Załącznik nr 1 do Zarządzenia nr ……..
Dyrektora Zespołu Szkolno - Przedszkolnego
w Słodkowie z dnia ……..

STANDARDY BEZPIECZEŃSTWA INFORMACJI

Zespół Szkolno - Przedszkolny w Słodkowie

Słodków 21

62-700 Turek

Zatwierdzam:

……
Data i podpis Administratora

Spis treści

Rozdział 1 Postanowienia ogólne

1. Standardy Bezpieczeństwa Informacji, zwana dalej SBI, opisuje zasady zarządzania bezpieczeństwem informacji w Zespole Szkolno - Przedszkolnym w Słodkowie. Działanie systemu zarządzania bezpieczeństwem informacji opiera się na modelu PDCA (Plan/Do/Check/Act). Stosowane w Standardach Bezpieczeństwa Informacji rozwiązania odpowiadają wymaganiom określonym w § 20 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.
2. Niniejsze Standardy Bezpieczeństwa Informacji dotyczy wszelkich danych przetwarzanych przez pracowników stanowiących informacje wytworzone w ramach działania i pracy 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 dyrektywy95/46/WE (ogólne rozporządzenie o ochronie danych);
   2) innych danych niż dane osobowe oraz informacji, które podlegają ochronie, niezależnie od formy, w jakiej są przechowywane (papierowej, elektronicznej) oraz technologii informatycznych wykorzystywanych do przetwarzania tych danych.
3. Elementami SBI 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, a także użytkowania systemów informatycznych.
4. Celem SBI 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 Zespołu Szkolno - Przedszkolnego w Słodkowie w dziedzinie bezpieczeństwa informacji;
   6) zaangażowanie wszystkich pracowników Zespołu Szkolno - Przedszkolnego w Słodkowie w ochronę informacji;
   7) wsparcie w zakresie utrzymania odpowiedniego poziomu bezpieczeństwa informacji poprzez zarządzanie ryzykiem, zarządzanie zmianami, zarządzanie ciągłością działania;
   8) stworzenie podstaw dla Systemu Zarządzania Bezpieczeństwem Informacji.
5. Za prawidłowe działanie systemu zarządzania bezpieczeństwem informacji odpowiada Dyrektor Zespołu Szkolno - Przedszkolnego w Słodkowie.
6. Ilekroć w niniejszych Standardach jest mowa o:
   1) Zespole – należy przez to rozumieć Zespół Szkolno - Przedszkolny w Słodkowie;
   2) Dyrektorze – należy przez to rozumieć Dyrektora Zespołu Szkolno - Przedszkolnego w Słodkowie;
   3) SZBI – należy przez to rozumieć system zarządzania bezpieczeństwem informacji stosowany w jednostce, czyli wszelkie procedury, regulaminy, instrukcje, zasady i inne dokumenty obowiązujące , których celem jest zapewnienie bezpieczeństwa informacjom.

4) Aktywie (zasobie) – należy przez to rozumieć wszystko co ma znaczenie dla jednostki, 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 Zespołu Szkolno - Przedszkolnego w Słodkowie 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 i osoby przez siebie wyznaczonej.
2. Do podstawowych zadań Dyrektora i powołanego ciała doradczego należy:
   1) przegląd i zatwierdzanie zmian w SBI;
   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 należą:
   1) Przestrzeganie wprowadzonych zasad bezpieczeństwa informacji i systemów informatycznych;
   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 …….. 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 Dyrektorowi;
   6) aktywny udział w procesie reagowania na incydenty w zakresie bezpieczeństwa oraz w usuwaniu ich skutków;
   7) inicjowanie zmian w systemach, SBI, 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 z Zespołem mogą okresowo lub stale współpracować osoby realizujące zadania na rzecz jednostki. 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 pacy 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 wrzuca się płyt CD/DVD oraz innych nośników – należy je przekazać Dyrektorowi Zespołu. 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 Zespołu, 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 jednostce 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 niniejszych standardów – 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 Zespole Szkolno - Przedszkolnym w Słodkowie.
3. Z instrukcją obowiązani są zapoznać się wszyscy pracownicy korzystający 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 oraz zapewnienie dostępności i zabezpieczenie zapisów (dowód wykonania czynności operacyjnych lub związanych z działaniami SZBI), informacji (danych) niezbędnych do prowadzenia działalności przez jednostkę 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 przechowywana.
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).
4) Zarządzanie dokumentami:
   a) dokumentacja wewnętrzna zarządzana jest zgodnie z zasadami określonymi w *Instrukcji Kancelaryjnej, Statucie oraz Instrukcji Archiwalnej/JRWA.*
   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 jednostce,
   c) zmiany w dokumentacji wewnętrznej wprowadzane są zgodnie z obowiązującymi w tym zakresie przepisami i rozwiązaniami przyjętymi w jednostce,
   d) o zmianach w dokumentacji informowani są pracownicy, jeśli zmiany ich dotyczą, zgodnie z obowiązującymi w jednostce procedurami,

