

Polityka Bezpieczeństwa Informacji w Publicznej Szkole Podstawowej im. Marszałka Józefa Piłsudskiego w Laskach

| | |
|---|---|
| Rozdział 1 Postanowienia ogólne | 1 |
| Rozdział 2 Organizacja bezpieczeństwa | 2 |
| Rozdział 3 Zarządzanie ryzykiem | 5 |
| Rozdział 4 Zabezpieczenia | 5 |
| Rozdział 5 Procedury systemowe | 5 |
| 1. Procedura nadzór nad dokumentami wpływającymi SZBI | 5 |
| 2. Procedura postępowania z incydentami | 6 |
| 3. Procedura zarządzania ciągłością działania | 7 |
| 4. Procedura audytu | 8 |
| 5. Procedura działania korygujące i naprawcze | 9 |
| Rozdział 6 Postanowienia końcowe | 9 |

Rozdział 1 Postanowienia ogólne

1. Polityka Bezpieczeństwa Informacji, zwana dalej **PBI**, opisuje zasady zarządzania bezpieczeństwem informacji w Publicznej Szkole Podstawowej im. Marszałka Józefa Piłsudskiego w Laskach. Działanie systemu zarządzania bezpieczeństwem informacji opiera się na modelu PDCA (Plan/Do/Check/Act). Stosowane w Polityce Bezpieczeństwa Informacji rozwiązania odpowiadają wymaganiom określonym w § 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.
2. Niniejsza Polityka Bezpieczeństwa Informacji dotyczy wszelkich danych przetwarzanych przez pracowników Publicznej Szkoły Podstawowej im. Marszałka Józefa Piłsudskiego w Laskach stanowiących informacje wytworzone w ramach działania i pracy Publicznej Szkoły Podstawowej im. Marszałka Józefa Piłsudskiego w Laskach tj:
 - 1) danych osobowych zgodnie z ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych oraz rozporządzeniem 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);
 - 2) innych danych niż dane osobowe, informacji, które podlegają ochronie; niezależnie od formy, w jakiej są przechowywane (papierowej, elektronicznej) oraz technologii informatycznych wykorzystywanych do przetwarzania tych danych przez szkołę.
3. Elementami PBI są:
 - 1) zasady zarządzania bezpieczeństwem informacji, w tym danych osobowych;
 - 2) procedury, instrukcje, regulaminy oraz inne dokumenty, które regulują szczegółowe zasady korzystania z zasobów informacyjnych pracy Publicznej Szkoły Podstawowej im. Marszałka Józefa Piłsudskiego w Laskach, a także użytkowania systemów informatycznych.

4. Celem PBI jest w szczególności:

- 1) zapewnienie standardów bezpieczeństwa informacji w oparciu o obowiązujące przepisy prawa;
- 2) określenie ról i zakresów odpowiedzialności związanych z bezpieczeństwem i ochroną informacji;
- 3) minimalizowanie ryzyka w obszarze bezpieczeństwa fizycznego, teleinformatycznego, organizacyjno – prawnego oraz osobowego;
- 4) ochrona informacji przed nieautoryzowanym dostępem, zmianą, utratą, uszkodzeniem, zniszczeniem lub zatajeniem;
- 5) stałe podnoszenie umiejętności i kwalifikacji pracowników szkoły w dziedzinie bezpieczeństwa informacji;
- 6) zaangażowanie wszystkich pracowników szkoły w ochronę informacji;
- 7) zapewnienie dobrego imienia szkole;
- 8) wspieranie dyrektora szkoły w zakresie utrzymania odpowiedniego poziomu bezpieczeństwa informacji poprzez zarządzanie ryzykiem, zarządzanie zmianami, zarządzanie ciągłością działania pracy Publicznej Szkoły Podstawowej im. Marszałka Józefa Piłsudskiego w Laskach;
- 9) stworzenie podstaw dla Systemu Zarządzania Bezpieczeństwem Informacji.

