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

System Zarządzania Bezpieczeństwem Informacji (SZBI) w szkole

SPIS TREŚCI

Deklaracja

Zgodnie z treścią § 20 ust. 1 Rozporządzenia Rady Ministrów 2 dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, 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.

SZBI w został opracowany zgodnie z obowiązującymi przepisami prawa, na podstawie Polskiej Normy PN-ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm z rodziny ISO 27000.

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.

dyrektor szkoły

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

1.1. 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.2021.0.1082 t.j.) 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

1.2. Powołania 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);
- Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2019 r. poz. 1781);
- Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2019 r. poz. 742);
- Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2017 r. poz. 2247).

1.3. Definicje

Zamieszczone poniżej definicje mają na celu przybliżenie i usystematyzowanie terminologii stosowanej w zakresie zarządzania bezpieczeństwem informacji oraz zdefiniowanie pojęć, których znajomość jest niezbędna do zrozumienia treści niniejszego dokumentu.

W podanym słowniku pojęć podano wyłącznie definicje zawarte w normach związanych z bezpieczeństwem i audytem systemów informatycznych Zdarza się, że ujęte w słowniku terminy definiowane są odmiennie przez różne źródła. Samodzielna interpretacja nie powinna jednak wypaczyć podstawowego charakteru określenia. Słownik podzielony został na grupy tematyczne.

- **bezpieczeństwo** (security) - stan lub ochrona przed niekontrolowanymi stratami lub skutkami, kombinacja usług zapewniających poufność, integralność i dostępność;
- **bezpieczeństwo informacji** (information security) - bezpieczeństwo polegające na zachowaniu poufności, integralności i dostępności informacji;
- **System Zarządzania Bezpieczeństwem Informacji (SZBI)** - z ang. ISMS (Information Security Management System) - część całościowego systemu zarządzania oparta na podejściu wynikającym z ryzyka biznesowego, odnosząca się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji. System zarządzania obejmuje strukturę organizacyjną, polityki, planowane działania, odpowiedzialności, zasady, procedury, procesy i zasoby (aktywa);
- **polityka bezpieczeństwa** (security policy) - zestaw praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji informacji wrażliwej wewnątrz określonego systemu;
- **bezpieczeństwo informacji** (information security) - zachowanie poufności, integralności i dostępności informacji; dodatkowo mogą być brane pod uwagę inne własności, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność;
- **bezpieczeństwo systemu informatycznego** (IT security) - wszystkie aspekty związane z definiowaniem, osiąganiem i utrzymywaniem poufności, integralności, dostępności, rozliczalności, autentyczności i niezawodności systemu informatycznego;
- **aktywa** (assets) - wszystko, co ma wartość dla organizacji;
- **zasoby** - to samo, co aktywa;
- **poufność** (confidentiality) - właściwość, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom;
- **integralność** (integrity) - właściwość zapewnienia dokładności i kompletności aktywów;
- **dostępność** (availability), zwana też dyspozycyjnością - jest zdefiniowana jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów wtedy, gdy jest to potrzebne lub dostępność - właściwość bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu;
- **autentyczność** (authenticity) - właściwość zapewniająca, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana; autentyczność dotyczy takich podmiotów, jak użytkownicy, procesy, systemy i informacja;

- **niezawodność** (reliability) - właściwość oznaczająca spójne, zamierzone zachowanie i skutki
- **rozliczalność** (accountability) - właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
- **zagrożenie** (threat) - potencjalna przyczyna niepożądanego incydentu, którego skutkiem może być szkoda dla systemu lub instytucji;
- **analiza zagrożeń** (threat analysis) - badanie działań i zdarzeń, które mogą szkodliwie wpływać na system przetwarzania danych;
- **podatność** (vulnerability) - słabość zasobu lub grupy zasobów, która może być wykorzystana przez zagrożenie;
- **zdarzenie związane z bezpieczeństwem informacji** (security information event) - jest określonym stanem systemu, usługi lub sieci, który wskazuje na możliwe przełamanie polityki bezpieczeństwa informacji, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem;
- **incydent związany z bezpieczeństwem informacji** (security information incident) - pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań i zagrażają bezpieczeństwu informacji;
- **następstwa** (impact) - rezultat niepożądanego incydentu;
- **ryzyko** (risk) - prawdopodobieństwo, że określone zagrożenie wykorzysta podatność zasobu lub grupy zasobów, aby spowodować straty lub zniszczenie zasobów;
- **zabezpieczenie** (safeguard) - praktyka, procedura lub mechanizm redukujący ryzyko;
- **analiza ryzyka** (risk analysis) - systematyczne wykorzystanie informacji do zidentyfikowania źródeł i oszacowania ryzyka;
- **szacowanie ryzyka** (risk assessment) - szacowanie zagrożeń, ich wpływu, podatności informacji i urządzeń do przetwarzania informacji oraz prawdopodobieństwa ich wystąpienia;
- **ocena ryzyka** (risk evaluation) - proces porównywania oszacowanego ryzyka z określonymi kryteriami w celu określenia znaczenia ryzyka;
- **audyt bezpieczeństwa** (security audit) - niezależny przegląd i sprawdzenie zapisów oraz funkcji systemu przetwarzania danych w celu sprawdzenia prawidłowości kontroli systemowej, zapewnienia zgodności z przyjętą polityką bezpieczeństwa i procedurami działania w celu wykrycia przełamania bezpieczeństwa oraz zalecenia określonych zmian w kontroli, polityce bezpieczeństwa i procedurach;

– **badanie zgodności** (validation) - przeprowadzenie testów i dokonanie ocen bezpieczeństwa w celu ustalenia zgodności ze specyfikacją i z wymaganiami systemu bezpieczeństwa;

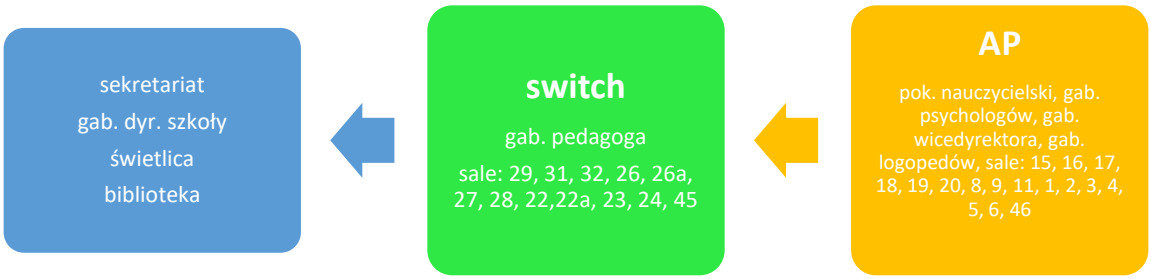
– **dokumentacja** (documentation) - pisemna lub zarejestrowana w innej formie informacja o przedmiocie oceny, wymagana do jego oceny;

– **ciągłość działania** (continuity operations) - utrzymanie niezbędnych usług systemu informatycznego po poważnej awarii w centrum informatycznym, która może być spowodowana przyczynami naturalnymi, takimi jak pożar lub trzęsienie ziemi, lub zdarzeniami wywołanymi .umyślnie, np. sabotażem

1.4. 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 (**O**gólnopolska **S**ieć **E**dukacyjna) 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 funkcjonuje system bezprzewodowego dostępu do internetu. Umożliwia on dostęp do sieci tylko zarejestrowanym użytkownikom (certyfikaty OSE/NASK).

