Zał 1 do Zarządzenia 9/2025

POLITYKA BEZPIECZEŃSTWA INFORMACJI W PODMIOCIE

Szkoła Podstawowa nr 2 im. Księdza Jana Twardowskiego w Białymstoku

Spis treści

1. Wstęp 2
2. Terminologia 2
5. Zakres Systemu Bezpieczeństwa Informacji 5
6. Deklaracja Najwyższego Kierownictwa w zakresie bezpieczeństwa informacji 6
7. Organizacja bezpieczeństwa informacji 6
8. Dokumentacja systemu zarządzania bezpieczeństwem informacji 7
9. Zasady współpracy ze stronami zainteresowanymi 7
10. Polityka kontroli dostępu do informacji 7
11. Klasyfikacja informacji 8
12. Zarządzanie aktywami i ryzykiem 8
13. Autoryzacja nowych urządzeń 9
14. Zarządzanie systemami i sieciami 9
15. Bezpieczeństwo zasobów ludzkich 9
17. Zarządzanie ciągłością działania 10
18. Zarządzanie zmianami 10
19. Dobór zabezpieczeń 11
20. Zgodność z wymaganiami prawnymi i regulacyjnymi 11
21. Deklaracja ochrony własności intelektualnej 11
22. Postanowienia końcowe 12

1. Przedmiot procedury
2. Zakres stosowania
3. Odpowiedzialność i uprawnienia
4. Opis postępowania

5. **Działania zapewniające przywrócenie zdolności realizacji działalności statutowej**
6. **Testowanie planu**
7. **Szkolenie dla uczestników planu**
8. **Aktualizacja planu**

1. Wstęp

Polityka Bezpieczeństwa Informacji w jednostce stanowi zestawienie zasad, praw i reguł oraz doświadczeń i dobrych praktyk w zakresie zarządzania i ochrony danych i informacji w naszej organizacji. Polityka określa techniczne i organizacyjne środki służące do osiągnięcia celów stawianych przed systemem zarządzania bezpieczeństwem informacji, jakimi są: zapewnienie spełnienia wymagań prawnych, właściwe zabezpieczenie aktywów informacyjnych, ochrona przetwarzania danych, niezawodność funkcjonowania systemów, zmniejszenie ryzyka utraty informacji oraz systematyczna edukacja użytkowników, a w efekcie pełne zaangażowanie wszystkich pracowników w ochronę informacji. O skuteczności działania i rozwoju każdej organizacji świadczy stopień osiągania zamierzonego celu. W procesie tym kluczowe jest stosowanie współczesnych technik i technologii, narzędzi i systemów informatycznych oraz przetwarzania i zarządzania informacją. Informacja jest jednym z najważniejszych zasobów jednostki, dlatego powinna być chroniona na każdym szczeblu organizacji. Jednostka chroni zarówno informacje własne, jak i powierzone. Poufność, dostępność i integralność informacji ma kluczowe znaczenie dla utrzymania zgodności z przepisami prawa oraz wizerunku podmiotu wobec stron zainteresowanych. Dokument ma charakter deklaratywny, zawiera ogólne ramy, wymagania, zasady, procedury i instrukcje w zakresie ochrony informacji przetwarzanych oraz nadrzędny w stosunku do pozostałych wewnętrznych aktów prawnych dotyczących bezpieczeństwa informacji obowiązujących w podmiocie, tworząc z nimi kompleksową dokumentację bezpieczeństwa.

Polityka Bezpieczeństwa Informacji została wdrożona i jest stale doskonalona w celu:

1) zapewnienia poufności, integralności i dostępności danych;
2) zapewnienia identyfikowalności czynności i zasobów podczas przetwarzania danych;
3) zapewnienia niezawodności działań;
4) podejmowania wysiłków prowadzących do poprawy poziomu bezpieczeństwa zasobów informacyjnych w jednostce.

Polityka Bezpieczeństwa Informacji jest dokumentem nadrzędnym w stosunku do wszystkich dokumentów systemowych z zakresu zarządzania bezpieczeństwem informacji.

