Szkoła Podstawowa nr 6 z Oddziałami Integracyjnymi im. Króla Władysława Jagiełły w Sochaczewie

(Polityka Bezpieczeństwa Informacji (PBI), System Zarządzania Bezpieczeństwem Informacji (SZBI) oraz Zasady Bezpieczeństwa Informacji (ZBI)

(wersja obowiązująca od 18.08.2025)

Spis treści

Deklaracja 4

Wstęp 5

I. Charakterystyka Szkoły Podstawowej nr 6 z Oddziałami Integracyjnymi im. Króla Władysława Jagiełły w Sochaczewie 6

1. Informacje ogólne 6
2. Przywołania normatywne 7
3. Infrastruktura systemu teleinformatycznego szkoły 8

II. Polityka Bezpieczeństwa Informacji (PBI) 9

1. Wprowadzenie 10
4. Cel Polityki Bezpieczeństwa Informacji 11
5. Wspierane cele szkoły: 11
6. Zakres PBI 11
7. Role i obowiązki w PBI 11

III. Role i obowiązki w SZBI 12

1. Cel 12
2. SZBI - role i obowiązki 12
3. Dyrektor szkoły 12
4. Inspektor Ochrony Danych 13
5. Nauczyciel/Pracownik 14
6. Uczeń 14

IV. Zasady bezpieczeństwa Informacji 15

1. Ogólne wytyczne 15
2. Praca zdalna 16
3. Bezpieczne logowanie i zarządzanie hasłami 16
4. Korzystanie z internetu, poczty elektronicznej, komunikatorów internetowych w szkole 17
5. Wymagania dotyczące korzystania do pracy lub nauki w szkole z urządzeń prywatnych użytkowników (BYOD) 18
6. Zabezpieczanie informacji 19
7. Bezpieczne miejsce pracy 19
8. Zgłaszanie incydentów i zdarzeń 19

9. Sankcje dyscyplinarne 20

V. Program Budowania Świadomości w Zakresie Cyberbezpieczeństwa w Szkole 20

1. Cel 21
2. Zakres treści 21
3. Role i obowiązki 21
4. Plan Komunikacji i Szkoleń w Zakresie Cyberbezpieczeństwa 22

VI. Załączniki 24

1. Załącznik nr 1. Zgłoszenie naruszenia bezpieczeństwa systemu informatycznego 24
2. Załącznik nr 2. Wniosek o nadanie uprawnień dla użytkownika w systemie informatycznym 25
3. Załącznik nr 3. Procedura oceny ryzyka bezpieczeństwa informacji 26

Deklaracja

Zgodnie z treścią § 19 Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2024 poz. 773), w Szkole Podstawowej nr 6 z Oddziałami Integracyjnymi im. Króla Władysława Jagiełły w Sochaczewie realizującej zadania publiczne, ustanawia się. wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

System Zarządzania Bezpieczeństwem Informacji (SZBI), będący częścią całościowego systemu zarządzania w szkole oparty został na podejściu wynikającym z ryzyka i odnosi się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji tj. ochrony informacji w każdym punkcie jej przetwarzania Wymagania SZBI mają charakter zintegrowany z innymi procesami realizowanymi w szkole.

Dyrektor, jako osoba kierująca szkołą, deklaruje w szczególności:

1. Zapewnienie dostępności zasobów potrzebnych do utrzymania, rozwoju i ciągłego doskonalenia SZBI,
2. Zaangażowanie w odniesieniu do SZBI, w tym w kompleksową ochronę informacji i aktywów wspierających ich przetwarzanie oraz promowanie ciągłego doskonalenia ustanowionego Systemu,
3. Kierowanie i aktywne wspieranie osób przyczyniających się do osiągnięcia skuteczności SZBI oraz stałe podnoszenie świadomości pracowników szkoły w zakresie bezpieczeństwa informacji,
4. Wprowadzenie skutecznych działań edukacyjnych w zakresie cyberbezpieczeństwa wśród uczniów i pracowników.

dyrektor szkoły

Wstęp

W związku z rosnącą potrzebą wprowadzenia skutecznych działań edukacyjnych w zakresie cyberbezpieczeństwa wśród uczniów i pracowników, przyjęcia czytelnych zasad korzystania z technologii, które pomogą zapobiegać cyberprzemocy, dezinformacji oraz innym zagrożeniom cyfrowym, budowania świadomość cyberzagrożeń w środowisku szkolnym, opracowano niniejszy dokument kodyfikujący ramy edukacji w zakresie cyberbezpieczeństwa, jak również zarządzania bezpieczeństwem informacji. Odpowiada on na wyzwania związane z zarządzaniem szkołą, a jego celem jest zapobieganie m.in. nieetycznym, niepewnym i ryzykownym zachowaniom osób korzystających z nowych technologii.

Niniejsze opracowanie zawiera opis narzędzi, które w swoim założeniu pozwolą na skuteczne wdrożenie program bezpieczeństwa informacji w szkole. Są to:

1. **Określenie ról i odpowiedzialności** (zadania związane z bezpieczeństwem informacji wszystkim pracownikom, od nauczycieli po kadrę zarządzającą; w sytuacji, gdy zasoby są ograniczone i priorytetem jest realizacja programu nauczania oraz opieka nad uczniami, ważne jest jasne określenie ról i odpowiedzialności za bezpieczeństwo informacji. To kluczowy pierwszy krok w budowaniu Systemu Zarządzania Bezpieczeństwem Informacji. Każdy członek społeczności szkolnej, od nauczycieli, wychowawców i pedagogów po psychologów i dyrekcję, ma swoją rolę w dbaniu o cyberbezpieczeństwo. Wyznaczenie odpowiednich ról i obowiązków zapewnia, że działania związane z bezpieczeństwem informacji będą skutecznie realizowane na wszystkich poziomach szkoły, a ustalone zasady będą przestrzegane),
2. **Ustanowienie polityk bezpieczeństwa** (**Polityka Bezpieczeństwa Informacji (PBI)** oraz **System Zarządzania Bezpieczeństwem Informacji (SZBI)** zapewniające ochronę danych w szkole; oba dokumenty mają w założeniu pomóc w skutecznym zarządzaniu bezpieczeństwem informacji w placówce. PBI określa cele, jakie szkoła chce osiągnąć. Z kolei dokument „**Zasady Bezpieczeństwa Informacji**” **(ZBI)** szczegółowo opisuje wdrożenie PBI. Zawiera on m.in. ogólne wytyczne, pracę zdalną, kontrolę dostępu, zarządzanie hasłami, korzystanie z Internetu i poczty oraz BYOD (używanie prywatnych urządzeń). Dokument określa zasady bezpieczeństwa, które muszą przestrzegać nauczyciele i uczniowie, zapewniając ochronę danych w szkole i podczas pracy zdalnej.

   Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w szkole opiera się na sprawdzonych metodach, które są powszechnie stosowane w biznesie, np.

zgodnie z normami bezpieczeństwa ISO 27001. Chociaż szkoły mają inne wyzwania niż firmy, niektóre rozwiązania, takie jak polityki bezpieczeństwa informacji, zasady akceptowalnego użycia zasobów IT czy zarządzanie urządzeniami mobilnymi, mogą zostać skutecznie zaadaptowane do potrzeb placówki oświatowej.