2. System Zarządzania Bezpieczeństwem Informacji

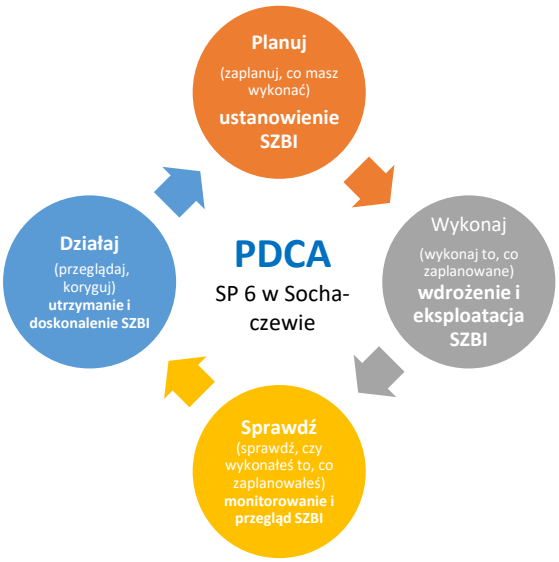
2.1. Postanowienia ogólne

Szkoła Podstawowa nr 6 z Oddziałami Integracyjnymi im. Króla Władysława Jagiełły w Sochaczewie opracowała, wdrożyła, stosuje, monitoruje, przegląda, utrzymuje i doskonali udokumentowany SZBI w kontekście całościowych działań dydaktycznych wychowawczych i opiekuńczych, z uwzględnieniem ryzyk, które występują na szkoły.

Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji zgodnego z postanowieniami międzynarodowej normy ISO 27001 jest strategiczną decyzją szkoły. Zastosowano procesowe podejście dla ustanawiania, wdrażania, stosowania, monitorowania, przeglądania, utrzymywania i doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji. Zastosowany proces opiera się na modelu Deminga **PDCA** (**P**lanuj → **W**ykonaj → **S**prawdź → **D**ziałaj):

- **P**lanuj - (ang. **P**lan) zapisz co zaplanowałeś wykonać;
- **W**ykonaj - (ang. **D**o) wykonaj to co zaplanowałeś, zrób to;
- **S**prawdź - (ang. **C**heck) sprawdź czy wykonałeś to co zaplanowałeś, czy się udało;
- **D**ziałaj - (ang. **A**ct) przeglądaj, zrób korektę by udoskonalić na przyszłość.

Działanie SZBI na szkoły jest procesem ciągłym, stale doskonalonym i dostosowywanym do zmieniających się okoliczności. Każdy z etapów dzieli się na bardziej szczegółowe działania, które dotyczą przede wszystkim polityki bezpieczeństwa, zarządzania zasobami i ryzykiem. Scalenie wszystkich działań w ciągły proces bezpiecznego zarządzania informacją, pozwoli na:



Rysunek 2. Pętla Deminga PDCA w odniesieniu do SZBI Szkoły Podstawowej nr 6 z Oddziałami Integracyjnymi im. Króla Władysława Jagiełły w Sochaczewie

- minimalizację ryzyka wycieku lub utraty cennych dla szkoły danych;
- wzrost poziomu bezpieczeństwa informacji w szkole;
- zapewnienie ciągłości funkcjonowania szkoły;
- wzrost konkurencyjności szkoły na rynku oświatowym;

- postrzeganie szkoły jako wiarygodnego, nowoczesnego, a przede wszystkim bezpiecznego partnera;
- określenie podstawowych zasad związanych z bezpiecznym przetwarzaniem informacji;
- określenie zasad postępowania w sytuacjach awaryjnych;
- zapewnienie bezpieczeństwa prawnego, przez spełnienie wymagań prawa w zakresie ochrony informacji.

2.2. Zasady ogólne

Każdy pracownik szkoły jest zapoznawany z regułami oraz z aktualnymi procedurami ochrony informacji w swojej komórce organizacyjnej. Poniższe uniwersalne zasady są podstawą realizacji polityki bezpieczeństwa informacji:

- **Zasada uprawnionego dostępu.** Każdy uprawniony pracownik przeszedł szkolenie z zasad ochrony informacji, spełnia kryteria dopuszczenia do informacji i o ile tyczy to danych osobowych podpisał stosowne oświadczenie o zachowaniu poufności;

- **Zasada przywilejów koniecznych.** Każdy pracownik posiada prawa dostępu do informacji, ograniczone wyłącznie do tych, które są konieczne do wykonywania powierzonych mu zadań;

- **Zasada wiedzy koniecznej.** Każdy pracownik posiada wiedzę o systemie, do którego ma dostęp, ograniczoną wyłącznie do zagadnień, które są konieczne do realizacji powierzonych mu zadań;

- **Zasada usług koniecznych.** szkoła świadczy tylko takie usługi, jakich wymagają przepisy zewnętrzne oraz statut placówki;

- **Zasada asekuracji.** Każdy mechanizm zabezpieczający powinien być ubezpieczony drugim, innym. W przypadkach szczególnych może być stosowane dodatkowe niezależne zabezpieczenie;

- **Zasada świadomości zbiorowej.** Wszyscy pracownicy są świadomi konieczności ochrony zasobów informacyjnych szkoły i aktywnie uczestniczą w tym procesie;

- **Zasada indywidualnej odpowiedzialności.** Za bezpieczeństwo poszczególnych elementów odpowiadają konkretne osoby;

- **Zasada obecności koniecznej.** Prawo przebywania w określonych miejscach mają tylko osoby upoważnione;

- **Zasada stałej gotowości.** System jest przygotowany na wszelkie zagrożenia. Niedopuszczalne jest tymczasowe wyłączanie mechanizmów zabezpieczających;

- **Zasada kompletności.** Skuteczne zabezpieczenie jest tylko wtedy, gdy stosuje się podejście kompleksowe, uwzględniające wszystkie stopnie i ogniwa ogólnie pojętego procesu przetwarzania informacji;

- **Zasada odpowiedniości.** Używane mechanizmy muszą być adekwatne do sytuacji;
- **Zasad akceptowanej równowagi.** Podejmowane środki zaradcze nie mogą przekraczać poziomu akceptacji.

2.3. Definicja bezpieczeństwa informacji

Utrzymanie bezpieczeństwa przetwarzanych przez Szkołę Podstawową nr 6 z Oddziałami Integracyjnymi im. Króla Władysława Jagiełły w Sochaczewie informacji rozumiane jest jako zapewnienie ich poufności, integralności i dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka związanego z zasobem stanowiącym przedmiot niniejszej Polityki.