2. Terminologia

Ilekroć w Polityce Bezpieczeństwa Informacji jest mowa o:

- **„Polityce"** - należy przez to rozumieć Politykę Bezpieczeństwa Informacji;

3. Podstawy prawne:

Polityka Bezpieczeństwa Informacji oraz pozostałe dokumenty dotyczące zarządzania bezpieczeństwem informacji w jednostce spełniają wymagania prawne i regulacyjne, zawarte w:

1) ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. 2019, poz. 700 ze zmianami);
2) ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2019, poz. 1781);
3) ustawie z dnia 06 września 2001 r. o dostępie do informacji publicznej (Dz.U. 2019, poz. 1429);
4) ustawie z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. 2019, poz. 162 ze zmianami);
5) ustawie z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz.U. 2019, poz. 848);
6) ustawie z dnia 19 lipca 2019 r. o zapewnianiu dostępności osobom ze szczególnymi potrzebami (Dz.U. 2019, poz. 1696 ze zmianami);
7) rozporządzeniu Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych Dz.U. 2024 poz. 773;
8) rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28 sierpnia 2014, str.73);
9) rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2018.119.1); 10) normie PN-ISO/IEC 27001:2017-06.

4. Definicje:

1) **Informacja –** wszelkie zapisy w formie papierowej, w systemach komputerowych oraz na innych nośnikach przetwarzane w systemach tradycyjnych, elektronicznych i komunikacyjnych będących własnością jednostki, funkcjonujących lub tylko administrowanych przez podmiot;
2) **Bezpieczeństwo informacji** – zachowanie poufności, integralności i dostępności informacji w wyniku stosowania procesu zarządzania ryzykiem;
3) **Aktyw/zasób** – wszystko to, co ma wartość dla organizacji w zakresie informacji (zarówno informacje, jak i środki techniczne oraz organizacyjne do ich przetwarzania).
4) **Poufność** – zapewnienie dostępu do informacji tylko osobom upoważnionym.
5) **Integralność** – zapewnienie że dokument nie zostanie zmieniony w sposób nieuprawniony.

6) **Dostępność** – zapewnienie, że osoby upoważnione będą miały dostęp do informacji zawsze gdy jest to im niezbędne.
7) **Ryzyko** – prawdopodobieństwo wystąpienia zagrożenia, które wykorzystując podatność(ci) aktywu, może doprowadzić do jego uszkodzenia lub zniszczenia.
8) **Szacowanie ryzyka** – całościowy proces analizy i oceny ryzyka.
9) **Postępowanie z ryzykiem** – proces wyboru i wdrażania środków modyfikujących ryzyko.
10) **Zarządzanie ryzykiem** – proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych przy zachowaniu akceptowalnego poziomu kosztów.
11) **Zdarzenie związane z bezpieczeństwem informacji** – określony stan systemu, usługi lub sieci, który wskazuje na możliwe naruszenie polityki bezpieczeństwa informacji, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem.
12) **Incydent bezpieczeństwa informacji** – pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji.
13) **Dane osobowe** – wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"). Osoba fizyczna możliwa do zidentyfikowania to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.
14) **Administrator** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania.
15) **Inspektor Ochrony Danych (IOD)** – wyznaczona przez Administratora osoba, do zadań którego należy zapewnienie przestrzegania przepisów o ochronie danych osobowych.

5. Zakres Systemu Bezpieczeństwa Informacji

SZBI w jednostce stanowi część Zintegrowanego Systemu Zarządzania, odnoszącą się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji. SZBI został opracowany i wdrożony.

Zakresy określone przez dokument Polityki Bezpieczeństwa Informacji mają zastosowanie do całego systemu informacyjnego podmiotu, w szczególności do:

1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są informacje podlegające ochronie;
2) informacji będących własnością jednostki;
3) informacji będących własnością klientów podmiotu, uzyskanych na podstawie zawartych umów;
4) wszystkich lokalizacji jednostki, czyli budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie;
5) wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, zleceniobiorców, konsultantów, wolontariuszy, stażystów, praktykantów i innych osób mających dostęp do informacji podlegających ochronie.