3. **Realizacja Programu Budowania Świadomości w Zakresie Cyberbezpieczeństwa w Szkole** (propozycje działań edukacyjnych, które pomogą zwiększyć świadomość cyberzagrożeń wśród uczniów i pracowników; Jednym z kluczowych elementów Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w szkole jest stworzenie programu szkoleniowego, który buduje i utrzymuje świadomość w zakresie cyberbezpieczeństwa. Edukacja w szkole skupia się na przekazywaniu nowej wiedzy, jednak równie ważne jest regularne przypominanie o obowiązujących zasadach, takich jak reguły bezpieczeństwa czy stosowanie silnych haseł. W tym kontekście szkoła powinna wprowadzić mechanizmy, które zapewnią regularne przypominanie i utrwalanie tych zasad. Należy pamiętać, że uczniowie nie mają takich obowiązków jak dorośli pracownicy, dlatego program budowania świadomości powinien być dostosowany do specyfiki szkolnej. Obejmuje on całą społeczność szkoły - zarówno pracowników, jak i uczniów - wspólnie stojącą po jednej stronie w walce z cyberzagrożeniami.

W niniejszym opracowaniu wykorzystano publikację M. Pękali: „*Podręcznik dla szkół średnich wspierający utrzymanie właściwego poziomu bezpieczeństwa informacji szkoły oraz wspierający edukację i świadomość w obszarze cyberbezpieczeństwa*”, projekt nr 2023-2-PL01-KA210-VET-000176822.

I. Charakterystyka Szkoły Podstawowej nr 6 z Oddziałami Integracyjnymi im. Króla Władysława Jagiełły w Sochaczewie

1. Informacje ogólne

Szkoła Podstawowa nr 6 z Oddziałami Integracyjnymi im. Króla Władysława Jagiełły w Sochaczewie jest szkołą publiczną działającą na podstawie art. 14 Ustawy z dnia 14 grudnia 2016 r. – Prawo oświatowe (Dz. U. z 2024 r. poz. 737, 854, 1562, 1635 i 1933 oraz z 2025 r. poz. 619, 620 i 622) oraz Uchwały nr XXXVII/405/18 Rady Miejskiej w Sochaczewie z dnia 27 czerwca 2018 r. w sprawie nadania imienia oraz zmiany nazwy Szkoły Podstawowej Nr 6 w Sochaczewie ul. Stanisława Staszica 106, 96-500 Sochaczew (Dz. Urz. Województwa Mazowieckiego z dnia 4 lipca 2018 r., poz. 6780). Organem prowadzącym jest Gmina Miasto

Sochaczew, a organem sprawującym nadzór pedagogiczny – Mazowiecki Kurator Oświaty w Warszawie.

Budynek szkoły znajduje się w Sochaczewie (woj. mazowieckie) przy ulicy Stanisława Staszica 106.

Placówka jest publiczną ośmioklasową szkołą podstawową w rozumieniu ustawy. W skład szkoły wchodzą: 8-letnia szkoła podstawowa oraz oddziały przedszkolne. Szkoła pełni funkcję szkoły obwodowej dla uczniów zamieszkałych w obwodzie, którego granice ustalone są w Uchwale nr XXIV/264/17 Rady Miejskiej w Sochaczewie z dnia 24 marca 2017 r. w sprawie dostosowania sieci szkół podstawowych i gimnazjów do nowego ustroju szkolnego w Gminie Miasto Sochaczew

2. Przywołania normatywne

- 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);
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji). Tekst mający znaczenie dla EOG.
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2025/327 z dnia 11 lutego 2025 r. w sprawie europejskiej przestrzeni danych dotyczących zdrowia oraz zmiany dyrektywy 2011/24/UE i rozporządzenia (UE) 2024/2847 (EHDS)
- Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2019 r. poz. 1781);
- Ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania 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 (ogólne rozporządzenie o ochronie danych) (Dz.U. 2019 poz. 730)
- Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U.2024.632);

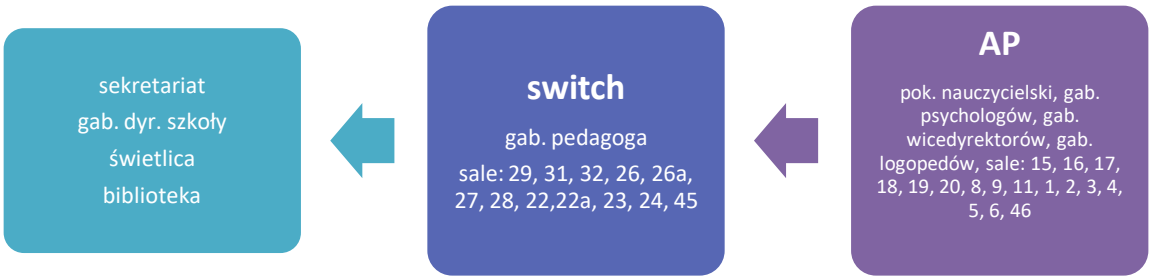
– Ustawa z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz.U. 2023 poz. 1440)
– Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2024 poz. 773).

3. Infrastruktura systemu teleinformatycznego szkoły

Istniejąca struktura teleinformatyczna Szkole Podstawowej nr 6 z Oddziałami Integracyjnymi im. Króla Władysława Jagiełły w Sochaczewie opiera się o sieć podłączoną do naukowo-akademickiej sieci światłowodowej **NASK.** Szkoła od 2019 roku jest fizycznie podłączona do sieci internet dzięki podpisanej umowie z NASK (Ogólnopolska Sieć Edukacyjna) Do sieci informatycznej podłączonych jest ponad 88 komputerów (58 do celów dydaktycznych) i urządzeń peryferyjnych (drukarki, urządzenia wielofunkcyjne, kopiarki). Cała sieć pracuje w technologii Ethernet. Szkielet sieci stanowi światłowód w technologii jednomodowej (pracuje na urządzeniach o symetrycznej przepustowości 100 Mb/s i więcej). Styk sieci szkoły z siecią OSE realizowany jest łączem o przepustowości 1 GB w technologii Ethernet i zlokalizowany jest w węźle sieci budynku szkoły. Pierwszym urządzeniem do obsługi routingu jest switch HUAWEI (S5720-28TP-LI-AC), który służy do dystrybucji sygnału do poszczególnych węzłów sieci w technologii 100 Mb/s z wykorzystaniem WLAN.

W sieci szkoły można wyróżnić następujące podsieci logiczne

– sieć uczniowska;
– sieć nauczycielska;
– sieć administracji.



Rysunek 1. Schemat infrastruktury informatycznej Szkoły Podstawowej nr 6 z Oddziałami Integracyjnymi im. Króla Władysława Jagiełły w Sochaczewie

Na terenie szkoły istnieje system bezprzewodowego dostępu do internetu. Umożliwia on dostęp do sieci tylko zarejestrowanym użytkownikom (certyfikaty OSE/NASK).
Ze względu na strukturę organizacyjną szkoły, podział logiczny sieci teleinformatycznej oraz posiadane zasoby bazodanowe można wyodrębnić następujących uprawnionych użytkowników:

Tabela 1. Przyporządkowanie elementów sieci do zakresu uprawnionych czynności

Elementy sieci	**Odpowiedzialni**	**Zakres działania**
Sieć szkolna (software)	dyrektor, wicedyrektor, wyznaczeni nauczyciele	strona WWW, nadzór nad strukturą i podziałem logicznym sieci
Sieć szkolna (hardware)	kierownik gospodarczy, zewnętrzna firma	nadzór nad poprawnością działania sieci komputerowej (usuwanie usterek, naprawa gniazd RJ-45, konfiguracja switchy, konfiguracja rutera)
Sieć administracyjna	dyrektor, wicedyrektor, wyznaczeni pracownicy administracyjni	Vulcan Optivum (Kadry, Sekretariat), e-ZUS, Rekrutacja, ……
Sieć świetlicowa	kierownik świetlicy, nauczyciele świetlicy	rejestrator wejścia i wyjścia podopiecznych do- i ze świetlicy
Systemu nauczania, w tym nauczania zdalnego	dyrektor, wicedyrektor, nauczyciele	nadawanie i odbieranie uprawnień dla nauczycieli, zastępstwa za nieobecnych nauczycieli (dyrektor, wicedyrektor, kier. świetlicy), nadawanie uprawnień dla uczniów i rodziców (wychowawcy)
Poczta szkolna	dyrektor, wicedyrektor, wyznaczeni pracownicy AiO	poczta
Biblioteka szkolna	biblioteka szkoły	nauczyciele-bibliotekarze, wicedyrektor

