*Załącznik Nr 1 do Zarządzenia nr 45/2019*

 *Dyrektora Szkoły Podstawowej nr 2 w Czeladzi z dn. 14sierpnia 2019r*

**Regulamin**

**Bezpieczeństwa Informacji**

**Szkoła Podstawowa nr 2 im. Marii Konopnickiej w Czeladzi**

**ul. Szkolna6, 41-250Czeladź**

Spis treści

[Opis firmy **Błąd! Nie zdefiniowano zakładki.**](#_Toc11750250)

[Definicja bezpieczeństwa i zakres systemu **Błąd! Nie zdefiniowano zakładki.**](#_Toc11750251)

[Cele bezpieczeństwa informacji i plany do ich osiągnięcia **Błąd! Nie zdefiniowano zakładki.**](#_Toc11750252)

[Polityka SZBI **Błąd! Nie zdefiniowano zakładki.**](#_Toc11750253)

[Zasady ogólne **Błąd! Nie zdefiniowano zakładki.**](#_Toc11750254)

[Organizacja bezpieczeństwa informacji **Błąd! Nie zdefiniowano zakładki.**](#_Toc11750255)

[Procedury Systemowe **Błąd! Nie zdefiniowano zakładki.**](#_Toc11750256)

[Analiza Ryzyka **Błąd! Nie zdefiniowano zakładki.**](#_Toc11750257)

[Kontekst organizacji **Błąd! Nie zdefiniowano zakładki.**](#_Toc11750258)

[Struktura zarządzania bezpieczeństwem **Błąd! Nie zdefiniowano zakładki.**](#_Toc11750259)

[Koncepcja dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji **Błąd! Nie zdefiniowano zakładki.**](#_Toc11750260)

[Struktura zarządzania bezpieczeństwem i podział odpowiedzialności **Błąd! Nie zdefiniowano zakładki.**](#_Toc11750261)

[Komunikacja **Błąd! Nie zdefiniowano zakładki.**](#_Toc11750262)

[Ciągłe Doskonalenie **Błąd! Nie zdefiniowano zakładki.**](#_Toc11750263)

[Zasoby **Błąd! Nie zdefiniowano zakładki.**](#_Toc11750264)

[Zasady współpracy z osobami trzecimi **Błąd! Nie zdefiniowano zakładki.**](#_Toc11750265)

[Zasady współpracy z innymi Organizacjami **Błąd! Nie zdefiniowano zakładki.**](#_Toc11750266)

[Zasady współpracy z Policją, Jednostkami Straży Pożarnej. **Błąd! Nie zdefiniowano zakładki.**](#_Toc11750267)

[Zarządzanie aktywami i ryzykami **Błąd! Nie zdefiniowano zakładki.**](#_Toc11750268)

[Autoryzacja nowych urządzeń **Błąd! Nie zdefiniowano zakładki.**](#_Toc11750269)

[Bezpieczeństwo zasobów ludzkich, kompetencje, szkolenia i świadomość pracowników. **Błąd! Nie zdefiniowano zakładki.**](#_Toc11750270)

[Bezpieczeństwo fizyczne i środowiskowe **Błąd! Nie zdefiniowano zakładki.**](#_Toc11750271)

[Zarządzanie systemami i sieciami **Błąd! Nie zdefiniowano zakładki.**](#_Toc11750272)

[Kontrola dostępu **Błąd! Nie zdefiniowano zakładki.**](#_Toc11750273)

[Wymiana informacji **Błąd! Nie zdefiniowano zakładki.**](#_Toc11750274)

[Korzystanie z zabezpieczeń Kryptograficznych **Błąd! Nie zdefiniowano zakładki.**](#_Toc11750275)

[Pozyskiwanie, rozwój i utrzymanie systemów informacyjnych **Błąd! Nie zdefiniowano zakładki.**](#_Toc11750276)

[Zarządzanie incydentami **Błąd! Nie zdefiniowano zakładki.**](#_Toc11750277)

[Zarządzanie ciągłością działania **Błąd! Nie zdefiniowano zakładki.**](#_Toc11750278)

[Zgodność **Błąd! Nie zdefiniowano zakładki.**](#_Toc11750279)

[Postanowienia końcowe **Błąd! Nie zdefiniowano zakładki.**](#_Toc11750280)

# Opis firmy

**Celem nadrzędnym Szkoły Podstawowej nr 2 im. Marii Konopnickiej w Czeladzi jest wychowanie i wykształcenie absolwenta, który jest dobrym i pogodnym człowiekiem, posiadającym rzetelną wiedzę i umiejętności oraz przygotowanym do mądrego i godnego życia w nowoczesnym społeczeństwie.**

