Zarządzenie nr 8/2024
Dyrektora ZSBiO w Łabiszynie
z dnia 28 listopada 2024 r. w sprawie funkcjonowania Krajowych Ram Interoperacyjności (KRI)

Na podstawie §20 Rozporządzenia 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

Dyrektor ZSBiO w Łabiszynie
zarządza, co następuje :

§1

Wprowadza się w życie zasady prowadzenie w ZSbiO w Łabiszynie działań zapewniających zgodność z Krajowymi Ramami Interoperacyjności, dalej KRI.

§ 2

1. KRI w szkole funkcjonują w oparciu o standardy zgodne z §20 ust. 1 i 2 z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych zgodnie z normą ISO 27001 przyjęte przez dyrektora szkoły, uwzględniające specyfikę szkoły, których wykaz stanowi załącznik nr 1 do zarządzenia.
2. Na działania podejmowane w ramach zapewnienia zgodności z KRI składają się:

   1)zasady zarządzania bezpieczeństwem informacji, w tym danych osobowych;

   2) procedury, instrukcje, regulaminy oraz inne dokumenty, które regulują szczegółowe zasady korzystania z zasobów informatycznych w ZSBiO w Łabiszynie.

3. Celem podejmowanych działań jest w szczególności:
   1) zapewnienie standardów bezpieczeństwa informacji w oparciu o obowiazujace 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 zmianami, zarządzanie ciągłością działania szkoły;
   9) stworzenie podstaw dla Systemu Zarządzania Bezpieczeństwem Informacji

§ 3

Zgodność ze standardami KRI osiąga się w szkole poprzez następujące działania:

1) opracowanie i wdrożenie wewnątrzszkolnych standardów i wskaźników bezpieczeństwa informacji;
2) opracowanie niezbędnych procedur, regulaminów i innych mechanizmów kontroli w zakresie bezpieczeństwa informacji;
3) prowadzenie instruktażu i szkoleń z zakresu dokumentacji regulującej zasady zapewniania bezpieczeństwa informacji;
4) sprawowanie nadzoru pedagogicznego;
5) prowadzenie kontroli wewnętrznej wszystkich obszarów pracy szkoły;
6) prognozowanie zagrożeń i ryzyk oraz mechanizmów ich zapobiegania;
7) monitorowanie i ocena funkcjonowania systemu bezpieczeństwa informacji.

§ 4

Celem zapewnienia zgodności pracy szkoły ze standardami KRI wprowadza się Politykę Bezpieczeństwa Informacji, która stanowi załącznik nr 2 do zarządzenia oraz Instrukcję Zarządzania Systemami Informatycznymi, która stanowi załącznik nr 3 do zarzadzenia.

§ 5

Zadania z zakresu zapewnienia bezpieczeństwa informacji realizują wszyscy nauczyciele i pracownicy szkoły, a za skuteczne, efektywne i adekwatne funkcjonowanie systemu bezpieczeństwa informacji odpowiedzialny jest dyrektor szkoły.

§ 6

Zobowiązuję wszystkich pracowników do zapoznania się z treścią niniejszego zarządzenia oraz do jego przestrzegania.

§ 7

Zarządzenie wchodzi w życie z dniem podpisania.

Załączniki do zarządzenia:

nr 1 - Standardy Bezpieczeństwa Informacji

nr 2 - Polityka Bezpieczeństwa Informacji

Załącznik nr 1
do zarządzenie nr 8
z dnia 28 listopada 2024 r.

Standardy bezpieczeństwa informacji w Zespole Szkół Branżowych i Ogólnokształcących w Łabiszynie w ramach Krajowych Ram Interoperacyjności

1) zapewnienie aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia;

2) utrzymywanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfiguracji;

3) przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;

4) podejmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji;

5) bezzwłoczna zmiana uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4;

6) zapewnienie szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:

a) zagrożenie bezpieczeństwa informacji,

b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,

c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich;

7) zapewnienia ochrony przetwarzanych informacji przed ich kradzieży, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:

a) monitorowanie dostępu do informacji,

b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,

c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;

8) ustanowienie podstawowych zasad gwarantujących bezpieczny pracę przy przetwarzaniu mobilnym i pracy na odległość;

9) zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;

10) zawieranie w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;

11) ustalenie zasad postępowania z informacjami, zapewniaJących minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;

12) zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:

a) dbałości o aktualizację oprogramowania,

b) minimalizowaniu ryzyka utraty informacji w wyniku awarii,

c) ochronie przed błędami, utratą, nieuprawnioną modyfikacją,

d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,

e) zapewnieniu bezpieczeństwa plików systemowych,

f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,

g) niezwłocznym podejmowaniu działań po dostrzeieniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,

h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;

13) bezzwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących;

14) zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok

Załącznik nr 2
do zarządzenie nr 8
z dnia 28 listopada 2024 r.