II. Polityka Bezpieczeństwa Informacji (PBI)

Właściwości dokumentu

Nazwa	**Polityka Bezpieczeństwa Informacji**

Zatwierdzanie i nadzór	Dyrektor Szkoły
Kontrola merytoryczna	Inspektor Ochrony Danych
Częstotliwość przeglądu	Raz w roku lub po każdej znaczącej zmianie w procesie
Lokalizacja przechowywania	Sekretariat szkoły

Historia wersji

Wersja	Data	Autor	Opis zmian
01	13.09.2022	Szkoła Podstawowa nr 6 z Oddziałami Integracyjnymi im. Króla Władysława Jagiełły w Sochaczewie	Opracowanie dokumentu
02	29.05.2025	Szkoła Podstawowa nr 6 z Oddziałami Integracyjnymi im. Króla Władysława Jagiełły w Sochaczewie	Zmiana podstaw prawnych
03	18.08.2025	Szkoła Podstawowa nr 6 z Oddziałami Integracyjnymi im. Króla Władysława Jagiełły w Sochaczewie	Zmiana struktury dokumentu, zmiany aktów normatywnych wyższego rzędu

1. Wprowadzenie

Odpowiedzialność za bezpieczeństwo informacji spoczywa na wszystkich pracownikach, klientach oraz kierownictwie Szkoły. Z kolei uczniowie odpowiadają za przestrzeganie wytycznych dotyczących bezpieczeństwa informacji przekazywanym im przez Dyrekcję Szkoły i nauczycieli. Szkoła prowadzi działalność edukacyjną w sposób, który chroni pracowników, uczniów, rodziców i klientów przed niepożądanymi zdarzeniami bezpieczeństwa, które wpływają na poufność, integralność i/lub dostępność przetwarzanych informacji.

Celem dokumentu jest ustanowienie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w Szkole, w tym definicja odpowiedzialności za jego funkcjonowanie i określenie ram ustalania konkretnych celów w zakresie bezpieczeństwa. Kierownictwo Szkoły zapewnia, że bezpieczeństwo informacji jest ważnym aspektem działalności Szkoły i deklaruje pełne zaangażowanie we wdrażanie i zarządzanie SZBI m.in. poprzez zapewnienie odpowiednich zasobów organizacyjnych i finansowych.

4. Cel Polityki Bezpieczeństwa Informacji

Celem SZBI jest zapewnienie bezpieczeństwa informacji zgodnie ze zidentyfikowanymi potrzebami i oczekiwaniami Dyrekcji, Pracowników, Uczniów, Rodziców i innych interesariuszy Szkoły.

5. Wspierane cele szkoły:

- zaangażowanie i wsparcie kierownictwa szkoły w działaniach na rzecz bezpieczeństwa informacji;
- ustanowienie odpowiednich zabezpieczeń w oparciu zidentyfikowane ryzyko;
- zgodność z wewnętrznymi i zewnętrznymi zobowiązaniami;
- zgodność z wymaganiami Organu Prowadzącego Organu Sprawującego Nadzór Pedagogiczny oraz innych instytucji, z którymi placówka jest związana umownymi zobowiązaniami w zakresie bezpieczeństwa informacji;
- zgodność z obowiązującymi wymogami dotyczącymi prywatności danych, w tym wymogom RODO.

Niniejsza Polityka Bezpieczeństwa Informacji jest wspierana i uzupełniana przez inne polityki, procedury oraz pozostałą dokumentację SZBI oraz Polityki RODO.

6. Zakres PBI

Niniejsza Polityka ma zastosowanie dla wszystkich zarządzanych przez Szkołę procesów i informacji, w tym a także usług chmurowych, oprogramowania, urządzeń, personelu i pomieszczeń.

7. Role i obowiązki w PBI

Mając na uwadze konieczność integracji procesów związanych z bezpieczeństwem informacji z bieżącą działalnością Szkoły, a także obowiązki operacyjne i sprawozdawcze, kierownictwo Szkoły określi odpowiednią strukturę ról i obowiązków, biorąc pod uwagę konieczność przypisania odpowiedzialności za całościowe działanie Polityki Bezpieczeństwem Informacji.

Inspektor Ochrony Danych w szkole jest odpowiedzialny za utrzymanie Polityki Bezpieczeństwa Informacji, wspieranie jej celów i doradztwo w zakresie jej wdrażania. Kadra (nauczyciele, wychowawcy, pedagodzy, pracownicy AiO) będzie odpowiedzialna za wdrożenie i realizację zapisów Polityki Bezpieczeństwa Informacji wraz z dokumentami towarzyszącymi w swoich obszarach. Uczniowie muszą być informowani o swoich obowiązkach w zakresie bezpieczeństwa informacji.

III. Role i obowiązki w SZBI

Właściwości dokumentu

Nazwa	**Polityka Bezpieczeństwa Informacji**
Zatwierdzanie i nadzór	Dyrektor Szkoły
Kontrola merytoryczna	Inspektor Ochrony Danych
Częstotliwość przeglądu	Raz w roku lub po każdej znaczącej zmianie w procesie
Lokalizacja przechowywania	Sekretariat szkoły

Historia wersji

Wersja	**Data**	**Autor**	**Opis zmian**
01	13.09.2022	Szkoła Podstawowa nr 6 z Oddziałami Integracyjnymi im. Króla Władysława Jagiełły w Sochaczewie	Opracowanie dokumentu
02	29.05.2025	Szkoła Podstawowa nr 6 z Oddziałami Integracyjnymi im. Króla Władysława Jagiełły w Sochaczewie	Zmiana podstaw prawnych
03	18.08.2025	Szkoła Podstawowa nr 6 z Oddziałami Integracyjnymi im. Króla Władysława Jagiełły w Sochaczewie	Zmiana struktury dokumentu, zmiany aktów normatywnych wyższego rzędu

1. Cel

Celem dokumentu jest zdefiniowanie ról i obowiązków, które są istotne dla efektywnego działania Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).

2. SZBI - role i obowiązki

- szkoła zidentyfikowała role i obowiązki w ramach SZBI.
- Role w SZBI mogą być łączone i wykonywane przez te same osoby, zgodnie z możliwościami placówki.

3. Dyrektor szkoły

Dyrektor szkoły zapewnia wizję, wspiera wdrożenie i funkcjonowanie SZBI oraz zapewnia ogólne wytyczne, kierunek i wsparcie dla funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji w Szkole. Do obowiązków Dyrektora szkoły należy:

- akceptacja celów i zakresu SZBI, z uwzględnieniem celów szkoły i wymagań prawnych;
- wyznaczanie ról i zatwierdzanie zmian organizacyjnych związanych z SZBI;
- zatwierdzenie Polityki Bezpieczeństwa Informacji;
- zatwierdzanie dokumentów SZBI wynikających z Polityki Bezpieczeństwa Informacji;
- zatwierdzanie akceptowalnego poziomu ryzyka, wyników analizy ryzyka i planów postępowania z ryzykiem w procesach objętych SZBI;
- zatwierdzanie budżetu związanego z SZBI;
- zatwierdzanie wyników audytów i przeglądów SZBI;
- podejmowanie decyzji w procesie zarządzania kryzysowego.