**Jednostka realizuje cele i zadania określone w ustawie – Prawo oświatowe oraz
w przepisach wykonawczych wydanych na jej podstawie, a także zawarte w**Programie Wychowawczo-Profilaktycznym, **dostosowanym do potrzeb rozwojowych uczniów oraz potrzeb danego środowiska.**

**Bezpieczeństwo i niezawodność**

Zapewniamy naszym dzieciom, rodzicom/opiekunom prawnym, pracownikom, kontrahentom najwyższy stopień bezpieczeństwa i niezawodności w przetwarzaniu informacji.

## Definicja bezpieczeństwa i zakres systemu

Celem Systemu Zarządzania jest zapewnienie bezpieczeństwa informacjom chronionym, zarówno własnym jak i powierzonym przez rodziców/opiekunów prawnych dzieci, pracowników i kontrahentów w tym danych osobowych, poprzez zapewnienie tym informacjom cech: poufności, integralności oraz dostępności.

**Zakresem systemu zarządzania bezpieczeństwem informacji objęte są:**

Informacje przetwarzane w ramach: usług wynikających ze statutu, związanych z zatrudnieniem i zawieraniem umów cywilnoprawnych.

Realizacja powyższych zadań odbywa się w placówce:

* **Szkoła Podstawowa nr 2 im. Marii Konopnickiej w Czeladzi, ul. Szkolna6, 41-250Czeladź;**

## Cele bezpieczeństwa informacji i plany do ich osiągnięcia

Cele bezpieczeństwa oraz plany do osiągnięcia w danym roku szkolnym każdorazowo określa Dyrektor jednostki według niżej przedstawionego wzoru formularza

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Cel | Osoba odpowiedzialna | Realizacja | Miernik | Ocena skuteczności |
| Poprawa bezpieczeństwa informacji w organizacji | Dyrektor  | Opracowanie i Wdrożenie zasad dotyczących bezpieczeństwa Informacji | Obniżenie ryzyka do poziomu akceptowalnego zgodnie z planem postępowania z ryzykiem  |  |
| Zapewnienie skuteczności działania SZBI | Dyrektor  | Monitorowanie stosowanych zabezpieczeń (pomiar skuteczności zabezpieczeń) | 100% skutecznych zabezpieczeń zgodnie z pomiarem skuteczności zabezpieczeń. Mierzone raz w roku.  |  |
| Poprawa bezpieczeństwa informacji | Dyrektor  | Realizacja planów ciągłości działania do końca roku. | 100% przetestowanych i działających prawidłowo planów ciągłości działania  |  |

# Polityka SZBI

Bezpieczeństwo informacji oraz systemów, w których są one przetwarzane jest jednym z kluczowych elementów jakości oferowanej rodzicom/opiekunom prawnym, dzieciom, pracownikom i kontrahentom przez **Szkołę Podstawową nr 2 im. Marii Konopnickiej w Czeladzi**oraz warunkiem ciągłego rozwoju **Jednostki**. Gwarancją sprawnej i skutecznej ochrony informacji jest zapewnienie odpowiedniego poziomu kultury bezpieczeństwa oraz zastosowanie przemyślanych rozwiązań technicznych.

**Dyrektor** wprowadzając Regulamin Bezpieczeństwa Informacji, deklaruje, że wdrożony System Zarządzania Bezpieczeństwem Informacji będzie podlegał ciągłemu doskonaleniu zgodnie z wymogami prawnymi.

Zakres zarządzania bezpieczeństwem informacji obejmuje dane i informacje powierzone Jednostce przez rodziców/opiekunów prawnych, pracowników, kontrahentów oraz informacje własne przetwarzane we wszystkich procesach.

Podejście do bezpieczeństwa informacji wywodzi się z trzech kluczowych kwestii:

* Zapewnienia, że informacja jest udostępniana jedynie osobom upoważnionym (tzw. reguła poufności informacji)
* Zapewnienia rzetelności i kompletności informacji oraz metod jej przetwarzania (tzw. reguła integralności informacji)
* Zapewnienia, że osoby upoważnione mają dostęp do informacji i związanych
z nią aktywów tylko wtedy, gdy istnieje taka potrzeba (tzw. reguła dostępności informacji).

