Polityka bezpieczeństwa informacji

w Szkole Podstawowej   
im. Tadeusza Kościuszki w Suchowoli

marzec 2019

Spis treści

[I. Podstawowe pojęcia 3](#_Toc3644703)

[II. STRATEGIA BEZPIECZEŃSTWA 3](#_Toc3644704)

[I.1 Cel strategii bezpieczeństwa 4](#_Toc3644705)

[I.2 Deklaracja Kierownictwa Szkoły Podstawowej im. Tadeusza Kościuszki w Suchowoli 4](#_Toc3644706)

[III. Zasady ogólne 4](#_Toc3644707)

[IV. Zasady ochrony zasobów informacyjnych 5](#_Toc3644708)

[V. Konsekwencje naruszenia Polityki Bezpieczeństwa Informacji. 6](#_Toc3644709)

[VI. Własność aktywów 6](#_Toc3644710)

[VI. Przegląd, ocena i doskonalenie PBI 6](#_Toc3644711)

[ZAŁĄCZNIKI (informacja poufna): 7](#_Toc3644712)

# Podstawowe pojęcia

1. **Aktywa** – wszystko to, co ma wartość dla Organizacji.
2. **Aktywa** informatyczne – sprzęt informatyczny, urządzenia sieciowe i telekomunikacyjne, wszystkie rodzaje oprogramowania, dane zgromadzone w systemach informatycznych.
3. **Aktywa nieinformatyczne** – pozostałe aktywa organizacji: sprzęt nieinformatyczny, dane nieinformatyczne, zasoby ludzkie.
4. **Analiza ryzyka** - proces identyfikacji ryzyka, określanie jego wartości, identyfikowanie zagrożeń i określanie niezbędnych zabezpieczeń.
5. **Informacje poufne** – kategoria informacji, których ujawnienie naraża organizację na szkodę.
6. **Kierownictwo** organizacji – osoby pełniący w organizacji stanowiska kierownicze średniego i wyższego stopnia uprawnieni do podejmowania decyzji w ramach pełnionego zakresu obowiązków
7. **Kontrahent / podmiot zewnętrzny** - podmiot posiadający dostęp do zasobów organizacji z racji powierzonych mu zadań, na podstawie przepisów prawa lub zawartych z nim umów, nie będący komórką organizacyjną lub jednostką organizacyjną.
8. **Organizacja** – **Szkoła Podstawowa im. Tadeusza Kościuszki w Suchowoli**
9. **PBI** – Polityka Bezpieczeństwa Informacji
10. **Podatność** (ang. Vulnerability) - słabość, brak odporności dot. braku wystarczającego zabezpieczenia na określone rodzaje zagrożenia dla systemu informatycznego, procedury, urządzenia czy rozwiązania technicznego.
11. **Pracownik** – osoba świadcząca pracę na rzecz organizacji niezależnie od jej formy: np. na podstawie umowy o pracę, cywilno-prawnej, stażowej, praktyki, wolonariatu
12. **Ryzyko** – prawdopodobieństwo wystąpienia/ziszczenia się zagrożenia.
13. **System informacyjny** - system, w którym w trakcie zachodzących w nim procesów gromadzi się, przetwarza, przechowuje i udostępnia informacje, niezależnie od sposobu realizacji tych procesów.
14. **System teleinformatyczny** - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, aplikacji, usług, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu elektronicznego przetwarzania danych stanowiących część systemu informacyjnego.
15. **Zagrożenie -** możliwość wystąpienia sytuacji niekorzystnej lub szkody, na skutek celowego lub przypadkowego wykorzystania określonej podatności.

# STRATEGIA BEZPIECZEŃSTWA

1. Bezpieczeństwo organizacji to stan określony przez przyjęty zbiór norm, zasad, rozwiązań oraz środków i metod ochrony zasobów, którego miarą jest poziom ryzyka naruszenia dostępności, poufności lub integralności tych zasobów.
2. Bezpieczeństwo organizacji jest zapewnione, jeżeli ryzyko naruszenia dostępności, poufności lub integralności chronionych zasobów nie przekracza akceptowalnych parametrów przy zachowaniu zasad sformułowanych w niniejszej Polityce.
3. Wprowadzenie PBI ma na celu obniżanie zidentyfikowanego ryzyka.

## I.1 Cel strategii bezpieczeństwa

1. Zapewnianie odpowiedniego zaangażowaniapracowników w utrzymanie bezpieczeństwa systemu informacyjnego.
2. Określanie kierunków rozwoju zarządzania bezpieczeństwem systemu informacyjnego.
3. Zapewnienie zgodności z obowiązującymi Organizację przepisami prawa polskiego i prawa UE.
4. Zagwarantowanie sprawnego funkcjonowania Organizacji.

## I.2 Deklaracja Kierownictwa Szkoły Podstawowej Tadeusza Kościuszki w Suchowoli

1. PBI wyznacza kierunek działania Kierownictwa oraz pracowników organizacji w celu zapewnienia systemowego nadzoru nad gromadzeniem, przetwarzaniem, przechowywaniem i udostępnianiem informacji, niezależnie od sposobu realizacji tych procesów.
2. Kierownictwo Organizacji zapewnia bezpieczeństwo informacji zawartych w systemach informacyjnych i poza nimi, w sposób opisany w PBI, ponieważ mają one fundamentalne znaczenie dla realizacji jej misji i celów statutowych.
3. PBI wyraża wolę Kierownictwa Organizacji w zakresie ochrony jej zasobów.
4. Kierownictwo Organizacji aktywnie wspiera procesy zmierzające do zapewnienia bezpieczeństwa przetwarzania informacji poprzez wdrażanie, rozwój, uaktualnianie PBI oraz regulacji z niej wynikających.
5. PBI oraz regulacje z niej wynikające obowiązują wszystkich pracowników, stażystów,  praktykantów, wolontariuszy oraz inne osoby fizyczne, prawne lub nieposiadające osobowości prawnej, które uzyskują dostęp do zasobów Organizacji, poza użytkownikami informacji publicznie dostępnych. Kierownictwo Organizacji odpowiada za zapewnienie środków na te cele.
6. Użytkowników serwisów internetowych Organizacji obowiązują regulacje wynikające z „Polityk prywatności” obowiązujących na tychże serwisach.
7. Każdy pracownik oraz inna osoba fizyczna, prawna lub nieposiadająca osobowości prawnej, która uzyskuje uprawnienie/upoważnienie dostępu do zasobów Organizacji dokumentuje zapoznanie się z PBI w formie oświadczenia lub poprzez odpowiednie zapisy w umowie współpracy.
8. PBI reguluje również kwestię ochrony danych osobowych.
9. PBI jest nadrzędna w stosunku do innych procedur i regulacji wewnętrznych Organizacji.

# Zasady ogólne

1. Życie i zdrowie osób jest dobrem najwyższym i ich ochrona w sytuacji zagrożenia jest ważniejsza niż ochrona jakichkolwiek innych zasobów.
2. Ponadto ochronie podlegają:
   1. informacje przetwarzane w Organizacji, niezależnie od ich formy i nośnika,
   2. aktywa Organizacji,
   3. pomieszczenia, w których znajduje się kluczowy sprzęt informatyczny, dokumenty zawierające tajemnice prawnie chronione, w tym dane osobowe,
   4. wizerunek i dobre imię Organizacji,
3. Celem ustanowienia PBI jest zapewnienie poufności, dostępności, integralności, przy zachowaniu autentyczności, niezaprzeczalności i rozliczalności, informacji przetwarzanych w Organizacji,
   1. **Poufność informacji** - oznacza, że jest ona dostępna wyłącznie dla osób, które zostały upoważnione do korzystania z danej informacji.
   2. **Dostępność informacji** - oznacza możliwość wykorzystania zasobu przez upoważnioną osobę, na każde uzasadnione żądanie, w ustalonym czasie.
   3. **Integralność informacji** - oznacza, że informacja nie uległa zmianie od czasu ostatniej autoryzowanej modyfikacji lub nie została usunięta w niekontrolowany sposób.
   4. **Autentyczność** - właściwość polegającą na tym, że pochodzenie lub zawartość danych jest taka, jak deklarowana.
   5. **Niezaprzeczalność** - brak możliwości zanegowania swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie.
   6. **Rozliczalność** - właściwość pozwalającą przypisać określone działanie do osoby fizycznej lub procesu oraz umiejscowić je w czasie.
4. Bezpieczeństwo informacji w Organizacji osiąga się wdrażając zabezpieczenia techniczne i organizacyjne w szczególności poprzez: zarządzenia i decyzje Kierownictwa wprowadzające PBI, jak również odpowiednie procedury.
5. Bezpieczeństwo informacji funkcjonuje dzięki strukturze organizacyjnej Organizacji, przypisaniu odpowiedzialności rolom i osobom oraz podlega okresowym przeglądom funkcjonowania celem stałego doskonalenia go.
6. Bezpieczeństwo Informacji w Organizacji obejmuje nie tylko jej siedzibę, ale także wszelkie sytuacje, w których informacje związane z działalnością Organizacji są przetwarzane poza jego siedzibą. Obejmuje to w szczególności zdalny dostęp do sieci komputerowej Organizacji.

# Zasady ochrony zasobów informacyjnych

1. Zadaniem zapisów zawartych w PBI jest ograniczenie ryzyka płynącego z zagrożeń do akceptowalnego poziomu, to znaczy zminimalizowanie możliwości naruszenia bezpieczeństwa zasobów informacyjnych Organizacji, umożliwienie wczesnego wykrycia takiego naruszenia, zminimalizowanie strat związanych z takim naruszeniem oraz sprawne usunięcie jego skutków.
2. Skuteczna ochrona zasobów Organizacji wymaga wspólnego działania, współpracy i zaangażowania wszystkich jej pracowników.
3. W sytuacjach kryzysowych ujawnienie informacji poufnych uznawane jest jako mniejsze zagrożenie od zniszczenia, utraty lub ujawnienia tych informacji. Nie dotyczy to informacji niejawnych w rozumieniu ustawy o ochronie informacji niejawnych.
4. Obowiązek ochrony informacji w przypadku współpracy z kontrahentami i jednostkami zewnętrznymi określany jest w ramach umów zawartych z tymi podmiotami.
5. W celu zapewnienia bezpieczeństwa zasobów informacyjnych w Organizacji stosuje się następujące ogólne zasady:
   1. **Zasada przywilejów koniecznych:** każdy pracownik posiada prawa dostępu do zasobów ograniczone wyłącznie do tych, które są konieczne do wykonywania powierzonych mu obowiązków.
   2. **Zasada wiedzy koniecznej:** pracownikom przekazuje się wiedzę o zasobach ograniczoną wyłącznie do zagadnień, które są konieczne do realizacji powierzonych im zadań.
   3. **Zasada asekuracji zabezpieczeń:** ochrona informacji powinna opierać się na co najmniej dwóch mechanizmach zabezpieczenia dla zagrożeń niosących największe ryzyko.
   4. **Zasada rozliczalności:** Kierownictwo Organizacji dąży do zapewnienia jednoznacznej odpowiedzialności pracowników za powierzone im zasoby oraz za przetwarzane przez nich informacje. Wszyscy użytkownicy zasobów informacyjnych ponoszą odpowiedzialność za
      1. realizowane czynności,
      2. za konsekwencje zaniedbanie swoich obowiązków (w tym dot. PBI),
      3. za konsekwencje nieuprawnionego przekazanie swoich przywilejów innym osobom,
      4. elektroniczne dokumentowanie tych czynności w rozsądnym zakresie przez korzystanie w tym celu z możliwości systemu teleinformatycznego.
6. Treść załączników do niniejszej polityki bezpieczeństwa informacji oraz powstałych na jej podstawie ewidencji stanowi informację poufną Organizacji ważą z punktu widzenia jej bezpieczeństwa oraz nie stanowi informacji publicznej. Dlatego informacje te mogą być przekazane tylko uprawnionym do tego organom państwowym.

# Konsekwencje naruszenia Polityki Bezpieczeństwa Informacji.

1. Nieprzestrzeganie przez pracownika Polityki Bezpieczeństwa Informacji jest równoznaczne z naruszeniem obowiązków pracowniczych.
2. Tryb postępowania przy udzielaniu kar dla pracowników określony jest w Regulaminie Pracy.
3. Za działania pracowników/kontrahentów niezgodne z przepisami dot. ochrony informacji prawnie chronionych grożą im odrębne kary wynikające z tychże przepisów, w szczególności dotyczy to ochrony danych osobowych i informacji niejawnych.
4. Naruszenie postanowień PBI przez kontrahenta lub jego pracowników stanowi podstawę do odstąpienia od umowy i żądania pokrycia powstałej szkody lub zapłaty kary umownej, jeżeli taki obowiązek wynika z zawartej umowy.

# Własność aktywów

1. Organizacja jest właścicielem wszystkich aktywów niezbędnych do przetwarzania informacji w komórkach organizacyjnych.
2. Kierownik Organizacji wyznacza osoby odpowiedzialne za poszczególne aktywa.

# VI. Przegląd, ocena i doskonalenie PBI

1. Przegląd PBI odbywa się jeden raz w roku.
2. Przegląd PBI polega na analizie raportu z przeprowadzanego audytu funkcjonowania systemu bezpieczeństwa informacji.
3. Dodatkowo dokonywany jest przegląd PBI w przypadku:
   1. Wystąpienia poważnego naruszenia bezpieczeństwa informacji,
   2. pojawienia się nowych i istotnych rodzajów ryzyka,
   3. istotnych zmian regulacji prawnych dot. bezpieczeństwa informacji,
   4. na wniosek Kierownika Organizacji
   5. na wniosek Inspektora Ochrony Danych Osobowych
4. Każdy przegląd jest udokumentowany protokołem.
5. Po dokonanym przeglądzie i stwierdzeniu konieczności dokonania zmian w PBI, należy przedstawić Kierownikowi Organizacji propozycje zmian w PBI.

# ZAŁĄCZNIKI (informacja poufna pkt 1-3):

1. Zasady prawidłowego i bezpiecznego przetwarzania danych osobowych
2. Wzór ewidencji aktywów wykorzystywanych do PDO
3. Wzór ewidencji procesów PDO
4. Regulamin monitoringu wizyjnego