Dążąc do możliwe jak najlepszego zabezpieczenia informacji i aktywów wspierających ich przetwarzanie wprowadza się do stosowania podstawowe zasady bezpieczeństwa informacji:

1) **zasada „adekwatności zabezpieczeń"** – stosowane zabezpieczenia muszą być adekwatne do zidentyfikowanych zagrożeń,
2) **zasada „bezpiecznego przetwarzania"** - przetwarzanie informacji szczególnie chronionych powinno odbywać się wyłącznie w bezpiecznych środowiskach, tj. w wydzielonych systemach informatycznych, zabezpieczonych pomieszczeniach etc.,
3) **zasada „bezpiecznej współpracy z podmiotami zewnętrznymi"** - dokumenty regulujące współpracę z podmiotami zewnętrznymi (m.in. treść umów i porozumień) zawierają zapisy dot. bezpieczeństwa informacji, w tym klauzule bezpieczeństwa o zachowaniu poufności,
4) **zasada „czystego biurka** – w celu wyeliminowania ryzyka przypadkowego lub celowego odczytania informacji, ich skopiowania, zniszczenia lub zmodyfikowania przez osoby nieuprawnione, opuszczając stanowisko pracy należy usunąć z blatu biurka dokumenty zawierające informacje inne niż informacje o charakterze jawnym, umieszczając je w przeznaczonych do tego celu zabezpieczonych meblach biurowych: szafach, szufladach lub sejfach,
5) **zasada „czystego ekranu"** - na czas nieobecności dostęp do komputera należy skutecznie blokować a po zakończeniu pracy komputer wyłączyć, chyba że musi on pracować w trybie ciągłym,
6) **zasada „doskonalenia SZBI"** - system zarządzania bezpieczeństwem informacji jest dostosowywany do zmieniających się warunków w oparciu o wyniki okresowo prowadzonego monitorowania i nadzoru,
7) **zasada „najsłabszego ogniwa"** – poziom bezpieczeństwa informacji wyznacza najsłabsze ogniwo (najsłabiej zabezpieczony element) SZBI,

8) **zasada „segregacji obowiązków i zadań"** - obowiązki i uprawnienia powinny być tak rozdzielone, aby pojedyncza osoba nie dysponowała pełnią uprawnień do wykonywania zadań w całości,

9) **zasada „uprawnionego dostępu"** – korzystanie z aktywów informacyjnych jednostki odbywać się może tylko w oparciu o formalne uprawnienia do korzystania z wybranych aktywów,

10) **zasada „wiedzy uzasadnionej"** – personel, o którym mowa w § 5 dysponuje wiedzą o aktywach informacyjnych w ograniczonym zakresie, niezbędnym do realizacji powierzonych im zadań.

Dodatkowe zasady bezpieczeństwa mogą zostać określone w pozostałych dokumentach wchodzących w skład dokumentacji bezpieczeństwa.

6. Deklaracja Najwyższego Kierownictwa w zakresie bezpieczeństwa informacji

Administrator, stojąc na stanowisku, że informacja jest newralgicznym zasobem jednostki, wdrożył w ramach Zintegrowanego Systemu Zarządzania system zarządzania bezpieczeństwem informacji i zobowiązuje się do podejmowania wszelkich działań prowadzących do kompleksowego zabezpieczenia informacji oraz zapewnienia środków niezbędnych do realizacji niniejszej Polityki.

7. Organizacja bezpieczeństwa informacji

Odpowiedzialność za realizację ochrony informacji w podmiocie ponoszą wszyscy pracownicy jednostki – proporcjonalnie do wykonywanych obowiązków i posiadanych uprawnień.

Zakres uprawnień i odpowiedzialności związany z zarządzaniem bezpieczeństwem informacji określony został w procedurach i instrukcjach Zintegrowanego Systemu Zarządzania w jednostce.

Administrator wyznaczył Inspektora Ochrony Danych.

Każdy pracownik jest zapoznawany z zasadami bezpieczeństwa oraz z aktualnymi procedurami ochrony informacji oraz zawartymi w Instrukcji podstawowych zasad bezpieczeństwa dla pracowników. Zleceniobiorcy, wolontariusze, stażyści oraz praktykanci również są zapoznawani z tymi zasadami. Fakt zapoznania się z dokumentacją, osoba potwierdza poprzez złożenie oświadczenia.

Właściciel aktywu odpowiada za bieżące nadzorowanie oraz zarządzanie aktywem.

8. Dokumentacja systemu zarządzania bezpieczeństwem informacji

Dokumentacja SZBI składa się z głównych elementów. Są nimi:

- Polityka Bezpieczeństwa Informacji,
- Deklaracja stosowania;
- Procedury i instrukcje z zakresu ochrony danych osobowych;
- Raporty z analizy ryzyka i plany postępowania z ryzykiem.

Uzupełnieniem dokumentacji SZBI jest Polityka bezpieczeństwa ochrony danych osobowych wraz z odpowiednimi procedurami.