4. Inspektor Ochrony Danych

Inspektor Ochrony Danych jest odpowiedzialny za działanie SZBI oraz przygotowanie wytycznych i nadzór nad bezpieczeństwem informacji. Do jego obowiązków należą:

- wprowadzanie zmian i nadzór nad spójnością dokumentacji SZBI oraz przeprowadzanie jej cyklicznych przeglądów i aktualizacji;
- podnoszenie świadomości pracowników i uczniów w zakresie zagadnień bezpieczeństwa informacji, w szczególności nadzór nad Programem Budowania Świadomości w Obszarze Cyberbezpieczeństwa w Szkole;
- wdrażanie i nadzór nad przestrzeganiem zasad i mechanizmów związanych z bezpieczeństwem informacji;
- ocena skuteczności realizacji wymagań wynikających z przepisów bezpieczeństwa informacji.

Istotne jest by dokumentacja SZBI i Polityki dotyczące ochrony danych były ze sobą zintegrowane. W rzeczywistości zgodność z RODO to jeden z celów SZBI.

IOD pomaga personelowi szkoły we wszystkich kwestiach związanych z ochroną danych. Do obowiązków IODa należą:

1. informowanie i doradzanie Dyrektorowi oraz pracownikom, o ich obowiązkach wynikających z przepisów o ochronie danych osobowych;
2. monitorowanie zgodności ze wszystkimi przepisami dotyczącymi ochrony danych, w tym w zakresie audytów, działań uświadamiających, a także szkolenia personelu zaangażowanego w operacje przetwarzania;

3. udzielanie porad w przypadku przeprowadzenia oceny ryzyka bezpieczeństwa informacji i monitorowanie jej wydajności (załącznik 3);
4. działanie jako punkt kontaktowy dla wniosków od osób fizycznych dotyczących przetwarzania ich danych i wykonywania ich praw;
5. współpraca z organami ochrony danych i pełnienie funkcji punktu kontaktowego dla organów ochrony danych w kwestiach związanych z przetwarzaniem danych;
6. wsparcie prac związanych z utrzymaniem i doskonaleniem SZBI w obszarze ochrony danych;
7. wsparcie w doborze środków ochrony odpowiednich do ilości i zakresu przetwarzania danych;
8. wsparcie prac projektowych nad systemami przetwarzającymi dane osobowe;
9. klasyfikacja operacji przetwarzania danych według ilości, rodzaju i celu przetwarzania;
10. prowadzenie ewidencji operacji przetwarzania danych.

5. Nauczyciel/Pracownik

Wszystkie osoby, które mają dostęp do zasobów informacyjnych Szkoły, w tym pracownicy, praktykanci, klienci, zewnętrzni dostawcy usług mają obowiązek:

1. przestrzegania Polityki Bezpieczeństwa Informacji i zasad bezpieczeństwa informacji ustanowionych w pozostałych dokumentach powiązanych;
2. przestrzegania Polityki Ochrony Danych i związanych z nią przepisów;
3. zgłaszania incydentów związanych z bezpieczeństwem informacji;
4. udział w programie szkoleń z obszaru bezpieczeństwa informacji.

6. Uczeń

Wszyscy uczniowie, mają dostęp do zasobów informacyjnych szkoły wyłącznie w zakresie wynikającym z zajęć, w których uczestniczą. Obowiązkiem uczniów jest:

1. przestrzeganie Polityki Bezpieczeństwa Informacji i zasad bezpieczeństwa informacji ustanowionych w pozostałych dokumentach powiązanych;
2. przestrzeganie Polityki Ochrony Danych i związanych z nią przepisów;
3. zgłaszanie incydentów związanych z bezpieczeństwem informacji;
4. udział w programie szkoleń z obszaru bezpieczeństwa informacji;
5. stosowanie się do poleceń nauczycieli i pozostałej kadry w zakresie korzystania z urządzeń elektronicznych i internetu na obszarze szkoły;

IV. Zasady bezpieczeństwa Informacji

Właściwości dokumentu

Nazwa	**Polityka Bezpieczeństwa Informacji**
Zatwierdzanie i nadzór	Dyrektor Szkoły
Kontrola merytoryczna	Inspektor Ochrony Danych
Częstotliwość przeglądu	Raz w roku lub po każdej znaczącej zmianie w procesie
Lokalizacja przechowywania	Sekretariat szkoły

Historia wersji

Wersja	**Data**	**Autor**	**Opis zmian**
01	13.09.2022	Szkoła Podstawowa nr 6 z Oddziałami Integracyjnymi im. Króla Władysława Jagiełły w Sochaczewie	Opracowanie dokumentu
02	29.05.2025	Szkoła Podstawowa nr 6 z Oddziałami Integracyjnymi im. Króla Władysława Jagiełły w Sochaczewie	Zmiana podstaw prawnych
03	18.08.2025	Szkoła Podstawowa nr 6 z Oddziałami Integracyjnymi im. Króla Władysława Jagiełły w Sochaczewie	Zmiana struktury dokumentu, zmiany aktów normatywnych wyższego rzędu

1. Ogólne wytyczne

1. Użytkownik, to każda osoba (pracownik szkoły oraz uczeń) korzystająca z zasobów informatycznych, w tym internetu, szkoły;
2. szkoła dostarcza pracownikowi sprzęt informatyczny jako narzędzie umożliwiające wykonywanie pracy (zadań) na rzecz szkoły;
3. użytkownik ponosi odpowiedzialność za powierzony mu sprzęt i oprogramowanie oraz sposób ich działania;
4. użytkownik ponosi konsekwencje finansowe i prawne posiadania nielegalnego oprogramowania na sprzęcie teleinformatycznym powierzonym mu przez szkołę;
5. surowo zabrania się testowania i/lub łamania zabezpieczeń urządzeń i systemu teleinformatycznego udostępnianego przez szkołę;
6. sprzęt powierzony przez Szkołę nie może być udostępniany osobom nieupoważnionym;

7. zabronione jest samodzielne dokonywanie jakichkolwiek zmian w konfiguracji dostarczonych urządzeń lub oprogramowania, chyba że zmiana została zaakceptowana przez Inspektora Ochrony Danych. Dotyczy to w szczególności zmian w ustawieniach związanych z zabezpieczeniami;
8. każdy użytkownik zobowiązany jest do zapoznania się ze wszystkimi regulacjami, instrukcjami i procedurami wewnętrznymi, które są wdrażane przez dyrekcję szkoły.

2. Praca zdalna

Uwaga! Zapisy dotyczą sprzętu zakupionego przez szkołę, a nie np. prywatnego laptopa wykorzystywanego do pracy przez nauczyciela. Do tej sytuacji będzie obnosił się punkt mówiący o pracy na prywatnych urządzeniach albo BYOD (Bring Your Own Device).

1. Wynoszenie powierzonego sprzętu mobilnego poza siedzibę szkoły musi być uzasadnione obowiązkami wykonywanymi przez użytkownika;
2. Użytkownik sprzętu mobilnego ma obowiązek go chronić. Należy unikać ryzykownych zachowań, które mogą obejmować m.in.:
   - pozostawienie sprzętu bez nadzoru (w samochodzie, pokojach hotelowych itp.),
   - pozostawienie torby z laptopem bez nadzoru,
   - niewylogowywanie się użytkownika w przypadku czasowej nieobecności lub braku aktywności,
   - ustawienie monitorów umożliwiające podgląd zawartości ekranu osobom nieupoważnionym.
3. W przypadku zagubienia powierzonego sprzętu mobilnego używanego poza szkołą, użytkownik powinien zwłocznie zgłosić powyższy fakt do Inspektora Ochrony Danych, a w przypadku kradzieży - dodatkowo zgłosić ten fakt Policji.