e) dokumentacja opisująca procedury bezpieczeństwa stosowane w jednostce 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.
3) Do typowych zagrożeń bezpieczeństwa informacji należą:
   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:
   a) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
   b) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych),
   c) 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 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 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, Dyrektor 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 Zespole 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, IOD, i pozostałe osoby wyznaczone przez Dyrektora.
4) Sztab kryzysowy jest odpowiedzialny za opracowanie procedur ciągłości działania i wyznaczenie odpowiedzialności sposób za realizację tych procedur.
5) Dyrektor Zespołu odpowiedzialny za identyfikację zdarzeń krytycznych, które wymagać będą uruchomienia planów postępowania w sytuacjach awaryjnych i Planów Ciągłości Działania. Zdarzenia te muszą powodować znaczne straty lub szkody.
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.
7) Dyrektor 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 „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 odpowiada 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 § 20 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz 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 jest odpowiedzialny za planowanie i przeprowadzanie audytów wewnętrznych z roczną częstotliwością lub częściej.
3) Dyrektor 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 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 IOD lub Dyrektor stwierdził konieczność podjęcia działań korygujących lub zapobiegawczych, określa:

a) źródło powstania incydentu / zagrożenia lub słabości,
b) zakres działań korygujących lub zapobiegawczych,
c) termin realizacji,
d) osobę odpowiedzialną.

5) Dyrektor jest odpowiedzialny za nadzór nad poprawnością i terminowością wdrażanych działań korygujących lub zapobiegawczych.
6) Po przeprowadzeniu działań korygujących lub zapobiegawczych, Dyrektor jest zobowiązany do oceny efektywności ich zastosowania.
7) Powyższe czynności rejestrowane są w załączniku nr 5 – Zadania Dyrektora.

Rozdział 6 Postanowienia końcowe

1. Nieprzestrzeganie zasad zawartych w dokumentach SBI, 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. SBI i dokumenty z nią związane są dostępne w pokoju Dyrektora.

POLITYKA ZARZĄDZANIA RYZYKIEM BEZPIECZEŃSTWA INFORMACJI

w Zespole Szkolno - Przedszkolnym w Słodkowie

ROZDZIAŁ 1

Postanowienia ogólne

§ 1.

Ilekroć w dokumencie jest mowa o:

- **ryzyku** – należy przez to rozumieć możliwość zaistnienia zdarzenia, które będzie miało wpływ na realizację założonych celów w zakresie zapewnienia bezpieczeństwa informacji. Ryzyko mierzone jest siłą skutku oddziaływania oraz prawdopodobieństwem jego wystąpienia;
- **zarządzaniu ryzykiem** – należy przez to rozumieć realizowany przez Dyrektora Zespołu proces, którego celem jest identyfikacja potencjalnych ryzyk, które mogą mieć wpływ na realizację celów i zadań jednostki w zakresie zapewniania bezpieczeństwa informacji;
- **mapie ryzyka** – tabela (macierz) odzwierciedlająca ocenę siły oddziaływania i prawdopodobieństwo wystąpienia zidentyfikowanego ryzyka w Zespole;
- **rejestrze ryzyk** – należy przez to rozumieć dokument odzwierciedlający przeprowadzoną identyfikację i analizę ryzyk, a także przyjętą reakcję na ryzyko;
- **dyrektorze**– należy przez to rozumieć Dyrektora Zespołu Szkolno - Przedszkolnego w Słodkowie;
- **jednostce** – należy przez to rozumieć Zespół Szkolno - Przedszkolny w Słodkowie;
- **SBI** – należy przez to rozumieć dokument Standardy Bezpieczeństwa Informacji.

§ 2.

Polityka zarządzania ryzykiem bezpieczeństwa informacji obejmuje:

- zakres zadań i obowiązków podmiotów uczestniczących w procesie zarządzania ryzykiem;
- zasady i tryb identyfikacji ryzyka;
- zasady i tryb dokonywania analizy ryzyka;
- zasady określania właściwej reakcji na ryzyko.

§ 3.

Polityka zarządzania ryzykiem ma zastosowanie dla wszystkich samodzielnych stanowisk wskazanych w Regulaminie Organizacyjnym Zespołu Szkolno - Przedszkolnego w Słodkowie.

§ 4.

Zarządzanie ryzykiem jest procesem ciągłym i nie ogranicza się do działań określonych w § 2.

§ 5.

Celem zarządzania ryzykiem bezpieczeństwa informacji jest zwiększenie prawdopodobieństwa osiągnięcia wyznaczonych celów i zadań, poprzez ograniczenie prawdopodobieństwa wystąpienia ryzyka oraz zabezpieczanie się przed jego skutkami. Następuje to poprzez:

- rozpoznanie – czyli identyfikowanie ryzyka, określenie rodzajów ryzyk, które wiążą się z działalnością Zespołu i dokonywanie ich pomiaru;
- ocenę ryzyka i jego istotności, przy pomocy skali określonej w § 9;
- zarządzanie ryzykiem, które polega na badaniu efektywności i skuteczności podejmowanych działań, poprzez system kontroli instytucjonalnej i zewnętrznej;
- kontrolę zarządzania ryzykiem, której istotą podjętych działań jest ocena zastosowanych metod redukcji ryzyka, prowadząca do skutecznego i efektywnego realizowania celów i nałożonych zadań.