Polityka Bezpieczeństwa Informacji

Rozdział 1

Postanowienia ogólne

1. Polityka Bezpieczeństwa Informacji, zwana dalej PBI, opisuje zasady zarządzania bezpieczeństwem informacji w Zespole szkół Branżowych i Ogólnokształcących w Łabiszynie. Działanie systemu zarządzania bezpieczeństwem informacji opiera się na modelu PDCA (Plan/Do/Check/Act). Stosowane w Polityce Bezpieczeństwa Informacji rozwiązania odpowiadają wymaganiom określonym w § 20 Rozporządzenia 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.

2. Niniejsza Polityka Bezpieczeństwa Informacji dotyczy wszelkich danych przetwarzanych przez pracowników Zespołu Szkół Branżowych i Ogólnokształcących w Łabiszynie stanowiących informacje wytworzone w ramach działania i pracy tj: Zespołu Szkół Branżowych i Ogólnokształcących w Łabiszynie

1) danych osobowych zgodnie z ustawą z dnia 10 maja 201g 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:

3) zasady zarządzania bezpieczeństwem informacji, w tym danych osobowych;
4) procedury, instrukcje, regulaminy oraz inne dokumenty, które regulują szczegółowe zasady korzystania z zasobów informacyjnych Zespołu Szkół Branżowych i Ogólnokształcących w Łabiszynie, a także użytkowania systemów informatycznych.

4. Celem PBI jest w szczególności:

10) zapewnienie standardów bezpieczeństwa informacji w oparciu o obowiązujące przepisy prawa;
11) określenie ról i zakresów odpowiedzialności związanych z bezpieczeństwem i ochroną informacji;

12) minimalizowanie ryzyka w obszarze bezpieczeństwa fizycznego, teleinformatycznego, organizacyjno — prawnego oraz osobowego;
13) ochrona informacji przed nieautoryzowanym dostępem, zmianą, utratą, uszkodzeniem, zniszczeniem lub zatajeniem;
14) stałe podnoszenie umiejętności i kwalifikacji pracowników szkoły w dziedzinie bezpieczeństwa informacji;
15) zaangażowanie wszystkich pracowników szkoły w ochronę informacji;
16) zapewnienie dobrego imienia szkole;
17) wspieranie dyrektora szkoły w zakresie utrzymania odpowiedniego poziomu bezpieczeństwa informacji poprzez zarządzanie ryzykiem, zarządzanie zmianami, zarządzanie ciągłością działania Zespołu Szkół Branżowych i Ogólnokształcących w Łabiszynie;
18) stworzenie podstaw dla Systemu Zarządzania bezpieczeństwem Informacji.

5. Za prawidłowe działanie systemu zarządzania bezpieczeństwem informacji odpowiada dyrektor Zespołu Szkół Branżowych i Ogólnokształcących w Łabiszynie

6. Ilekroć w niniejszej Polityce jest mowa o:

1) Szkole — należy przez to rozumieć Zespół Szkół Branżowych i Ogólnokształcących w Łabiszynie;
2) dyrektorze — należy przez to rozumieć dyrektora Zespołu Szkół Branżowych i Ogólnokształcących w Łabiszynie;
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 jako zespół do spraw bezpieczeństwa, składający się z Inspektora Ochrony Danych, Administratora Systemu Informatycznego.
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) definiowane 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 udziału w szkoleniach dotyczących bezpieczeństwa informacji i systemów informatycznych;

4) niezwłoczne informowanie o incydentach w zakresie bezpieczeństwa informacji oraz systemów informatycznych;

S) aktywny udziału we wdrażania 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 (płyt 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;

s) 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 *sq* świadomi konieczności ochrony zasobów, zapewnienia ich dostępności, poufności, integralności i aktywnie w tym procesie uczestniczą;

11) weryfikacji przenośnych nośników informacji każdy pracownik korzystających z pen-driveów czy dysków przenośnych obowiązany jest sprawdzić programem antywirusowym nośnik przy każdy 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. Zasady postępowania dotyczące pracy na odległość oraz urządzeń przenośnych i nośników danych wynoszonych poza siedzibę szkoły:

Praca na odległość może być wykonywana wyłącznie przez pracowników posiadających umowę o odpowiedzialności materialnej za powierzone mienie.