9. Zasady współpracy ze stronami zainteresowanymi

W jednostce wdrożono standard bezpieczeństwa fizycznego w odniesieniu do klientów i podmiotów wykonujących prace zlecone. Ponadto instrukcja ogólna w zakresie wymagań dla umów przygotowywanych w jednostce klauzule poufności różnego stopnia szczegółowości, niezbędne przy zawieraniu umów. Celem takiego postępowania jest zapewnienie bezpieczeństwa informacji przed dostępem osób niepowołanych, uszkodzeniem lub innymi zakłóceniami w obiektach oraz systemach. Wyodrębnione zostały również obszary niedostępne dla klientów i osób trzecich z uwagi na przetwarzane informacje bądź funkcje techniczne.

10. Polityka kontroli dostępu do informacji

Dostęp do informacji przechowywanych i przetwarzanych w jednostce jest poddany kontroli wynikającej z obowiązujących przepisów prawa powszechnego oraz dodatkowych wymagań bezpieczeństwa. Kontrola polega na:

1) wydzieleniu obszarów przeznaczonych do przechowywania oraz przetwarzania poszczególnych zbiorów danych i zapewnieniu odpowiednich barier fizycznych przeciwdziałających nieuprawnionemu dostępowi;
2) zarządzaniu uprawnieniami poszczególnych użytkowników w sposób zapewniający dostęp wyłącznie do danych wymaganych do wykonywania obowiązków służbowych, jeśli dane te podlegają ochronie z jakiejkolwiek przyczyny;
3) stosowaniu bezpiecznych systemów przetwarzania informacji;
4) nadzorowaniu działalności stron trzecich, mogących wpłynąć na bezpieczeństwo informacji;
5) bieżącym informowaniu pracowników o wszelkich zmianach w zakresie regulacji dotyczących przechowywania, przetwarzania i udostępniania informacji.

Adekwatność i skuteczność stosowanych w podmiocie środków kontroli dostępu do informacji podlega bieżącej weryfikacji w ramach audytów wewnętrznych, zmian dokumentacji i metod postępowania wynikających z ewolucji uregulowań prawnych oraz systemów przetwarzania danych a także reagowania na zagrożenia ujawnione przez inne strony.

11. Klasyfikacja informacji

Klasyfikacja została wprowadzona w celu uporządkowania w jednostce postępowania z różnymi rodzajami informacji, które są głównym zasobem naszej organizacji. W szczególny sposób potraktowano informację, której ujawnienie może narazić pracodawcę na szkodę.

Podstawowym elementem klasyfikacji są grupy informacji. W grupach informacji zebrane zostały dokumenty logicznie ze sobą powiązane o podobnych wymaganiach związanych z bezpieczeństwem. Do określenia poziomu bezpieczeństwa danej grupy informacji przyjęto wskaźniki definiujące poufność, integralność oraz dostępność danej grupy informacji.

Przez poufność rozumiemy zapewnienie, iż dostęp do informacji mają tylko i wyłącznie osoby uprawnione. Przez integralność rozumiemy zapewnienie, iż informacje nie zostały zmienione lub zniszczone w nieautoryzowany sposób (niezgodny z wewnętrznymi regulacjami podmiotu).

Przez dostępność rozumiemy możliwość dostępu do informacji w takim czasie, jaki jest oczekiwany przez użytkownika. Ze względu na charakter pracy jednostki i cel jego funkcjonowania do określenia wskaźników bezpieczeństwa największy nacisk położono na parametr integralności. Zdefiniowano trzy poziomy dla każdego z powyższych wskaźników po to, aby możliwe było powiązanie danej grupy informacji z określonym poziomem zdefiniowanego wskaźnika w skali 1-3.

Struktura klasyfikacji informacji w podmiocie opiera się na założeniu istnienia trzech poziomów postrzegania informacji:

1) **informacje jawne** – informacje publicznie dostępne,
2) **informacje wewnętrzne** – informacje, których przetwarzanie i udostępnianie podlega restrykcjom z uwagi na szczególne znaczenie dla pracodawcy (właściciela informacji):
   a) informacje **wewnętrzne dostępne** – informacje dostępne dla wszystkich pracowników,
   b) informacje **wewnętrzne wrażliwe** – informacje dostępne dla grupy pracowników upoważnionych z uwagi na realizowane zadania regulaminowe,
   c) informacje **stanowiące tajemnicę pracodawcy** – informacje, których przetwarzanie i udostępnianie może narazić pracodawcę na szkodę;
3) **informacje ustawowo chronione** – tajemnice określone w odrębnych przepisach.