§ 6.

Niezbędnymi warunkami wdrożenia polityki zarządzania ryzykiem są:

- określenie jasnych, spójnych i zgodnych z misją jednostki celów i zadań;
- ustalenie mierzalnych wskaźników realizacji wyznaczonych celów i zadań;
- określenie poziomu ryzyka akceptowalnego dla wyznaczonych celów i zadań;
- prowadzenie bieżącego monitoringu realizacji celów i zadań;
- prowadzenie analizy poprawności i stosowania mechanizmów kontroli zarządczej.

ROZDZIAŁ 2

Zakresy zadań i obowiązków

§ 7.

1. Za realizację polityki zarządzania ryzykiem bezpieczeństwa informacji odpowiada Dyrektor Zespołu Szkolno - Przedszkolnego w Słodkowie poprzez:
    - kształtowanie i wdrażanie polityki zarządzania ryzykiem;
    - nadzór i monitorowanie skuteczności procesu zarządzania ryzykiem;
    - wyznaczanie poziomu akceptowalnego dla każdego ryzyka;
    - podejmowanie decyzji dotyczących sposobu reakcji na poszczególne ryzyka.

2. Pracownicy na samodzielnych stanowiskach odpowiadają za zarządzanie ryzykiem poprzez:
    - identyfikację ryzyk związanych z realizacją przydzielonych zadań;
    - wskazywanie właścicieli zidentyfikowanych ryzyk;
    - przeprowadzanie analizy zidentyfikowanego ryzyka;
    - proponowanie sposobu postępowania w odniesieniu do poszczególnych ryzyk;
    - wdrażanie działań zaradczych w stosunku do zidentyfikowanego ryzyk.

3. Pracownicy wymienieni w ust. 2 są zobowiązani do współpracy z Dyrektorem Zespołu Szkolno - Przedszkolnego w Słodkowie.

ROZDZIAŁ 3
Identyfikacja ryzyka

§ 8.

1. Identyfikacja ryzyk prowadzona jest na poziomie jednostki i na poziomie poszczególnych samodzielnych stanowisk pracy.
2. Proces identyfikacji ryzyka odbywa się jednokrotnie w ciągu roku kalendarzowego tj. nie później niż w ostatnim dniu roboczym stycznia i nie później niż w ostatnim dniu roboczym listopada.
3. W procesie identyfikacji ryzyka uwzględnia się czynniki sprzyjające wystąpieniu ryzyk według obszarów wrażliwych, określonych w załączniku nr 1 do Polityki Zarządzania Ryzykiem.
4. W procesie identyfikacji ryzyka uwzględnia się czynniki je kształtujące. Ze względu na ich źródło ryzyka dzielą się na:
    - zewnętrzne – rodzaj ryzyka determinowanego przez czynniki zewnętrzne;
    - wewnętrzne – ryzyko to obejmuje działania wewnętrzne jednostki i może być zarządzane wewnątrz jednostki.

5. Każde zidentyfikowane ryzyko ujmuje się w rejestrze, stanowiącym załącznik nr 2 do Polityki Zarządzania Ryzykiem.
6. Dla każdego zidentyfikowanego ryzyka ustala się jego właściciela.
7. Każdy pracownik ma prawo i obowiązek zgłaszania swojemu bezpośredniemu przełożonemu ryzyk zidentyfikowanych podczas wykonywania przydzielonych zadań.

ROZDZIAŁ 4

Analiza ryzyka

§ 9.

1. Każde ryzyko podlega analizie pod kątem jego istotności na osiąganie celów i zadań. Istotność ryzyka jest iloczynem skali prawdopodobieństwa jego wystąpienia i wartości oszacowanych potencjalnych skutków.
2. Każde ryzyko jest oceniane pod względem prawdopodobieństwa jego wystąpienia i skutku oddziaływania.
3. W celu dokonania oceny ryzyka wykorzystuje się Mapę Ryzyka, którą stanowi macierz prawdopodobieństwo – skutek – załącznik nr 3 do Polityki Zarządzania Ryzykiem.
4. Mapa ryzyka definiuje ryzyka na:
    - niskie o wartości 10 i mniejszej;
    - średnie o wartości powyżej 10 i mniejszej lub równej 50;
    - wysokie – o wartości powyżej 50.
5. Przy ocenie prawdopodobnych skutków wystąpienia ryzyka przyjmuje się skalę punktową od 1 do 5, gdzie;
    - 1-2 – oznacza skutek nieznaczny;
    - 3-4 – oznacza skutek mały;
    - 5-6 – oznacza skutek średni;
    - 7-8 – oznacza skutek poważny;
    - 9-10 – oznacza skutek katastrofalny.