3. Bezpieczne logowanie i zarządzanie hasłami

Polityka haseł powinna być zgodna z bieżącymi wytycznymi CERT Polska[1].

1. użytkownik ponosi odpowiedzialność za wszelkie czynności wykonywane przy użyciu jego identyfikatora i hasła.
2. hasła użytkowników lub inne poświadczenia podlegają specjalnej ochronie.
3. każdy użytkownik mający dostęp do systemu informatycznego szkoły zobowiązany jest do:

[1] https://cert.pl/posts/2022/01/kompleksowo-o-haslach/

- zachowania w tajemnicy wszystkich swoich haseł lub innych danych uwierzytelniających wykorzystywanych do pracy w systemie informatycznym szkoły,
- niezwłocznej zmiany hasła w przypadku podejrzenia lub faktycznego ujawnienia hasła;
- używać haseł o minimalnej długości 14 znaków, hasło musi zawierać wielkie i małe litery oraz cyfry i/lub znaki specjalne;
- zaleca się stosowanie uwierzytelniania dwuskładnikowego wszędzie gdzie to możliwe.

4. hasła nie mogą być zapisywane w żaden jednoznaczny sposób (np. pliki tekstowe, notatnik itp.).
5. dozwolone jest korzystanie z zatwierdzonego systemu dedykowanego do bezpiecznego przechowywania haseł (menedżer haseł)
6. zabronione jest logowanie się do systemu przy użyciu danych uwierzytelniających innego użytkownika.
7. użytkownik zobowiązany jest do blokowania komputera, który nie jest obecnie używany, przed nieautoryzowanym dostępem, wymuszając chronioną hasłem blokadę ekranu (zasada czystego ekranu).

4. Korzystanie z internetu, poczty elektronicznej, komunikatorów internetowych w szkole

1. Korzystanie z internetu w szkole, musi bezwzględnie wiązać się z unikaniem ryzykownych zachowań, w tym:
   - przeglądania stron internetowych zawierających treści niepożądane, w szczególności stron pornograficznych, rasistowskich, nawołujących do nienawiści, promujących sekty, hazardowych lub w jakikolwiek sposób obrażających uczucia innych osób lub naruszających szeroko rozumiane zasady współżycia społecznego;
   - przeglądanie stron internetowych zawierających wszelkiego rodzaju złośliwe oprogramowanie (np. malware, exploity itp.);
   - przeglądanie stron internetowych zawierających kody umożliwiające złamanie lub ominięcie ochrony praw autorskich;
   - pobieranie z internetu, instalowanie, przechowywanie lub rozpowszechnianie oprogramowania, które nie jest autoryzowane przez szkołę.

2. Zabronione jest uzyskiwanie dostępu do stron internetowych, które są wykorzystywane do nielegalnej dystrybucji treści (utworów) z naruszeniem przepisów o ochronie praw autorskich;
3. Skrzynki pocztowe z podanym przez szkołę adresem e-mail mogą być wykorzystywane wyłącznie do korespondencji związanej z działalnością placówki;
4. Nie zaleca się przekazywania wiadomości pocztowych do skrzynek niezwiązanych ze szkołą, w szczególności prywatnych;
5. W przypadku wysyłania załączników stanowiących tajemnicę szkoły lub chronionych odpowiednimi przepisami prawa (np. zawierających dane osobowe), załącznik taki musi być zaszyfrowany hasłem spełniającym wymagania określone w punkcie trzecim zasad. Hasło nie może zostać wysłane tym samym kanałem komunikacyjnym, co wiadomość.

5. Wymagania dotyczące korzystania do pracy lub nauki w szkole z urządzeń prywatnych użytkowników (BYOD)

1. Można stosować wyłącznie urządzenia i systemy wspierane przez producenta (dla których dostarczane są poprawki bezpieczeństwa);
2. W przypadku:
   - utraty prywatnego sprzętu (np. w wyniku utraty lub kradzieży) służącego do przetwarzania poufnych danych Szkoły,
   - podejrzenie ujawnienia poufnych danych, użytkownik niezwłocznie informuje o wystąpieniu takiego zdarzenia Inspektora Ochrony Danych.
3. W przypadku zagubienia prywatnego urządzenia użytkownika, jego sprzedaży lub zakończenia współpracy ze szkołą, użytkownik wyraża zgodę na usunięcie przez szkołę wybranych lub wszystkich (w zależności od możliwości technicznych) danych należących do szkoły.
4. W przypadku zakończenia współpracy ze szkołą, zaprzestania korzystania z urządzenia na potrzeby BYOD lub utylizacji prywatnego urządzenia służącego do przetwarzania danych na rzecz Szkoły, użytkownik zobowiązuje się do skontaktowania się z Inspektorem Ochrony Danych szkoły w celu trwałego usunięcia z niego danych będących własnością szkoły.

6. Zabezpieczanie informacji

1. Obowiązkiem użytkownika jest podjęcie kroków w celu zabezpieczenia informacji, które opracowuje lub tworzy. Użytkownik ma następujące opcje zabezpieczania informacji (plików):
   - zaleca się umieszczanie danych w katalogu/nośniku wskazanym przez Inspektora Ochrony Danych,
   - korzystanie z zaakceptowanego przez szkołę rozwiązania do przechowywania danych.
2. Inne rozwiązania do przechowywania danych szkoły są zabronione.
3. Zabronione jest przetwarzanie informacji na zewnętrznych nośnikach danych (np. pen-drive, dysk przenośny), które nie są własnością szkoły i nie zostały zabezpieczone.
4. Zabronione jest ujawnianie informacji (danych, plików) należących do szkoły osobom nieupoważnionym.

7. Bezpieczne miejsce pracy

W celu ograniczenia ryzyka nieuprawnionego dostępu, utraty lub uszkodzenia informacji w godzinach pracy i poza ich godzinami, użytkownik zobowiązany jest:

- przestrzegać zasady nie pozostawiania otwartych i niezabezpieczonych drzwi umożliwiających dostęp do pomieszczenia,
- zabezpieczać klucze do pomieszczeń służbowych, a w przypadku ich zgubienia niezwłocznie poinformować o tym fakcie przełożonych,
- przechowywać dokumenty papierowe i wymienne nośniki informacji w odpowiednio zabezpieczonych meblach biurowych,
- po zakończeniu pracy zorganizować swoje miejsce pracy, zapobiegając nieautoryzowanemu dostępowi do dokumentów zawierających chronione informacje (zasada „czystego biurka").

8. Zgłaszanie incydentów i zdarzeń

1. W przypadku zauważenia zdarzenia, które może być świadectwem lub dowodem naruszenia bezpieczeństwa, nieprawidłowego działania oprogramowania, błędów lub awarii systemu, użytkownik powinien:
   - zaprzestać pracy przy komputerze,

- niezwłocznie poinformować informatyka i/lub bezpośredniego przełożonego/Dyrekcję o zajściu, który podejmuje analizę w zakresie konieczności odłączenia komputera od sieci.

2. Zgłoszenie można wykonywać:
   - pocztą elektroniczną
   - osobiście osobom, o których mowa w pkt. 1
3. Wniosek powinien zawierać:
   - wskazanie użytkownika lub obszaru, który był świadkiem/uczestnikiem zdarzenia,
   - wskazanie lub identyfikacja systemu, którego dotyczy incydent,
   - przybliżony czas wystąpienia incydentu,
   - opis okoliczności i miejsc, w których doszło do zdarzenia oraz symptom /opis zdarzenia.