5. Za prawidłowe działanie systemu zarządzania bezpieczeństwem informacji odpowiada dyrektor pracy Publicznej Szkoły Podstawowej im. Marszałka Józefa Piłsudskiego w Laskach

6. Ilekroć w niniejszej Polityce jest mowa o:

- 1) Szkole – należy przez to rozumieć pracę Publiczną Szkołę Podstawową im. Marszałka Józefa Piłsudskiego w Laskach;
- 2) dyrektorze – należy przez to rozumieć dyrektora pracy Publicznej Szkoły Podstawowej im. Marszałka Józefa Piłsudskiego w Laskach;
- 3) **SZBI** – należy przez to rozumieć system zarządzania bezpieczeństwem informacji stosowany w szkole, czyli wszelkie procedury, regulaminy, instrukcje, zasady i inne dokumenty obowiązujące w szkole, których celem jest zapewnienie bezpieczeństwa informacjom, które są w posiadaniu szkoły;
- 4) aktywie (zasobie) - należy przez to rozumieć wszystko co ma znaczenia dla szkoły, w szczególności pracownicy i współpracownicy, infrastruktura, infrastruktura IT, oprogramowanie, dokumentacja;
- 5) incydencie – należy przez to rozumieć pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia właściwej realizacji zadań szkoły i zagrażają bezpieczeństwu informacji;
- 6) informacji, danych - czynnik, któremu można przypisać określone znaczenie, aby móc go wykorzystywać do różnych celów.

Rozdział 2

Organizacja bezpieczeństwa

1. Dyrektor zobowiązany jest do zdefiniowania wyraźnego kierunku działań i udzielenia zauważalnego wsparcia dla inicjatyw w dziedzinie bezpieczeństwa informacji. W tym celu może powołać ciało doradcze składające się z Inspektora Ochrony Danych.

2. Do podstawowych zadań dyrektora i powołanego ciała doradczego należy:

- 1) przegląd i zatwierdzanie zmian w PBI;
- 2) ustalanie podziału odpowiedzialności i ról w SZBI;
- 3) monitorowanie istotnych zmian dla zagrożeń aktywów informacyjnych;

- 4) przegląd i monitorowanie naruszeń bezpieczeństwa informacji;
- 5) szybkie reagowania na incydenty w zakresie bezpieczeństwa systemu informatycznego i podejmowanie ewentualnych działań dyscyplinujących;
- 6) zatwierdzanie ważniejszych przedsięwzięć zmierzających do podniesienia poziomu bezpieczeństwa informacji;
- 7) identyfikacja aktywów, ich właścicieli, przeprowadzenie klasyfikacji informacji oraz określenie zagrożeń dla aktywów;
- 8) ustanowienie zasad i celów bezpieczeństwa informacji;
- 9) systematyczna weryfikacja i analiza standardów związanych z bezpieczeństwem teleinformatycznym (normy, zalecenia, akty prawne);
- 10) sformułowanie i wdrożenie planu postępowania z ryzykiem;
- 11) wdrażanie i eksploatowanie zabezpieczeń w kontekście kompleksowego zarządzania ryzykiem w organizacji;
- 12) opracowanie raportu z szacowania ryzyka;
- 13) przeprowadzanie w zaplanowanych odstępach czasu audytów wewnętrznych SZBI;
- 14) przeprowadzanie przeglądu SZBI;
- 15) podejmowanie działań korygujących lub zapobiegawczych;
- 16) nadzór nad realizacją procedur;
- 17) nadzoru nad dokumentami i zapisami SZBI
- 18) ciągłe doskonalenie SZBI;
- 19) nadawanie i odbieranie uprawnień pracownikom w zakresie dostępu do informacji przetwarzanych w systemach informatycznych i usług udostępnianych przez te systemy;
- 20) zapewnianie pracownikom szkoleń związanych z zapewnianiem bezpieczeństwa informacji;
- 21) definiowanie potrzeb w zakresie poprawy ochrony informacji i bezpieczeństwa systemów przetwarzających dane w organizacji;
- 22) akceptacja lub wyrażenie potrzeby obniżenia poziomu ryzyka związanego z przetwarzaniem informacji;
- 23) zapewnienie wsparcia organizacyjno-finansowego przy wdrażaniu mechanizmów zabezpieczenia informacji i systemów informatycznych;
- 24) prawna odpowiedzialność za przestrzeganie wymagań związanych z zabezpieczeniem informacji i systemów informatycznych.