6. Przy ocenie prawdopodobieństwa wystąpienia ryzyka przyjmuje się skalę punktową od 1 do 5, gdzie:

- 1-2 – oznacza prawdopodobieństwo bardzo małe (0-20 %);
- 3-4 – oznacza prawdopodobieństwo małe (21 - 40%);
- 5-6 – oznacza prawdopodobieństwo średnie (41 - 60 %);
- 7-8 – oznacza prawdopodobieństwo duże (61 - 80 %);
- 9-10 – oznacza prawdopodobieństwo bardzo duże (81 -100 %).

7. Wskaźniki do punktacji oceny prawdopodobieństwa i skutków ryzyka określa załącznik nr 4.

8. Dyrektor Zespołu Szkolno - Przedszkolnego w Słodkowie oznacza poziom akceptowalny dla danego ryzyka – oznacza go ukośnymi zakreśleniami w mapach opracowanych na dany rok kalendarzowy.

ROZDZIAŁ 5

Reakcja na ryzyko

§ 10.

Dla każdego istotnego zidentyfikowanego ryzyka właściciel ryzyka wskazuje optymalną reakcję. Przyjmuje się niżej wymienione reakcje na ryzyko:

1. tolerowanie – będzie to miało miejsce w przypadkach, kiedy koszty skutecznego przeciwdziałania ryzyku mogą przekraczać jego potencjalne korzyści, zdolności do skutecznego przeciwdziałania są ograniczone lub wykraczające poza decyzje i działania wewnętrzne;
2. przeniesienie – dotyczyć to będzie kategorii ryzyk w odniesieniu, do których nastąpi przeniesienie ich na inną instytucję, między innymi poprzez ubezpieczenie lub zlecenie usług na zewnątrz;
3. wycofanie się – dotyczyć to będzie grupy ryzyk, dla których mimo podejmowanych działań nie udało się zmniejszyć ich istotności do akceptowanego poziomu;
4. przeciwdziałanie – dotyczyć to będzie kategorii ryzyk, które wymagać będą podjęcia zdecydowanych, przemyślanych i zaplanowanych działań prowadzących do ich likwidacji, lub znacznego ograniczenia.

ROZDZIAŁ 6

Postanowienia końcowe

§ 11.

1. Polityka Zarządzania Ryzykiem obowiązuje od …….. roku.
2. Pracownicy Zespołu Szkolno - Przedszkolnego w Słodkowie obowiązani są do systematycznej analizy wystąpienia ryzyk na stanowiskach pracy i zgłaszania ich Dyrektorowi.

_____
/ Dyrektor/

Załączniki do Polityki Zarządzania Ryzykiem Bezpieczeństwa Informacji:

1. Załącznik nr 1 – Wykaz obszarów ryzyka w Zespole Szkolno - Przedszkolnym w Słodkowie;
2. Załącznik nr 2 – Rejestr ryzyk – wzór dokumentu;
3. Załącznik nr 3 – Mapa ryzyka – wzór dokumentu;
4. Załącznik nr 4 – Wytyczne do oceny prawdopodobieństwa wystąpienia i siły oddziaływania ryzyk.