9. Sankcje dyscyplinarne

1. nieprzestrzeganie zasad określonych w niniejszych Zasadach może prowadzić do odpowiednich sankcji dyscyplinarnych;
2. w przypadku, gdy naruszenie określonych zasad doprowadzi do podejrzenia naruszenia prawa, Dyrekcja przekaże wszelkie dowody organom ścigania do dalszego postępowania.
3. każdy użytkownik zobowiązany jest do respektowania wszelkich regulaminów, instrukcji i procedur wewnętrznych, które są wprowadzane przez dyrektora;
4. w przypadku wprowadzenia nowego dokumentu (regulamin, procedura, instrukcje itp.), Inspektorem Ochrony Danych i/lub bezpośredni przełożony jest odpowiedzialny za zapewnienie skutecznego sposobu komunikowania powyższych przepisów użytkownikom;
5. nieznajomość aktualnych przepisów bezpieczeństwa nie może być podstawą do domniemania niewinności użytkownika i może prowadzić do postępowania dyscyplinarnego.

V. Program Budowania Świadomości w Zakresie Cyberbezpieczeństwa w Szkole

Właściwości dokumentu

Nazwa	**Polityka Bezpieczeństwa Informacji**
Zatwierdzanie i nadzór	Dyrektor Szkoły
Kontrola merytoryczna	Inspektor Ochrony Danych
Częstotliwość przeglądu	Raz w roku lub po każdej znaczącej zmianie w procesie
Lokalizacja przechowywania	Sekretariat szkoły

Historia wersji

Wersja	Data	Autor	Opis zmian
01	18.08.2025	Szkoła Podstawowa nr 6 z Oddziałami Integracyjnymi im. Króla Władysława Jagiełły w Sochaczewie	Przygotowanie projektu dokumentu

1. Cel

Celem niniejszej polityki jest zapewnienie, że wszyscy pracownicy szkoły oraz uczniowie, otrzymują odpowiednie szkolenia oraz regularne aktualizacje zasad i procedur organizacyjnych dotyczących bezpieczeństwa informacji. Dyrektor dąży do zapewnienia bezpieczeństwa uczniom i pracownikom poprzez szkolenia i inne działania podnoszące świadomość w obszarze cyberzagrożeń.

2. Zakres treści

Program budowania świadomości porusza następujące zagadnienia:

- zasady bezpieczeństwa informacji;
- odpowiedzialność za działania uczniów i pracowników oraz sankcje dyscyplinarne;
- informacje dotyczące zgłaszania incydentów;
- edukacja w obszarze szeroko pojętego bezpieczeństwa cyfrowego.

Plan Komunikacji i Szkoleń w zakresie cyberbezpieczeństwa stanowi integralną część Programu. Załącznik jest aktualizowany co roku przed rozpoczęciem roku szkolnego.

3. Role i obowiązki

Inspektor Ochrony Danych lub inny pracownik szkoły na zlecenie dyrektora jest odpowiedzialny za całościowe funkcjonowanie Programu. Nauczyciele wspomagają realizację programu. Uczniowie zobowiązani są do uczestnictwa w Programie w ramach zajęć w szkole.

4. Plan Komunikacji i Szkoleń w Zakresie Cyberbezpieczeństwa

Co komunikujemy?	**Kiedy komunikujemy?**	**W jaki sposób komunikujemy? (metoda szkoleniowa)**	**Kto jest odpowiedzialny /szkoli?**	**Dla kogo?**	**Czy przeprowadzono zgodnie z planem?**	**Dowody na realizacje zgodną z planem**
Polityki Bezpieczeństwa Informacji Szkoły i Zasady Bezpieczeństwa Informacji	Wrzesień	Rada Pedagogiczna	Dyrekcja / wyznaczony pracownik	Nauczyciele i pracownicy administracyjni		
Zasady Bezpieczeństwa Informacji	Wrzesień	Godzina wychowawcza - prezentacja zasad w formie wykładu	Wychowawca	Uczniowie		
Lekcja: Phishing	Październik	Godzina wychowawcza - prezentacja szkoleniowa i warsztat	Wychowawca/nauczyciel informatyki	Uczniowie		
Lekcja: Hasła - jak tworzyć i zarządzać hasłami?	Listopad	Godzina wychowawcza - prezentacja szkoleniowa i warsztat	Wychowawca/nauczyciel informatyki			
Incydenty - jak reagować na zagrożenia?	Grudzień	Godzina wychowawcza - prezentacja szkoleniowa i warsztat	Wychowawca/nauczyciel informatyki	Uczniowie		
Cyberprzemoc - jak jej zapobiegać i na nią reagować?	Styczeń	Godzina wychowawcza - prezentacja szkoleniowa i warsztat	Wychowawca/pedagog	Uczniowie		

Dezinformacja - jak rozpoznać fałszywe informacje?	Luty/Marzec	Godzina wychowawcza - prezentacja szkoleniowa i warsztat	Wychowawca	Uczniowie		
Wizyta przedstawiciela policji	Cały rok, np. kwiecień	Szkolenie dla całej szkoły	Zaproszony przedstawicieli	Uczniowie i nauczyciele		
Ad hoc - wiadomości dotyczące bieżących zagrożeń cybernetycznych	Cały rok szkolny	Newsletter oraz w trakcie zebrań, godzin wychowawczych	Dyrekcja / wyznaczony pracownik	Wszyscy (uczniowie, nauczyciele, rodzice)		
Sprawozdania z udziału szkoły w konferencjach/wydarzeniach dotyczących bezpieczeństwa cyfrowego	po wydarzeniu, np.. Maj	Zebranie, prezentacja raportu	Dyrekcja / wyznaczony pracownik	Dyrekcja, nauczyciele, rodzice		
Prezentacje uczniów biorących udział w projektach/konkursach dotyczących bezpieczeństwa cyfrowego	po wydarzeniu, np.. Czerwiec	Zebranie, specjalne wydarzenie poświęcone cyberbezpieczeństwu	Uczniowie z opiekunem	Uczniowie i nauczyciele		

VI. Załączniki

1. Załącznik nr 1.
Zgłoszenie naruszenia bezpieczeństwa systemu informatycznego

DO:	**Inspektor Ochrony Danych**			
OD:	Nazwisko i imię	Stanowisko	Telefon	Podpis
Data i czas zajścia/zgłoszenia incydentu:				
Opis incydentu:				
Jakie przeciwdziałania zostały podjęte?				
Kto uczestniczył w incydencie?				
Kto został poinformowany o incydencie?				

Nazwisko (czytelne) i podpis osoby przyjmującej zgłoszenie

2. Załącznik nr 2.
Wniosek o nadanie uprawnień dla użytkownika w systemie informatycznym

- ☐ Nowy użytkownik
- ☐ Modyfikacja uprawnień
- ☐ Odebranie uprawnień w systemie

Dotyczy systemu lub aplikacji *(nazwa aplikacji lub bazy danych , w której przetwarzane są dane osobowe*):

Imię i nazwisko użytkownika:	**Jednostka organizacyjna**	
Pokój nr (jeśli dotyczy):	**Adres email:**	
Posiada upoważnienie do przetwarzania danych osobowych:	**TAK**	**NIE**
Data zgłoszenia:	**Przełożony użytkownika systemu:**	

Decyzja w sprawie nadania uprawnień dla użytkownika

W systemie informatycznym

W odpowiedzi na wniosek z dn. …… opiniuję pozytywnie/negatywnie:

- ☐ nadanie uprawnień dla nowego użytkownika
- ☐ wyrażam zgodę na modyfikację uprawnień
- ☐ wyrażam zgodę na odebranie uprawnień w systemie

....

data pieczęć i podpis dyrektora szkoły

3. Załącznik nr 3.
Procedura oceny ryzyka bezpieczeństwa informacji

1. Cel procedury

Celem procedury jest zapewnienie że:

1) proces szacowania ryzyka jest kompletny oraz daje szczegółowe, porównywalne i odtwarzalne rezultaty;
2) kryteria oceny ryzyka są ustanowione i spójne z rzeczywistym stanem bezpieczeństwa aktywów na wydziale oraz dostarczają rzetelnych wyników na temat faktycznego poziomu ryzyka;
3) zidentyfikowano potencjalne ryzyko, opisano w kategoriach ilościowych i zarządza się nim świadomie;
4) dokumentacja szacowania ryzyka jest poddawana cyklicznym przeglądom oraz jest zatwierdzana przez kompetentny personel.