Celem wdrożonego Systemu Zarządzania Bezpieczeństwem Informacji jest osiągnięcie takiego poziomu organizacyjnego i technicznego, który:

* będzie gwarantem pełnej ochrony danych rodziców/opiekunów prawnych, dzieci, pracowników, kontrahentów oraz ciągłości procesu ich przetwarzania,
* zapewni zachowanie poufności informacji szczególnie chronionych, integralności
i dostępności informacji szczególnie chronionych oraz informacji zdefiniowanych jako dane zwykłe,
* zagwarantuje odpowiedni poziom bezpieczeństwa informacji, bez względu na jej postać, we wszystkich systemach jej przetwarzania,
* maksymalnie ograniczy występowanie zagrożeń dla bezpieczeństwa informacji, które wynikają z celowej bądź przypadkowej działalności człowieka oraz ich ewentualne wykorzystanie na szkodę Jednostki,
* zapewni poprawne i bezpieczne funkcjonowanie wszystkich systemów przetwarzania informacji,
* zapewni gotowość do podjęcia działań w sytuacjach kryzysowych dla bezpieczeństwa Jednostki, jej interesów oraz posiadanych i powierzonych jej informacji.

Powyższe cele realizowane są poprzez:

* wyznaczenie struktury organizacyjnej zapewniającej optymalny podział
i koordynację zadań i odpowiedzialności związanych z zapewnieniem bezpieczeństwa informacji,
* wyznaczenie właścicieli dla kluczowych aktywów przetwarzających informację, którzy zobowiązani są do zapewnienia im możliwie jak najwyższego poziomu bezpieczeństwa,
* przyjęcie za obowiązujące przez wszystkich pracowników polityk
i procedur bezpieczeństwa obowiązujących w Jednostce,
* podziale informacji na klasy i przyporządkowanie im zasad postępowania,
* określeniu zasad przetwarzania informacji, w tym stref, w których może się ono odbywać,
* przegląd i aktualizację polityk i procedur postępowania dokonywaną przez odpowiedzialne osoby w celu jak najlepszej reakcji na zagrożenia i incydenty,
* ciągłe doskonalenie systemu zapewnia bezpieczeństwo informacjom funkcjonującym
w Jednostce zgodnie z wymaganiami prawa i zaleceniami wszystkich zainteresowanych stron.

# Zasady ogólne

Każdy pracownik powinien być zapoznany z regułami oraz z kompletnymi i aktualnymi procedurami ochrony informacji. Poniższe uniwersalne zasady są podstawą realizacji regulaminu bezpieczeństwa informacji:

* Zasada uprawnionego dostępu.Każdy pracownik przeszedł szkolenie z zasad ochrony informacji, spełnia kryteria dopuszczenia do informacji i podpisał stosowne oświadczenie o zachowaniu poufności.
* Zasada przywilejów koniecznych.Każdy pracownik posiada prawa dostępu do informacji, ograniczone wyłącznie do tych, które są konieczne do wykonywania powierzonych mu zadań.
* Zasada wiedzy koniecznej. Każdy pracownik posiada wiedzę o systemie, do którego ma dostęp, ograniczoną wyłącznie do zagadnień, które są konieczne do realizacji powierzonych mu zadań.
* Zasada usług koniecznych. Jednostka świadczy tylko takie usługi, jakich wymaga prawo.
* Zasada asekuracji.Każdy mechanizm zabezpieczający musi być ubezpieczony drugim, innym (podobnym). W przypadkach szczególnych może być stosowane dodatkowe (trzecie) niezależne zabezpieczenie.
* Zasada świadomości zbiorowej. Wszyscy pracownicy są świadomi konieczności ochrony zasobów informacyjnych Jednostki i aktywnie uczestniczą w tym procesie.
* Zasada indywidualnej odpowiedzialności. Za bezpieczeństwo poszczególnych elementów odpowiadają konkretne osoby.
* Zasada obecności koniecznej. Prawo przebywania w określonych miejscach mają tylko osoby upoważnione.
* Zasada stałej gotowości. System jest przygotowany na wszelkie zagrożenia. Niedopuszczalne jest tymczasowe wyłączanie mechanizmów zabezpieczających.
* Zasada najsłabszego ogniwa. Poziom bezpieczeństwa wyznacza najsłabszy (najmniej zabezpieczony) element.
* Zasada kompletności. Skuteczne zabezpieczenie jest tylko wtedy, gdy stosuje się podejście kompleksowe, uwzględniające wszystkie stopnie i ogniwa ogólnie pojętego procesu przetwarzania informacji.
* Zasada ewolucji. Każdy system musi ciągle dostosowywać mechanizmy wewnętrzne do zmieniających się warunków zewnętrznych.
* Zasada odpowiedniości. Używane mechanizmy muszą być adekwatne do sytuacji.
* Zasad akceptowanej równowagi. Podejmowane środki zaradcze nie mogą przekraczać poziomu akceptacji.
* Zasada świadomej konwersacji. Nie zawsze i wszędzie trzeba mówić, co się wie, ale zawsze i wszędzie trzeba wiedzieć, co, gdzie i do kogo się mówi.