WYKAZ OBSZARÓW RYZYKA
W ZESPOLE SZKOLNO - PRZEDSZKOLNYM W SŁODKOWIE

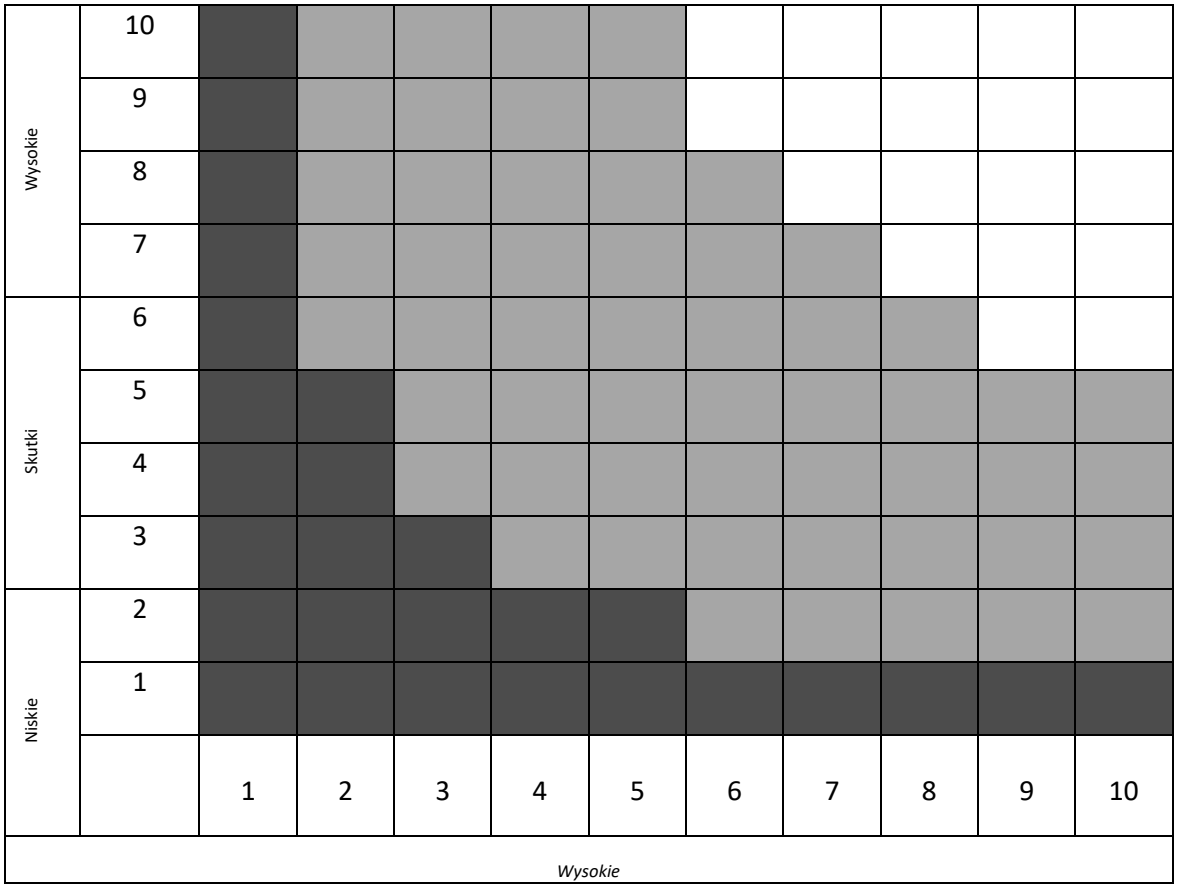
1. Administracja.
2. Bezpieczeństwo, w tym bezpieczeństwo uczniów.
3. Realizacja zadań statutowych Zespołu, w tym realizacja podstaw programowych.
4. Zagrożenia epidemiologiczne.
5. Usługi zewnętrzne i ich jakość.
6. Bezpieczeństwo systemów informatycznych.
7. Zdarzenia losowe – pożar, powódź, zalanie, awarie.

REJESTR RYZYK
W ZESPOLE SZKOLNO - PRZEDSZKOLNYM W SŁODKOWIE

Numer ryzyka	Zdefiniowane ryzyko	Prawdopodobieństwo wystąpienia	Skutek	Plan rekcji
1	Atak terrorystyczny			▪ Ubezpieczenie ▪ Współpraca z organami ścigania
2	Awaria instalacji technicznych			▪ Remonty, przeglądy ▪ Zapasowe sieci
3	Awaria łączy internetowych			▪ Korzystanie z łączy alternatywnych
4	Awaria łączy telekomunikacyjnych			▪ Korzystanie z łączy alternatywnych ▪
5	Awaria zasilania			▪ Remonty i przeglądy sieci elektrycznej ▪ Zasilanie awaryjne
6	Awaria systemu komputerowego			▪ System kopii zapasowych ▪ Serwis
7	Celowa nieautoryzowana modyfikacja danych			▪ System kopii zapasowych ▪ Postępowanie dyscyplinarne ▪ Współpraca z organami ścigania
8	Choroba pracownika			▪ Praca zdalna ▪ Zastępstwa
9	Epidemia			▪ Praca zdalna
10	Katastrofa budowlana			▪ Ubezpieczenie ▪ System kopii zapasowych
11	Kradzież danych			▪ System kopii zapasowych ▪ Współpraca z UODO i organami ścigania
12	Kradzież sprzętu			▪ Ubezpieczenie ▪ Kopie zapasowe
13	Nie stosowanie się do regulaminów			▪ Szkolenia ▪ Postępowanie dyscyplinarne
14	Nieautoryzowane wpięcie do sieci			▪ Kopie zapasowe ▪ Współpraca z UODO i organami ścigania
15	Nieprawidłowe działanie oprogramowania			▪ Serwis ▪ Modyfikacja
16	Nieświadomość pracownika			▪ Szkolenia

17	Nieumyślna modyfikacja danych			▪ Kopie zapasowe ▪ Współpraca z UODO i organami ścigania
18	Nieumyślne niszczenie danych			▪ Kopie zapasowe ▪ Współpraca z UODO i organami ścigania
19	Udostępnienie informacji osobom nieuprawnionym			▪ Szkolenia ▪ Współpraca z UODO i organami ścigania
20	Podszycie się pod inną osobę			▪ Szkolenia ▪ Współpraca z UODO i organami ścigania
21	Podsłuch			▪ System zabezpieczeń sieci teleinformatycznej ▪ Współpraca z UODO i organami ścigania
22	Powódź			▪ Ubezpieczenie ▪ System kopii zapasowych
23	Pożar			▪ Ubezpieczenie ▪ System kopii zapasowych
24	Przekroczenia kompetencji			▪ Szkolenia ▪ Postępowanie dyscyplinarne
25	Sabotaż			▪ System zabezpieczeń sieci teleinformatycznej ▪ Współpraca z organami
26	Uchybienia proceduralne			▪ Szkolenia ▪ Postępowanie dyscyplinarne
27	Umyślne zniszczenie informacji			▪ System kopii zapasowych ▪ Współpraca z UODO i organami ścigania ▪
28	Utrata kopii zapasowych			▪ System kopii zapasowych
29	Włamanie			▪ Ubezpieczenie ▪ Współpraca z UODO i organami ścigania
30	Włamanie o systemu			▪ Współpraca z organami ścigania ▪ Współpraca z UODO i organami ścigania