2. Przedmiot procedury

Przedmiotem procedury jest ustalenie metodyki oceny ryzyka bezpieczeństwa informacji oraz skutecznego pomiaru wyselekcjonowanych zabezpieczeń i grup zabezpieczeń poprzez mierniki oceny skuteczności. Na proces oceny ryzyka składa się:

1) Przeprowadzenie oceny ryzyka w kontekście utraty integralności, poufności i/lub dostępności danego aktywa.
2) Opracowanie planu postępowania z ryzykiem w oparciu o przyjęte kryteria akceptacji ryzyka z uwzględnieniem powtórnej analizy, w ramach wdrożonych działań korygujących i/lub zapobiegawczych, zidentyfikowanych nowych podatności i zagrożeń oraz dokonanych incydentów dotyczących naruszenia bezpieczeństwa informacji.

Procedura swoim zakresem obejmuje Szkołę Podstawową nr 6 z Oddziałami Integracyjnymi im. Króla Władysława Jagiełły w Sochaczewie, zwanej dalej: szkołą, po przeprowadzeniu inwentaryzacji aktywów zgodnie z procedurą Analizy ryzyka bezpieczeństwa informacji.

3. Kompetencje i odpowiedzialność

Inspektor Ochrony Danych lub wskazany przez dyrektora pracownik odpowiada za merytoryczne przygotowanie oraz nadzorowanie rozpowszechnianie, analizowanie, zatwierdzanie oraz przechowywanie oryginałów dokumentów szacowania ryzyka.

Każdy pracownik szkoły zobowiązany jest zgłaszać Inspektorowi Ochrony Danych lub przełożonemu zaobserwowane lub potencjalne zagrożenie oraz incydenty związane z bezpieczeństwem informacji.

4. Tryb postępowania

4.1. Ocena ryzyka

Istotą procesu oceny ryzyka jest określenie znaczenia ryzyka na podstawie porównania wyznaczonych wartości ryzyk dla zidentyfikowanych aktywów z kryteriami akceptowania ryzyka w kontekście celów strategicznych i biznesowych organizacji oraz spełnienia przepisów prawa. Ocena ryzyka powinna być prowadzona na właściwym stopniu szczegółowości z uwzględnieniem strat finansowych, wizerunkowych i informacyjnych, które organizacja doświadczyła bądź może doświadczyć w przyszłości, polega to na przypisywaniu wartości liczbowej prawdopodobieństwu wystąpienia, podatności oraz skutkom zdarzeń.
Inspektor Ochrony Danych (lub wskazany przez dyrektora pracownik) po przeprowadzeniu analizy ryzyka zgodnie z zasadami określonymi w procedurze analizy ryzyka bezpieczeństwa informacji, przedstawia opracowaną dokumentację do weryfikacji dyrektorowi. Dyrektor po zweryfikowaniu dokumentów analizy ryzyka wspólnie z powołanym zespołem przeprowadza szacowanie ryzyka. W skład zespołu wchodzą wyznaczeni pracownicy.

4.1.1. Identyfikowanie potencjalnych zagrożeń i podatności

Ocena ryzyka przeprowadzana jest dla każdego zidentyfikowanego podczas inwentaryzacji aktywa, rozpatruje trzy obszary:

- prawdopodobieństwo wystąpienia zagrożenia;
- podatność aktywów na zagrożenia;
- skutków potencjalnych zagrożeń;

biorąc pod uwagę następstwa naruszenia lub utraty:

- poufności,
- integralności,
- dostępności,

które mogą nastąpić w wyniku działań:

- umyślnych - (U),
- przypadkowych - (P),
- naturalnych - (N).

Przyjmuje się, że zagrożenia (U,P) są wynikiem działań ludzkich, natomiast źródła zagrożeń (N) są niezależne od człowieka.

Listę potencjalnych i realnych dla szkoły zagrożeń umieszczono w Tabeli 1. Wymienione zagrożenia należy uwzględnić podczas szacowania prawdopodobieństwa, podatności oraz skutków zdarzeń. Należy uwzględnić, że podatność, nie powoduje jeszcze szkody, ale należy zgodnie z Tabelą 2 oszacować stopień zabezpieczenia aktywa pod kątem zidentyfikowanych zagrożeń.

Tabela nr 1. Typowe zagrożenia - przykłady

Lp.	Rodzaj	Zagrożenie	Źródło
1	Zniszczenia fizyczne	pożar, zalanie , zanieczyszczenie, poważny wypadek, zniszczenie urządzeń lub nośników, pył, korozja, wychłodzenie	P,U,N
2	Zjawiska naturalne	zjawiska klimatyczne, zjawiska pogodowe, powódź	N
3	Naruszenie bezpieczeństwa informacji	podsłuch, kradzież nośników lub dokumentów, kradzież urządzenia, szpiegostwo, kopiowanie danych, odtworzenie wyrzuconych nośników	U
		ujawnienie informacji, dane z niewiarygodnych źródeł, sfałszowanie oprogramowania, brak spełnienia wymagań prawnych dotyczących archiwizowania dokumentacji	P,U
4	Awarie techniczne	awaria urządzenia, niewłaściwe funkcjonowanie urządzenia, niewłaściwe funkcjonowanie oprogramowania	P
		umyślne uszkodzenie urządzenia lub oprogramowania	U
5	Utrata usług	awaria systemu klimatyzacji, utrata dostaw prądu, awaria urządzenia telekomunikacyjnego	P,U,N
6	Zakłócenia spowodowane promieniowaniem	promieniowanie elektromagnetyczne, promieniowanie cieplne, impuls elektromagnetyczny	P,U,N
7	Nieautoryzowane działania	niewłaściwe funkcjonowanie urządzeń, niewłaściwe funkcjonowanie oprogramowania	P

		przeciążenie systemu informacyjnego, naruszenie zdolności utrzymania systemu informacyjnego	P,U
8	Naruszenie bezpieczeństwa funkcji	błąd użytkowania	P
		naruszenie praw	P,U
		fałszowanie praw, odmowa działania	U
		naruszenie dostępności personelu	P,U,N

Tabela 2. Typowe podatności - przykłady

Rodzaj	Przykład podatności	Przykłady zagrożeń
Sprzęt	Niezabezpieczone urządzenie do przechowywania danych	Kradzież danych lub dokumentów
	Brak staranności przy pozbywaniu się nośników	Kradzież nośników lub danych
	Niekontrolowane kopiowanie	Kradzież danych
	Wrażliwość na wilgoć, pył, zanieczyszczenie	Pył, korozja, wychłodzenie
	Wrażliwość na zmiany temperatury	Zjawiska pogodowe lub aspekty produkcyjne
	Wrażliwość na zmiany napięcia zasilania	Utrata zasilania
	Brak planów okresowej wymiany sprzętu	Zniszczenie lub awaria urządzenia lub nośników
Oprogramowanie	Brak wylogowania przy opuszczaniu stacji roboczej	Nadużycie praw
	Błędne przypisanie praw dostępu	Nadużycie praw
	Brak mechanizmów identyfikacji i uwierzytelnienia użytkownika	Fałszowanie praw
	Złe zarządzanie hasłami	Fałszowanie praw
	Brak fizycznej kontroli budynków, drzwi i okien	Kradzież nośników lub danych
	Brak skutecznej kontroli zmian	Zakłócenie procesu
Sieć	Niezabezpieczone linie telefoniczne	Podsłuch