12. Zarządzanie aktywami i ryzykiem

Jednostka zarządza swoimi aktywami informacyjnymi poprzez zapewnienie im wymaganego poziomu bezpieczeństwa. Identyfikowane są aktywa informacyjne i klasyfikowane zgodnie ze stawianymi im wymaganiami w zakresie ochrony. Ważnym elementem zarządzania aktywami i bezpieczeństwem informacji jest przeprowadzanie okresowej analizy ryzyka i opracowywanie planów postępowania z ryzykiem. Analiza wyników stanowi podstawę podejmowania wszelkich działań w zakresie doskonalenia ochrony zasobów. Na podstawie wyników analizy ryzyka opracowywane są plany postępowania z ryzykiem dla aktywów o ryzykach większych niż ustalony poziom ryzyka akceptowalnego. Ryzyka są przeglądane na przeglądach kierownictwa oraz po zmianach mających wpływ na system bezpieczeństwa informacji.

13. Autoryzacja nowych urządzeń

Każde nowe lub zmienione urządzenie służące do przetwarzania informacji lub mogące w jakikolwiek inny sposób wpływać na bezpieczeństwo informacji jest weryfikowane na zgodność z wymaganiami systemu bezpieczeństwa informacji i zaakceptowane przez uprawnioną osobę.

Urządzenia służące do przetwarzania informacji nie będące własnością jednostki mogą być używane (po sprawdzeniu sprzętu pod względem kryteriów bezpieczeństwa) wyłącznie za zgodą osoby upoważnionej.

14. Zarządzanie systemami i sieciami

Podmiot dba o przestrzeganie zasad związanych z utrzymywaniem i użytkowaniem systemów informatycznych i sieci. Celem takiego postępowania jest zapewnienie poufności, integralności i dostępności przetwarzanej przez nie informacji własnych. Skuteczna realizacja postawionego celu możliwa jest dzięki:

1) kompetencjom i świadomości pracowników oraz podpisanym umowom ze specjalistycznymi firmami administrującymi zasobami informatycznymi;
2) opracowanym zasadom konserwacji urządzeń w celu zapewnienia ich ciągłej pracy;
3) kontrolowaniu wprowadzania wszelkich zmian do infrastruktury technicznej,
4) prowadzeniu prac rozwojowych i testowych na oddzielnych urządzeniach lub środowiskach w celu zapewnienia bezpieczeństwa systemów produkcyjnych;
5) nadzorowaniu usług dostarczanych przez strony trzecie, w szczególności odbieraniu ich i akceptowaniu w sposób świadomy uwzględniający jego wpływ na istniejący system bezpieczeństwa;
6) wdrożeniu zabezpieczeń chroniących przed oprogramowaniem złośliwym i mobilnym;
7) systematycznemu tworzeniu i testowaniu kopii bezpieczeństwa;
8) przestrzeganiu opracowanych zasad postępowania z nośnikami;
9) bieżącemu monitorowaniu aktywów informacyjnych.

Podmiot monitoruje możliwość wystąpienia incydentów bezpieczeństwa i posiada mechanizmy reagowania w przypadkach ich wystąpienia. Szczegółowy sposób postępowania zawiera *„Procedura zgłaszania incydentów"*.

15. Bezpieczeństwo zasobów ludzkich

Podmiot zapewnia kompetentną kadrę pracowniczą do realizacji wyznaczonych zadań. Celem takiego postępowania jest ograniczenie ryzyka błędu ludzkiego, kradzieży, nadużycia lub niewłaściwego użytkowania zasobów. Realizacja postawionego celu możliwa jest dzięki ustanowionym praktykom i podziałowi odpowiedzialności związanemu z weryfikacją kandydatów do pracy podczas naboru, zasadom zatrudniania pracowników oraz ustalonej procedurze rozwiązywania umów o pracę.

16. Bezpieczeństwo fizyczne, sprzętu i infrastruktury technicznej

W podmiocie określono następujące kierunkowe standardy:

- standard bezpieczeństwa fizycznego;
- standard bezpieczeństwa sprzętu i okablowania;
- standard konfiguracji eksploatacji sieci.

Z uwagi na to, że standardy zawierają informacje, których ujawnienie nieuprawnionym stronom trzecim mogłoby w istotnym stopniu obniżyć poziom bezpieczeństwa informacji, są udostępnione tylko pracownikom podmiotu wykonującym zadania określone w standardach.

Przedmiot poszczególnych standardów:

1) standard bezpieczeństwa fizycznego: parametr bezpieczeństwa fizycznego, kontrola fizycznych wejść, zabezpieczenie biur, pokoi i urządzeń, ochrona przed zagrożeniami zewnętrznymi i środowiskowymi, praca w obszarach zabezpieczonych, obszary ogólnie dostępne, obszary dostaw i załadunku;

2) standard bezpieczeństwa sprzętu i okablowania: rozmieszczenie i ochrona sprzętu, urządzenia wspomagające, bezpieczeństwo okablowania, utrzymanie sprzętu, bezpieczeństwo sprzętu znajdującego się poza terenem organizacji, bezpieczne usuwanie sprzętu, wynoszenie majątku;

3) standard konfiguracji i eksploatacji sieci: środki kontroli przeciwko kodowi złośliwemu i mobilnemu, środki kontroli sieci, bezpieczeństwo usług sieciowych, polityki i procedury dotyczące wymiany informacji, przesyłanie wiadomości drogą elektroniczną, korzystanie z usług sieciowych, identyfikacja sprzętu w sieciach, ochrona portu służącego do zdalnego diagnozowania i konfiguracji, segregacja w sieciach, kontrola połączeń sieci, routing, nadzorowanie słabości technicznych.

17. Zarządzanie ciągłością działania

Podmiot dba o zapewnienie ciągłości funkcjonowania usług związanych z przetwarzaniem danych. Celem takiego postępowania jest przeciwdziałanie przerwom w działalności oraz ochrona krytycznych procesów przed rozległymi awariami lub katastrofami. Realizacja postawionego celu możliwa jest dzięki ustanowionym praktykom i podziałowi odpowiedzialności związanemu z zarządzeniem ciągłością działania tak, aby ograniczyć do akceptowalnego poziomu skutki wypadków i awarii. Plany awaryjne podlegają systematycznemu testowaniu. Szczegółowe zasady dot. zarządzania ciągłością działania zostały uregulowane w „Procedurze Plan ciągłości działania" stanowiącej załącznik nr 1 do niniejszej *Polityki*. Bazowy plan ciągłości działania do dokumentacji zarządzania ciągłością działania stanowi załącznik nr 2 do Polityki.

18. Zarządzanie zmianami

Podmiot, mając na uwadze konieczność szybkiego dostosowywania się do wymagań stron zainteresowanych, ciągłe zmiany przepisów prawnych oraz dążenie do wzrostu efektywności i wydajności pracy, zapewnia metody postępowania dla skutecznej i terminowej obsługi zmian w infrastrukturze teleinformatycznej przy utrzymaniu pożądanego poziomu bezpieczeństwa przetwarzanych danych i ograniczeniu ryzyka negatywnego wpływu zmiany na obsługę teleinformatyczną organizacji.

Proces zarządzania zmianą w jednostce przebiega w następujących etapach:

1) ustalenie celu zmiany;
2) rozważenie wielkości i ważności zmiany dla organizacji;
3) określenie momentów krytycznych we wdrożeniu zmiany;

4) zainicjowanie zmiany, przeprowadzenie testów, wdrożenie w systemie produkcyjnym;
5) aktywne włączenie pracowników w proces zmiany;
6) monitorowanie i raportowanie kolejnych kroków wdrożenia zmiany.

19. Dobór zabezpieczeń

Cele i dobór zabezpieczeń w SZBI prowadzony jest w oparciu o aktualne wymogi prawa powszechnie obowiązującego oraz wyniki monitorowania Systemu, w szczególności wyniki szacowania ryzyka w bezpieczeństwie informacji.

Stosowane zabezpieczenia fizyczne, techniczne i organizacyjne powinny uzupełniać się wzajemnie, zapewniając wymagany poziom bezpieczeństwa informacji.

20. Zgodność z wymaganiami prawnymi i regulacyjnymi

Podmiot dba o zapewnienie zgodności postępowania z przepisami obowiązującego prawa, przyjętych uwarunkowań umownych i normatywnych oraz wypracowanych własnych standardów. Celem takiego postępowania jest unikanie naruszania jakichkolwiek przepisów prawnych, zobowiązań wynikających z ustaw, zarządzeń lub umów oraz wymagań bezpieczeństwa. Realizacja postawionego celu możliwa jest dzięki ustanowionym praktykom i podziałowi odpowiedzialności związanemu z identyfikacją wymagań prawnych w zakresie bezpieczeństwa informacji. Prowadzone są audyty wewnętrzne i zewnętrzne funkcjonowania systemu.

21. Deklaracja ochrony własności intelektualnej

W podmiocie zostały wdrożone mechanizmy zapobiegające naruszeniom przepisów prawa powszechnego związanych z ochroną własności intelektualnej. Przede wszystkim zabezpieczono stacje robocze przed możliwością instalacji oprogramowania z naruszeniem właściwej licencji. Sieć podlega ciągłemu monitorowaniu, a dostęp do stron oraz usług internetowych, co do których zachodzi podejrzenie naruszania własności intelektualnej lub ryzyko infekcji systemu złośliwym oprogramowaniem, może zostać zablokowany.

W ramach usług domeny wprowadzono filtrowanie plików użytkownika, blokując te z formatów, które nie będąc z założenia wynikającego z funkcjonalności przydatnymi w pracy zawodowej, mogłyby zarazem być nośnikami treści naruszających prawa autorskie i pokrewne. Prowadzona jest bieżąca ewidencja licencji oprogramowania, co zapewnia, że pracownicy upoważnieni do instalacji oprogramowania działają w granicach praw nabytych. Nadzorowana jest także własność intelektualna powierzona lub przekazana przez osoby trzecie, zarówno klientów, jak i kontrahentów.

22. Postanowienia końcowe

Najwyższe kierownictwo podmiotu zapoznaje pracowników, zleceniobiorców, wolontariuszy, stażystów i praktykantów z dokumentem Polityki Bezpieczeństwa Informacji. Naruszenia świadome, bądź przypadkowe niniejszej Polityki Bezpieczeństwa Informacji (wraz z wszystkimi dokumentami operacyjnymi) powodują skutki prawne zgodnie z

Regulaminem Pracy, a w przypadkach zastrzeżonych przez ustawodawcę – karne wynikające z odpowiedzialności określonej przez przepisy prawa.

Załącznik Nr 1

PROCEDURA - PLAN CIĄGŁOŚCI DZIAŁANIA

I. Celem procedury jest konieczność zabezpieczenia możliwości ciągłości działania dla następujących elementów:
   A) z wykorzystaniem systemów informatycznych,
   B) bez udziału systemów informatycznych.

II. **Zapewnienie ciągłości pracy systemu przetwarzania informacji (w tym danych osobowych) z udziałem systemów informatycznych**

A) Zapewnienie ciągłości pracy systemów informatycznych

1. Wprowadza się procedurę zgłaszania awarii systemów informatycznych wykorzystywanych do przetwarzania informacji.
2. Każdy z użytkowników systemu informatycznego, w sytuacji wystąpienia awarii tego systemu, ma obowiązek niezwłocznego zgłoszenia awarii tego systemu Administratorowi Systemu Informatycznemu (ASI). Bezpośredni numer kontaktowy do zgłaszania awarii 85 742 03 04 (wewn. 42).
3. Do czasu usunięcia awarii systemu informatycznego, podmiot wykorzystuje dokumentację papierową, która po usunięciu awarii systemu informatycznego jest niezwłocznie wprowadzana przez upoważnioną osobę do systemu.
4. Wzór dokumentacja papierowej wykorzystywanej alternatywnie w trakcie awarii systemu informatycznego nie musi być ściśle określony. Powinien jednak zawierać elementy niezbędne do kompletnego wprowadzenia informacji do systemu informatycznego. Jeśli dostawca oprogramowania informatycznego przewidział taką sytuację, stosuje się szablony dokumentów papierowych dostarczonych przez dostawcę oprogramowania.
5. Po usunięciu awarii osoba obsługująca podmiot pod względem informatycznym weryfikuje prawidłowość bazy danych, która jest uzupełniana o informacje wytworzone za pomocą zastępczej dokumentacji papierowej.
6. W przypadku uszkodzenia bazy danych należy wykorzystać kopię zapasową w celu przywrócenia poprawności systemu informatycznego.
7. Z czynności mających na celu przywrócenie pracy systemu Administrator Systemu Informatycznego sporządza stosowną notatkę.