Mapa ryzyka



Wytyczne do oceny prawdopodobieństwa wystąpienia i siły oddziaływania ryzyka

Opis prawdopodobieństwa Wystąpienia	*Oszacowane ryzyko*	*Opis oddziaływania (skutków)*	*Oszacowane ryzyko*
Ryzyko nie występuje lub może wystąpić w zupełnie wyjątkowych sytuacjach. Obszar działania / proces nie dotyczy zadań strategicznych, nie należy do priorytetowych czynności generujących ryzyko. Przy realizacji zadań w ramach danego obszaru / procesu współpracuje się z jednym bądź dwoma komórkami organizacyjnymi. Dany obszar działania / proces funkcjonuje powyżej roku od wprowadzenia zmian technologicznych, organizacyjnych i kadrowych. Oceniany obszar / proces uregulowany jest wyłącznie regulacjami wewnętrznymi.	**1-2** **Bardzo małe**	**Organizacyjne:** Niska niezgodność z procedurami / przepisami prawa. Nie występuje zagrożenie utraty informacji ani dobrego wizerunku. Ewentualne zakłócenia bez wpływu na realizację zadań i osiąganie celów. Ewentualne skutki ograniczane (neutralizowane) przez istniejące mechanizmy kontrolne. **Finansowe:** Nie przewiduje się wystąpienia straty finansowej, dodatkowych kosztów - bądź nieznaczne do 1000 zł.	**1-2** **nieznaczne**
Ryzyko prawdopodobnie nie wystąpi. Przy realizacji zadań w ramach danego obszaru / procesu współpracuje się z małą (ograniczoną) liczbą komórek organizacyjnych. W ostatnim okresie (np. 1 rok) obszar / proces nie podlegał zmianom technologicznym, organizacyjnym i kadrowym, bądź podlegał zmianom w minimalnym stopniu i uznaje się je za wdrożone. Obszar / proces w małym zakresie objęty regulacjami o charakterze zewnętrznym. Nie podlegały one zmianom. Niepożądane zakłócenia mogą powodować utrudnienia w realizacji zadań. Potencjalne zakłócenia wykonywania zadań nie mają wpływu na realizację celów.	**3-4** **małe**	**Organizacyjne:** Średnia niezgodność z procedurami lub niska niezgodność z postanowieniami umów. Małe zakłócenia pracy, ewentualne utrudnienia w realizacji zadań, nie mające wpływu na osiąganie celów. Istniejące mechanizmy kontrolne powinny ograniczyć skutki ewentualnych zakłóceń. Małe zagrożenie utraty informacji dobrego wizerunku. **Finansowe:** >1 000 do 5 000 zł	**3-4** **małe**
Ryzyko prawdopodobnie wystąpi w najbliższym okresie (od roku do pięciu lat). Przy realizacji zadań w ramach danego	**5-6** **średnie**	**Organizacyjne:** Niska niezgodność z przepisami prawa lub średnia niezgodność	**5-6** **średnie**