Poniżej opisane jest rozumienie wyżej wymienionych pojęć w odniesieniu do informacji i aplikacji:

- **Poufność informacji** - rozumiana jako zapewnienie, że tylko uprawnieni pracownicy mają dostęp do informacji,
- **Integralność informacji** - rozumiana jako zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania,
- **Dostępność informacji** - rozumiana jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne,
- **Zarządzanie ryzykiem** - rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych.

Dodatkowo zarządzanie bezpieczeństwem informacji wiąże się z zapewnieniem:

- **Niezaprzeczalności odbioru** - rozumianej jako zdolność systemu szkoły do udowodnienia, że adresat informacji otrzymał ją w określonym miejscu i czasie,
- **Niezaprzeczalności nadania** - rozumianej jako zdolność systemu szkoły do udowodnienia, że nadawca informacji faktycznie ją nadał lub wprowadził do systemu w określonym miejscu i czasie.
- **Rozliczalności działań** - rozumianej jako zapewnienie, że wszystkie działania istotne dla przetwarzania informacji zostały zarejestrowane w systemie i możliwym jest zidentyfikowanie użytkownika, który działania wykonał.

Ilekroć w dokumencie jest mowa o:

- **RODO** - 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)
- **Inspektor Ochrony Danych** (**Inspektor**) - to osoba, której Administrator Danych Osobowych wyznaczył pełnienie obowiązków Inspektor Ochrony Danych w odniesieniu do systemu nadzoru nad informacją (aktywami) w odniesieniu do systemów informatycznych;
- **Administratorze Systemów Informatycznych** (**ASI**) - rozumie się przez osobę, której Administrator Danych Osobowych powierzył pełnienie obowiązków Administratora

Systemów Informatycznych w odniesieniu do systemu nadzoru nad informacją (aktywami) funkcjonującą w systemach informatycznych;

- **Administrator Danych Osobowych** (ADO) - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych
- **danych -** rozumie się przez to dane będące w posiadaniu szkoły w postaci elektronicznej lub w innej formie, będące w zbiorach szkoły, wykorzystywane przez szkołę lub osoby trzecie, a niezbędne do wykonywania jej zadań;
- **danych osobowych** - oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora, takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
- **szczególnych kategorii danych osobowych** - rozumie się przez to dane określone w art. 9 ut,1 oraz art. 10 RODO, a więc dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym;
- **haśle** - rozumie się przez to co najmniej 8-znakowy ciąg znaków literowych, cyfrowych, zawierający duże i małe litery oraz znaki specjalne, znany jedynie osobie uprawnionej do pracy w systemie informatycznym, Administratorowi Danych Osobowych oraz Administratorowi Systemu Informatycznego
- **identyfikatorze użytkownika** - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w wyznaczonych przez administratora danych osobowych obszarach systemu informatycznego Szkoły Podstawowej nr 6 z Oddziałami Integracyjnymi im. Króla Władysława Jagiełły w Sochaczewie;
- **incydent bezpieczeństwa** - czynności, zjawiska naruszające zapisy Polityki Bezpieczeństwa Informacji oraz jej procedury mogące zagrozić utracie aktywów Szkoły Podstawowej nr 6 z Oddziałami Integracyjnymi im. Króla Władysława Jagiełły w Sochaczewie, ich integralności lub dostępności, a także dopuścić do nieuprawnionego dostępu do danych, jednoznaczne z sytuacją kryzysową;
- **procedurach ochrony danych osobowych -** rozumie się przez to sposób przetwarzania danych osobowych oraz warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych w taki sposób, by zachować ich tajemnicę, zapewnić ochronę przed zniszczeniem i kradzieżą, określone wymogami wynikające z przeprowadzonego szacowania ryzyka przetwarzania danych osobowych, wymogami niniejszej Instrukcji;
- **przetwarzaniu danych** - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak: zbieranie, wprowadzanie do systemu Szkoły Podsta-

wowej nr 6 z Oddziałami Integracyjnymi im. Króla Władysława Jagiełły w Sochaczewie, przechowywanie, opracowywanie, zmienianie, usuwanie i udostępnianie;
- **szkole** - identyfikuje się jako Szkołę Podstawową nr 6 z Oddziałami Integracyjnymi im. Króla Władysława Jagiełły w Sochaczewie;
- **służbach informatycznych szkoły** - rozumie się przez to informatyków zatrudnionych w szkole;
- **systemie informatycznym szkoły** - rozumie się przez to sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych;
- **systemy przetwarzania informacji** tzn. informacje mogą być przetwarzane wyłącznie w systemach, które spełniają warunki opisane w PBI;
- **sytuacją kryzysową** - jest to wystąpienie, zagrożenie lub domniemanie kradzieży, nieautoryzowanego dostępu, modyfikacji, zatajenia lub utraty (zniszczenia) przetwarzanej w systemie informacji zastrzeżonej. Każdy system informatyczny (SI) powinien przechodzić okresowe audyty bezpieczeństwa;
- **użytkowniku** - rozumie się przez to pracownika szkoły, zatrudnionego na podstawie umowy o pracę, umowy zlecenia lub innej umowy przewidzianej przepisami prawa oraz osobę odbywającą na szkoły staż absolwencki, praktykę studencką, wolontariat, który przetwarza dane osobowe znajdujące się w zbiorach danych szkoły;
- **zbiorze danych osobowych** - rozumie się przez to każdy posiadający strukturę zestaw danych osobowych, dostępnych wg określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony czy podzielony funkcjonalnie.

2.4. Zakres działania administratorów szkoły

Ze względu na strukturę organizacyjną szkoły, podział logiczny sieci teleinformatycznej oraz posiadane zasoby bazodanowe można wyodrębnić następujących administratorów:

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, na-	rejestrator wejścia i wyjścia podopiecz-

	uczyciele świetlicy	nych 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), nadawanie uprawnień dla uczniów i rodziców (wychowawcy)
Poczta szkolna	dyrektor, wicedyrektor, wyznaczeni pracownicy sekretariatu	poczta
Biblioteka szkolna	biblioteka szkoły	Zintegrowany system biblioteczny, OPAC

2.5. System Helpdesk

W podstawowej funkcjonalności Helpdesk IT jest obsługą zdarzeń zgłoszonych przez użytkowników końcowych szkoły oraz przez systemy monitorujące. System realizuje pełny cykl życia zgłoszenia od rejestracji, przez obsługę, a kończąc na zamknięciu zgłoszenia. System pomocy jest oparty na następujących ogniwach:

1. W zakresie aplikacji działających w podsieciach logicznych (przyjmowanie, rozwiązywanie i monitorowanie nieskomplikowanych zgłoszeń dotyczących systemów IT) – dyrektor, wicedyrektor, kierownik świetlicy, wyznaczeni nauczyciele;
2. W zakresie aplikacji działających w podsieciach logicznych, których użytkowanie związane jest z opłatami abonamentowymi – firma sprzedająca licencję;
3. W zakresie hardware'u – kierownik gospodarczy szkoły, firmy zewnętrzne, z którymi podpisano stosowne umowy;
4. W zakresie hardware'u i software'u sprzętu przekazanemu szkole w użytkowanie – instytucja będąca faktycznym właścicielem sprzętu.