B) Zapewnienie ciągłości pracy sprzętu, na którym przetwarzane są informacje (w tym dane osobowe)

1. Wprowadza się procedurę zgłaszania awarii urządzeń wykorzystywanych do przetwarzania informacji
2. Każdy z użytkowników, w sytuacji wystąpienia awarii sprzętu służącego do przetwarzania informacji ma obowiązek niezwłocznego zgłoszenia awarii tego sprzętu Administratorowi Systemu Informatycznego (ASI). Bezpośredni numer kontaktowy do zgłaszania awarii 85 742 03 04 (wewn. 42).
3. Do czasu usunięcia awarii, podmiot wykorzystuje dokumentację papierową, która po usunięciu awarii jest niezwłocznie wprowadzana przez upoważnioną osobę do systemu.

C) Zapewnienie ciągłości pracy w przypadku braku zasilania elektrycznego w sieci energetycznej

1. Każdy użytkownik systemu ma obowiązek niezwłocznego zgłoszenia braku zasilania sieci energetycznej po jej wystąpieniu z wykorzystaniem numeru 85 742 03 04 (wewn. 42).
2. Użytkownik komputera przenośnego jest zobowiązany do takiej organizacji pracy, aby zapewnić przez cały jej okres maksymalny poziom naładowania baterii, która umożliwi jego pracę bez zasilania, co najmniej przez 2 godziny.
3. Jeżeli użytkownik podejrzewa, że naprawa dostawy prądu może wydłużyć się ponad czas naładowania baterii jest zobowiązany do bezpiecznego przerwania pracy i wyłączenia sprzętu komputerowego.
4. W przypadku braku zasilania użytkownik komputera stacjonarnego ma niezwłoczny obowiązek bezpiecznego zakończenia pracy i wyłączenia stacji roboczej.
5. W przypadku wystąpienia braku zasilania, jeśli serwer bazy danych nie ma takiej opcji, Administrator systemu lub upoważniony przez niego pracownik wyłącza serwer bazy danych.

D) Zapewnienie ciągłości pracy w przypadku braku dostępu do sieci internetowej

1. Jeżeli użytkownik stwierdzi brak dostępu do sieci internetowej należy to zgłosić niezwłocznie na numer pomocy technicznej dostawcy, który jest wywieszony w rejestracji.
2. W przypadku konieczności użytkowania sieci i przedłużającej się awarii należy skorzystać z Internetu mobilnego - o ile jest dostępny- w podmiocie jako alternatywne źródło.
3. Za uruchomienie łącza alternatywnego odpowiada Administrator Systemu Informatycznego (ASI) lub wskazana przez niego osoba.

III. Zapewnienie ciągłości pracy systemu przetwarzania informacji bez udziału systemów informatycznych

1. Sytuacjami, które mogą uniemożliwiać przetwarzanie informacji bez wykorzystania systemów informatycznych mogą być:
   a) brak możliwości dostępu do pomieszczeń, w których przetwarzane są informacje,
   b) brak możliwości wykorzystania pomieszczeń, w których przetwarzane są informacje ze względu na awarię np. zalanie pomieszczenia, awaria ogrzewania.
2. W przypadku wystąpienia sytuacji, o których mowa w niniejszym rozdziale każdy z użytkowników przetwarzających informacje ma obowiązek kontaktu telefonicznego i zgłoszenia tego faktu Administratorowi Systemu Informatycznego za pośrednictwem numeru 85 742 03 04 (wewn. 42).
3. Administrator Systemu Informatycznego według najlepszej wiedzy i uznania niezwłocznie zgłasza zaistniałe usterki kompetentnym podmiotom według właściwości ich działania.
4. W przypadku braku możliwości wykorzystania pomieszczeń do przetwarzania informacji z powodu awarii, Administrator Systemu Informatycznego jest zobowiązany wskazać użytkownikowi inne, spełniające wszystkie normy pomieszczenie na terenie jednostki, w którym będzie on mógł kontynuować swoje obowiązki.

Zatwierdzam i nakazuję stosować

Dyrektor
Szkoły Podstawowej Nr 2
im. Ks. Jana Twardowskiego
w Białymstoku
mgr Halina Puchalska

12.02.2025

data i podpis Administrator