# Organizacja bezpieczeństwa informacji

## Procedury Systemowe

Jednostka ze względu na fakt, iż obowiązujące standardy nie nakłada obowiązku posiadania udokumentowanych procedur systemowych, a obecne funkcjonują prawidłowo zdecydowała o pozostawieniu ich w obecnej formie.

Procedury nadzoru nad zapisami i dokumentami traktują o udokumentowanej informacji. Procedura działań korygujących opisuje sposób postępowania z niezgodnościami, oraz działania zapobiegawcze, które nie zostały zidentyfikowane podczas analizy ryzyka. Procedura audytów wewnętrznych określa sposób prowadzenia i planowania audytów.

## Analiza Ryzyka

Podstawowym elementem budowy systemu jest analiza ryzyka. Organizacja szacując ryzyko wzięła pod uwagę wymagania z załącznika A normy ISO 27001 oraz normy ISO 27005. Plany postępowania z ryzykiem zostały opracowane w korelacji ze słabościami wynikającymi z deklaracji stosowania.

## Kontekst organizacji

Zewnętrzny kontekst organizacji z jednej strony nie zawiera istotnych dostawców, którzy mieliby wpływ na SZBI z drugiej składa się z rodziców/opiekunów prawnych, dzieci, pracowników i kontrahentów Jednostki, których informacja przechowywana jest na nośnikach elektronicznych oraz w postaci papierowej i jest najwrażliwszym punktem SZBI.

Wewnętrzny kontekst to pracownicy posiadający dostęp do tych danych.

Podstawowe zainteresowane strony i ich wymagania:

1.kuratorium oświaty, organ prowadzący

- realizacja postanowień zawartych w zakresach obowiązków.

- wymagania prawne w zakresie SZBI

2.UODO

- ustawa o ochronie danych osobowych.

- rozporządzenie parlamentu Europejskiego

3. Urząd Skarbowy

- przepisy Karno-Skarbowe

4. Pracownicy

- kodeks Pracy.

- dokumentacja SZBI

- stosowanie przepisów prawa

5.Personel/Podwykonawcy. Dostawcy ujęci w dokumentacji.

- zapisy w umowach dotyczące poufności

- zapisy w umowach dotyczące zakresu prac/zadań

- zapisy w umowach dotyczące bezpieczeństwa informacji

6. Rodzic/opiekun prawny/dziecko

-RODO

- ustawa o ochronie danych osobowych,

- poufność zebranych informacji

## Struktura zarządzania bezpieczeństwem

Przyjmuje się, że podstawowymi zasadami przy tworzeniu struktur zarządzających bezpieczeństwem są:

* bezwzględne oddzielenie funkcji zarządzających i kontrolnych od funkcji wykonawczych
* uniemożliwienie nadużyć i maksymalne ograniczenie błędów popełnianych przez pojedyncze osoby w sferze jednoosobowej odpowiedzialności
* zapewnienie niezależności i bezinteresowności jednostek dokonujących audytu bezpieczeństwa przy zapewnieniu rękojmi zachowania tajemnicy

Wszystkie procesy bezpieczeństwa, a także rozwiązania bezpieczeństwa oraz organizacja jego zapewniania, muszą być zgodne z powyższymi zasadami.

## Koncepcja dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji

Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji składa się
z czterech głównych elementów. Są nimi:

* Polityka bezpieczeństwa informacji
* Deklaracja Stosowania zabezpieczeń
* Polityki Procedur i instrukcje bezpieczeństwa, które określają szczegółowo zasady postępowania,
* Raporty z analizy ryzyka i plany postępowania z ryzykiem

## Struktura zarządzania bezpieczeństwem i podział odpowiedzialności

Odpowiedzialność za bezpieczeństwo informacji w **Jednostce** ponoszą wszyscy pracownicy zgodnie z posiadanymi zakresami obowiązków.