2.6. Audyt sprzętu i oprogramowania

1. Za system audytu sprzętu i oprogramowania licencjonowanego odpowiada kierownik gospodarczy szkoły, prowadząc stosowny ich rejestr w księgach inwentarzowych;
2. Systemowi audytu sprzętu i oprogramowania podlega każdy komputer, którego właścicielem jest szkoła i który został podłączony do sieci teleinformatycznej;
3. Audytowi podlega również sprzęt i oprogramowanie, które nie są częścią sieci, ale pozostają w ewidencji placówki;
4. Na każdym komputerze podłączonym do sieci IT szkoły należy zainstalować i uruchomić „certyfikat NASK", za co odpowiadają uprawnieni pracownicy;
5. Użytkownik nie ma prawa samodzielnie odinstalować lub dezaktywować certyfikatu, pod rygorem wyłączenia dostępu do sieci;

6. Na wniosek ASI lub jego pełnomocnika oraz kierownika gospodarczego, użytkownik ma obowiązek odinstalować oprogramowanie, które zostało zdiagnozowane jako „nielegalne” lub „nieaktualne”;
7. Komputery incydentalne, podłączane za wiedzą ASI, ale niebędące środkami trwałymi szkoły, nie podlegają audytowi. Takie komputery są rejestrowane i autoryzowane w systemie za pomocą certyfikatu NASK instalowanego tymczasowo przez wyznaczonego pracownika szkoły.

3. Instrukcja bezpieczeństwa

3.1. Opis zdarzeń naruszających ochronę danych

Podział zagrożeń:

1. Zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, ciągłość systemu zostaje zakłócona - nie dochodzi do naruszenia poufności danych.
2. Zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu - może nastąpić naruszenie poufności danych.
3. Zagrożenia zamierzone, świadome i celowe - najpoważniejsze zagrożenia, naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te można podzielić na:
   – nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu),
   – nieuprawniony dostęp do systemu z jego wnętrza,
   – nieuprawniony przekaz danych,
   – pogorszenie jakości sprzętu i oprogramowania,
   – bezpośrednie zagrożenie materialnych składników systemu.

Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe to głównie:

1. Sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.,
2. Niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,
3. Awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru,
4. Pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,

5. Jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
6. Nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,
7. Stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
8. Nastąpiła niedopuszczalna manipulacja danymi osobowymi w systemie,
9. Ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń,
10. Praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych - np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.,
11. Ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. „bocznej furtki", itp.,
12. Podmieniono lub zniszczono nośniki z danymi osobowymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub kopiowano dane osobowe,
13. Rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (niewylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na kserokopiarce, niezamknięcie pomieszczenia z komputerem, niewykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.).

Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych, w tym także osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, dyskietkach, pendrive czy przenośnych dyskach w formie niezabezpieczonej itp.

3.2. Bezpieczeństwo fizyczne i środowiskowe

3.2.1. Fizyczne zabezpieczenie wejścia do pomieszczeń

Strefy bezpieczeństwa takie jak archiwa, sekretariat, gabinety specjalistów, wydzielone klasopracownie są zabezpieczone przed dostępem osób nieuprawnionych poprzez stosowanie zabezpieczeń fizycznych i proceduralnych typu:

- przegrody oddzielające pracownika od osoby zewnętrznej,
- linie wyznaczające fizyczny,
- zamykane na klucz szafy, szafki itp.

3.2.2. Zabezpieczenie biur, pomieszczeń i urządzeń IT

Zabezpieczenie biur, pomieszczeń i urządzeń realizowane jest przez stosowanie zabezpieczeń fizycznych i proceduralnych wskazanych w pkt. 3.2.1.

W Szkole Podstawowej nr 6 z Oddziałami Integracyjnymi im. Króla Władysława Jagiełły w Sochaczewie pomieszczenia ogólnodostępne i tzw. strefy bezpieczeństwa (o szczególnym

nadzorze, takie jak wydzielone części sekretariatu, gabinety specjalistów czy klasopracownie), po opuszczeniu pomieszczeń należy zamknąć pokój na klucz.
Klucze zapasowe do pomieszczeń w strefach bezpieczeństwa - przechowywane są w zabezpieczonej szafie w pokoju kierownika gospodarczego. W zakresie kluczy do szaf, szafek, szuflad w pomieszczeniach biurowych obowiązuje indywidualna polityka zarządzania tymi kluczami z zachowaniem zasady, że ktoś, kto nie powinien mieć do nich dostępu nie wie, gdzie są przechowywane. Generalnie na biurku czy szafce nie powinno być nic - prócz aktualnie wykorzystywanych dokumentów i sprzętu.

3.2.3. Zabezpieczenie przed zagrożeniami zewnętrznymi i środowiskowymi

Ochrona fizyczna przed zagrożeniami zewnętrznymi i środowiskowymi jest zaplanowana i wdrożona. We wszystkich budynkach szkoły są gaśnice oraz instrukcje bezpieczeństwa przeciwpożarowego. Należy pamiętać, że nie wolno pozostawiać włączonego sprzętu IT bez nadzoru poza godzinami pracy - w szczególności w godzinach nocnych.

3.2.4. Urządzenia podtrzymujące napięcie

Sprzęt jest chroniony przed awariami zasilania i innymi zakłóceniami elektrycznymi poprzez:

- zapewnienie odpowiednich warunków w pomieszczeniu, w którym znajdują się komputery poprzez, w miarę możliwości, fizyczne odsunięcie ich od źródeł ciepła i nadmiernego nasłonecznienia;
- urządzenia podtrzymujące zasilanie UPS przy każdym stanowisku komputerowych o ile jest to wskazane;
- listwy przeciwprzepięciowe przy każdym stanowisku komputerowym, w którym przetwarzane są dane osobowe;
- urządzenia podtrzymujące UPS w sekretariacie i gabinecie dyrektora w ilości uzasadnionej topologią sieci

3.2.5. Bezpieczeństwo okablowania

Kable zasilające i sieciowe są schowane, tak aby zabezpieczyć je przed uszkodzeniem. Są stosowane oznaczenia kabli, gniazdek oraz jest zachowana rozdzielność kabli sieciowych, zasilających i telekomunikacyjnych.

3.2.6. Zabezpieczenie sprzętu poza siedzibą szkoły

Obowiązuje zasada, że sprzęt i nośniki nie są wynoszone poza siedzibę szkoły. W szczególnych przypadkach sprzęt IT jest wydawany po wypełnieniu odpowiedniego rewersu, który jest ewidencjonowany przez kierownika gospodarczego. W przypadku osób upoważnionych lub uprzywilejowanych obowiązują pewne zasady postępowania w celu zapewnienia bezpieczeństwa informacji.