obszaru / procesu współpracuje się z innymi komórkami, bądź z podmiotami zewnętrznymi. W ciągu ostatniego roku obszar / proces podlegał ograniczonym zmianom organizacyjnym, technologicznym i kadrowym. Obszar / proces objęty w małym stopniu regulacjami zewnętrznymi, które mogły podlegać w ostatnim okresie zmianom. Może dotyczyć zadań o istotnym znaczeniu dla celów działalności.		z postanowieniami umów lub poważna niezgodność z procedurami. Średnie zakłócenia pracy. Potencjalne zagrożenia mogą doprowadzić do niewykonywania podstawowych zadań w określonym zakresie. Istniejące mechanizmy kontrolne tylko w pewnym stopniu mogą ograniczyć skutki ewentualnych zakłóceń. Średnie zagrożenie utraty informacji oraz dobrego wizerunku. **Finansowe:** > 5 000 do 10 000 zł.	
Istnieje duże prawdopodobieństwo na wystąpienie ryzyka w ciągu najbliższego okresu od roku do trzech lat. Obszar / proces wymaga współpracy z innymi komórkami bądź z podmiotami zewnętrznymi. W ciągu ostatniego roku obszar / proces podlegał zmianom technologicznym, organizacyjnym i kadrowym, z których część może wymagać poprawek i działań dostosowawczych. Obszar / proces objęty dużą liczbą regulacji prawnych (zewnętrznych i wewnętrznych). Zagrożenia mogą wywierać istotny wpływ na obszary działalności / procesy, mogą odnosić się do realizacji celów operacyjnych i strategicznych.	**7-8** **duże**	**Organizacyjne:** Średnia niezgodność z przepisami prawa lub poważna niezgodność z postanowieniami umów. Brak szczegółowych procedur dla prowadzonych procesów. Poważne zakłócenia pracy. Mogą doprowadzić do nie wykonania celów cyklicznie (stałe zagrożenie). Niska skuteczność istniejących mechanizmów kontrolnych. Wysokie zagrożenie utraty informacji oraz dobrego wizerunku. **Finansowe:** > 10 000 do 50 000 zł.	**7-8** **duże**
Ryzyko z pewnością wystąpi w ciągu najbliższego roku. Obszar / proces związany jest z działalnością większej liczby komórek organizacyjnych, wymaga współpracy z podmiotami zewnętrznymi. W ciągu ostatniego roku obszar / proces podlegał istotnym zmianom technologicznym, organizacyjnym i kadrowym / obszar podlega częstym zmianom tego typu / obszar jest w trakcie zmian. Obszar działania / proces uregulowany jest dużą liczbą regulacji prawnych	**9-10** **Bardzo duże**	Organizacyjne: Poważna niezgodność z przepisami prawa. Brak procedur dla danego procesu. Olbrzymie zakłócenia pracy. Zagrożenia spowodują brak zachowania ciągłości procesów działania, utrzymania funkcjonalności systemów niezbędnych do wykonywania podstawowych celów. Brak	**9-10** **Bardzo duże**

(wewnętrznych i zewnętrznych). Zagrożenia dotyczą zadań w ramach celów strategicznych i należących do priorytetowych czynności / obszarów generujących ryzyko.		osiągnięcia kluczowych celów. Brak odpowiednich mechanizmów kontrolnych bądź istniejące mechanizmy okazują się nieskuteczne. Bardzo wysokie zagrożenie utratą informacji oraz dobrego wizerunku. Zagrożenie bezpieczeństwa ludzi. Finansowe: > 50 000 zł, utrata znacznego majątku.	

Załącznik nr 2 Wykaz dokumentów i zapisów poddanych nadzorowi w ramach SZBI do Standardów 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	Wyznaczony pracownik ma uprawnienia do tworzenia, modyfikacji, usuwania dokumentów	Dyrektor zatwierdza dokument poprzez umieszczenie go na serwerze (tylko na ma do tego uprawnienia)	Dostęp „do odczytu" do wersji elektronicznej dokumentacji mają wszyscy pracownicy	Aktualizacja dokumentu polega na zmianie pliku na serwerze (Zmiana Numeru wersji i Daty wydania)
Dokumenty systemu ISO 27001 – Wersja papierowa	Wyznaczony pracownik ma uprawnienia do tworzenia, modyfikacji, usuwania dokumentów	Dyrektor zatwierdza dokument (Księgę jakości i politykę jakości) pisemnie	Dostęp do dokumentów w wersji papierowej mają wszyscy pracownicy	Aktualizacja wersji papierowej w segregatorze
Dokumenty wewnętrzne – Wersja elektroniczna na serwerze	Dyrektor lub osoba upoważniona przez Dyrektora ma uprawnienia do tworzenia, modyfikacji, usuwania dokumentów	Dyrektor zatwierdza dokument poprzez umieszczenie go na serwerze (tylko on ma do tego uprawnienia)	Dostęp „do odczytu" do wersji elektronicznej dokumentacji mają wszyscy pracownicy	Aktualizacja dokumentu polega na zmianie pliku na serwerze (Zmiana Numeru wersji i daty wydania)
Dokumenty wewnętrzne – Wersja papierowa	Dyrektor lub osoba upoważniona przez Dyrektora ma uprawnienia do tworzenia, modyfikacji, usuwania dokumentów	Dyrektor zatwierdza dokument i wprowadza zarządzeniem dokument	Dostęp do dokumentów w wersji papierowej mają wszyscy pracownicy	Aktualizacja wersji papierowej w księdze zarządzeń

Szczegółowy spis dokumentów wewnętrznych:

1) Standardy Bezpieczeństwa Informacji
2) Polityka zarządzania ryzykiem w bezpieczeństwie informacji
3) Instrukcja Zarządzania Systemem Informacji
4) Polityka Bezpieczeństwa Informacji
5) Plan ciągłości działania
6) Instrukcja kancelaryjna
7) Instrukcja archiwalna
8) Rejestr upoważnień