1) użytkownik otrzymujący komputer przenośny podpisuje umowę, w której zobowiązuje się do przestrzegania zaleceń związanych z ochroną laptopa:

a) laptop powinien być transportowany pod kontrolą użytkownika lub innej upoważnionej osoby,

b) laptop nie powinien być pozostawiany w sposób narażający go na kradzież,

c) dyski na komputerze przenośnych są szyfrowane,

d) nie zezwala się na pracę nad informacjami wrażliwymi w miejscach publicznych,

e) użytkownicy laptopów powinni zapewnić systematyczne tworzenie kopii zapasowych,

f) użytkownicy są zobowiązani do aktualizacji systemów operacyjnych z zachowaniem rozwiązań organizacyjnych wskazanych przez ADO,

2) zabrania się kopiowania i przechowywania danych stanowiących własność szkoły na smartfonach,

3) zabrania się korzystania z prywatnych laptopów i innych urządzeń przenośnych do kopiowania i przetwarzania danych należących do szkoły,

4) zobowiązuje się przy korzystaniu z urządzeń mobilnych do korzystania wyłącznie z bezpiecznych sieci.

Pracownicy użytkujący przenośne komputery, w których przetwarzane są dane osobowe, zobowiązani są zachować szczególną ostrożność podczas transportu i i przechowywania tego komputera. W celu zabezpieczenia ingerencji osób niepowołanych, dostęp do komputera musi być zabezpieczony hasłem i zabronione jest użytkowanie komputera osobom nieupoważnionym. Komputera przenośnego nie należy pozostawiać w miejscu, w którym może wystąpić niebezpieczeństwo utraty lub wycieku danych.

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

10. 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. lnstrukcja 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:
    a) sposób zatwierdzania, wydawania, wycofywania, przeglądu, aktualizacji, wersjonowania, dystrybucji, oznaczania dokumentów zewnętrznych i wewnętrznych,
    b) sposób oznaczania, przechowywania, wyszukiwania, ochrony i usuwania zapisów bezpieczeństwa oraz określa czas ich przechowywania.
    c) Nadzorowi poddaje się:dokumentację SZBI,
    d) 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).

e) dokumenty zewnętrzne (akty prawne, wymagania prawne, normy, regulacje zewnętrzne, które określają sposób wykonywania czynności w szkole).

3) Zarządzanie dokumentami:

a) dokumentacja wewnętrzna zarządzana jest zgodnie z zasadami określonymi w *Instrukcji Kancelaryjnej, Statucie* oraz *Instrukcji Archiwalnej.*

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,

ą) 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 wchodzą: 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 wymagań 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 lkkorygujących, 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 § 20 Rozporządzenia 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 normą ISO 27001 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 załączniltiem nr 4 *Protokół audytu.*

9) Dyrektor dokonuje przeglądu i analizy wyniku audytu oraz decyduje o inicjowaniu działań korygujących, w przypadku zaistnienia powainych 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) ASl 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.

7j 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 *sq* dostępne w Zespole Szkół Branżowych i Ogólnokształcących w Łabiszynie.