1. Osoba używająca komputer przenośny zawierający dane osobowe zobowiązana jest zachować szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych osobowych na szkoły.
2. Osoba używająca komputer przenośny zawierający dane osobowe w szczególności powinna:

- zabezpieczyć dostęp do komputera na poziomie systemu operacyjnego - identyfikator i hasło;
- nie zezwalać na używanie komputera osobom nieupoważnionym do dostępu do danych osobowych;
- nie wykorzystywać komputera przenośnego do przetwarzania danych osobowych w obszarach użyteczności publicznej;
- zachować szczególną ostrożność przy podłączaniu do sieci publicznych poza obszarem przetwarzania danych osobowych.

3. W przypadku podłączania komputera przenośnego do sieci publicznej poza siecią szkolną należy zastosować firewall zainstalowany bezpośrednio na tym komputerze oraz system antywirusowy.
4. Użytkownik powinien zachować wyjątkową ostrożność podczas korzystania z zasobów sieci publicznej.
5. Za wszelkie działania wykonywane na komputerze przenośnym odpowiada jego formalny użytkownik.

3.3 Kontrola dostępu

Dostęp do chronionych pomieszczeń mogą mieć jedynie osoby upoważnione, wyznaczone przez dyrektora szkoły. Dotyczy to w szczególności następujących pomieszczeń:

- sekretariat (przestrzeń za konsolą),
- archiwum,
- gabinet dyrektora, wicedyrektora, kierownika świetlicy (nie dotyczy części ogólnodostępnych);
- gabinety: pedagogów, psychologów, logopedów (nie dotyczy części ogólnodostępnej);
- biblioteki szkolnej (nie dotyczy części ogólnodostępnej).

3.4 Ochrona antywirusowa

1. Na każdej stacji roboczej w sieci powinno być zainstalowane oprogramowanie antywirusowe skanujące na bieżąco system informatyczny.
2. Oprogramowanie antywirusowe powinno być zainstalowane tak aby użytkownik nie był w stanie wyłączyć lub pominąć etapu skanowania.
3. Kontrola antywirusowa powinna być przeprowadzana na wszystkich nośnikach magnetycznych i optycznych, służących zarówno do przetwarzania danych osobowych w systemie, jak i do celów instalacyjnych.
4. Należy stosować wersje programów antywirusowych z aktualną bazą sygnatur wirusów.
5. Nowe wersje oprogramowania antywirusowego oraz uaktualnienia bazy sygnatur wirusów instalują upoważnieni pracownicy niezwłocznie po ich otrzymaniu lub ścią-

gnięciu, uprzednio weryfikując pochodzenie oprogramowania (o ile nie odbywa się to w sposób zautomatyzowany, zdalny).

6. Administratorzy Systemu mają prawo odłączyć od sieci stację roboczą, na której zostanie zlokalizowany wirus, jeśli uznają, że dalsze pozostawienie go w sieci zagraża innym stacjom roboczym.
7. Użytkownik systemu na stanowisku komputerowym, importujący dane osobowe do systemu informatycznego jest odpowiedzialny za sprawdzenie tych danych pod kątem możliwości występowania wirusów.

3.5 Postępowanie przy stwierdzeniu zdarzeń naruszających bezpieczeństwo informacji

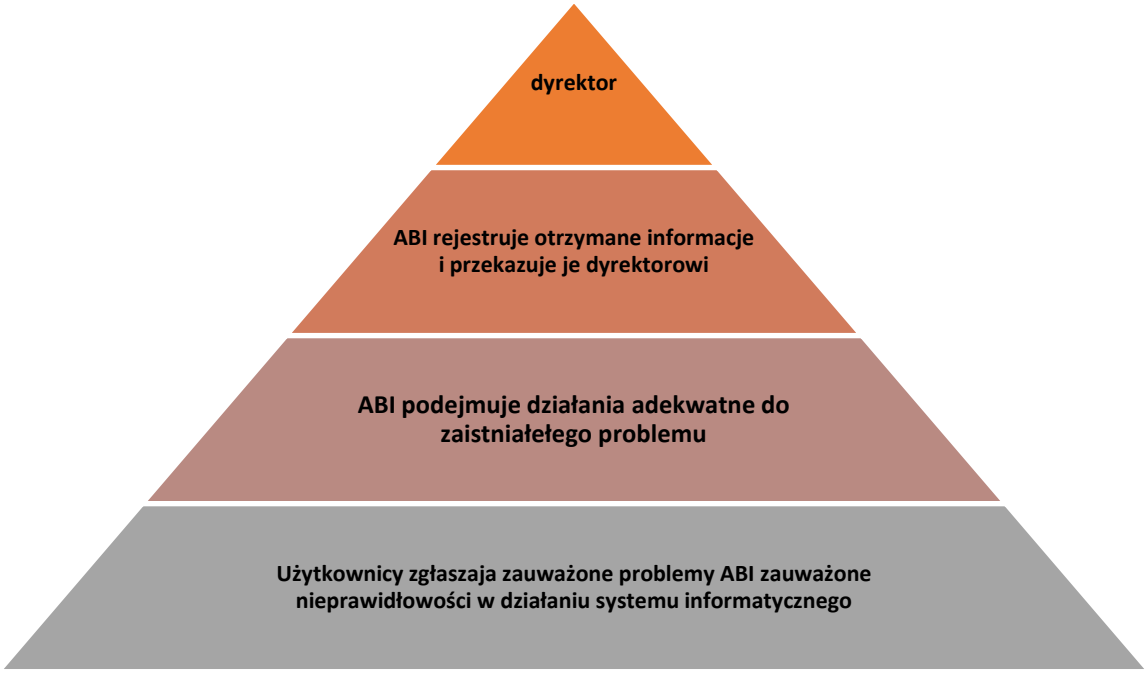
Instrukcja

1. Użytkownik zobowiązany jest powiadomić Administratora Systemów Informatycznych oraz Administratora Bezpieczeństwa Informacji lub uprzednio wskazanego przez dyrektora szkoły pracownika o każdym naruszeniu lub podejrzeniu naruszenia bezpieczeństwa systemu, a w szczególności o:
   - naruszeniu identyfikatora i hasła (system nie reaguje na hasło lub je ignoruje bądź można przetwarzać dane bez wprowadzenia hasła),
   - częściowym lub całkowitym braku danych,
   - braku dostępu do właściwej aplikacji lub zmianie zakresu wyznaczonego dostępu do zasobów serwera,
   - wykryciu wirusa komputerowego,
   - zauważeniu elektronicznych śladów próby włamania do systemu informatycznego szkoły,
   - podejrzeniu kradzieży sprzętu komputerowego lub dokumentów zawierających dane osobowe,
   - zauważeniu śladów usiłowania lub dokonania włamania do pomieszczeń lub zamykanych szaf.
2. Do czasu przybycia na miejsce Administratora Systemów Informatycznych należy:
   - niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego zdarzenia, o ile istnieje taka możliwość,
   - następnie uwzględnić w działaniu również ustalenie jego przyczyn i sprawców,
   - rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
   - zaniechać - o ile to możliwe - dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,
   - zastosować się do instrukcji i regulaminów lub dokumentacji aplikacji, jeśli odnoszą się one do zaistniałego przypadku,
   - udokumentować w formie dokumentacji urzędowej wstępnie zaistniałe naruszenie,
   - nie opuszczać bez uzasadnionej przyczyny miejsca zdarzenia do czasu przybycia Administratora Systemów Informatycznych.
3. Administrator Systemów Informatycznych po otrzymaniu zawiadomienia, o którym mowa w ust.1, powinien niezwłocznie:

- przeprowadzić postępowanie wyjaśniające, w celu ustalenia okoliczności naruszenia ochrony danych osobowych,
- podjąć działania chroniące system przed ponownym naruszeniem,
- w przypadku stwierdzenia faktycznego naruszenia bezpieczeństwa systemu, sporządzić raport naruszenia bezpieczeństwa systemu informatycznego szkoły (wg wzoru załącznika nr 1)

4. W dalszym trybie postępowania należy, przekazać sporządzony raport dyrektorowi oraz podjąć inne, szczególne czynności zapewniające bezpieczeństwo systemu informatycznego szkoły, bądź podjąć środki ochrony fizycznej.
5. Administrator Systemów Informatycznych przekazuje, po przeanalizowaniu i zarejestrowaniu raportu na temat naruszenia bezpieczeństwa systemu informatycznego, informacje dyrektorowi o awariach systemu informatycznego szkoły, zauważonych przypadkach naruszenia niniejszej instrukcji przez użytkowników danych, w szczególności o przypadkach posługiwania się przez użytkowników nieautoryzowanymi programami, nieprzestrzegania zasad używania programów antywirusowych, niewłaściwego wykorzystania sprzętu komputerowego lub przetwarzania danych w sposób niezgodny z procedurami ochrony danych osobowych.

Proces przekazywania informacji na temat zaistniałego incydentu związanego z naruszeniem bezpieczeństwa systemu informatycznego szkoły obrazuje poniższy diagram na rysunku nr 2.



Rysunek 3. Piramida przepływu informacji związanych z naruszeniem bezpieczeństwa IT

3.6 Rozpoczęcie, zawieszenie i zakończenie pracy w systemie IT

Przed przystąpieniem do pracy z systemem, użytkownik obowiązany jest dokonać sprawdzenia stanu urządzeń informatycznych oraz oględzin swojego stanowiska pracy, ze zwróceniem szczególnej uwagi, czy nie zaszły okoliczności wskazujące na naruszenie ochrony danych osobowych.

W przypadku stwierdzenia bądź podejrzenia, iż miało miejsce naruszenie ochrony danych osobowych, użytkownik systemu zobowiązany jest postępować zgodnie z procedurą opisaną w punkcie 3.5 niniejszej instrukcji.

3.6.1. Procedura rozpoczęcia pracy w systemie IT

1. Uruchomić komputer wchodzący w skład systemu informatycznego szkoły, który jest podłączony fizycznie do sieci lokalnej lub wydzielonej i zalogować się podając identyfikator i hasło dostępu do odpowiedniego zasobu IT szkoły.
2. Uruchomić wybraną aplikację (w szczególności aplikację bazodanową m.in. przetwarzającą dane osobowe).
3. Zalogować się do aplikacji za pomocą przydzielonego przez ASI loginu i hasła uwierzytelniającego.

3.6.2. Procedura zawieszenia pracy w systemie IT

1. W trakcie pracy, przy każdorazowym opuszczeniu stanowiska komputerowego, dopilnować, aby na ekranie nie były wyświetlane dane osobowe,
2. Przy opuszczaniu pokoju na dłuższy czas ustawić ręcznie blokadę klawiatury i wygaszacz ekranu.

3.6.3. Procedura zakończenia pracy w systemie IT

1. Zamknąć aplikację,
2. Zamknąć system,
3. Wyłączyć monitor i ewentualnie drukarkę.

Nie wolno bez nadzoru pozostawiać po godzinach pracy włączonego sprzętu IT.

4. Polityka bezpieczeństwa informacji Szkoły Podstawowej nr 6 z Oddziałami Integracyjnymi im. Króla Władysława Jagiełły w Sochaczewie

4.1. Polityka szacowania ryzyka

Polityka szacowania ryzyka związanego z bezpieczeństwem informacji stanowi załącznik do niniejszego SZBI. Polityka zawiera metodologię szacowania ryzyka oraz podejście do szacowania ryzyka z uwzględnieniem bezpieczeństwa informacji w kontekście organizacyjnym oraz wymagań prawnych.

Celem Polityki szacowania ryzyka jest zapewnienie, że metodyka szacowania ryzyka przyjęta w szkole jest spójna ze zidentyfikowanymi wymaganiami organizacyjnymi i prawnymi w zakresie ochrony bezpieczeństwa informacji, zawiera kryteria akceptacji ryzyka i że zapewnia uzyskanie porównywalnych wyników w całej organizacji podczas kolejnych szacowań ryzyka.

4.2. Proces nadawania uprawnień użytkownikom

Rozdział ten zawiera podstawowe informacje o procedurach nadawania, zmiany oraz rejestracji uprawnień do przetwarzania danych przyjętych do stosowania w systemach informatycznych

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

4.3. Zasady nadawania uprawnień

1. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych, zwłaszcza osobowych musi zapoznać się z:
   - **RODO -** 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)
   - Ustawą z dnia 10 maja 2018r. o ochronie danych osobowych (Dz. U. z 2018r. ,poz. 1000),
   - Obowiązującą w Szkole Podstawowej nr 6 z Oddziałami Integracyjnymi im. Króla Władysława Jagiełły w Sochaczewie Polityką bezpieczeństwa informacji
   - Niniejszą instrukcją
2. Jedynie prawidłowo wypełniony wniosek o nadanie uprawnień (załącznik nr 2) w systemie informatycznym szkoły lub zmianę tych uprawnień jest podstawą rejestracji uprawnień w systemie.
3. Stosowany w Szkole Podstawowej nr 6 z Oddziałami Integracyjnymi im. Króla Władysława Jagiełły w Sochaczewie schemat uprawnień dostępu do zasobów informatycznych sieci LAN zakłada, iż użytkownicy uzyskują dostęp do sieci na pewnym, z góry zdefiniowanym poziomie.
4. Autoryzacja odbywa się na zasadzie autoryzowania sprzętu i jest w pełni automatyczna.
5. Niniejsza instrukcja przedstawia procesy związane z nadawaniem, zmianą i usuwaniem uprawnień dotyczących obsługi danych osobowych oraz innych newralgicznych systemów bazodanowych (np. e-learning, zasoby biblioteczne itp.)