* Kierownictwo – Dyrektor jest odpowiedzialny za zapewnienie zasobów niezbędnych dla opracowania, wdrożenia, funkcjonowania, utrzymania i doskonalenia Systemu Zarządzania Bezpieczeństwem informacji oraz poszczególnych zabezpieczeń. Wydaje zgodę na użytkowanie urządzeń służących do przetwarzania informacji i zabezpieczeń. Decyduje również o współpracy w zakresie bezpieczeństwa z innymi podmiotami. Kierownictwo może również wyrazić zgodę na udostępnienie stronom trzecim informacji stanowiących tajemnicę **Jednostki**. Jego codzienne postępowanie stanowi przykład dla innych pracowników, że aspekty bezpieczeństwa informacji posiadają wysoki priorytet we wszystkich podejmowanych i planowanych działaniach.
* Pracownik wyznaczony przez Dyrektora ds. SZBI odpowiedzialny jest za wdrożenie
i koordynację zapewnienia bezpieczeństwa informacji oraz związanych z nim polityk
i procedur.
* Właściciel aktywu odpowiada za bieżące nadzorowanie oraz zarządzanie aktywem
* Administrator aktywu odpowiada za realizację i nadzór nad technicznymi aspektami aktywu w ścisłej kooperacji z Właścicielem aktywu.

Poniższy schemat przedstawia organizację zarządzania bezpieczeństwem informacji
w Organizacji.



W powyższej strukturze możliwe jest wyróżnienie trzech poziomów działań:

* Na poziomie strategicznym prowadzona jest generalna polityka bezpieczeństwa informacji w odniesieniu do wcześniej rozpoznanego, określonego, a także poddanego analizie ryzyka i zasadniczych oczekiwań, co do poziomu bezpieczeństwa informacji oraz w odniesieniu do wynikających z nich modelowych zadań i rozwiązań. Dlatego też
w procesy decyzyjne tego poziomu zaangażowane jest Dyrektor Jednostki określające zasadnicze użytkowe kryteria bezpieczeństwa informacji (pochodne od kryteriów normatywnych i możliwe do zrealizowania na bazie zidentyfikowanych atrybutów informacji) .
* Na poziomie taktycznym tworzone są standardy bezpieczeństwa informacji oraz zasady kontroli ich wypełniania w stosowanych rozwiązaniach i systemach informatycznych oraz przestrzegania w praktyce używania tych rozwiązań i systemów (stosownie do założonych poziomów bezpieczeństwa: standardowego, podwyższonego lub specjalnego). W te procesy decyzyjne zaangażowany jest (głównie) Dyrektor Jednostki.
* Na poziomie operacyjnym prowadzona jest kontrola przez inspektora ds. ochrony danych osobowych pod kątem pełnego stosowania standardów bezpieczeństwa oraz rozwiązywania sytuacji zakłóceń wynikających z naruszenia tych standardów (intencjonalnego lub przypadkowego).

Diagram przedstawiony poniżej prezentuje graficznie przedstawiony podział.



## Komunikacja

Placówka komunikuje na zewnątrz tylko informacje, których komunikację umożliwiają przepisy prawa. Zasady SZBI oraz informacje powierzone przez rodzica/opiekuna prawnego dziecka nie są komunikowane na zewnątrz.

Wewnątrz organizacji komunikowane są pojawiające się problemy, incydenty bezpieczeństwa oraz funkcjonujące procedury. Za komunikowanie tych elementów odpowiada wyznaczony pracownik ds. SZBI. Komunikacja odbywa się mailowo lub podczas spotkań z pracownikami/nauczycielami.

## Ciągłe Doskonalenie

Jednostka stale doskonali swój system poprzez analizowanie wyników audytów wewnętrznych, wyników analizy ryzyka, pomiaru skuteczności zabezpieczeń i przeglądu zarządzania. Na podstawie tych elementów podejmowane są plany i działania mające pozytywnie wpłynąć na bezpieczeństwo informacji. Plany te zawarte są w planach postępowania z ryzykiem lub raporcie z przeglądu zarządzania.

## Zasoby

Jednostka zapewnia zasoby niezbędne do realizacji SZBI, wszelkie słabości zostały zidentyfikowane podczas analizy ryzyka, a plany postępowania z ryzykiem uwzględniają potrzeby dotyczące zasobów.

Dodatkowo w trakcie przeglądów zarządzania identyfikowane są potrzeby dotyczące zasobów, które mogą pojawić się w przyszłości.

