dokumentem Polityki Bezpieczeństwa Informacji oraz Instrukcją podstawowych zasad bezpieczeństwa dla pracowników Korczakowskiej Szkoły Marzeń - Niepublicznej Szkoły Podstawowej w Warszawie. Administrator jest odpowiedzialny za zebranie od podległych pracowników oświadczeń o zapoznaniu się z instrukcją i przyjęciu jej do stosowania. Naruszenia świadome, bądź przypadkowe niniejszej Polityki Bezpieczeństwa Informacji (wraz z wszystkimi dokumentami operacyjnymi) powodują skutki prawne zgodnie z Regulaminem Pracy, a w przypadkach zastrzeżonych przez ustawodawcę – karne wynikające z odpowiedzialności określonej przez przepisy prawa.