4.3.1. Procedura nadawania uprawnień

1. Dyrektor, lub osoba przez niego upoważniona:
   a) nadaje upoważnienie do przetwarzania danych osobowych osobie, która w związku z wykonywanymi przez siebie obowiązkami będzie miała dostęp do danych osobowych;
   b) wypełnia i podpisuje wniosek nadania uprawnień dla osoby upoważnionej do przetwarzania danych osobowych (załącznik nr 2);
   c) przekazuje wypełniony dokument w postaci papierowej do ASI, w celu kontrasygnaty;

ASI sprawdza poprawność przesłanego wniosku oraz:

d) w przypadku braku uwag przekazuje go ze swoją adnotacją referentowi ds. kadr oraz nadaje uprawnienia użytkownikowi w systemie,
e) w przypadku uwag, np. gdy użytkownik nie został zapoznany z przepisami o ochronie danych osobowych, zwraca dokument dyrektorowi; na dokumencie dokonuje adnotacji, w której podaje przyczynę odmowy zatwierdzenia dokumentu.

2. Kroki a-c powtarza się do czasu uzyskania akceptacji dokumentu przez ASI.
3. ASI odpowiednio, zgodnie z przekazanym dokumentem:
   a) rejestruje użytkownika w systemie i nadaje mu określone uprawnienia
   b) generuje użytkownikowi tymczasowe hasło
   c) informuje dyrektora oraz pracownika ds. kadr o nadaniu uprawnień w celu aktualizacji ewidencji osób upoważnionych do przetwarzania danych osobowych w systemie
4. Użytkownik uwierzytelnia się w systemie,
5. Użytkownik zmienia nadane mu przez ASI hasło i rozpoczyna pracę w aplikacji.

Procedurę nadania uprawnień do przetwarzania danych osobowych w systemie należy stosować odpowiednio w przypadku zmiany uprawnień w systemie albo odebrania uprawnień w systemie

4.3.2. Ewidencjonowanie uprawnień

1. Referent ds. kadr w porozumieniem z Administratorem Systemów Informatycznych (ASI) prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych w systemie informatycznym, o której mowa 4.3.
2. Ewidencja osób upoważnionych może przyjmować formę elektroniczną - w takim przypadku należy jednak zapewnić ograniczenie dostępu do ewidencji, do kręgu osób upoważnionych.
3. Ewidencja praw dostępu do sieci lokalnej jest prowadzona zgodnie z zasadami określonymi w odpowiedniej dokumentacji.

4.4. Bezpieczna eksploatacja systemów informatycznych

Bezpieczna eksploatacja systemów informatycznych przetwarzających wszelkiego rodzaj dane zostaje zapewniona poprzez przestrzeganie następujących zasad:

1. Użytkownikom zabrania się wprowadzania zmian do oprogramowania, sprzętu informatycznego poprzez jego samodzielne konfigurowanie i wyposażanie;
2. Użytkownikom zabrania się umożliwiania stronom trzecim uzyskiwania nieupoważnionego dostępu do systemów informatycznych;
3. Użytkownikom nie wolno instalować nowego lub aktualizować już zainstalowanego oprogramowania;
4. Użytkownikom nie wolno korzystać z systemów informatycznych dla celów innych niż związane z wykonywaniem obowiązków służbowych;
5. Użytkownikom nie wolno podejmować prób testowania, modyfikacji i naruszenia zabezpieczeń systemów informatycznych lub jakichkolwiek działań noszących takie znamiona,

6. Informacje przetwarzane przy użyciu współdzielonych aplikacji sieciowych na stacjach roboczych muszą być zapisywane na dyskach stosownego serwera,
7. Wszystkie aplikacje sieciowe, współdzielone zasoby użytkowe muszą być ulokowane na przeznaczonych do tego celu serwerach.
8. Nieautoryzowane podłączenie własnego lub strony trzeciej urządzenia teleinformatycznego do systemu informatycznego szkoły jest zabronione.

4.5. Metody i środki uwierzytelnienia użytkownika w systemie informatycznym

1. Identyfikatory i hasła są sposobem zagwarantowania rozliczalności, poufności i integralności danych osobowych przetwarzanych w systemach informatycznych. Służą do weryfikowania tożsamości użytkownika, uzyskania dostępu do określonych zasobów, kont uprzywilejowanych lub uruchomienia określonej funkcjonalności.
2. Identyfikatory i hasła użytkownik uzyskuje w procesie opisanym w punkcie 4.2 i 4.3 niniejszej instrukcji
3. Mając na uwadze zagwarantowanie wysokiego poziomu bezpieczeństwa przetwarzania danych osobowych oraz zagwarantowania użytkownikom pełnej rozliczalności wykonywanych przez nich operacji w systemach informatycznych, wszyscy użytkownicy przy uwierzytelnianiu do systemów informatycznych powinni stosować się do poniższych zasad:
   – Użytkownik systemu powinien posiadać unikalny identyfikator do swojego osobistego i wyłącznego użytku;
   – Hasła dostępu do systemów informatycznych powinny być tworzone przez użytkownika i stanowią tajemnicę służbową, znaną wyłącznie temu użytkownikowi;
   – Użytkownik ponosi pełną odpowiedzialność za utworzenie hasła dostępu oraz jego przechowywanie;
   – Hasła nie mogą być ujawniane lub przekazywane komukolwiek, bez względu na okoliczności;
   – Użytkownik nie powinien przechowywać haseł w widocznych miejscach, nie powinien umieszczać haseł w żadnych automatycznych procesach logowania (skryptach, makrach lub pod klawiszami funkcyjnymi);
   – Zabronione jest wykorzystywanie dostępnej w niektórych przeglądarkach funkcjonalności automatycznego wypełniania formularzy logowania lub zachowywania danych logowania do witryn
4. Użytkownicy są odpowiedzialni za wszelkie działania w systemach informatycznych prowadzone z użyciem ich identyfikatora i hasła.
5. Administrator Systemów Informatycznych (ASI) jest odpowiedzialny za okresowe sprawdzanie, usuwanie lub blokowanie zbędnych identyfikatorów użytkowników oraz kont w systemach za które są odpowiedzialni.
6. ASI powinien przeprowadzać przegląd autoryzacji i uprawnień nie rzadziej niż co 6 miesięcy.
7. Administratorzy zakładają na stacjach roboczych specjalne konta (profile) służące do zarządzania daną stacją roboczą.