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	Ustawa z dnia 10 maja 2018r. o ochronie danych osobowych;
2	Ustawa z dnia 5 września 2016r. o usługach zaufania oraz identyfikacji elektronicznej;
3	Ustawa z dnia 4 kwietnia 2019r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych;
4	Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 stycznia 2007r. w sprawie Biuletynu Informacji Publicznej;
5	Rozporządzenie Ministra Kultury z dnia 16 września 2002r. (w sprawie postępowania z dokumentacją, zasad jej klasyfikowania i kwalifikowania oraz zasad i trybu przekazywania materiałów archiwalnych do archiwów państwowych (Dz. U. nr 167, poz. 1375);
6	Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 30 października 2006r. w sprawie niezbędnych elementów struktury dokumentów elektronicznych;
7	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);
8	Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych;
9	Ustawa z dnia 4 lutego 1994r. o prawie autorskim i prawach pokrewnych;
10	Art. 68 ustawy z dnia 27 sierpnia 2009r. o finansach publicznych;
11	Komunikat Ministerstwa Finansów nr 23 z dnia 16 grudnia 2009r. w sprawie „Standardów kontroli zarządczej dla sektora finansów publicznych" (Dz. Urzędowy Ministra Finansów Nr 15 poz. 84)
12	Rozporządzenie Prezesa Rady Ministrów z dnia 18 stycznia 2011r. 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	Kopie bezpieczeństwa oraz szafa z dokumentacją	2 lata
Zapisy bezpieczeństwa		Serwer lub segregator	Kopie bezpieczeństwa oraz szafa z dokumentacją	2 lata
Zapisy operacyjne (logi systemowe)		Serwer lub dokumentacja w poszczególnych działach	Kopie bezpieczeństwa oraz zabezpieczenie pomieszczeń działowych	5 lat

PLAN CIĄGŁOŚCI DZIAŁANIA
ZESPOŁU SZKOLNO - PRZEDSZKOLNEGO W SŁODKOWIE

Plan ciągłości działania na wypadek pożaru

1. Zgłaszanie incydentu:
   a) Pracownik, który zidentyfikował pożar niezwłocznie powiadamia straż pożarną pod numerem 112, Dyrektora Zespołu Szkolno - Przedszkolnego w Słodkowie;
   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 i hydrantów znajdujących się w budynku,
   b) do czasu przybycia Jednostek straży pożarnej, kierownictwa akcją obejmuje Dyrektor Zespołu 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 (ognie żgące), 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 Zespołu, przeprowadzka do wyznaczonych i zaplanowanych wcześniej lokalizacji i pomieszczeń – odpowiedzialny: Dyrektor Zespołu,
d) podanie informacji przez Dyrektora do wszystkich 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 Zespołu Szkolno - Przedszkolnego w Słodkowie wypłata odszkodowania: kontakt z firmą ubezpieczeniową – odpowiedzialny: Dyrektor Zespołu,
   b) sprawdzenie poprawności funkcjonowania zabezpieczeń p-poż,
   c) powiadomienie społeczności Zespołu o przywróceniu rutynowych działań operacyjnych,
   d) podjęcie działań (ew. dyscyplinarnych) w przypadku ujawnienia jako przyczyny pożaru – działalności pracownika,
   e) organizacja szkolenia w zakresie ochrony p-poż oraz zachowywania się w trakcie pożaru,
   f) 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 Dyrektor kontaktuje się z dostawcą prądu ……
   telefon kontaktowy……..

2. W przypadku awarii prądu trwającej dłużej niż wystarczy zasilane przez baterię laptopa to Dyrektora 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 Dyrektor
   do ……
   telefon kontaktowy ……..

Załącznik nr 4 Protokół audytu bezpieczeństwa informacji do Standardów Bezpieczeństwa Informacji

PROTOKÓŁ AUDYTU BEZPIECZEŃSTWA INFORMACJI W ZESPOLE SZKOLNO - PRZEDSZKOLNYM W SŁODKOWIE

Wzór

Audytor: ……..

Data opracowania: ……

Wstęp

O 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 Interoperacyjności.

Zastosowane kryteria oceny

Niniejsze opracowanie zawiera ocenę stosowanych rozwiązań oraz 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 przetwarzania informacji obejmującej ich rodzaj i konfigurację.
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 oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy.
5. 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 informacji.
6. Zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji za szczególnym uwzględnieniem takich zagadnień, jak:

- zagrożenia bezpieczeństwa informacji,

Skutki naruszenia zasad bezpieczeństwa 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 informacji 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

Określone w Rozporządzeniu o KRI wymogi zakładają zaplanowanie, wdrożenie i eksploatację Systemu Zarządzania Bezpieczeństwem Informacji w rozumieniu normy ISO 27001. Jak stwierdzono w Rozporządzeniu, posiadanie certyfikatu zgodności z powyższą normą jest warunkiem wystarczającym do stwierdzenia pełnego spełnienia wymogów. W przypadku nieposiadania certyfikatu na zgodność z ISO 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 przeprowadzony 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 KRI, §20 ust. 24
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 środków chroniących przed nieautoryzowanym dostępem.

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

.....

.....

.....

Wnioski

.....

.....

.....

Ustanowienie podstawowych zasad gwarantujących bezpieczną 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

……

……

……

Zawieranie 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 wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok

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

……

……

……

Wnioski

……

……

……

Podsumowanie

……

……

……

Wyszczególnienie załączników stanowiących składową część sprawozdania z audytu:

……

……

……

……..
data, miejsce i podpis audytora