3. Do podstawowych zadań pracowników szkoły należą:

- 1) przestrzeganie zasad bezpieczeństwa informacji i systemów informatycznych wprowadzonych w szkole;
- 2) przestrzeganie nadanych uprawnień do systemów informatycznych;
- 3) aktywny udział w szkoleniach dotyczących bezpieczeństwa informacji i systemów informatycznych;
- 4) niezwłoczne informowanie o incydentach w zakresie bezpieczeństwa informacji oraz systemów informatycznych;
- 5) aktywny udział we wdrażaniu mechanizmów bezpieczeństwa poprzez ocenę ich skuteczności na swoim stanowisku pracy;
- 6) ochrony przetwarzanych danych zgodnie z określonymi zasadami poufności.

4. Za prawidłowe funkcjonowanie systemów informatycznych odpowiada **Administrator Systemu Informatycznego (ASI)**, do którego obowiązków należą:

- 1) implementacja odpowiednich mechanizmów bezpieczeństwa w administrowanej infrastrukturze informatycznej;
- 2) zapewnienie pomocy użytkownikom przy korzystaniu z systemu informatycznego;
- 3) tworzenie kopii zapasowych informacji przechowywanych w systemach informatycznych;

- 4) instalacja i uaktualnianie oprogramowania oraz zarządzanie licencjami;
- 5) monitorowanie działania systemu informatycznego i przekazywanie informacji o zagrożeniach administratorowi bezpieczeństwa informacji;
- 6) aktywny udział w procesie reagowania na incydenty w zakresie bezpieczeństwa oraz w usuwaniu ich skutków;
- 7) inicjowanie zmian w systemach, PBI, zapewniających bezpieczne funkcjonowanie i korzystanie z systemów informatycznych.

5. W procesie zapewniania bezpieczeństwa danych dotyczących ochrony danych osobowych bierze także udział Inspektor Ochrony Danych, który realizuje zadania określone Ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych.

6. Oprócz stałych pracowników ze szkołą mogą okresowo lub stale współpracować osoby realizujące zadania na rzecz szkoły. Osoby takie, o ile korzystają z systemu informatycznego organizacji, obowiązane są przestrzegać obowiązujących zasad ochrony informacji. Warunek ten za każdym razem unormowany będzie odpowiednimi zapisami w umowie o współpracy, w tym umową o zachowaniu poufności.

7. Do podstawowych zasad bezpieczeństwa informacji (także w trakcie pracy zdalnej) należą zasady:

- 1) chronienia pomieszczeń – pod nieobecność osoby uprawnionej w pomieszczeniach (poza ogólnodostępnymi typu korytarze) nie mogą przebywać osoby postronne, po opuszczeniu pomieszczenia osoba odpowiedzialna zamyka je na klucz (bez pozostawiania kluczy w zamkach – wyjątek stanowi ewakuacja);
- 2) czystego biurka – zarówno dokumentów papierowych, jak i jakichkolwiek innych nośników informacji (płyty CD, DVD, pen-drivów i innych typów pamięci przenośnych), nie pozostawia się bez nadzoru;
- 3) czystej drukarki – wszyscy pracownicy, praktykanci zobowiązani są do zabierania dokumentów z drukarek zaraz po ich wydrukowaniu;
- 4) czystego ekranu (pulpitu) – wszyscy pracownicy korzystający z komputerów każdorazowo opuszczając stanowisko pracy obowiązani są blokować komputer; każdy użytkownik systemu zobowiązany jest zadbać, aby po zakończeniu pracy sprzęt został poprawnie wyłączony;
- 5) czystego kosza – nieprzydatne dokumenty, brudnopisy, zbędne kopie muszą zostać trwale zniszczone w sposób uniemożliwiający odtworzenie zawartych w nich informacji. Zasada ta dotyczy również informacji zapisanych w innej niż papierowa formie – na nośnikach elektronicznych. Do kosza na śmieci nie wyrzuca się płyt CD/DVD oraz innych nośników – należy je przekazać ASI. Do niszczenia dokumentów papierowych służy niszczarka;
- 6) legalności oprogramowania – zabrania się samodzielnego instalowania oprogramowania, a także przechowywania na komputerach treści naruszających prawo;
- 7) nadzorowania kluczy – pobrane klucze do pomieszczeń powinny być w każdym czasie pod kontrolą. Ponadto pracownicy odpowiedzialni są za należyte zabezpieczenie kluczy do biurek stanowiskowych oraz szaf biurowych, w których przechowywane są dokumenty;
- 8) odpowiedzialności za zasoby (aktywa) – każdy, kto przetwarza informacje jest odpowiedzialny za zapewnienie ich dostępności, poufności i integralności poprzez przestrzeganie procedur ich bezpiecznego przetwarzania oraz ochronę przyznanych zasobów, w tym za szkody wyrządzone w systemie informatycznym przez nieautoryzowane oprogramowanie lub niewłaściwe korzystanie z urządzeń systemu informatycznego;
- 9) świadomej konwersacji – pracownicy nie przekazują w przestrzeni publicznej informacji dotyczących zasobów szkoły, nie rozmawiają także na ten temat z osobami nieuprawnionymi do otrzymywania tych informacji, szczególną ostrożność należy zachować prowadząc rozmowy telefoniczne;

- 10) świadomości zbiorowej – wszyscy są świadomi konieczności ochrony zasobów, zapewnienia ich dostępności, poufności, integralności i aktywnie w tym procesie uczestniczą;
- 11) weryfikacji przenośnych nośników informacji – każdy pracownik korzystający z pendrivów czy dysków przenośnych obowiązany jest sprawdzić programem antywirusowym nośnik przy każdym jego uruchomieniu;
- 12) wiedzy koniecznej – w myśl której dostęp do informacji ograniczony jest do tych, które są niezbędne do prawidłowego wykonywania obowiązków na danym stanowisku;
- 13) zgłaszania zdarzeń, incydentów, nieprawidłowej pracy sprzętu – każdy użytkownik systemu zobowiązany jest do zgłaszania wszelkich zauważonych nietypowych zdarzeń, incydentów oraz nieprawidłowej pracy sprzętu.

8. Cele stosowania zabezpieczeń i zabezpieczenia powinny być dobierane adekwatnie do wymagań prawnych i wyników analizy ryzyka dla bezpieczeństwa informacji.

9. Zabezpieczenia fizyczne, techniczne i organizacyjne powinny uzupełniać się wzajemnie zapewniając wspólnie wymagany poziom bezpieczeństwa informacji.

Rozdział 3 Zarządzanie ryzykiem

1. Zarządzanie ryzykiem odnosi się do aktywów organizacji, które zostały zidentyfikowane w szkole i które poddawane są kontroli i analizie pod kątem zagrożeń, jakim podlegają i jakie niosą one ze sobą skutki. Na tej podstawie szacowane jest ryzyko a następnie podejmowane decyzje mające na celu obniżenie ryzyka do poziomu akceptowalnego.

2. Przebieg procesu analizy opisuje **załącznik nr 1** do niniejszej polityki – Polityka zarządzania ryzykiem bezpieczeństwa informacji.

Rozdział 4 Zabezpieczenia

1. Zabezpieczenia organizacyjne, fizyczne oraz infrastruktury zostały opisane w Instrukcji zarządzania systemami informatycznymi, która podlega corocznym audytom, aby zapewnić jej aktualność.

2. Instrukcja zarządzania systemami informatycznymi jest spójna z dokumentacją dotyczącą przetwarzania danych osobowych w szkole.

3. Z instrukcją obowiązani są zapoznać się wszyscy pracownicy szkoły korzystających z systemów informatycznych, w których przetwarzane są informacje.

Rozdział 5 Procedury systemowe

1. Procedura nadzoru nad dokumentami stanowiącymi SZBI

- 1) Procedura ma na celu uporządkowanie zasad zarządzania dokumentami, które definiują SZBI szkoły oraz zapewnienie dostępności i zabezpieczenie zapisów (dowód wykonania czynności operacyjnych lub związanych z działaniami SZBI), informacji (danych) niezbędnych do prowadzenia działalności przez szkołę w kontekście jej bezpieczeństwa.
- 2) Procedura opisuje:
 1. sposób zatwierdzania, wydawania, wycofywania, przeglądu, aktualizacji, wersjonowania, dystrybucji, oznaczania dokumentów zewnętrznych i wewnętrznych,
 2. sposób oznaczania, przechowywania, wyszukiwania, ochrony i usuwania zapisów bezpieczeństwa oraz określa czas ich przechowywania.

- 3) Nadzorowi poddaje się:
 - a) dokumentację SZBI,
 - b) dokumenty wewnętrzne organizacji sklasyfikowane jako aktywa SZBI, np. proces, procedura, instrukcja, regulamin, formularz, wytworzony przez organizację, który określa sposób wykonania czynności w organizacji, w tym również:
 - protokoły SZBI (raporty z audytów, raporty z przeglądu zarządzania, wyniki analizy ryzyka),
 - zapisy operacyjne (logi systemowe).
 - c) dokumenty zewnętrzne (akty prawne, wymagania prawne, normy, regulacje zewnętrzne, które określają sposób wykonywania czynności w szkole).
- 4) Zarządzanie dokumentami:
 - a) dokumentacja wewnętrzna zarządzana jest zgodnie z zasadami określonymi w Instrukcji Kancelaryjnej, Statucie.
 - b) dokumentacja aktualizowana jest w każdym momencie, gdy dokumentacja zewnętrzna ulega zmianie, nowelizacji bądź pojawia się nowa dokumentacja zewnętrzna, która ma wpływ na regulacje wewnętrzne obowiązujące w szkole,
 - c) zmiany w dokumentacji wewnętrznej wprowadzane są zgodnie z obowiązującymi w tym zakresie przepisami i rozwiązaniami przyjętymi w szkole,
 - d) o zmianach w dokumentacji informowani są pracownicy szkoły, jeśli zmiany ich dotyczą, zgodnie z obowiązującymi w szkole procedurami,
 - e) dokumentacja opisująca procedury bezpieczeństwa stosowane w szkole nie stanowi informacji publicznej i nie może być udostępniana osobom, które nie biorą udziału w procesie tworzenia i utrzymywania zabezpieczeń,
 - f) wykaz dokumentów i zapisów poddanych nadzorowi znajduje się w **załączniku nr 2** Wykaz dokumentów i zapisów nadzorowanych.

2.Procedura postępowania z incydentami

- 1) Celem instrukcji jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa, ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.
- 2) Każdy pracownik w przypadku stwierdzenia zagrożenia lub naruszenia bezpieczeństwa informacji, zobowiązany jest niezwłocznie poinformować bezpośredniego przełożonego lub Pełnomocnika SZBI.
- 3) Do typowych zagrożeń bezpieczeństwa informacji:
 - a) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
 - b) niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,
 - c) nieprzestrzeganie zasad ochrony informacji przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).
- 4) Do typowych incydentów bezpieczeństwa danych osobowych należą:
 - d) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
 - e) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych),
 - f) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).
- 5) W przypadku stwierdzenia wystąpienia zagrożenia, dyrektor lub wskazany przez niego pracownik szkoły prowadzi postępowanie wyjaśniające w toku, którego:

- a) ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki,
 - b) inicjuje ewentualne działania dyscyplinarne,
 - c) rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości,
 - d) dokumentuje prowadzone postępowania.
- 6) W przypadku stwierdzenia incydentu (naruszenia), dyrektor lub wskazany przez niego pracownik szkoły we współpracy z IOD prowadzi postępowanie wyjaśniające w toku, którego:
- a) ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały,
 - b) zabezpiecza ewentualne dowody,
 - c) ustala osoby odpowiedzialne za naruszenie,
 - d) podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody),
 - e) inicjuje działania dyscyplinarne,
 - f) wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości,
 - g) dokumentuje prowadzone postępowania,
 - h) w przypadku gdy incydent dotyczy naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu.
- 7) Dyrektor lub wskazana przez niego osoba dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze w dokumencie: Formularz rejestracji incydentu.

3. Procedura zarządzania ciągłością działania

- 1) Celem procedury jest zapewnienie ciągłości działania organizacji w sytuacji kryzysowej, gdy skutki zaistniałych incydentów zagrażają jej funkcjonowaniu.
- 2) W szkole powołuje się Sztab kryzysowy ustanowiony na stałe, dedykowany do bieżącego prowadzenia przygotowań do świadomego i planowego stawiania czoła zakłóceniom działalności operacyjnej.
- 3) W skład Sztabu wchodzi: dyrektor, Administrator Systemu Informatycznego (ASI), IOD, i pozostałe osoby wyznaczone przez dyrektora.
- 4) Sztab kryzysowy jest odpowiedzialny za opracowanie procedur ciągłości działania i wyznaczenie odpowiedzialności osób za realizację tych procedur.
- 5) ASI jest odpowiedzialny za identyfikację zdarzeń krytycznych, które wymagać będą uruchomienia planów postępowania w sytuacjach awaryjnych i Planów Ciągłości Działania. Zdarzenia te muszą powodować znaczne straty dla szkoły.
- 6) Pod uwagę brane są straty bezpośrednie - związane z brakiem możliwości realizacji kluczowych procesów biznesowych, wynikające z niedostępności systemu informatycznego oraz straty pośrednie - utrata dobrego imienia szkoły.
- 7) ASI we współpracy z dyrektorem jest odpowiedzialny za opracowanie i wdrożenie procedur odbudowy dla poszczególnych zdarzeń krytycznych zgodnie z **załącznikiem nr 3 Plan ciągłości działania**.
- 8) Procedury odbudowy zawierają następujące elementy:
 - a) zgłaszanie incydentu / awarii,
 - b) działania awaryjne - Zadania podejmowane po wystąpieniu incydentu,
 - c) przywrócenie działania tymczasowego / naprawa z wykorzystaniem tymczasowych metod,
 - d) odbudowa i przywracanie do stanu normalnego,

- e) wznowienie działalności - podejmowane w celu przywrócenia normalnej działalności operacyjnej.
- 9) Testowanie planów ciągłości działania:
 - a) testowanie różnych scenariuszy przywracania działalności szkoły „na papierze”,
 - b) symulacje (w szczególności, w celu przeszkolenia pracowników do pełnienia określonych funkcji po wystąpieniu incydentu lub przy zarządzaniu sytuacjami kryzysowymi),
 - c) testowanie technicznych możliwości przywrócenia stanu sprzed awarii,
 - d) testowanie odtworzenia stanu poprzedniego,
 - e) testy urządzeń i usług dostawców (zapewniając, że usługi i produkty dostarczane przez zewnętrznych dostawców będą zgodne z uzgodnieniami wynikającymi z umów),
 - f) próby generalne (sprawdzanie, czy instytucja, pracownicy, sprzęt, instalacje i procesy radzą sobie z przerwami w działaniu).
- 10) Plan podlega aktualizacji w przypadku zmian kadrowych, kontaktowych, strategii, ryzyka, procesów, wyposażenia, lokalizacji, urządzeń i zasobów, przepisów prawnych, kontrahentów, dostawców, petentów.
- 11) Dyrektor odpowiada za szkolenie pracowników w zakresie efektywnego wykonywania procedur przywracania.
- 12) Dyrektor oraz ASI odpowiadają za wyciąganie wniosków z incydentów i awarii oraz podejmowanie działań korygujących, aby zdarzenia te nie pojawiały się w przyszłości lub aby ich skutki były możliwie najmniej dotkliwe.

4. Procedura audytu

- 1) Celem audytów wewnętrznych jest ocena czy system zarządzania bezpieczeństwem informacji jest skutecznie wdrożony, funkcjonuje zgodnie z wymaganiami § 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 oraz, czy występują potrzeby doskonalenia jego elementów. Audyty prowadzone są w sposób obiektywny i bezstronny.
- 2) Dyrektor we współpracy z ASI jest odpowiedzialny za planowanie i przeprowadzanie audytów wewnętrznych z roczną częstotliwością lub częściej.
- 3) Dyrektor we współpracy z ASI opracowuje programy audytów biorąc pod uwagę ważność procesów oraz audytowanych obszarów, jak też wyniki wcześniejszych audytów. Określa on kryteria audytu, jego cel, zakres i ewentualnie metody.
- 4) Osoba wyznaczona przez dyrektora, zwana dalej audytorem, realizuje działania audytowe mające na celu uzyskanie obiektywnych dowodów potwierdzających poprawność realizowanych zadań, procedur, polityk, zabezpieczeń, celów, spełniania wymagań ustawowych, dokonywania zapisów, nadzoru nad dokumentami.
- 5) Osoba powołana na audytora nie może audytować swojej własnej pracy.
- 6) W przypadku stwierdzenia uchybień mających wpływ na skuteczność działania Systemu Zarządzania Bezpieczeństwem Informacji, audytor identyfikuje tzw. niezgodności lub spostrzeżenia. Audytor odpowiedzialny jest także za identyfikację potrzeb mających wpływ na doskonalenie Systemu Zarządzania Bezpieczeństwem Informacji.
- 7) Osoba odpowiedzialna za audytowany dział / proces / obszar oraz osoba audytowana ma obowiązek przekazywania prawdziwych, możliwie najpełniejszych informacji, udostępniania wszystkich związanych z procesem dokumentów i zapisów, o które poprosi audytor.

- 8) Wynik audytu zostaje niezwłocznie udokumentowany przez audytora w wypełnionym formularzu audytu i przekazany dyrektorowi najpóźniej w ciągu dwóch dni po jego zakończeniu zgodnie z **załącznikiem nr 4** Protokół audytu.
- 9) Dyrektor dokonuje przeglądu i analizy wyniku audytu oraz decyduje o inicjowaniu działań korygujących, w przypadku zaistnienia poważnych niezgodności. Jest to dokumentowane w Protokole audytu.
- 10) Wyniki przeprowadzonego audytu dyrektor uwzględnia w szacowaniu wartości ryzyka i skutków wystąpienia naruszenia.

5. Procedura prowadzenia działań korygujących i naprawczych

- 1) Celem procedury jest uporządkowanie i przedstawienie czynności związanych z: inicjowaniem oraz realizacją działań korygujących i zapobiegawczych wynikających z zaistnienia incydentów bezpieczeństwa, słabości lub potrzeby doskonalenia systemu zarządzania bezpieczeństwem informacji.
- 2) Każdy pracownik ma obowiązek zgłoszenia każdego zaistniałego, potencjalnego problemu bądź zadania, który może wpłynąć na bezpieczeństwo realizacji pracy, jak również na funkcjonowanie systemu zarządzania bezpieczeństwem informacji.
- 3) Typowymi innymi źródłami informacji o incydentach, zagrożeniach lub słabościach są:
 - a) alarmy z systemów informatycznych,
 - b) analizy incydentów,
 - c) wyniki audytów / kontroli,
 - d) przeglądy zarządzania.
- 4) Gdy ASI, IOD lub dyrektor stwierdzi konieczność podjęcia działań korygujących lub zapobiegawczych, określa:
 - e) źródło powstania incydentu / zagrożenia lub słabości,
 - f) zakres działań korygujących lub zapobiegawczych,
 - g) termin realizacji,
 - h) osobę odpowiedzialną.
- 5) ASI jest odpowiedzialny za nadzór nad poprawnością i terminowością wdrażanych działań korygujących lub zapobiegawczych.
- 6) Po przeprowadzeniu działań korygujących lub zapobiegawczych, ASI jest zobowiązany do oceny efektywności ich zastosowania.
- 7) Powyższe czynności rejestrowane są w **załączniku nr 5** - Zadania_ASI.

Rozdział 6

Postanowienia końcowe

1. Nieprzestrzeganie zasad zawartych w dokumentach PBI, jest naruszeniem obowiązków pracowniczych wynikających w szczególności z ustaw o pracownikach samorządowych, ustawy Kodeks Pracy, ustawy Karta Nauczyciela i może pociągnąć za sobą skutki dyscyplinarne oraz spowodować pociągnięcie do odpowiedzialności wynikającej z przepisów prawa.

2. PBI i dokumenty z nią związane są dostępne na stronie internetowej: www.psplaskipl oraz BIPIe szkoły.

Załączniki:

- 1) **Załącznik nr 1** – Polityka zarządzania ryzykiem bezpieczeństwa informacji,
- 2) **Załącznik nr 2** – Wykaz dokumentów i zapisów nadzorowanych,
- 3) **Załącznik nr 3** – Plan ciągłości działania,

- 4) Załącznik nr 4 – Protokół audytu,**
- 5) Załącznik nr 5 – Zadania ASI.**