	Złe łączenie kabli	Awaria urządzenia telekomunikacyjnego
	Brak identyfikacji i uwierzytelniania nadawcy i odbiorcy	Fałszowanie praw
	Niezabezpieczone połączenie z siecią publiczną	Nieautoryzowane użycie urządzeń
	Uszkodzenie fizyczne sieci lub kabli	Zatrzymanie procesu
Personel	Nieobecność personelu	Naruszenie danych, brak dostępności
	Niewystarczające szkolenie z bezpieczeństwa, użycia oprogramowania lub sprzętu	Błąd użytkowania
	Brak mechanizmów monitorowania	Nielegalnie przetwarzanie danych
	Praca personelu zewnętrznego lub sprzątającego bez nadzoru	Nieautoryzowane użycie urządzeń
Siedziba	Zużycie infrastruktury	Zalanie
	Brak fizycznej ochrony budynków, drzwi i okien	Kradzież, zniszczenie
Organizacja	Brak procedur regulujących bezpieczeństwo aktywów	Utrata danych, Niezgodność z przepisami prawa, Nieautoryzowany dostęp
	Brak regularnego nadzoru	Nadużycie praw
	Brak zdefiniowanego postępowania dyscyplinarnego	Kradzież urządzenia

4.1.2. Metodyka Oceny Ryzyka

Metodyka Oceny Ryzyka w szkole została ustanowiona w zgodzie z rzeczywistym stanem bezpieczeństwa aktywów w organizacji, oraz dostarcza rzetelnych wyników na temat faktycznego poziomu ryzyka. Za dane wejściowe do procesu oceny uważa się wszelkie informacje przedstawione w analizie ryzyka (dane z inwentaryzacji), a w szczególności miejsce, obecne zabezpieczenia oraz wagę przypisaną przez właściciela aktywa. Ponadto każde

szacowanie prawdopodobieństwa, podatności oraz skutków zdarzenia powinno się odbywać w relacji z Tabelą nr 1. i 2. niniejszej procedury według zadanych kryteriów:

Szacowanie prawdopodobieństwa Tabela nr 2

Badane kryterium	Ryzyko	Wartość
(Po) Prawdopodobieństwo (możliwość wystąpienia)	niskie, odległe, mało realne szanse na zdarzenie	1
	może się zdarzyć lub zdarza się sporadycznie	2
	bardzo realne szanse wystąpienia	3

Szacowanie podatności Tabela nr 3

Badane kryterium	Ryzyko	Wartość
(PR) Podatność (słabość aktywa)	aktywa bardzo dobrze zabezpieczone	1
	aktywa dostatecznie zabezpieczone	2
	aktywa słabo lub nie zabezpieczone	3

Szacowanie skutków Tabela nr 4

Badane kryterium	Ryzyko	Wartość
(S) Skutek (wpływ na organizację i/lub proces)	utrata danych nie spowoduje utrudnień w pracy przedsiębiorstwa lub danego procesu, odtworzenie danych nie wymaga dużych nakładów czasu	1
	utrata danych spowoduje zakłócenia w funkcjonowaniu i/lub wizerunku przedsiębiorstwa , odtworzenie danych jest możliwe ale pracochłonne	2
	utrata danych spowoduje zatrzymanie procesu i/lub wywoła poważne konsekwencje prawne, odtworzenie danych i reputacji będzie trudne i kosztowne.	3

4.1.3. Kategoria Ryzyka

Kategoria ryzyka zostaje ustanowiona zgodnie ze wzorem:

$$\mathbf{R = Pr \bullet Po \bullet S}$$

gdzie:

PR – Prawdopodobieństwo; **PO –** Podatność; **S -** Skutek

Wynik z działania zgodnie z poniższą tabelą należy przypisać ustanowionym kategoriom ryzyka, a następnie uruchomić czynności doskonalące bezpieczeństwo informacji w celu redukcji ryzyka do poziomu akceptowalnego. W uzasadnionych przypadkach dyrektor może zaakceptować ryzyko kategorii drugiej lub trzeciej, szczególnie gdy działania profilaktyczne odnoszą się do długoterminowych i kosztownych inwestycji na rzecz bezpieczeństwa danego aktywa.

Wytyczne do postępowania z ryzykiem Tabela nr 5

Klasa Kategorii	Kategoria Ryzyka	Wartość Ryzyka	Akceptacja Ryzyka: Tak / Nie	Działania zapobiegawcze
1	Małe	1- 7	TAK	Podejmowanie działań nie jest konieczne, zalecane jest utrzymywanie ryzyka na obecnym poziomie. Można podjąć działania doskonalące
2	Średnie	8 - 17	NIE	Należy zredukować ryzyko do poziomu akceptowalnego poprzez rozwiązania infrastrukturalne i/lub proceduralne
3	Duże	18 - 27	NIE	Należy zdecydowanie zredukować ryzyko do poziomu akceptowalnego poprzez rozwiązania infrastrukturalne i/lub proceduralne usuwając lub przenosząc aktywa w bezpieczniejsze miejsce.

4.1.4. Działania doskonalące bezpieczeństwo informacji

Procesy doskonalące bezpieczeństwo informacji prowadzone są w oparciu o podjęte działania zapobiegawcze i/lub korygujące adekwatnie do wagi potencjalnych problemów. W tym celu dyrektor uruchamia plan postępowania z ryzykiem. W wyniku tych działań należy według powyższych zasad powtórnie dokonać analizy w celu sprawdzenia skuteczności i odporności

systemu na przypadek zaistnienia zadanych w pierwszej fazie oceny zagrożeń naruszających poufność, dostępność i/lub integralność. Wynik z powtórnej analizy stanowi o ryzyku szczątkowym, które jest pozostałością po podjęciu wszystkich możliwych kroków zmierzających do unikania ryzyka, jego kontrolowania lub przeniesienia (transferu).

4.1.5. Plan postępowania z ryzykiem

Dyrektor, dla aktywów gdzie ryzyko było nieakceptowalne, formułuje plan postępowania z ryzykiem, w którym określone zostają odpowiednie działania, odpowiedzialności oraz chronologiczne priorytety w celu redukcji ryzyka do poziomu bezpiecznego - akceptowalnego. W tym celu wdraża adekwatne do wynikającego ryzyka zabezpieczenia oraz mierzy ich skuteczność. Ostatecznie zatwierdzone i wdrożone zabezpieczenia należy wpisać w dokument szacowania ryzyka w kolumnie działań zapobiegawczych i/lub korygujących w celu poddania aktywa ponownej ocenie ryzyka.

5. Wprowadzanie zmian

Dokonywanie zmian w ocenie ryzyka odbywa się w wyniku każdorazowego podjęcia działań korygujących i/lub zapobiegawczych, zidentyfikowania nowego - realnego zagrożenia oraz dokonanego incydentu naruszającego bezpieczeństwo informacji. Zapisy sporządzone w ocenie ryzyka nie ulegają przedawnieniu i są trwałe, w związku z czym każde działanie mające na celu ponowną ocenę ryzyka bezwzględnie dokonuje się w kolejnym cyklu analizy.