4.6. Wymogi dotyczące uwierzytelnienia

1. Wszystkie konta dostępowe (identyfikatory) do systemów informatycznych powinny być chronione hasłem lub innym bezpiecznym, zaakceptowanym przez ASI sposobem uwierzytelniania.
2. Identyfikator oraz nadane uprawnienia powinny umożliwiać wykonywanie czynności wyłącznie zgodnych z zakresem powierzonych obowiązków.
3. Identyfikator użytkownika powinien być niepowtarzalny a po wyrejestrowaniu się z systemu informatycznego nie powinien być przydzielany innej osobie.
4. Identyfikator, który utracił ważność nie może być ponownie przydzielony innemu użytkownikowi.
5. Hasło początkowe, które jest przydzielane przez ASI, powinno umożliwiać użytkownikowi zarejestrowanie się w systemie **tylko jeden raz** i powinno być natychmiast zmienione przez użytkownika.
6. Użytkownicy powinny wybierać hasła dobrej jakości:
   – długości co najmniej 8 znaków,
   – które są łatwe do zapamiętania, a trudne do odgadnięcia,
   – nie są oparte na prostych skojarzeniach, łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących właściciela konta (np. imię, nazwisko, data urodzenia itp.),
   – w których występuje przynajmniej jedna duża litera, jedna mała litera, jedna cyfra lub znak specjalny,
   – w których nie występują kolejne znaki, które nie są topologiczne (tzn. wynikające z układu klawiszy na klawiaturze, typu „qwer6., „zaq1xsw2CDE#. itp.).
7. Hasła nie mogą być takie same jak identyfikator użytkownika oraz nie mogą być zapisywane w systemach w postaci jawnej.
8. Hasła powinny być utrzymywane w tajemnicy również po upływie ich ważności.
9. Należy unikać ponownego lub cyklicznego używania starych haseł.
10. Rutynowe działania użytkownika nie powinny być prowadzone z wykorzystaniem kont uprzywilejowanych.
11. Udostępnienie hasła osobie postronnej należy traktować jako poważny incydent naruszenia ochrony danych osobowych.

4.7. Wymogi dotyczące zmiany haseł

1. Użytkownik jest zobowiązany zmieniać hasło, w którego posiadaniu się znajduje:
   – Okresowo, zgodnie z wymaganiami dla danego systemu informatycznego (przed upływem terminu ważności hasła).
   – W przypadku ujawnienia lub podejrzenia ujawnienia hasła.
2. W przypadku braku dostępu do konta chronionego hasłem, w którego posiadaniu się znajduje, użytkownik zobowiązany jest wystąpić o zmianę hasła do ASI, w sytuacji:
   – Zapomnienia/zgubienia hasła.
   – Wygaśnięcia ważności hasła.
   – Zablokowania konta spowodowanego nieprawidłowym wprowadzeniem hasła.

– Braku uprawnień/interfejsu umożliwiających samodzielną zmianę hasła.

3. Zmiana haseł użytkowników powinna być wymuszana przez system co 30 dni, w przypadku braku wymuszenia przez system, użytkownik sam jest zobowiązany do zmiany hasła co 30 dni.

4.8. Kopie bezpieczeństwa

1. Kopie zapasowe zbiorów danych osobowych oraz programów i narzędzi programowych służących do ich przetwarzania powinny być wykonywane na bieżąco przez Administratora Systemu Informatycznego.
2. Kopie zapasowe należy opisywać w sposób umożliwiający szybką i jednoznaczną identyfikację zawartych w nich danych.
3. Tworzenie, przechowywanie i likwidację kopii zapasowych powinny regulować szczegółowe instrukcje operacyjne dla poszczególnych systemów informatycznych, opracowywane przez ASI, z uwzględnieniem niniejszych postanowień.
4. Kopie zapasowe powinny być tworzone w bezpiecznym systemie archiwizacji, który powinien zapewniać ograniczony dostęp fizyczny do nośników oraz przyznanie uprawnień dostępu tylko wyznaczonemu imiennie ASI oraz Inspektora.
5. Dane z kopii zapasowych powinny być odtwarzane wyłącznie przez ASI.
6. Kopie zapasowe, które uległy uszkodzeniu powinny podlegać natychmiastowemu zniszczeniu. Niszczenia kopii zapasowych, na nośnikach magnetycznych dokonuje ASI lub inna upoważniona osoba.
7. Automatyczne dzienne kopie bezpieczeństwa winny być zapisywane na urządzeniach magazynujących znajdujących się w innym pomieszczeniu (innej serwerowni)
8. Centralnym punktem zapisu kopii bezpieczeństwa poszczególnych systemów informatycznych jest archiwum szkolne (kasa pancerna) którą zarządza sekretariat. Urządzeniem magazynującym jest pendrive lub dysk przenośny.

5. Polityka bezpieczeństwa w zakresie ochrony danych osobowych

Polityka bezpieczeństwa w zakresie danych osobowych związanego z bezpieczeństwem informacji stanowi odrębny dokument związany z niniejszym SZBI - Zarządzenie Nr 1 dyrektora Szkoły Podstawowej Nr 6 w Sochaczewie z 1 września 2017 r. (z późn.zm.).
Zasady przetwarzania danych osobowych w zbiorach doraźnych:

1. Dostęp do danych osobowych powinien odbywać się poprzez dedykowane aplikacje, działające w architekturze klient-serwer, lub przynajmniej, przechowujące dane na serwerach plików, nie zaś na indywidualnych stanowiskach komputerowych pracowników. Gdy zachodzi potrzeba przetwarzania danych na stacji lokalnej lub w innym formacie, np. dane w postaci pliku arkusza kalkulacyjnego, można tego dokonać w doraźnym zbiorze danych osobowych pod warunkiem, że zapisane dane będą należycie chronione, tj.
   – uniemożliwi się dostęp do danych osobom nieuprawnionym,
   – uniemożliwi się zmiany danych, a tym samym zafałszowanie informacji pochodzących z systemu,
   – zabezpieczy się bezpośredni dostęp do danych hasłem;

2. Doraźny zbiór danych osobowych należy usunąć z nośnika danych, na którym został utworzony lub zniszczyć nośnik, nie później niż 3 dni po wykorzystaniu danych.
3. Zawiadamiać IOD i ASI w przypadku podejrzenia lub stwierdzenia dostępu do zbioru osób nieuprawnionych.

6. Spis rysunków

7. Załączniki

Załącznik nr 1

Zgłoszenie naruszenia bezpieczeństwa systemu informatycznego

DO:	**Inspektor Ochrony Danych/Administrator Systemu Informatycznego**			
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

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

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 szczegółowej 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

Administrator Systemu Informatycznego odpowiada za merytoryczne przygotowanie oraz nadzorowanie rozpowszechnianie, analizowanie, zatwierdzanie oraz przechowywanie oryginałów dokumentów szacowania ryzyka.
Każdy pracownik szkoły zobowiązany jest zgłaszać ASI 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.
ASI 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	Nieautoryzowanie 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 ASI w konsultacji z Dyrektorem 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 ASI 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

ASI 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 Pełnomocnik w porozumieniu z dyrektorem szkoły wdraża adekwatne do wynikającego ryzyka zabezpieczenia oraz mierzy ich skuteczność. Pomiar skuteczności odbywa się w relacji z Załącznikiem A Normy PN-ISO/IEC 27001:20013 (Cele stosowania zabezpieczeń i zabezpieczenia) - Zabezpieczenie uważa się za skuteczne, gdy posiada wszelkie cechy narzucone przez Normę.
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.