## Zasady współpracy z osobami trzecimi

Osoba trzecia, która wykonuje prace zlecone na terenie Jednostkizobligowana jest do przestrzegania następujących procedur:

* do podpisania deklaracji o poufności, jeżeli prace te wiążą się z dostępem do informacji
* do przestrzegania reguł bhp,
* do przestrzegania reguł bezpieczeństwa przeciwpożarowego,

Każda osoba trzecia, która narusza sferę bezpieczeństwa nie zostaje pozostawiona bez nadzoru personelu Jednostki. Dostęp do biur, gabinetów i sal dydaktycznych wszelkiego personelu technicznego zajmującego się konserwacją sprzętu, ochrony, kontrahentów i innych osób jest nadzorowany przez wyznaczonego pracownika Jednostki.

### Zasady współpracy z innymi Organizacjami

Współpraca Jednostki z innymi Organizacjami oparta jest na umowach. Zawierając te umowy Jednostka ma zawsze na względzie, aby obejmowały one deklarację o zachowanie poufności.

### Zasady współpracy z Policją, Jednostkami Straży Pożarnej.

Wymiana informacji o zagrożeniach w zakresie bezpieczeństwa osób i mienia oraz zakłócenia spokoju i porządku publicznego następuje poprzez:

* Udzielanie wzajemnej pomocy w realizacji zadań ochrony, zapobieganiu przestępczości.
* Udzielanie wyczerpujących informacji o zagrożeniu dla bezpieczeństwa
i porządku publicznego,
* Współdziałanie w zabezpieczeniu powstałych awarii na obiekcie.

Współdziałanie przy zabezpieczeniu miejsc popełnienia przestępstw i wykroczeń
w granicach chronionych obiektów realizowane jest poprzez:

* Zabezpieczenie śladów na miejscu zdarzenia,
* Ustalenie świadków zdarzenia, a także wykonywanie innych czynności, jakie zleci Policja,
* Niedopuszczenie osób postronnych na miejsce przestępstwa, wykroczenia.
* Zabezpieczenie mienia jednostki na wypadek pożaru lub awarii:
* O zaistniałym pożarze lub awarii pracownik natychmiast zawiadamia Straż Pożarną , Dyrektora Jednostki,
* Przybyłe jednostki ratownicze natychmiast kieruje na miejsce akcji.

Informacje kontaktowe dostępne są w sekretariacie Jednostki.

# Zarządzanie aktywami i ryzykami

Jednostka uważnie zarządza swoimi aktywami informacyjnymi. Celem takiego postępowania jest zapewnienie im wymaganego poziomu bezpieczeństwa.

Identyfikowane są aktywa informacyjne i klasyfikowane zgodnie ze stawianymi im wymaganiami w zakresie ochrony. Szczególnie traktowane są kluczowe informacje - informacje powierzone nam przez rodziców/opiekunów prawnych, dzieci, pracowników, kontrahentów. Określone są szczegółowe zasady postępowania z danymi grupami informacji oraz grupy pracowników posiadające do nich dostęp.

Ważnym elementem zarządzania aktywami i bezpieczeństwem informacji w całej Jednostki jest przeprowadzanie okresowej analizy ryzyka i opracowania planów postępowania z ryzykiem. Analiza jej wyników stanowi podstawę podejmowania wszelkich działań w zakresie doskonalenia ochrony zasobów Jednostki.

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 Dyrektora Jednostki oraz po zmianach mających wpływ na system bezpieczeństwa informacji.

## Autoryzacja nowych urządzeń

Każde nowe lub zmienione urządzenie służące do przetwarzania informacji lub mogące w jakikolwiek inny sposób wpływać na bezpieczeństwo informacji musi zostać zweryfikowane na zgodność z wymaganiami systemu bezpieczeństwa informacji
i zaakceptowane przez wskazaną osobę. O ile nie zostało to określone szczegółowo
w innych opracowaniach, za dopuszczenie do użytkowania nowych urządzeń odpowiada Dyrektor.

# Bezpieczeństwo zasobów ludzkich, kompetencje, szkolenia i świadomość pracowników.

Jednostka dba o zapewnienie kompetentnych pracowników do realizacji wyznaczonych w procesach zadań. Celem takiego postępowania jest ograniczenie ryzyka błędu ludzkiego, kradzieży, nadużycia lub niewłaściwego użytkowania zasobów.

Skuteczna realizacja postawionego celu możliwa jest dzięki ustanowionym praktykom i podziałowi odpowiedzialności związanemu z weryfikacją kandydatów do pracy podczas naboru, zasadom zatrudniania personelu i pracowników oraz ustalonym procedurom rozwiązywania umów o pracę. Pracownicy są okresowo szkoleni z wymagań bezpieczeństwa.