Załącznik nr 2

do Polityki Bezpieczeństwa Informacji

Wykaz dokumentów i zapisów poddanych nadzorowi w ramach SZBI Dokumenty wewnętrzne

Typ dokumentów	**Tworzenie, modyfikacja, usuwanie dokumentów**	**Zatwierdzanie dokumentów**	**Zasady dostępu**	**Aktualizacja**
Dokumenty systemu ISO 27001 – wersja elektroniczna na serwerze	ASI ma uprawnienia do tworzenia, modyfikacji, usuwania dokumentów	Dyrektor zatwierdza dokument poprzez umieszczenie go na serwerze	Dostęp do odczytu do wersji elektronicznej dokumentacji mają wszyscy pracownicy	Aktualizacja dokumentu polega na zmianie plikuna serwerze (zmiana numeru wersji i daty wydania)
Dokumenty systemu ISO 27001 – wersja papierowa	ASI ma uprawnienia do tworzenia, modyfikacji, usuwania dokumentów	Dyrektor zatwierdza dokument	Dostęp do dokumentów w wersji papierowej mają wszyscy pracownicy	Aktualizacja wersji papierowej w segregatorach
Dokumenty wewnętrzne – wersja elektroniczna na serwerze	Dyrektor lub upoważniona przez niego osoba ma uprawnienia do tworzenia, modyfikacji, usuwania dokumentów	Dyrektor zatwierdza dokument poprzez umieszczenie go na serwerze	Dostęp do odczytu do wersji elektronicznej dokumentacji maja wszyscy pracownicy	Aktualizacja dokumentu polega na zmianie pliku na serwerze (zmiana numeru wersji i daty wydania)
Dokumenty wewnętrzne – wersja papierowa	Dyrektor lub upoważniona przez niego osoba ma uprawnienia do tworzenia, modyfikacji, usuwania dokumentów	Dyrektor zatwierdza dokument i wprowadza go zarządzeniem	Dostęp do dokumentów w wersji papierowej maja wszyscy pracownicy	Aktualizacja wersji papierowej w księdze zarządzeń

Szczegółowy spis dokumentów wewnętrznych:

1) Polityka Bezpieczeństwa Informacji
2) Polityka zarządzania ryzykiem w bezpieczeństwie informacji
3) Instrukcja Zarządzania Systemem Informacji
4) Polityka Ochrony Danych Osobowych
5) Regulamin Ochrony Danych Osobowych
6) Plan ciągłości działania
7) Instrukcja kancelaryjna
8) Instrukcja archiwalna
9) Instrukcja inwentaryzacyjna
10) Prawidłowy przepływ informacji
11) Rejestr upoważnień
12) Instrukcja obiegu dokumentów księgowych
13) Instrukcja w sprawie działania składnicy akt.

Dokumenty zewnętrzne

1. Zasady dostępu: Dostęp do dokumentów zewnętrznych posiadają osoby korzystające z informacji w nich zawartych
2. Aktualizacja: Aktualizacja polega na okresowym i systematycznym sprawdzeniu zawartości dokumentów zewnętrznych

LP	Dokumenty zewnętrzne
1	Ustawia z dnia 10 maja 2018 r. o ochronie danych osobowych;
2	Ustawa x dnia 5 września 2016 r. o uslugach zaufania oraz identyfikacji elektronicznej;
3	Ustawa z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych;
4	Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 stycznia 2007 r. w sprawie Biuletynu Informacji Publicznej;
5	Rozporządzenie Ministra Kultury z dnia 16.09.2002 r. (w sprawie postępowania z dokumentacją, zasad jej klasyfikowania i kwalifikowania oraz zasad i trybu przekazywania materia??ów archiwalnych do archiwów państwowych (Dz.U. nr 167, poz.1375)
8	Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 30 października 2006 w sprawie niezbędnych elementów struktury dokumentów elektronicznych;

9	Rozporządzenie 'Ministra Spraw Wewnętrznych i Administracji z dnia 30 października 2006r. w sprawie szczegółowego sposobu postępowania z dokumentami elektronicznymi (Dz.U. Nr 206 poz. 1518);
10	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;
11	Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych;
12	Art. 68 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych;
13	Komunikacie Ministerstwa Finansów nr 23 z dnia 16.12.2009 r. w sprawie „Standardów kontroli zarządczej dla sektora finansów publicznych“ (Dz. Urzędowy Ministra Finansów Nr 15 poz. 84);
14	Rozporządzenie Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych

Zapisy

Typ zapisów	Dodatkowe informacje o zapisach	Miejsce przechowywania	**Zabezpieczenie**	**Czas** przechowywania
Protokoły systemu 27001:2005		Serwer lub segregator ASI	Kopie bezpieczeństwa oraz szafa z dokumentacją ASI	2 lata
Zapisy bezpieczeństwa		Serwer lub segregator ASI	Kopie bezpieczeństwa oraz szafa z dokumentacją ASI	2 lata
Zapisy operacyjne (logi systemowe)		Serwer lub dokumentacja w poszczególnych działach	Kopie bezpieczeństwa oraz zabezpieczenie pomieszczeń działowych	5 lat

Załącznik nr 3
do Polityki Bezpieczeństwa Informacji

Plan ciągłości działania
w Zespole Szkół Branżowych i Ogólnokształcących w Łabiszynie

Plan ciągłości działania na wypadek pożaru

1. Zgłaszanie *incydentu*

a) Pracownik, który zidentyfikował pożar niezwłocznie powiadamia straż pożarną pod numerem 112, dyrektora szkoły oraz sekretarza.

b) Po uzyskaniu telefonicznego połączenia ze Strażą Pożarną należy wyraźnie podać:

dokładny adres, nazwę obiektu lub jego części, w której powstał pożar,

- co się pali (np. pali się pomieszczenie magazynku podręcznego, archiwum, komputer w pomieszczeniu biurowym itp.)

- czy istnieje zagrożenie życia ludzkiego, nr telefonu z którego się dzwoni i swoje nazwisko.

2. Działania awaryjne

a) Równocześnie z alarmowaniem Jednostek straży pożarnej należy przystąpić do akcji ratowniczo-gaśniczej przy pomocy gaśnic znajdujących się w budynku.

b) Do czasu przybycia Jednostek straży pożarnej, kierownictwo akcją obejmuje dyrektor szkoły lub osoba upoważniona w razie nieobecności dyrektora - osoba dorosła najbardziej energiczna i opanowana.

c) Zasady uczestnictwa w gaszeniu pożaru:

- w pierwszej kolejności należy przeprowadzić ratowanie zagrożonego życia, ewakuację ludzi a następnie ewakuację mienia, w tym dokumentacji i kopii zapasowych,

- wyłączyć dopływ prądu elektrycznego do pomieszczeń objętych pożarem,

- nie wolno gasić wodą jak i również gaśnicą pianową instalacji i urządzeń elektrycznych będących pod napięciem,

- usunąć z zasięgu ognia wszelkie materiały palne, a w szczególności butle z gazami palnymi, naczynia z płynami łatwopalnymi, cenne materiały, maszyny, urządzenia itp.,

- nie otwierać bez potrzeby drzwi, okien do pomieszczeń, w których powstał pożar, ponieważ dopływ powietrza sprzyja rozprzestrzenianiu się ognia,

- przestrzegać w czasie gaszenia zasad bezpieczeństwa. Otwierając drzwi do pomieszczeń w których powstał pożar należy zachować szczególną ostrożność. Wskazane jest schowanie się za ścianę od strony klamki w drzwiach lub otwieranie zza drzwi,

- wchodząc do zadymionych pomieszczeń lub przechodząc przez nie, należy ograniczyć ilość wdychanych produktów spalania. Poruszać się w pozycji pochylonej, jak najbliżej podłogi i zasłaniać usta, np. wilgotną chustką,

- po przyjeździe jednostki straży pożarnej do pożaru udzielić niezbędnych informacji i podporządkować się decyzji Kierującego Działaniami Ratowniczymi w zakresie działalności ratowniczo — gaśniczej,

- zabezpieczyć mienie pozostałe na pogorzelisku, do ukończenia akcji gaśniczej.

3. Przywrócenie działania tymczasowego / naprawa z wykorzystaniem tymczasowych metod

a) Jeśli zniszczeniu uległa infrastruktura IT a w szczególności serwer — przejść do realizacji procedury Plan awaryjny odtworzenie systemu informatycznego.

b) Jeśli zniszczeniu uległy media, uruchomić ich ponowną dostawę (energia, internet, telekomunikacja) Plan awaryjny na wypadek braku zasilania

c) Jeśli zniszczeniu uległy pomieszczenia, organizacja tymczasowej lokalizacji szkoły. Przeprowadzka do wyznaczonych i zaplanowanych wcześniej lokalizacji i pomieszczeń - odpowiedzialny: dyrektor szkoły.

d) Podanie informacji przez dyrektora do WSZ$5tkiCh zainteresowanych o ewentualnych zmianach w adresie lokalizacji i procedurach operacyjnych.

4. Wznowienie działalności

a) Podjęcie działań mających na celu likwidację szkód odniesionych w wyniku pożaru. Osoba odpowiedzialna: dyrektor szkoły.

b) Wypłata odszkodowania: Kontakt z Firmą ubezpieczeniową - Odpowiedzialny: sekretarz szkoły.

c) Sprawdzenie poprawności funkcjonowania zabezpieczeń p-poz.

d) Powiadomienie społeczności szkolnej o przywróceniu rutynowych działań operacyjnych

e) Podjęcie działań (ew. dyscypłinarnych) w przypadku ujawnienia jako przyczyny pożaru — działalności pracownika.

f) Organizacja szkolenia w zakresie ochrony p-poz oraz zachowywania sie w trakcie pożaru.

g) Co najmniej raz w roku przeprowadzenie testów w zakresie pozorowanego pożaru wraz z oceną zachowania koordynatora oraz pracowników.

Plan awaryjny na wypadek braku zasilania w sieci komputerowej

1. W przypadku stwierdzenia braku zasilania w sieci komputerowej ASl/dyrektor kontaktuje się z dostawcą prądu ENEA, tel. kontaktowy 991 lub 611111111

2. W przypadku awarii prądu trwającej dłużej niż wystarczy zasilanie przez baterię laptopa to ASI/dyrektor zobowiązany jest do powiadomienia wszystkich użytkowników o konieczności zapisania swojej pracy i zakończenia pracy w systemach.

Plan awaryjny na wypadek utraty dostępu do sieci internetowej

1. W przypadku niedostępności internetu awarię zgłasza ASi/ dyrektor do Orange pod numerem telefonu: 510 100 100

Załącznik nr 4 do Polityki Bezpieczeństwa Informacji

i. e

PROTOKÓŁ AUDYTU BEZPIECZEŃSTWA INFORMACJI w Zespole Szkół Branżowych i Ogólnokształcących w Łabiszynie

Wzór

Audytor: _____
Data opracowania: _____

Wstęp

0 opracowaniu

Niniejsze opracowanie wykonane zostało na zlecenie _____i ma na celu ocenę jakości stosowanego w organizacji Systemu Zarządzania Bezpieczeństwem Informacji. W ramach prac audytowych przeprowadzonych w dniach _____dokonano oceny rozwiązań technicznych, informatycznych oraz organizacyjnych stosowanych w celu zapewnienia bezpieczeństwa informacji, a w szczególności spełnienia wymogów określonych w rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012r, w sprawie Krajowych Ram lnteroperacyjności.

Zastosowane kryteria oceny

Niniejsze opracowanie zawiera ocenę stosowanych rozwiązań oi aż sugestie dotyczące możliwości podniesienia poziomu bezpieczeństwa rozumianego jako jednoczesne spełnienie kryteriów: poufności, integralności, dostępności oraz rozliczalności. Propozycje dotyczące usprawnień przygotowane zostały w oparciu o aktualnie panujące standardy branżowe oraz tzw. „dobre praktyki", z uwzględnieniem wysokiego poziomu bezpieczeństwa informacji jako podstawowego kryterium.

Program audytu

Audyt Systemu Zarządzania Bezpieczeństwem Informacji

Przeprowadzenie audytu ma na celu ustalenie stopnia spełnienia wymogów bezpieczeństwa informacji zdefiniowanych w rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012r. w sprawie Krajowych Ram Interoperacyjności. W ramach prac audytowych dokonano oceny Systemu Zarządzania Bezpieczeństwem Informacji i poddano weryfikacji następujące jego cechy (na podstawie §20 ww. rozporządzenia):

1. Zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia;

2. Utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwai'zania informacji obejmującej ich rodzaj i konfiguracji

3. Przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;

4. Podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na *celu* zapewnienia bezpieczeństwa *in*formacji;

5. Bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o l‹tórycli mowa w pkt 4;

6. Zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:

- zagrożenia bezpieczeństwa informacji,
- skut1‹i naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,
- stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich;

7. Zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawniony dostępem, uszkodzeniami lub zakłóceniami, przez:

- monitorowanie dostępu do informacji,
- czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,
- zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;

8, Ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;

9. Zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;

10. Zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;

11. Ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;

12. Zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:

- dbałości o aktualizację oprogramowania,
- minimalizowaniu ryzyka utraty informacji w wyniku awarii,
- ochronie przed błędami, utratą, nieuprawnioną modyfikacją,
- stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,
- zapewnieniu bezpieczeństwa plików systemowych,
- redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,
- niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,
- kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;

13. Bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa inrormacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.
14. Zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

Stopień spełnienia wymogów KRI dotyczących bezpieczeństwa informacji

0kreslone w Rozporządzeniu o KRl wymogi zakładają zaplanowanie, wdrożenie i eksploatacji Systemu Zarządzania Bezpieczeństwem Informacji w rozumieniu normy 150 27001. Jak stwierdzono w rozporządzeniu, posiadanie certyfikatu zgodności z powyższą normą jest warunkiem wystarczającym do stwierdzenia pełnego spełnienia wymogów. W przypadku nieposiadania certyfil‹atu na zgodność z 150 27001 konieczne jest spełnienie minimum 14 wymogów zdefiniowanych w rozporządzeniu.
Stopień dostosowania do powyższych założeń oceniony został w oparciu o prowadzone prace audytowe, w tym: obserwacje przeprowadzone na miejscu, analizę dokumentacji oraz ankietę-wywiad przeprowadzoną z pracownikami jednostki. Poniżej zaprezentowano wnioski i ewentualne zalecenia dotyczące możliwych usprawnień w zakresie każdego z 14 wymogów wymienionych w punkcie 2.1.

Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji

Wymóg: Rozporządzenie KRI, §20 ust. 1
Podejmowane działania

Wnioski

Zapewnienie aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia.

Wymóg: Rozporządzenie KRI, §20 ust. 2.1
Podejmowane działania

Wnioski

Utrzymywanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.

Wymóg: Rozporządzenie **KRI,** §20 ust. 2.2
Podejmowane działania

Wnioski

Przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy.

Wymóg: Rozporządzenie KRI, §20 ust. 2.3
Podejmowane działania

Wnioski

Podejmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji.

Wymóg: Rozporządzenie KRl, §20 ust. 2.4 Podejmowane działania

Wnioski

Bezzwłoczna zmiana uprawnień, w przypadku zmiany zadań osób, o których mowa w punkcie poprzednim

Wymóg: Rozporządzenie KRI, §20 ust. 2.5 Podejmowane działania

Wnioski

Zapewnienie szkolenia osób zaangażowanych w proces przetwarzania informacji

Wymóg: Rozporządzenie KRI, §20 ust. 2.6 Podejmowane działania

Wnioski

Zapewnienie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez monitorowanie, wykrywanie nieautoryzowanych działań i zastosowanie śroćlków chroniących przed nieautoryzowanym dostępem.

Wymóg: Rozporządzenie KRI, §20 ust. 2.7 Podejmowane działania

Wnioski

Ustanowienie podstawowych zasad gwarantujących bezpieczny pracę przy przetwarzaniu mobilnym i pracy na odległość

Wymóg: Rozporządzenie KRI, §20 ust. 2.8 Podejmowane działania

Wnioski

Zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie

Wymóg: Rozporządzenie KRI, §20 ust. 2.9
Podejmowane działania

Wnioski

Zapewnienie w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.

Wymóg: Rozporządzenie KRI, §20 ust. 2.10
Podejmowane działania

Wnioski

Ustalenie zasad postępowania z informacjami zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych

Wymóg: Rozporządzenie KRI, §20 ust. 2.11
Podejmowane działania

Wnioski

Zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych

Wymóg: Rozporządzenie KRI, §20 ust. 2.12
Podejmowane działania
Wnioski

Bezzwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób umożliwiający szybkie podjęcie działań korygujących

Wymóg: Rozporządzenie KRI, §20 ust. 2.13
Podejmowane działania

Wnioski

Zapewnienie okresowego audytu wewnetrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok

Wymóg: Rozporządzenie KRI, §20 ust. 2.14
Podejmowane działania

Wnioski

Podsumowanie

Wyszczególnienie załączników stanowiących składowa część sprawozdania z audytu

…….
Data, miejsce i podpis audytora