Zasoby ludzkie są ważnym czynnikiem analizowanym podczas przeprowadzania okresowej analizy ryzyka. Tylko kompetentni i zaufani pracownicy są gwarantem dostarczenia rodzicom/opinkom prawnym, dzieciom, pracownikom, kontrahentom usług o odpowiednim poziomie jakości i bezpieczeństwa.

Dyrektor podejmuje wraz z inspektorem ds. ochrony danych osobowych działania mające na celu podnoszenie świadomości dotyczącej bezpieczeństwa informacji wśród pracowników. Działania te przejawiają się w publikowaniu materiałów informacyjnych, informowaniu
o zmianach i potrzebach SZBI.

Jednostka zarządza również bezpieczeństwem pracowników/personelu poprzez dobór
i przeszkolenie kluczowego personelu pod kątem możliwości realizacji prac zastępczych na wypadek nieprzewidzianych sytuacji.

# Bezpieczeństwo fizyczne i środowiskowe

Jednostka dba o zapewnienie wysokiego poziomu bezpieczeństwa fizycznego
i środowiskowego. Celem takiego postępowania jest zapewnienie bezpieczeństwa informacji przed dostępem osób niepowołanych, uszkodzeniem lub innymi zakłóceniami
w siedzibie Jednostki w odniesieniu do informacji. W przypadku danych pozyskanych od rodziców/opiekunów prawnych najistotniejsze jest zapewnienie wszystkich trzech podstawowych aspektów bezpieczeństwa poufności danych oraz ich dostępności
i integralności. Podobnie sytuacja wygląda w przypadku danych własnych.

Skuteczna realizacja postawionego celu możliwa jest dzięki ustanowionym praktykom
i podziałowi odpowiedzialności związanemu z wyznaczeniem stref bezpieczeństwa, zasadami pracy oraz administrowaniem prawami dostępu do nich.

Placówka kieruje się następującą zasadą: „Blokuj dostęp do wszystkich miejsc przetwarzania informacji poza wyraźnie dozwolonymi, bo od tego zależy bezpieczeństwo również Twoich chronionych informacji”.

# Zarządzanie systemami i sieciami

Jednostka 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:

* kompetencjom i świadomości pracowników oraz podpisanym umowom ze specjalistycznymi firmami administrującymi zasobami informatycznymi
i wspomagającymi Jednostkę.
* opracowanym zasadom konserwacji urządzeń w celu zapewnienia ich ciągłej pracy.
* kontrolowaniu wprowadzania wszelkich zmian do infrastruktury technicznej.
* usługi dostarczane przez strony trzecie są nadzorowane, w szczególności wszelkie wprowadzane do nich zmiany. Po zakupie, lub wprowadzeniu zmiany do systemu jest on odbierany i akceptowany w sposób świadomy, uwzględniający jego wpływ na istniejący system bezpieczeństwa.
* wdrożone są zabezpieczenia chroniące przed oprogramowaniem złośliwym
* usystematyzowanemu tworzeniu i testowaniu kopii bezpieczeństwa
* przestrzeganiu opracowanych zasad postępowania z nośnikami
* bieżącym monitorowaniu aktywów informacyjnych, w tym informatycznych, pod kątem wcześniejszego wykrycia wszelkich niebezpieczeństw mogących zagrozić bezpieczeństwu systemów.
* Jednostka monitoruje poziom incydentów w systemach informatycznych i posiada mechanizmy reagowania w przypadkach ich wystąpienia.

# Kontrola dostępu

Jednostka zarządza kontrolą dostępu. Celem takiego postępowania jest zapewnienie, że dostęp do informacji, miejsc, urządzeń lub systemów ich przetwarzania mają tylko osoby uprawnione.

Skuteczna realizacja postawionego celu możliwa jest dzięki ustanowionym praktykom
i podziałowi odpowiedzialności. Pomieszczenia w Jednostce (zgodnie z załącznikiem A do Polityki Bezpieczeństwa) zamykane są na klucz.

# Wymiana informacji

Każda informacja udostępniana stronom trzecim (zewnętrznym) podlega ochronie. **Przed udostępnieniem/wymianą informacji** każdy pracownik jest odpowiedzialny za upewnienie się, że może informacje przekazać. W przypadku wątpliwości o przekazaniu informacji decyduje właściwy przełożony.

# Korzystanie z zabezpieczeń Kryptograficznych

Organizacja nie stosuje zaawansowanych zabezpieczeń kryptograficznych.

W ramach stosowanych zabezpieczeń, szyfrowanie jest używane podczas przesyłania danych osobowych drogą elektroniczną w formie zaszyfrowanych plików.

# Pozyskiwanie, rozwój i utrzymanie systemów informacyjnych

Jednostka zapewnia, że wszystkie procesy związane z pozyskaniem, rozwojem bądź utrzymaniem systemów informacyjnych, w tym systemów i aplikacji informatycznych własnych, wykorzystywanych wewnętrznie lub oferowanych rodzicom/opiekunom prawnym, prowadzone jest w sposób nadzorowany, gwarantujący utrzymanie odpowiedniego poziomu bezpieczeństwa. Na to zapewnienie składa się:

* Uwzględnianie wymogów bezpieczeństwa podczas zakupu lub produkcji nowych systemów,
* Dopuszczenie nowego systemu poprzedzone jest zawsze fazą testowania.
* Wdrożone procedury kontroli zmian/ aktualizacji oprogramowania.

# Zarządzanie incydentami

W przypadku wszelkich incydentów w Jednostce powiadamiany jest inspektor ds. ochrony danych osobowych. Z jego udziałem dokonywana jest wstępna analiza incydentu, po czym podejmowane są działania zgodne z zasadami reakcji na zdarzenia. Po wystąpieniu incydentu natychmiast podejmowane są działania mające usunąć ewentualne skutki zaistnienia incydentu, a następnie wszystkie incydenty są szczegółowo analizowane
i podejmowane są dalsze decyzje właściwe dla danej sytuacji.

Incydenty są rejestrowane i analizowane przez inspektora ds. ochrony danych osobowych
i Dyrektora.

Szczegółowy opis postępowania z incydentami zawiera procedura „Zarządzanie Incydentami”

# Zarządzanie ciągłością działania

Jednostka dba o zapewnienie ciągłości funkcjonowania usług związanych
z przetwarzaniem danych. Celem takiego postępowania jest przeciwdziałanie przerwom
w działalności oraz ochrona krytycznych procesów biznesowych przed rozległymi awariami lub katastrofami.

Skuteczna realizacja postawionego celu możliwa jest dzięki ustanowionym praktykom
i podziałowi odpowiedzialności związanemu z zarządzeniem ciągłością działania tak, aby ograniczać do akceptowalnego poziomu skutków wypadków i awarii. W sposób systemowy tworzone są plany postępowania w sytuacjach kryzysowych. Powyższe zasady zapewniają, że Jednostka jest przygotowana na działanie również w przypadkach odbiegających od normy.

# Zgodność

Jednostka dba o zapewnienie zgodności zasad postępowania z przepisami obowiązującego prawa, przyjętych uwarunkowań umownych i normatywnych oraz wypracowanych własnych standardów. Celem takiego postępowania jest unikanie naruszania jakichkolwiek przepisów prawa karnego lub cywilnego, zobowiązań wynikających z ustaw, zarządzeń lub umów i jakichkolwiek wymagań bezpieczeństwa.

Skuteczna realizacja postawionego celu możliwa jest dzięki ustanowionym praktykom i podziałowi odpowiedzialności związanemu z identyfikacją wymagań prawnych w zakresie bezpieczeństwa informacji. Prowadzony jest nadzór nad komplementarnością stosowanych urządzeń technicznych oraz prowadzone są audyty wewnętrzne funkcjonowania systemu.

# Postanowienia końcowe

Jednostka dba o zapoznanie pracowników z dokumentacją Regulaminu Bezpieczeństwa Informacji. Za złożenie przez pracowników stosownych oświadczeń oraz uzyskanie niezbędnych praw dostępu (do pomieszczeń i systemów informatycznych), stosownie do przypisanej roli odpowiada Dyrektor.

Bieżący nadzór nad przestrzeganiem przyjętych zasad w zakresie bezpieczeństwa informacji pełni wyznaczony pracownik ds. SZBI.

**Naruszenia świadome, bądź przypadkowe niniejszego Regulaminu Bezpieczeństwa (wraz z wszystkimi dokumentami wykonawczymi) powoduje skutki prawne zgodnie
z kodeksem pracy a w przypadkach zastrzeżonych przez ustawodawcę – karne wynikające z odpowiedzialności określonej przez sąd**.

W ramach doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji deklarowana jest wola współpracy w zakresie poprawy stanu ochrony aktywów informacyjnych z:

* Ekspertami w zakresie bezpieczeństwa
* oraz pozostałymi instytucjami (Rodzic/opiekun prawny/dziecko, pracownikami i kontrahentami i innymi zainteresowanymi stronami)

**Załącznik nr 1.**

**Wykaz zmian**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **Data zmiany** | **Nr strony** | **Krótki opis zmiany** | **Wprowadził** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |