ZARZĄDZENIE NR 17/2021/2022
Dyrektora Szkoły Podstawowej nr 1 im. Wojska Polskiego
z dnia 22 lutego 2022 r.

w sprawie wdrożenia Regulaminu Bezpieczeństwa Informacji oraz instrukcji i procedur dotyczących bezpieczeństwa informacji

W związku z wejściem w życie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dziennik Urzędowy UE - 4.5.2016 L 119/3) oraz Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r., poz. 1781.)

Zarządza się, co następuje:

§ 1.

Wprowadzam w życie w Szkole Podstawowej nr 1 im. Wojska Polskiego (dalej SP1 w Porębie) Regulamin Bezpieczeństwa Informacji, który stanowi załącznik 1 do zarządzenia wraz z procedurami postępowania stanowiącymi integralną część ochrony danych osobowych

§ 2.

Zadania związane z prawidłowością przetwarzania danych osobowych w SP1 w Porębie realizują wszyscy pracownicy, zatrudnieni w Jednostce, a za skuteczne funkcjonowanie Regulaminu Bezpieczeństwa Informacji jak też instrukcji i procedur postępowania odpowiedzialny jest Dyrektor oraz Inspektor Ochrony Danych w SP1 w Porębie.

§ 3.

Zasady ochrony danych określone są w Polityce Ochrony Danych, Instrukcji Zarządzania Systemami Informatycznymi, oraz zdefiniowanymi i wdrożonymi procedurami postępowania stanowiącymi ogół wytycznych w celu skutecznej ochrony danych osobowych, na które składa się:

a) Procedura dostępu do pomieszczeń i przydziału kluczy
b) Główne aspekty ochrony danych osobowych zabezpieczenia organizacyjno-techniczne
c) Zasady postępowania użytkownika systemu teleinformatycznego obowiązujące podczas przetwarzania danych osobowych

§ 4.

Zobowiązuję wszystkich pracowników do zapoznania się z przepisami ochrony danych, obowiązujących w SP1 w Porębie oraz złożenie pisemnego oświadczenia o zapoznaniu się z dokumentacją z zakresu ochrony danych osobowych.

§ 5.

Funkcję Inspektora Ochrony Danych sprawuje od 2 września 2020 r. Pan Marek Woźniak. Dane do kontaktu: e-mail iod@sp1poreba.pl.

§ 6.

Zarządzenie wchodzi w życie z dniem 22 lutego 2022 roku.

Załączniki do zarządzenia:

1. Regulamin Bezpieczeństwa Informacji
2. Polityka ciągłości działania
3. Polityka czystego biurka
4. Polityka kontroli oprogramowania
5. Polityka postępowania ze sprzętem i nośnikami
6. Polityka szacowanie ryzyka
7. Polityka zarządzania incydentami
8. Regulamin pomiaru skuteczności zabezpieczeń i systemu zarządzania bezpieczeństwem informacji
9. Procedury metodyki szacowania ryzyka
10. Procedura zarządzania zmianami
11. Instrukcja zarządzania incydentami w zakresie systemu cyberbezpieczeństwa
12. Zasady postępowania użytkownika obowiązujące podczas przetwarzania danych osobowych

Załącznik nr 1
do zarządzenia 17/2021/2022
dyrektora Szkoły Podstawowej nr 1 w Porębie

Regulamin
Bezpieczeństwa Informacji

Szkoła Podstawowa nr 1 im. Wojska Polskiego
ul. Wojska Polskiego 4, 42-480 Poręba

Spis treści

Załącznik nr 1
do zarządzenia 17/2021/2022
dyrektora Szkoły Podstawowej nr 1 w Porębie

Opis placówki

Celem nadrzędnym **Szkoły Podstawowej nr 1 im. Wojska Polskiego** 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.

Placówka 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 uczniom, 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 uczniów, 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 1 im. Wojska Polskiego, ul. Wojska Polskiego 4, 42-480 Poręba;**

Cele bezpieczeństwa informacji i plany do ich osiągnięcia

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

Cel	Osoba odpowiedzialna	Realizacja	Miernik	Ocena skuteczności
Poprawa bezpieczeństwa informacji w placówce	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	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, uczniom, pracownikom i kontrahentom przez **Szkołę Podstawową nr 1 im. Wojska Polskiego** oraz warunkiem ciągłego rozwoju placówki. 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 placówce 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, uczniów, 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 placówki,
- zapewni poprawne i bezpieczne funkcjonowanie wszystkich systemów przetwarzania informacji,
- zapewni gotowość do podjęcia działań w sytuacjach kryzysowych dla bezpieczeństwa placówki, 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 placówce,
- 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 placówce 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**. placówka 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 placówki 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

Placówka ze względu na fakt, iż obowiązujące standardy nie nakładają 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. Placówka szacując ryzyko wzięła pod uwagę wymagania z załącznika A normy ISO 27001 oraz normy ISO 27005.

Kontekst placówki

Zewnętrzny kontekst placówki z jednej strony nie zawiera istotnych dostawców, którzy mieliby wpływ na SZBI z drugiej składa się z rodziców/opiekunów prawnych, uczniów, pracowników i kontrahentów placówki, 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. Pracownicy
- kodeks Pracy.
- dokumentacja SZBI
- stosowanie przepisów prawa

4. 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/uczeń
-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 trzech głównych elementów. Są nimi:

- Polityka bezpieczeństwa informacji
- Procedury i instrukcje bezpieczeństwa, które określają szczegółowo zasady postępowania,
- Raporty z analizy ryzyka i plany postępowania z ryzykiem

Struktura zarządzania bezpieczeństwem i podział odpowiedzialności

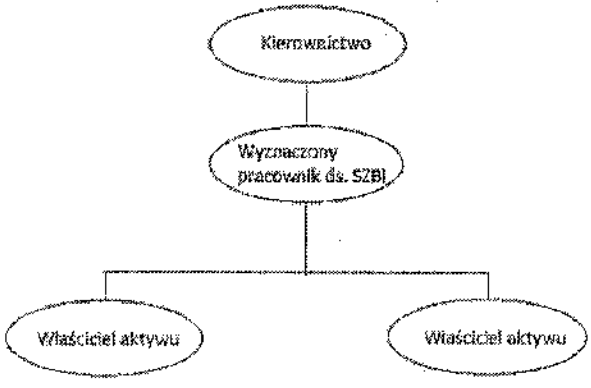
Odpowiedzialność za bezpieczeństwo informacji w placówce ponoszą wszyscy pracownicy zgodnie z posiadanymi zakresami obowiązków.

- 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 placówki. 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

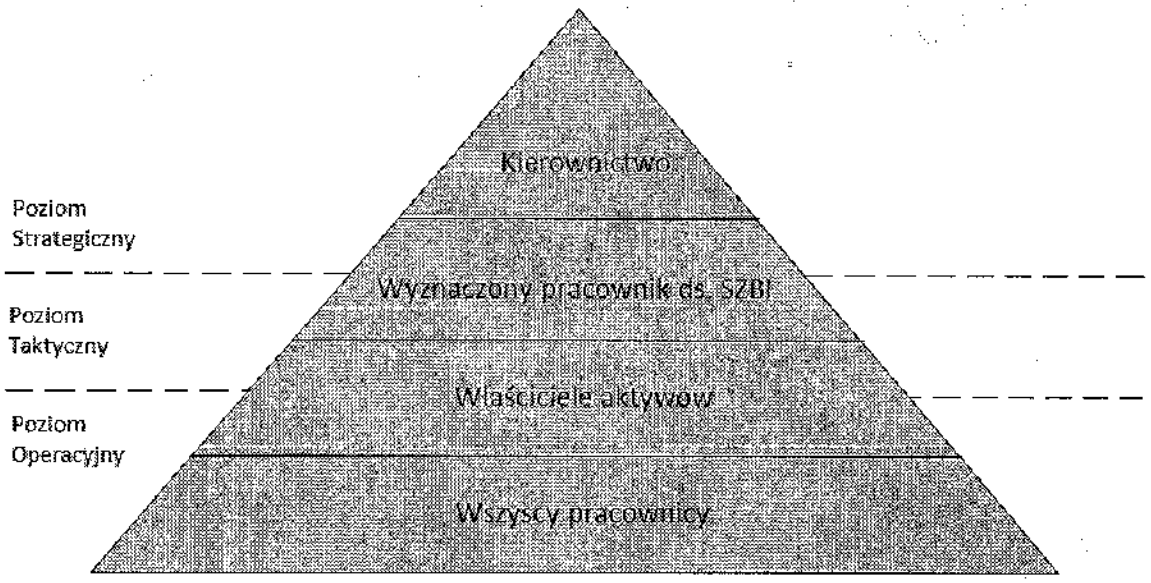
Poniższy schemat przedstawia organizację zarządzania bezpieczeństwem informacji w placówce.



W powyższej strukturze możliwe jest wyróżnienie trzech poziomów działań:

- Na **poziomie strategicznym** prowadzona jest 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 zaangażowany jest Dyrektor placówki 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 placówki.
- 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 ucznia nie są komunikowane na zewnątrz.

Wewnątrz placówki 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

Placówka 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

Placówka 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 placówki zobligowana 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 placówki. Dostęp do biur, gabinetów i sal dydaktycznych wszelkiego personelu technicznego zajmującego się konserwacją sprzętu, ochrony, kontrahentów i innych osób jest nadzorowany przez wyznaczonego pracownika placówki.

Zasady współpracy z innymi Organizacjami

Współpraca placówki z innymi Organizacjami oparta jest na umowach. Zawierając te umowy placówka 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 placówki na wypadek pożaru lub awarii:
- O zaistniałym pożarze lub awarii pracownik natychmiast zawiadamia Straż Pożarną , Dyrektora placówki,
- Przybyłe jednostki ratownicze natychmiast kieruje na miejsce akcji.

Informacje kontaktowe dostępne są w sekretariacie placówki.

Zarządzanie aktywami i ryzykami

Placówka 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, uczniów, 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 placówce jest przeprowadzanie okresowej analizy ryzyka i opracowania planów postępowania z ryzykiem. Analiza jej wyników stanowi podstawę podejmowania wszelkich działań w zakresie doskonalenia ochrony zasobów placówki.
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 przez Dyrektora placówki 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.

Placówka 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/opiekunom prawnym, uczniom, 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.
Placówka 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

Placówka 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 placówki 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

Placówka 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 placówkę.
- 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.
- Placówka monitoruje poziom incydentów w systemach informatycznych i posiada mechanizmy reagowania w przypadkach ich wystąpienia.

Kontrola dostępu

Placówka 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 placówce 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

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

Pozyskiwanie, rozwój i utrzymanie systemów informacyjnych

Placówka 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,
- Wdrożone procedury kontroli zmian/ aktualizacji oprogramowania.

Zarządzanie incydentami

W przypadku wszelkich incydentów w placówce 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 przez Dyrektora lub osobę wyznaczoną przez Dyrektora, natomiast analizowane przez inspektora ds. ochrony danych osobowych i Dyrektora placówki.

Szczegółowy opis postępowania z incydentami zawiera procedura „Zarządzanie Incydentami"

Zarządzanie ciągłością działania

Placówka 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.
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 placówka jest przygotowana na działanie również w przypadkach odbiegających od normy.

Zgodność
Placówka 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
Placówka 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/uczeń, pracownikami i kontrahentami i innymi zainteresowanymi stronami)

Załącznik nr 1.

Wykaz zmian

Lp.	Data zmiany	Nr strony	Krótki opis zmiany	Wprowadził

Załącznik nr 2
do zarządzenia 17/2021/2022
dyrektora Szkoły Podstawowej nr 1 w Porębie

Polityka Ciągłości Działania

1. CEL

Zapewnienie ciągłości działania i ochrona procesów przed skutkami zdarzeń losowych i sytuacji kryzysowych.

2. ZAŁOŻENIA

2.1. Nieprzestrzeganie niniejszej Polityki będzie skutkować pociągnięciem do odpowiedzialności dyscyplinarnej.

- **Szkoła Podstawowa nr 1 im. Wojska Polskiego** posiada Plan Ochrony ppoż. i ustalony sposób komunikacji na wypadek klęsk żywiołowych: zalanie, pożar itp.
- W zakresie ciągłości funkcjonowania placówka wykonuje kopie zapasowe w wersji elektronicznej wszystkich istotnych danych dotyczących działalności placówki oraz przeprowadza cykliczne sprawdzanie poprawności ich działania.
- Archiwizowane dane elektroniczne przechowane są w szafie pancernej.
- Dokumenty papierowe archiwizowane są w archiwum – nie wykonuje się kopii zapasowej tych dokumentów. Pomieszczenie zabezpieczone jest odpowiednim zamkiem oraz systemem alarmowym.
- Instrukcja ppoż. jest opracowywana i aktualizowana przez inspektora BHP, który odpowiedzialny jest za jej dostępność oraz przeszkolenie pracowników placówki.
- Instrukcje ppoż. przeglądane są pod kątem ich adekwatności i aktualności przez Inspektora BHP.
- Za przestrzeganie zasad wynikających z tej polityki odpowiedzialny jest Dyrektor.
- Dyrektor odpowiada za bezpieczeństwo pracy użytkowanych pomieszczeń i aktualną instrukcje ppoż., by była dostępna w miejscu jej stosowania oraz za organizację szkoleń pracowników w tym zakresie.
- W przypadku utraty danych elektronicznych dane te są odtwarzane z kopii zapasowych.
- Dyrektor odpowiada za organizację, wyznaczenie osób odpowiedzialnych za ewakuację z pomieszczeń placówki dokumentów, danych i sprzętu w przypadku pożaru lub zalania użytkowanych pomieszczeń.

Nr egz:	Stanowisko	Imię i nazwisko	Data	Podpis
Zatwierdził	Dyrektor	Agnieszka Andrzejewska		

Załącznik nr 3
do zarządzenia 17/2021/2022
dyrektora Szkoły Podstawowej nr 1 w Porębie

Polityka Czystego Biurka i pulpitu

1. CEL

Zapobieganie utracie, uszkodzeniu lub możliwości nieuprawnionego dostępu do informacji oraz do urządzeń przetwarzających informacje.

2. ZAKRES

Procedura swoim zakresem obejmuje wszystkich pracowników.

3. OPIS POSTĘPOWANIA

3.1 Nieprzestrzeganie niniejszej procedury będzie skutkować pociągnięciem do odpowiedzialności dyscyplinarnej.

3.2 Aby zapewnić bezpieczeństwo danych obowiązuje szereg zasad czystego biurka i czystego pulpitu.

3.3 Czynności

3.3.1 Biurko

- Wszystkie dokumenty i ruchome nośniki danych (płyty CD, dyski przenośne, pamięć zewnętrzna itp.) nie są pozostawiane na biurku. W momencie, gdy przestają być używane – chowane są do szafek i biurek. W przypadku informacji wrażliwych / zastrzeżonych, zamykane są na klucz, a dane z nich usuwa się gdy stają się niepotrzebne.
- Na biurku znajdują się jedynie dokumenty aktualnie wykorzystywane przez pracownika/personel. W przypadku opuszczenia stanowiska pracy (wyjście do WC, na przerwę śniadaniową / obiadową, poza siedzibę) wszystkie dokumenty i ruchome nośniki danych oraz pieczęcie znajdują się w szafkach i szufladach. W przypadku informacji wrażliwych i zastrzeżonych, ruchome nośniki i pieczęcie, zamykane są na klucz.
- Dyrektor lub pracownik wyznaczony przez Dyrektora przeprowadza po godzinach pracy okresowe przeglądy z zakresu stosowania postanowień czystego biurka i pulpitu oraz zabezpieczenia informacji wrażliwych/ zastrzeżonych przed nieuprawnionym dostępem.

3.3.2. Pulpit

- W odniesieniu do urządzeń przetwarzających informacje (komputer) stosuje się zasadę czystego pulpitu – nie prowadzi się zapisywania, tymczasowego zapisywania plików. Na pulpicie znajdują się tylko skróty do plików oraz katalogów.
- Po odejściu od stanowiska pracy należy się wylogować (przełączenie użytkownika).
- Dyrektor lub pracownik wyznaczony przez Dyrektora przeprowadza po godzinach pracy okresowe przeglądy z zakresu stosowania postanowień czystego pulpitu oraz wylogowania się z sieci w przypadku opuszczenia stanowiska pracy.

Nr egz:	Stanowisko	Imię i nazwisko	Data	Podpis
Zatwierdził	Dyrektor	Agnieszka Andrzejewska		

Załącznik nr 4
do zarządzenia 17/2021/2022
dyrektora Szkoły Podstawowej nr 1 w Porębie

Polityka Kontroli Oprogramowania

1. CEL

Zapewnienie bezpieczeństwa, poufności, integralności i dostępności informacji i oprogramowania.

2. ZAŁOŻENIA

2.1. Nieprzestrzeganie niniejszej Polityki będzie skutkować pociągnięciem do odpowiedzialności dyscyplinarnej.

1. Ochrona przed szkodliwym oprogramowaniem:

- Szkodliwe oprogramowanie to wirusy komputerowe, robaki sieciowe, konie trojańskie i inne oprogramowanie mogące skutkować naruszeniem bezpieczeństwa, poufności, integralności i dostępności informacji.
- Na komputerach z systemem operacyjnym Windows, które są podłączone do Internetu instalowane jest oprogramowanie antywirusowe.
- Oprogramowanie antywirusowe na komputerach jest regularnie aktualizowane.
- Aktualizacja oprogramowania następuje automatycznie gdy pojawiają się jego nowsze wersje bezpośrednio z serwera producenta oprogramowania.
- Wszystkie pliki zewnętrzne i wewnętrzne (w tym poczta e-mail) są automatycznie monitorowane i skanowane przez program antywirusowy.

2. Kontrola legalności oprogramowania komputerowego:

- Obowiązuje bezwzględny zakaz instalowania bez zgody Dyrektora nielegalnego lub zewnętrznego (nie zakupionego przez placówkę) oprogramowania komputerowego na komputerach (także laptopach) będących własnością placówki.
- Nowe oprogramowanie jest nadzorowane przez Administratora systemów informatycznych (Informatyka lub pracownika placówki wyznaczonego przez Dyrektora.
- Prowadzony jest rejestr oprogramowania zainstalowanego na każdym komputerze w postaci „Zestawienia Zbiorczego dla Zestawu" (użytkownik, oprogramowanie).
- Obowiązuje bezwzględny zakaz udostępniania programów będących własnością placówki osobom trzecim, oraz instalowania programów jednostanowiskowych na innych stanowiskach.
- Licencje oprogramowania są przechowywane w segregatorach i szafkach przez Administratora systemów informatycznych(Informatyka lub pracownika placówki wyznaczonego przez Dyrektora).

3. Pracownik placówki ma obowiązek niezwłocznie zgłosić do Administratora systemów informatycznych (Informatyka lub pracownika placówki wyznaczonego przez Dyrektora) każdy problem związany z niewłaściwym funkcjonowaniem sprzętu komputerowego lub oprogramowania.

4. Instalację lub reinstalację oprogramowania systemowego i użytkowego na stanowiskach komputerowych dokonuje Administrator systemów informatycznych (Informatyk lub pracownik placówki wyznaczony przez Dyrektora) na wniosek Dyrektora lub użytkownika sprzętu.

5. System komputerowy jest chroniony przed wirusami komputerowymi poprzez regularne, automatyczne skanowanie systemu programem antywirusowym.

Nr egz:	Stanowisko	Imię i nazwisko	Data	Podpis
Zatwierdził	Dyrektor	Agnieszka Andrzejewska		

Załącznik nr 5
do zarządzenia 17/2021/2022
dyrektora Szkoły Podstawowej nr 1 w Porębie

Polityka Postępowania ze Sprzętem i Nośnikami

1. **CEL**

Zapobieganie utracie, uszkodzeniu, możliwości nieuprawnionego dostępu do sprzętu i nośników danych lub innym naruszeniom bezpieczeństwa danych.

2. **ZAŁOŻENIA**

2.1. **Nieprzestrzeganie niniejszej Polityki będzie skutkować pociągnięciem do odpowiedzialności dyscyplinarnej.**

2.2. **Rozmieszczenie, ochrona i konserwacja sprzętu:**

- Sprzęt należy ustawiać w taki sposób, aby zminimalizować niepożądany dostęp do obszarów roboczych; monitory komputerowe powinny być ustawione tyłem do drzwi, drukarki, kopiarki, faksy i inne urządzenia służące do gromadzenia lub przetwarzania danych powinny znajdować się w pokojach służbowych.
- Urządzenia do przetwarzania informacji wrażliwych i informacji niejawnych są odizolowane – umiejscowione w strefach bezpieczeństwa.
- Spożywanie posiłków odbywa się w wyznaczonym do tego miejscu z dala od urządzeń przetwarzających informacje oraz od dokumentów papierowych.
- Sprzęt jest konserwowany i przeglądany przez Administratora systemów informatycznych (Informatyka lub osobę wyznaczoną przez Dyrektora) w miarę bieżących potrzeb oraz na podstawie zgłoszenia awarii.

2.3. **Zapewnienie zasilania, łączności i innych warunków środowiskowych:**

- Sprzęt komputerowy chroniony jest przed awariami zasilania i innymi zakłóceniami elektrycznymi poprzez zapewnienie właściwego zasilania zgodnie z zaleceniami producenta – stosowanie zabezpieczeń typu dwustopniowe zabezpieczenia przeciw przepięciowe, urządzenia podtrzymujące zasilanie (UPS)

2.4. **Zabezpieczenie danych w siedzibie:**

- Prowadzone są spisy inwentaryzacyjne sprzętu.
- Nośniki danych zawierające informacje wrażliwe i zastrzeżone każdorazowo są chowane przy wyjściu do toalety i do domu – zasada czystego biurka. Szafki oraz biurka gdzie przechowywane są nośniki danych zamykane są na klucz.
- Dostęp do Internetu oraz do poczty elektronicznej zabezpieczony jest poprzez Firewall.
- Komputery automatycznie wylogowują użytkownika i wygaszają ekran w przypadku dłuższej bezczynności, po zakończeniu pracy każdy pracownik ma obowiązek wylogować się z systemu.
- Każdy użytkownik komputera ma nadane hasło i login, które musi wprowadzać za każdym razem po uruchomieniu, wygaszeniu lub wylogowaniu. Hasło jest zmieniane co 1 miesiąc.
- Wszelkie drukowane oraz kopiowane dokumenty zabierane są od razu z drukarki lub kopiarki

2.5. **Zabezpieczenie sprzętu i danych poza siedzibą:**

- Obowiązuje zasada, że sprzęt komputerowy, dokumenty, dane oraz nośniki danych nie są wynoszone poza siedzibę placówki.
- Tylko osoby, które otrzymały zezwolenie na wyniesienie poza siedzibę sprzętu lub nośników danych (pendrive, taśmy, dokumentacja papierowa) mogą wynosić w/w zasoby. Osoby te ponoszą pełną odpowiedzialność za powierzone zasoby.
- Sprzęt i nośniki zabierane z siedziby nie są pozostawiane bez nadzoru w miejscach publicznych (np. nie są pozostawiane w samochodzie). Należy odpowiednio obchodzić się ze sprzętem (zgodnie z zaleceniami producenta) oraz chronić go przed zniszczeniem i utratą (nie rzucać sprzętu, przewozić w taki sposób, który nie zdradza zawartości bagażu). Sprzęt należy odpowiednio zabezpieczyć przed dostępem osób niepowołanych – hasło, login.
- Dane na nośnikach magnetycznych należy chronić przed polem magnetycznym oraz wysoką temperaturą.

2.6. **Zasady postępowania z nośnikami danych (taśmy, dyski, kasety, płyty CD/DVD, dyskietki, pendrive, pamięć zewnętrzna, kartki papieru – wydruki, dokumenty, rejestry, itp.):**

- Nośniki danych np. dyski twarde, nosiki USB, płyty CD/DVD (niewłaściwie nagrane dane) które są już zużyte, niszczone są fizycznie lub dane na nich są trwale usuwane (wielokrotne nadpisanie danych).
- W przypadku zmiany nośnika lub właściciela sprzętu każda informacja zawarta na dysku jest usuwana lub pozostawiona (zależy to od przeznaczenia nośnika).
- Uszkodzone dyski są utylizowane przez firmę zewnętrzną, która posiada uprawnienia do wykonywania takich usług.
- W przypadku zmiany właściciela sprzętu dysk jest formatowany w taki sposób, aby danych z dysku nie można było odtworzyć i tylko taki sprzęt jest przekazany nowemu użytkownikowi.
- Nośniki z danymi wrażliwymi lub zastrzeżonymi powinny być każdorazowo chowane – zamykane na klucz w szafie lub biurku w sytuacji opuszczenia stanowiska pracy (wyjście do ubikacji, do domu). Obowiązuje zasada czystego biurka.
- W przypadku przechowywania danych przez dłuższy czas należy je odświeżyć w zależności od nośnika w celu sprawdzenia dostępności i integralności danych.

3. **CZYNNOŚCI**

- Każdy pracownik stosuje zasadę czystego biurka i czystego pulpitu.
- Administrator systemów informatycznych (Informatyk lub pracownik placówki wyznaczony przez Dyrektora) usuwa w sposób trwały informacje z nośników danych - jeżeli wymaga tego sytuacja.
- Administrator systemów informatycznych (Informatyk lub pracownik placówki wyznaczony przez Dyrektora deponuje uszkodzone nośniki w zamykanej szafie (w uzasadnionych przypadkach przekazuje je firmie utylizującej).

Nr egz:	Stanowisko	Imię i nazwisko	Data	Podpis
Zatwierdził	Dyrektor	Agnieszka Andrzejewska		

Załącznik nr 6
do zarządzenia 17/2021/2022
dyrektora Szkoły Podstawowej nr 1 w Porębie

Polityka Szacowania Ryzyka

1. **Cel**

Zapewnienie, że Metodyka Szacowania Ryzyka przyjęta w placówce jest spójna ze zidentyfikowanymi wymaganiami prawnymi w zakresie ochrony bezpieczeństwa informacji, zawiera kryteria akceptacji ryzyka i zapewnia uzyskanie porównywalnych wyników w placówce podczas kolejnych szacowań ryzyka.

2. **Założenia**

2.1 **Nieprzestrzeganie niniejszej Polityki będzie skutkować pociągnięciem do odpowiedzialności dyscyplinarnej.**

2.2 **Szacowanie ryzyka prowadzi wyznaczony pracownik ds.ZSBI wraz z Inspektorem ds. ochrony danych osobowych.**

2.3 **Szacowanie ryzyka przeprowadzane jest przynajmniej raz do roku oraz w przypadku zajścia następujących zdarzeń:**

- zidentyfikowania zasobów informacyjnych, co do których dotychczas nie przeprowadzono szacowania ryzyka,
- zmian w technologii (w tym informatycznej), mogących powodować zmianę zagrożenia bezpieczeństwa informacji,
- zidentyfikowania nowych lub zmienionych procesów zachodzących, które wykraczają poza dotychczas zdefiniowany zakres systemu SZBI.

2.4 **W szacowaniu ryzyka biorą udział właściciele zasobów po to, aby:**

- zapewnić poczucie odpowiedzialności właściciela za powierzony mu zasób i zwiększyć jego świadomość co do wagi bezpieczeństwa informacji,
- zapewnić realistyczne oszacowanie rodzaju zagrożeń, wartości zasobu, podatności i prawdopodobieństwa wystąpienia zagrożeń.

2.5 **Właściciel ryzyka uczestniczy w szacowaniu ryzyka wspólnie z Inspektora ds. ochrony danych osobowych, który je scala, a następnie analizuje.**

Nr egz:	Stanowisko	Imię i nazwisko	Data	Podpis
Zatwierdził	Dyrektor	Agnieszka Andrzejewska		

Załącznik nr 7
do zarządzenia 17/2021/2022
dyrektora Szkoły Podstawowej nr 1 w Porębie

Polityka Zarządzania Incydentami

1. **Cel**

Zapewnienie, że incydenty i słabości związane z systemami informacyjnymi są zarządzane tak, aby umożliwić podejmowanie we właściwy sposób działań korygujących.

2. **Założenia**

2.1 Nieprzestrzeganie niniejszej Polityki będzie skutkować pociągnięciem do odpowiedzialności dyscyplinarnej.

2.2 *Incydent* rozumiany jest jako zdarzenie, które stwarza wzrost prawdopodobieństwo zakłócenia funkcjonowania i zagrażają bezpieczeństwu informacji np. włamanie do siedziby, pozostawienie wrażliwych danych na ekranie komputera, dokumentów bez nadzoru itp.

2.3 *Słabość systemu* rozumiana jest jako stan mogący powodować wystąpienie incydentu, np. zawieszenie się komputera, niezamknięte drzwi, próba włamania do systemu, do siedziby, podejrzenie o włamaniu itp.

3. **Czynności**

3.1 W przypadku wystąpienia jakiegokolwiek incydentu, (np. Osoby nieupoważnione bez nadzoru w strefach bezpieczeństwa, dokumenty zawierające dane wrażliwe pozostawione bez nadzoru w miejscu ogólnie dostępnym), osoba, która zauważy zdarzenie ma obowiązek niezwłocznie poinformować Dyrektora o zaistniałej sytuacji i rozpocząć doraźne działania adekwatne do zaistniałej sytuacji. Zostają ustalone kroki postępowania.

3.2 W przypadku wystąpienia incydentu typu pożar, zalanie itp. Pracownicy postępują zgodnie z instrukcjami ppoż. i bezpieczeństwa oraz wytycznymi Dyrektora i Inspektora ds. BHP. Kierownictwo współpracuje ze sztabem kryzysowym oraz odpowiednimi władzami w celu usunięcia skutków incydentu i dojścia do przyczyny jego wystąpienia. Po uzyskaniu informacji, przekazywane są one do Inspektora ds. ochrony danych osobowych celem podjęcia szacowania ryzyka i zabezpieczenia.

3.3 W przypadku wystąpienia incydentu związanego z awarią sprzętu / sieci komputerowej, np. zawieszenie się systemu, próba włamania, nieoczekiwany komunikat na ekranie komputera, należy niezwłocznie zgłosić zdarzenie Administratorowi systemów informatycznych (Informatykowi lub pracownikowi wyznaczonemu przez Dyrektora) i nie podejmować żadnych działań na własną rękę. Administrator systemów informatycznych (Informatyk lub wyznaczony pracownik przez Dyrektora) informuje Inspektora ds. Ochrony danych osobowych o zaistniałym incydencie oraz podejmuje odpowiednie działania.

3.4 Wyznaczona osoba prowadzi Rejestr Incydentów, gdzie odnotowane są wszystkie zgłoszenia błędów, awarii systemu oraz innych incydentów.

3.5 Administrator systemów informatycznych (Informatyk lub osobowa wyznaczona przez Dyrektora) prowadzi okresowe przeglądy rejestru incydentów oraz dokonuje analizy wpisów. W uzasadnionych sytuacjach podejmuje działania korygujące lub zapobiegawcze zgodnie z procedurą działań korygujących i zapobiegawczych. Wyniki analiz są przedstawiane na Przeglądach Zarządzania.

Nr egz:	Stanowisko	Imię i nazwisko	Data	Podpis
Zatwierdził	Dyrektor	Agnieszka Andrzejewska		

Załącznik nr 8
do zarządzenia 17/2021/2022
dyrektora Szkoły Podstawowej nr 1 w Porębie

RAPORT ANALIZY RYZYKA

Z przeprowadzonej analizy szacowania ryzyka wynika, że w 1 przypadku wymagane jest podjęcie działań korygujących. Działania te należy wykonać w odniesieniu do następujących aktywów:

Lp.	Dział	Aktyw	Decyzja
1.	Sekretariat	Dane uczniów	zabezpieczenia
2.			
3.			
4.			
5			
6			
7			
8			
9			
10			

.....
/data i podpis Inspektora ds. ochrony danych osobowych

.....
/data i podpis Dyrektora/

Załącznik nr 8
do zarządzenia 17/2021/2022
dyrektora Szkoły Podstawowej nr 1 w Porębie

REGULAMIN POMIARU SKUTECZNOŚCI ZABEZPIECZEŃ I SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

§ 1.
Organizacja procesu pomiaru skuteczności zabezpieczeń i systemu zarządzania bezpieczeństwem informacji

1. Nadzór nad procesem pomiaru skuteczności zabezpieczeń oraz SZBI sprawuje Dyrektor/Administrator Danych Osobowych lub pracownik wyznaczony ds. SZBI przez Dyrektora.

§ 2.
Pomiary skuteczności zabezpieczeń i SZBI

1. Właściciele Aktywów gromadzą dane zgodnie z określonymi w załączniku nr 1 zasadami i przekazują pracownikowi wyznaczonemu przez ADO ds. SZBI, który wykonuje pomiar skuteczności.
2. Pracownik wyznaczony przez ADO ds. SZBI wykonuje analizę wyników pomiaru i określa wskaźnik bezpieczeństwa, wykorzystując wyniki pomiarów z poprzednich okresów pomiarowych.

Załącznik nr 1 do Regulaminu
Lista zabezpieczeń oraz elementów systemu zarządzania bezpieczeństwem informacji objęta programem pomiarów skuteczności

Pkt	Zabezpieczenie	Miernik/wskaźnik	Częstotliwość pomiaru
A.5.1.1	Dokument polityki bezpieczeństwa informacji	Ilość pracowników przeszkolonych z PBI/Ilość zatrudnionych	1/rok
A.5.1.2	Przegląd polityki bezpieczeństwa informacji		
A.6.1.1	Zaangażowanie kierownictwa w bezpieczeństwo informacji	Ilość stanowisk z określonym zakresem czynności, odpowiedzialności/ ilości wszystkich stanowisk	1/rok
A.6.1.2	Koordynacja bezpieczeństwa informacji		
A.6.1.3	Przypisanie odpowiedzialności w zakresie bezpieczeństwa informacji		
A.6.1.4	Umowy o zachowaniu poufności	Ilość umów zawierających klauzule poufności/Ilości wszystkich umów	1/rok
A.6.1.5	Kontakty z organami władzy	Ilość zdarzeń wymagających kontaktów z organami władzy	1/rok
A.6.1.6	Kontakty z grupami zainteresowania bezpieczeństwem		

A.6.1.7	Niezależny przegląd bezpieczeństwa informacji	Ilość niezgodności stwierdzonych podczas auditów zewnętrznych	1/rok
A.6.2.1	Określenie ryzyk związanych ze stronami zewnętrznymi	1. Ilość umów bez deklaracji poufności/ilości umów ogółem 2. Ilość incydentów związanych ze stronami trzecimi	1/rok
A.6.2.2	Bezpieczeństwo w kontaktach z klientami		
A.6.2.3	Bezpieczeństwo w umowach ze stroną trzecią		
A.7.1.1	Inwentaryzacja aktywów	Częstotliwość zmian w analizie ryzyka	1/rok
A.7.1.2	Własność aktywów		
A.7.1.3	Akceptowalne użycie aktywów		
A.8.1.1	Role i odpowiedzialności	Ilość pracowników z wymaganymi kwalifikacjami/Ilośc i wszystkich pracowników.	1/rok
A.8.1.2	Postępowanie sprawdzające		
A.8.1.3	Zasady i warunki zatrudnienia		
A.8.2.1	Odpowiedzialność kierownictwa	Liczba pracowników przeszkolonych z zakresu SZBI/Ilości pracowników ogółem w stosunku do których zaplanowano szkolenie	1/rok
A.8.2.2	Uświadomienie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji		
A.8.2.3	Postępowanie dyscyplinarne	Ilość pracowników zwolnionych ze względu na nie przestrzeganie PBI	1/rok
A.8.3.1	Odpowiedzialności związane z zakończeniem zatrudnienia	Ilość utraconych aktywów Ilość niezgodności związanych z nieodebraniem praw dostępu	1/rok
A.8.3.2	Zwrot aktywów		
A.8.3.3	Odebranie praw dostępu		
A.9.1.1	Fizyczna granica obszaru bezpiecznego	1. Ilość nieautoryzowanych wejść do obiektu/incydentów 2. Ilość zdarzeń związanych z brakiem dostępu lub nieupoważnionym dostępem do dokumentów z powodu niedostatecznego zabezpieczenia kluczy do szaf	1/rok
A.9.1.2	Fizyczne zabezpieczenie wejścia		
A.9.1.3	Zabezpieczenie biur, pomieszczeń i urządzeń		
A.9.1.4	Ochrona przed zagrożeniami zewnętrznymi i środowiskowymi		
A.9.1.5	Praca w obszarach bezpiecznych		
A.9.2.1	Lokalizacja i ochrona sprzętu	1. Ilość uszkodzeń sprzętu/utraty danych spowodowanych zakłóceniami zasilania	1/rok
A.9.2.2	Systemy wspomagające		
A.9.2.3	Konserwacja sprzętu		
A.9.2.4	Bezpieczeństwo sprzętu poza siedzibą		
A.9.2.5	Bezpieczne zbywanie lub przekazywanie do ponownego użycia		

A.9.2.6	Wynoszenie mienia		
A.10.3.1	Zarządzanie pojemnością systemów	Ilość incydentów związanych z brakiem możliwości zapisania danych w związku z niedostateczna ilością miejsca na dysku/serwerze	1/rok
A.11.3.1	Używanie haseł	Ilość niezgodności podczas auditów	1/rok
A.11.3.2	Pozostawienie sprzętu użytkownika bez opieki		
A.11.3.3	Polityka czystego biurka i czystego ekranu		
A.11.7.1	Przetwarzanie i komunikacja mobilna	1. Ilość incydentów związanych z utraceniem danych	1/rok
A.11.7.2	Praca na odległość		
A.13.1.1	Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji	Ilość incydentów rozwiązanych/Ilość zgłoszonych incydentów	1 / rok
A.13.1.2	Zgłaszanie słabości systemu bezpieczeństwa		
A.13.2.1	Odpowiedzialność i procedury	Czas rozwiązania incydentów w odniesieniu do założonego czasu	1 / rok
A.13.2.2	Wyciąganie wniosków z incydentów związanych z bezpieczeństwem informacji		
A.13.2.3	Gromadzenie materiału dowodowego		
A.15.1.1	Określenie odpowiednich przepisów prawnych	Zgodność z przepisami	1/rok
A.15.1.3	Ochrona zapisów placówki	Ilość zniszczonych dokumentów i zapisów przed upływem okresu archiwizacji	1/rok

Załącznik nr 10
do zarządzenia 17/2021/2022
dyrektora Szkoły Podstawowej nr 1 w Porębie

Procedura Zarządzania Zmianami

Wszelkie zmiany systemów informatycznych muszą być poprzedzone następującymi działaniami:

1. Zdefiniowanie wymagań funkcjonalnych dla nowych lub modyfikowanych systemów oraz utrzymywanie kontroli wersji oprogramowania.
2. Oszacowaniem ryzyka oraz analizą wpływu zmian na istniejące zabezpieczenia.
3. Analiza modyfikacji, zatwierdzenie lub odrzucenie.
4. Podpisanie umowy z firmą zewnętrzną na wykonanie zmiany lub realizacja projektu we własnym zakresie.
5. Ustalenie kanałów komunikacji i osób odpowiedzialnych za proces.
6. Testowanie i ewentualne poprawki, w przypadku nowego systemu zaakceptowanie testów sytemu oraz podpisanie protokołu odbioru.
   W odniesieniu do systemów niekrytycznych zaleca się stosowanie automatycznych uaktualnień (wgrywanie łat, uaktualnienia serwisowe).
7. Stworzenia kopii zapasowej przed wgraniem zmian na system produkcyjny.

.....
/data i podpis Inspektora ds. ochrony danych osobowych/

.....
/data i podpis Dyrektora/

Instrukcja zarządzania incydentami w zakresie systemu cyberbezpieczeństwa w Szkole Podstawowej nr 1 im. Wojska Polskiego ul. Wojska Polskiego 4, 42-480 Poręba

Załącznik nr 11
do zarządzenia 17/2021/2022
dyrektora Szkoły Podstawowej nr 1 w Porębie

W związku z realizacją wytycznych ustawy z dnia 5 lipca 2018 roku (Dz.U.2018.1560) o krajowym systemie cyberbezpieczeństwa w Szkole Podstawowej nr 1 im. Wojska Polskiego, ul. Wojska Polskiego 4, 42-480 Poręba (dalej: **SP1 w Porębie)** wprowadzona zostaje procedura mająca na celu prawidłowe wywiązanie się z nałożonych obowiązków w zakresie cyberbezpieczeństwa w **SP1 w Porębie**, określająca zasady postępowania w chwili wystąpienia zagrożenia lub ataku, która przedstawia się następująco:

1. Do monitorowania przypadków mogących mieć negatywny wpływ na cyberbezpieczeństwo, wyznacza się Informatyka w **SP1 w Porębie** w osobie: **Przemysław Drabek** przy czym każdy pracownik Jednostki, który zauważy wystąpienie zdarzeń (zachowań w obsługiwanych systemach) mogących wskazywać na ingerencję w system osób trzecich, zobowiązany jest zawiadomić Kierownika Jednostki.

2. ASI/Informatyk monitoruje w szczególności wystąpienie z poziomu Internetu i/lub domeny przypadków:
   a) skanowania,
   b) spamu przesyłanego za pośrednictwem polskich serwerów,
   c) ataków typu DoS (Denial of Service) i DDoS (Distributed Denial of Service),
   d) włamań i prób włamania.

3. Informatyk reaguje na każde zgłoszenie dokonane przez pracownika Jednostki dotyczące zdarzeń mogących wskazywać na cyberatak, lub inną formę ingerencji w systemy eksploatowane
   w Jednostce, która wskazuje na niekontrolowane działanie osób trzecich oraz weryfikuje zgłoszenie i podejmuje stosowne działania, o których mowa w pkt. 5.

4. Na podstawie opublikowanego corocznego raportu CERT Polska z 2018 roku (https://www.cert.pl/news/single/zgloszenia-i-incydenty-w-2018-roku/), wykaz incydentów, w tym incydentów występujących najczęściej ze szczegółowym podziałem na poszczególne kategorie według klasyfikacji eCSIRT.net[1] przedstawia tabela 1.

5. Incydent w podmiocie publicznym – **SP1 w Porębie**, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego Informatyk zgłasza niezwłocznie:

   a) Kierownikowi Jednostki, w celu umożliwienia realizacji obowiązku wynikającego z art. 22 ust. 1 pkt 2 Ustawy o krajowym systemie cyberbezpieczeństwa tj. zgłoszenia incydentu niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia, do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV zawierającego informacje, o których mowa w *załączniku nr 1* do niniejszej instrukcji.

[1] Projekt współpracy zespołów CSIRT

b) Inspektorowi ochrony danych (IOD) w **SP1 w Porębie**, na adres poczty elektronicznej: iodo@marwikpoland.pl poprzez przesłanie wypełnionego formularza stanowiącego *załącznik nr 1* do niniejszej instrukcji, oraz telefonicznie na numer kom: 694 167 023.

IOD dokonuje ustalenia czy zidentyfikowany incydent nie stanowi jednocześnie naruszenia ochrony danych osobowych, a w konsekwencji czy nie wymaga podjęcia stosownych działań w tym zakresie tj. oceny wagi ryzyka naruszenia praw i wolności osób fizycznych, oceny zasadności odnotowania incydentu w rejestrze incydentów i naruszeń, zgłoszenia naruszenia do PUODO, i/lub zawiadomienia osób fizycznych których dane dotyczą.

Tabela 1. Wykaz incydentów w podziale na kategorie wg klasyfikacji eCSIRT.net

Obraźliwe i nielegalne treści	**Spam**
	Dyskredytacja, obrażanie
	Pornografia dziecięca, przemoc
	Niesklasyfikowane
Złośliwe oprogramowanie	**Wirus**
	Robak sieciowy
	Koń trojański
	Oprogramowanie szpiegowskie
	Dialer
	Rootkit
	Niesklasyfikowane
Gromadzenie informacji	Skanowanie
	Podsłuch
	Inżynieria społeczna
	Niesklasyfikowane
Próby włamań	Wykorzystanie znanych luk systemowych
	Próby nieuprawnionego logowania
	Wykorzystanie nieznanych luk systemowych
	Niesklasyfikowane
Włamania	Włamanie na konto uprzywilejowane
	Włamanie na konto zwykłe
	Włamanie do aplikacji
	Bot
	Niesklasyfikowane
Dostępność zasobów	Atak blokujący serwis (DoS)
	Rozproszony atak blokujący serwis (DDoS)
	Sabotaż komputerowy
	Przerwa w działaniu usług (niezłośliwe)
	Niesklasyfikowane
Atak na bezpieczeństwo informacji	Nieuprawniony dostęp do informacji
	Nieuprawniona zmiana informacji
	Niesklasyfikowane
Oszustwa komputerowe	Nieuprawnione wykorzystanie zasobów
	Naruszenie praw autorskich
	Kradzież tożsamości, podszycie się
	Phishing
	Niesklasyfikowane
Podatne usługi	Otwarte serwisy podatne na nadużycia
	Niesklasyfikowane
inne	...

Załącznik 2

FORMULARZ ZGŁOSZENIA INCYDENTU

Dane osoby dokonującej zgłoszenia:

Imię i nazwisko	
Stanowisko służbowe	
Kontakt (e-mail, nr tel.)	

Czy incydent miał/ma wpływ na realizację zadań publicznych? Jeśli tak, na jakie?

Kliknij lub naciśnij tutaj, aby wprowadzić tekst.

Dokładna lub przybliżona liczba osób, na które ma wpływ incydent?

Kliknij lub naciśnij tutaj, aby wprowadzić tekst.

Moment wystąpienia i wykrycia incydentu oraz przybliżony czas jego trwania

Kliknij lub naciśnij tutaj, aby wprowadzić tekst.

Zasięg geograficzny obszaru którego dotyczy incydent

Kliknij lub naciśnij tutaj, aby wprowadzić tekst.

Skutki oddziaływania incydentu na systemy informacyjne w Podmiocie

Kliknij lub naciśnij tutaj, aby wprowadzić tekst.

Informacje o przyczynie i źródle incydentu

Kliknij lub naciśnij tutaj, aby wprowadzić tekst.

Opis przebiegu incydentu (najdokładniej jak to możliwe)

Kliknij lub naciśnij tutaj, aby wprowadzić tekst.

Informacje o podjętych działaniach zapobiegawczych

Kliknij lub naciśnij tutaj, aby wprowadzić tekst.

Informacje o podjętych działaniach naprawczych

Kliknij lub naciśnij tutaj, aby wprowadzić tekst.

Inne istotne informacje

Kliknij lub naciśnij tutaj, aby wprowadzić tekst.

Wyciąg z Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa

Rozdział 5

Obowiązki podmiotów publicznych

Art. 21.

1. Podmiot publiczny, o którym mowa w art. 4 pkt 7–15, realizujący zadanie publiczne zależne od systemu informacyjnego jest obowiązany do wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.

2. Organ administracji publicznej może wyznaczyć jedną osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa w zakresie zadań publicznych zależnych od systemów informacyjnych, realizowanych przez jednostki jemu podległe lub przez niego nadzorowane.

3. Jednostka samorządu terytorialnego może wyznaczyć jedną osobę odpowiedzialną za utrzymywanie kontaktów
z podmiotami krajowego systemu cyberbezpieczeństwa w zakresie zadań publicznych zależnych od systemów informacyjnych, realizowanych przez jej jednostki organizacyjne.

Art. 22.

1. Podmiot publiczny, o którym mowa w art. 4 pkt 7–15, realizujący zadanie publiczne zależne od systemu informacyjnego:

1) zapewnia zarządzanie incydentem w podmiocie publicznym;

2) zgłasza incydent w podmiocie publicznym niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia, do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV;

3) zapewnia obsługę incydentu w podmiocie publicznym i incydentu krytycznego we współpracy z właściwym CSIRT MON, CSIRT NASK lub CSIRT GOV, przekazując niezbędne dane, w tym dane osobowe;

4) zapewnia osobom, na rzecz których zadanie publiczne jest realizowane, dostęp do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami, w szczególności przez publikowanie informacji w tym zakresie na swojej stronie internetowej;

5) przekazuje do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV dane osoby, o której mowa w art. 21, obejmujące imię i nazwisko, numer telefonu oraz adres poczty elektronicznej, w terminie 14 dni od dnia jej wyznaczenia, a także informacje o zmianie tych danych w terminie 14 dni od dnia ich zmiany.

2. Zgłoszenie, o którym mowa w ust. 1 pkt 2, przekazywane jest w postaci elektronicznej, a w przypadku braku możliwości przekazania go w postaci elektronicznej – przy użyciu innych dostępnych środków komunikacji.

Art. 23.

1. Zgłoszenie, o którym mowa w art. 22 ust. 1 pkt 2, zawiera:

1) dane podmiotu zgłaszającego, w tym nazwę podmiotu, numer we właściwym rejestrze, siedzibę i adres;

2) imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby składającej zgłoszenie;

3) imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby uprawnionej do składania wyjaśnień dotyczących zgłaszanych informacji;

4) opis wpływu incydentu w podmiocie publicznym na realizowane zadanie publiczne, w tym:

   a) wskazanie zadania publicznego, na które incydent miał wpływ,

   b) liczbę osób, na które incydent miał wpływ,

   c) moment wystąpienia i wykrycia incydentu oraz czas jego trwania,

   d) zasięg geograficzny obszaru, którego dotyczy incydent,

   e) przyczynę zaistnienia incydentu i sposób jego przebiegu oraz skutki jego oddziaływania na systemy informacyjne podmiotu publicznego;

5) informacje o przyczynie i źródle incydentu;

6) informacje o podjętych działaniach zapobiegawczych;

7) informacje o podjętych działaniach naprawczych;

8) inne istotne informacje.

2. Podmiot publiczny, o którym mowa w art. 4 pkt 7–15, przekazuje informacje znane mu w chwili dokonywania zgłoszenia, które uzupełnia w trakcie obsługi incydentu w podmiocie publicznym.

Załącznik nr 12
do zarządzenia 17/2021/2022
dyrektora Szkoły Podstawowej nr 1 w Porębie

ZASADY POSTĘPOWANIA UŻYTKOWNIKA OBOWIĄZUJĄCE PODCZAS PRZETWARZANIA DANYCH OSOBOWYCH W SZKOLE PODSTAWOWEJ NR 1 IM. WOJSKA POLSKIEGO UL. WOJSKA POLSKIEGO 4, 42-480 PORĘBA

Niniejsze zasady stanowią wyciąg z najistotniejszych zapisów zawartych w Polityce bezpieczeństwa danych osobowych oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Obowiązują pracowników etatowych, osoby świadczące pracę na podstawie umowy cywilnoprawnej (współpracowników), kontrahentów i usługodawców wykonujących usługi wymagające dostępu do danych osobowych Administratora Danych, stażystów, praktykantów i wolontariuszy, którzy wykonują zadania lub realizują obowiązki związane z przetwarzaniem danych osobowych w Szkole Podstawowej nr 1 w Porębie (dalej: ADO)

SPIS TREŚCI

1. Zasady bezpiecznego użytkowania sprzętu IT

1.1. Sprzęt IT służący do przetwarzania zbioru danych osobowych jest zasobem informatycznym rzeczywistym (sprzętowym) bądź wirtualnym. Zasób obejmuje serwery, komputery stacjonarne lub mobilne, wydzielone ich części (przestrzeń dyskowa, udział sieciowy), urządzenia peryferyjne i komunikacji elektronicznej (telefony komórkowe), informatyczne nośniki danych (dyskietki, dyski CD, DVD, Blu-ray, pamięci USB), drukarki.

1.2. Użytkownik zobowiązany jest korzystać ze sprzętu informatycznego w sposób zgodny z jego przeznaczeniem i chronić go przed jakimkolwiek zniszczeniem lub uszkodzeniem. W przypadku zaistnienia takiego zdarzenia niezwłocznie zgłasza ten fakt przełożonemu.

1.3. Samowolne otwieranie (demontaż) sprzętu IT, instalowanie bez zezwolenia przełożonego dodatkowych urządzeń lub podłączanie do zasobu informatycznego jakichkolwiek urządzeń o niepotwierdzonej legalności jest zabronione. Zabronione jest zdejmowanie plomb gwarancyjnych a także dokonywanie samowolnych zmian w konfiguracji sprzętowej.

1.4. W przypadku konieczności zabrania do naprawy sprzętu zawierającego na dyskach twardych informacje chronione, dane te muszą być przez ADO, Informatyka lub osobę wyznaczoną przez ADO lub firmę serwisową wymontowane pod nadzorem odpowiedzialnego pracownika i pozostawione u użytkownika (zamontowane ponownie po dokonanie naprawy). W przypadku uszkodzenia dysku twardego zawierającego informacje chronione w sposób uniemożliwiający ich odzyskanie dysk taki należy zniszczyć w sposób uniemożliwiający ponowne odczytanie. Sposób trwałego usunięcia danych uzgodnić z ADO, Informatykiem lub osobą wyznaczoną przez ADO. Odrębnego postępowania wymaga sytuacja, gdy dysk jest na gwarancji.

1.5. Zasady zabezpieczenia osobistego sprzętu komputerowego, danych oraz ich nośników (pen-drive, przenośny dysk twardy, dyskietki, taśmy, CD-ROM'y, karty pamięci itp.) przed dostępem osób niepowołanych do zasobów informacyjnych obejmują:

1.5.1. Wyłączenie albo wylogowanie się z używanych aktualnie systemów każdorazowo w sytuacji opuszczenia stanowiska pracy z komputerem (dla sprzętu PC zaleca się stosowanie aplikacji klasy save-screen (wygaszacz ekranu) z aktywną opcją „password" lub inne równoważne zabezpieczenie);

1.5.2. Zabezpieczenie tworzonych przez siebie danych (plików) na własnych komputerach, okresowe przeglądanie ich zawartości i usuwanie danych zbędnych. Dane uznane przez użytkownika za szczególnie chronione np. dane osobowe muszą być przechowywane miejscach określonych przez ADO a ponadto sposób ich zabezpieczenia uzgodnić należy każdorazowo z ADO, Informatykiem lub osobą wyznaczoną przez ADO.

1.5.3. Wykonywanie kopii bezpieczeństwa jest obowiązkiem użytkownika końcowego w przypadku tworzenia dokumentów w pamięci swojej stacji roboczej, poza zasobami sieciowymi udostępnionymi przez Administratora Danych, dla których wykonywane są kopie bezpieczeństwa centralnie przez uprawnionych pracowników;

1.5.4. Asystowanie przy prowadzonych pracach serwisowych przy sprzęcie za który odpowiedzialność ponosi pracownik;

1.5.5. Wnioskowanie (w ramach posiadanych kompetencji i zgodnie z uzgodnionymi i obowiązującymi w danym Projekcie procedurami) o dostęp do zasobów i usług dla przypadków rzeczywiście uzasadnionych (zasada „need to know" - minimum tego co konieczne);

1.5.6. Niezwłoczne informowanie ADO o zmianach lub odebraniu wcześniej wnioskowanych przez użytkownika uprawnień (dostęp do systemów, aplikacji, folderów...) w przypadku ustania przyczyn (zmiana stanowiska, komórki organizacyjnej, zakończenia pracy itp.);

1.5.7. Udostępnianie własnych zasobów (dzielenie (share) dysków komputerów własnych) w sieci jedynie w sytuacjach wyjątkowych i na czas możliwie najkrótszy tylko dla współpracowników w projekcie posiadających odpowiednie uprawnienia i upoważnienia, za zgodą

odpowiedniego kompetentnego przełożonego. Za ewentualne skutki wynikłe z takiej sytuacji odpowiedzialny jest użytkownik.

1.6. Korzystanie z wszelkiego rodzaju łącz i serwisów modemowych w czasie realizacji swoich obowiązków przy korzystaniu z bazy danych stanowiących informacje chronione, wymaga uzyskania zgody ADO. Użytkownik odpowiedzialny jest za wykorzystanie takich połączeń w sposób zgodny z otrzymanym pozwoleniem.

1.7. Użytkowanie mobilnych nośników informatycznych do przetwarzania danych osobowych możliwe jest za zgodą przełożonego. Takie nośniki jak laptop, smartfon, tablet czy pen-drive jest przypisany imiennie do użytkownika i podlega ewidencjonowaniu jeśli zawiera dane osobowe. Zaleca się, by dostęp do składowanych tam danych osobowych wymuszał podanie indywidualnego hasła, PIN-u lub innego kodu dostępu. Fakt używania przenośnych informatycznych nośników danych do przetwarzania danych osobowych, wymaga zgłoszenia do ADO, Informatyka lub osoby wyznaczonej przez ADO, która prowadzi centralną ewidencję takich nośników.

1.8. Pracownik użytkujący mobilny sprzęt informatyczny do wykonywania pracy na odległość (telepraca) przetwarzający dane osobowe, powinien posiadać zgodę kompetentnego przełożonego i na tej podstawie zgłosić zamiar wykonywania pracy zdalnej do ADO w celu zestawienia bezpiecznych kanałów do łączenia się z serwerem firmowym i bezpiecznego korzystania z zasobów firmowych. Użytkownik zachowuje szczególną ostrożność podczas transportu, przechowywania i użytkowania sprzętu IT poza obszarem bezpiecznego przetwarzania.

1.9. Do podstawowych zasad bezpiecznego użytkowania informatycznego sprzętu mobilnego (komputery przenośne, urządzenia PDA – palmtopy, smartfony itp.) należy:

1.9.1. Utrzymywanie w tajemnicy kodów PIN posiadanych kart SIM i kart tokenowych RSA;

1.9.2. Stosowanie przygotowanych przez ADO mechanizmów zabezpieczających klasy firewall, zabezpieczeń antywirusowych i szyfrowania zawartości dysków;

1.9.3. Stosowanie w uzgodnieniu z ADO, Informatykiem lub osobą wyznaczoną przez ADO dedykowanego mechanizmu ochrony danych chronionych, polegającego na synchronizacji katalogów na dyskach lokalnych z ich odpowiednikami na serwerach;

1.9.4. Przestrzeganie zakazu aktywowania modemów i kart transmisji danych GSM z jednoczesnym wpięciem do sieci komputerowej;

1.9.5. Zakaz udostępnienia sprzętu osobom postronnym;

1.9.6. Niezwłocznego poinformowania ADO, Informatyka lub osoby wyznaczonej przez ADO w przypadku zagubienia lub kradzieży komputera, palmtopu czy karty tokenowej.

1.10. Zabronione jest podejmowanie prób włamywania się lub omijania zabezpieczeń, instalacji i wykorzystywania oprogramowania penetracyjnego i skanującego. Zakaz obejmuje również instalację i wykorzystywanie urządzeń aktywnych, dostępu do innych sieci.

1.11. Zabronione jest przesyłanie za pośrednictwem sieci, danych niemających związku z wykonywanymi obowiązkami (w systemie poczty elektronicznej), powielania i przekazywania danych użytkownikom, których one nie dotyczą.

2. Zasady korzystania z oprogramowania

2.1. Używanie jedynie oprogramowania pochodzącego z legalnych źródeł i zgodnie z warunkami udzielonej licencji. (na podstawie ustawy z dnia 4 lutego 1994 roku o prawie autorskim i

prawach pokrewnych. Użytkownicy oprogramowania wykorzystują udostępnione im zasoby informatyczne jedynie do celów służbowych związanych z ich działalnością zawodową.

2.2. Instalowanie oprogramowania w zasobach informatycznych oraz wykonywanie kopii zapasowych oprogramowania może się odbywać na warunkach umowy licencyjnej oraz w zgodzie z przepisami ustawy o prawie autorskim i prawach pokrewnych.

2.3. Instalowanie lub używanie oprogramowania innego niż przekazanego bądź udostępnionego użytkownikom przez Administratora Danych, zwłaszcza prywatnie zakupionych dyskietek, płyt CD, programów ściąganych ze stron internetowych jak również odpowiadanie na samoczynnie pojawiające się reklamy internetowe jest zabronione.

2.4. Użytkownik nie ma prawa do powielania danych lub programów zainstalowanych w komputerze przez administratora oprogramowania (licencji) na swoje własne potrzeby ani na potrzeby osób trzecich.

2.5. Zabronione jest samowolne instalowanie oprogramowania i dokonywanie zmian w ustawieniach sieciowych komputera (np. zmiana nazwy czy przyznanego adresu IP, itp.). oraz aktywowanie modemów również tych stanowiących stały element konstrukcyjny urządzeń.

2.6. Wyznaczony Informatyk (również z firmy zewnętrznej) lub osoba wyznaczona przez ADO jest zobowiązana do prowadzenia okresowych kontroli legalności oprogramowania.

2.7. W przypadku podejmowania prób przełamywania lub omijania zabezpieczeń oprogramowania i sieci lub naruszenia któregokolwiek z powyższych postanowień, kierownik jednostki organizacyjnej ma prawo (bez uprzedzenia) zażądać usunięcia nielegalnie lub niewłaściwie zainstalowanego oprogramowania. Ponadto, niezależnie od odpowiedzialności dyscyplinarnej lub porządkowej może dochodzić naprawienia poniesionej szkody na podstawie kodeksu cywilnego.

3. Zasady korzystania z Internetu

3.1. Korzystanie z zasobów sieci Internet dozwolone jest jedynie w zakresie związanym z wykonywaniem obowiązków służbowych.

3.2. Wszystkie dane otrzymane poprzez Internet, w tym pocztą elektroniczną muszą być traktowane ze szczególną ostrożnością pod kątem obecności wirusów oraz ich autentyczności i prawdziwości.

3.3. Korzystanie z aplikacji, usług i serwisów oferowanych przez Internet niesie ryzyko łatwej identyfikacji użytkownika.

3.4. Przesyłanie danych (np. zestawień finansowych, danych osobowych, informacji stanowiących tajemnicę przedsiębiorstwa, strategii, projektów itp.), których przechwycenie może stanowić zagrożenie dla interesów lub prestiżu organizacji za pomocą zewnętrznej (internetowej) poczty elektronicznej bez specjalnych zabezpieczeń jest niedozwolone. Sposób zabezpieczeń (szyfrowanie) zostało opisane w pkt.4.

3.5. Przechowywanie danych i korzystanie z kont pocztowych na serwerach zewnętrznych (w tym darmowych) jest niedopuszczalne.

3.6. Pracodawca zastrzega sobie prawo do kontrolowania i monitorowania pracowników w zakresie sposobu korzystania przez nich z Internetu, w tym kontroli czasu spędzonego przez pracowników w Internecie oraz przestrzegania przez nich wyżej wymienionych zasad bezpieczeństwa.

3.7. Umieszczanie w Internecie informacji zawierających dane osobowe kierownictwa, pracowników, klientów, dostawców lub kontrahentów, wymaga zgody zarówno osoby fizycznej, której dane dotyczą, jak i kierownika jednostki organizacyjnej.

3.8. Pracodawca zastrzega sobie prawo do blokowania dostępu do niektórych portali, stron lub treści dostępnych za pośrednictwem Internetu bez uprzedzenia użytkowników.

4. Polityka haseł

4.1. Użytkownik sam definiuje hasło dostępu zarówno do systemu operacyjnego, jak również do systemów
i aplikacji w których są przetwarzane dane osobowe. Hasło musi składać się co najmniej z **8 znaków** (wielkich i małych liter oraz z cyfr lub znaków specjalnych). Użytkownik osobiście odpowiada za utrzymanie hasła w tajemnicy (zakaz ujawniania innym osobom).

4.2. Zmiana hasła następuje nie rzadziej, niż co **30 dni** oraz niezwłocznie w przypadku podejrzenia, że hasło mogło zostać ujawnione. Zmianę hasła może być wymuszana przez system IT. Jeśli system nie posiada takiej funkcji, to użytkownik jest zobowiązany do jego zmiany we własnym zakresie.

4.3. Należy unikać stosowania tego samego hasła w przypadku posiadania uprawnień do wielu zasobów, systemów lub aplikacji.

4.4. Użytkownik jest zobowiązany się do zachowania hasła w poufności, nawet po utracie przez nie ważności.

4.5. Zabronione jest pozostawianie haseł w formie jawnej w postaci, zbiorów (plików) tekstowych, nalepek na monitorach itp.

4.6. Hasła nie mogą być zbyt łatwe do odgadnięcia. W szczególności nie należy ich tworzyć z powszechnie używanych pojęć i znaczeń, jak np. daty, imiona, nazwiska, inicjały stanowisk, numery rejestracyjne samochodów, numery telefonów, itp.

4.7. W razie konieczności przekazania hasła w celach serwisowych (naprawy lub instalacji oprogramowania) dokonania jego zmiany niezwłocznie po zakończeniu takich prac.

4.8. Należy staranni wykonywać proces logowania (następujące po sobie błędne wprowadzenie hasła traktowane jest przez systemy jako próby włamania, skutkiem czego następuje czasowa lub całkowita blokada konta użytkownika – w takich przypadkach na żądanie administratora systemu użytkownik zobowiązany jest do złożenia dodatkowych wyjaśnień).

4.9. Aktywacja zablokowanych kont (zmiana hasła), zmiany udostępnień do folderów, serwisów drukarkowych itp. wymagają zgłoszenia tego faktu do ADO, Informatyka lub osoby wyznaczonej przez ADO

5. Zasady korzystania z poczty elektronicznej

5.1. System poczty elektronicznej (SPE) powinien być wykorzystywany do prowadzenia korespondencji służbowej, stąd listy elektroniczne wysyłane za pośrednictwem SPE traktowane są jako korespondencja służbowa konieczna do wykonywania zadań i obowiązków służbowych.

5.2. Użytkownicy mają prawo korzystać z SPE dla celów prywatnych wyłącznie okazjonalnie i powinno być to ograniczone do niezbędnego minimum.

5.3. Korzystanie z poczty elektronicznej dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez Użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych.

5.4. Użytkownicy nie mają prawa korzystać z poczty elektronicznej w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub nieetycznym i naruszającym cudzą godność i prywatność

5.5. Zabrania się dokonywanie w sieci zakupów, rezerwacji usług lub świadczeń na rzecz użytkownika oraz dokonywania bankowych z prywatnego konta.

5.6. Administrator Danych ma prawo do monitorowania SPE. W przypadku nieobecności pracownika oraz konieczności wglądu do korespondencji nieobecnego pracownika, celem ochrony prywatności pracownika ma zastosowanie wytyczna wyrażona w Załączniku nr 1 do Rozporządzenia Ministra Pracy i Polityki Socjalnej z dnia 1 grudnia 1998 r. w sprawie bezpieczeństwa i higieny pracy na stanowiskach wyposażonych w monitory ekranowe (pkt 10e).

5.7. Użytkownik bez zgody Pracodawcy nie ma prawa wysyłać wiadomości zawierających dane osobowe dotyczące Pracodawcy, jego pracowników, klientów, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej.

5.8. Wszelkie przesyłanie dokumentów, opracowań, jak i innych treści przesyłane przez użytkownika podlegają zasadom ochrony prawa autorskiego i prawa własności przemysłowej, które użytkownik jest obowiązany przestrzegać.

5.9. Niedozwolone jest przesyłanie wiadomości e-mail do więcej niż jednego adresata w taki sposób, że dla każdego z nich widoczne są, bądź będą adresy poczty elektronicznej pozostałych odbiorców, w szczególności gdy zawierają w swej treści dane osobowe klientów organizacji.
Przy wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW". Zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości".

5.10. Każdy użytkownik przed wysłaniem poczty jest zobowiązany sprawdzić poprawność adresu odbiorcy dokumentu.

5.11. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.

5.12. Nakazuje się okresowe czyszczenie poczty z nieaktualnych e- mali i opróżnianie kosza.

5.13. Zakazuje się wysyłania korespondencji służbowej na prywatne skrzynki pocztowe pracowników lub innych osób.

5.14. Użytkownicy nie powinni otwierać przesyłek e-mail i uruchamiać wykonywalnych załączników dołączonych do korespondencji elektronicznej nadesłanej od nieznanych sobie nadawców, których adres nie wskazuje na związek z wypełnianymi przez nich obowiązkami służbowymi. Zabrania się, bez weryfikacji wiarygodności nadawcy „klikać" na hiperlinki w mailach. Nieprzestrzeganie tej zasady może doprowadzić do zainfekowania komputera użytkownika i innych pracujących w sieci.

5.15. W przypadku przesyłania plików zawierających dane osobowe, użytkownik zobowiązany jest do ich spakowania i zabezpieczenia hasłem, tj. wykorzystywać mechanizmy kryptograficzne (hasłowanie wysyłanych dokumentów lub plików zzipowanych) . W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 8 znaków: duże i małe litery i

cyfry lub znaki specjalne a hasło należy przesłać odrębnym mailem lub inną metodą, np. telefonicznie lub SMS-em.

5.16. Dokumenty źródłowe zawierające dane osobowe sporządzone jednorazowo, przesyłane innym jednostkom/odbiorcom powinny być zniszczone po ich wykorzystaniu.

5.17. Wszystkie przypadki e-maili budzących podejrzenie należy zgłaszać administratorowi sieci/ informatykowi.

5.18. Skrzynki pocztowe osób, które przestają być pracownikami, stażystami, praktykantami lub współpracownikami, niezwłocznie podlegają procedurze ich zamykania.

6. Ochrona antywirusowa

6.1. Każdy system informatyczny musi być wyposażony w program antywirusowy oraz firewall, stanowiące kluczowy środek zabezpieczenia przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego. Takie same zabezpieczenia muszą być stosowane na urządzeniach mobilnych używanych służbowo.

6.2. Zabronione jest zgrywanie na dysk twardy komputera oraz uruchamianie nielegalnych programów i plików pobranych z niewiadomego źródła.

6.3. Użytkownicy zobowiązani są do skanowania plików wprowadzanych z zewnętrznych nośników programem antywirusowym zainstalowanym na danym komputerze.

6.4. Zakazane jest wyłączanie systemu antywirusowego podczas pracy systemu informatycznego przetwarzającego dane osobowe.

6.5. W przypadku stwierdzenia zainfekowania systemu, użytkownik obowiązany jest wyłączyć komputer z sieci, poinformować niezwłocznie o tym fakcie ADO.

6.6. Bieżące aktualizowanie systemu operacyjnego komputera, systemu antywirusowego oraz firewalli odbywa się pod nadzorem ADO, Informatyka (również z firmy zewnętrznej) lub osoby wyznaczonej przez ADO

6.7. W przypadku braku reakcji użytkownika i stwierdzenia przez administratora obecności wirusów, w trosce o bezpieczeństwo pracy pozostałych użytkowników, zablokowany zostanie dostęp do sieci, a za skutki wynikłe z takiej sytuacji odpowiedzialny będzie użytkownik.

7. Przestrzeganie zasad bezpieczeństwa podczas korzystania z elektronicznego sprzętu mobilnego (komputery przenośne, palmtopy, smartfony itp.)

7.1. Utrzymywanie w tajemnicy kodów PIN posiadanych kart SIM i kart tokenowych RSA,

7.2. Stosowanie przygotowanych przez Administratora systemu informatycznego mechanizmów zabezpieczających klasy firewall, zabezpieczeń antywirusowych i szyfrowania zawartości dysków,

7.3. Stosowanie, w uzgodnieniu z Administratorem systemu, mechanizmu ochrony danych, polegającego na synchronizacji katalogów na dyskach lokalnych z ich odpowiednikami na serwerach,

7.4. Zakaz aktywowania modemów i kart transmisji danych GSM i jednoczesnego wpięcia do sieci komputerowej,

7.5. Zakaz udostępnienia sprzętu osobom postronnym,

7.6. Niezwłocznego informowania ADO w przypadku zagubienia lub kradzieży komputera, palmtopu czy karty tokenowej.

8. Nadawanie upoważnień i uprawnień do przetwarzania danych osobowych

8.1. Za nadawanie i odwoływanie upoważnień do przetwarzania danych osobowych (dalej upoważnienie) odpowiada Administrator Danych Osobowych dalej ADO
8.2. Upoważnienia mogą być nadawane w postaci papierowej lub elektronicznej,
8.3. Upoważnienia nadawane są do poszczególnych zbiorów danych osobowych prowadzonych w formie papierowej i elektronicznej umieszczonych w wykazie (rejestrze czynności przetwarzania danych osobowych) prowadzonych przez ADO
8.4. ADO prowadzi w formie papierowej i elektronicznej centralną ewidencję osób upoważnionych do przetwarzania danych osobowych
8.5. Pracownik przetwarzający dane osobowe w formie papierowej oraz użytkownik systemu informatycznego używanego do przetwarzania danych osobowych przed nadaniem upoważnienia musi:
   a. zostać zaznajomiony z przepisami o ochronie danych osobowych oraz obowiązującymi w Firmie dokumentami takimi jak: polityka bezpieczeństwa danych osobowych i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
   b. podpisać stosowne oświadczenie o zachowaniu w poufności danych umieszczone na upoważnieniu.
8.6. W przypadku, gdy upoważnienie nadawane jest pracownikowi do procesu - zbioru w formie elektronicznej, ADO otwiera konto oraz przydziela uprawnienia oraz identyfikator w danym systemie. .
8.7. Zwolnienie z pracy lub zmiana stanowiska pracy związana ze zmianą dostępu do określonych procesów - zbiorów danych osobowych, wiąże się z koniecznością odwołania danego upoważnienia oraz zablokowania konta lub anulowania uprawnień w systemie.

9. Zasady rozpoczęcia, zawieszenia i zakończenia pracy

9.1. Użytkownik rozpoczyna pracę z systemem informatycznym przetwarzającym dane osobowe z użyciem identyfikatora i hasła,
9.2. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np. klientom, innym pracownikom) wgląd do danych wyświetlanych na monitorach komputerowych stosując zasadę czystego ekranu,
9.3. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu lub wylogować się z systemu,
9.4. Po zakończeniu pracy, użytkownik zobowiązany jest:
   a. wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy
   b. zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz elektroniczne nośniki danych, na których znajdują się dane osobowe.

10. Postępowanie z informatycznymi nośnikami zawierającymi dane osobowe

10.1. Informatyczne nośniki danych są mobilną częścią zasobów informatycznych Podmiotu. Są nimi głównie dyskietki, dyski CD-R, DVD, Blu-ray, rodzaje pamięci USB, które podlegają oznaczeniu i ewidencji,
10.2. ADO prowadzi rejestr elektronicznych nośników zawierających dane osobowe,
10.3. Posługiwanie się tego rodzaju nośnikami zawierającymi dane osobowe wymaga zgody ADO. Podobnie, jak w przypadku konieczności przetwarzania danych na odległość, przy użyciu komputera przenośnego zawierającego dane osobowe,
10.4. Użytkownicy tego typu nośników szyfrują część lub całość dysku urządzenia, kiedy transportują, przechowują i użytkują je poza obszarem przetwarzania.

10.5. W przypadku uszkodzenia lub zużycia nośnika zawierającego dane osobowe należy je przekazać do ADO celem dalszego procedowania.

11. Postępowanie z dokumentami papierowymi zawierającymi dane osobowe

11.1. Pracownicy upoważnieni do przetwarzania danych w formie tradycyjnej papierowej, odpowiadają za zabezpieczenie i ochronę danych osobowych przetwarzanych w kartotekach, skorowidzach, księgach czy wykazach,

11.2. Tego typu papierowe urządzenia ewidencyjne oraz sporządzone z nich wydruki chroni się przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, zmianą, utratą, uszkodzeniem lub zniszczeniem

11.3. Dokumenty i wydruki zawierające dane osobowe przechowuje się w zamykanych na klucz szafach kartotekowych, zamykanych regałach biurowych lub biurkach znajdujących się w zamykanych pomieszczeniach, stanowiących obszar przetwarzania danego zbioru,

11.4. Przetwarzający dane są zobowiązani do stosowania „polityki czystego biurka". Polega ona na bieżącym użytkowaniu dokumentów tylko niezbędnych do wykonania zadania, przechowywaniu dokumentów w zamykanych regałach, szafach i biurkach oraz stosowaniu zabezpieczeń przed kradzieżą lub wglądem osób nieupoważnionych w trakcie godzin pracy jak i po jej zakończeniu,

11.5. Użytkownicy zobowiązani są do niszczenia dokumentów i tymczasowych wydruków w niszczarkach niezwłocznie po ustaniu celu ich przetwarzania.

12. Zasady czystego biurka i zasada czystego pulpitu

12.1. Wszystkie dokumenty i ruchome nośniki danych (płyty CD, dyski przenośne, pamięć zewnętrzna itp.) nie są pozostawiane na biurku. W momencie, gdy przestają być używane – chowane są do szafek i biurek. W przypadku informacji wrażliwych / zastrzeżonych, zamykane są na klucz, a dane z nich usuwa się gdy stają się niepotrzebne.

12.2. Na biurku znajdują się jedynie dokumenty aktualnie wykorzystywane przez pracownika/personel.
W przypadku opuszczenia stanowiska pracy (wyjście do WC, na przerwę śniadaniową / obiadową, poza siedzibę) wszystkie dokumenty i ruchome nośniki danych oraz pieczęcie znajdują się w szafkach i szufladach. W przypadku informacji wrażliwych i zastrzeżonych, ruchome nośniki i pieczęcie, zamykane są na klucz.

12.3. Dyrektor lub pracownik wyznaczony przez Administratora Danych Osobowych przeprowadza po godzinach pracy okresowe przeglądy z zakresu stosowania postanowień czystego biurka i pulpitu oraz zabezpieczenia informacji wrażliwych/zastrzeżonych przed nieuprawnionym dostępem.

12.4. W odniesieniu do urządzeń przetwarzających informacje (komputer) stosuje się zasadę czystego pulpitu – nie prowadzi się zapisywania, tymczasowego zapisywania plików. Na pulpicie znajdują się tylko skróty do plików oraz katalogów.

12.5. Po odejściu od stanowiska pracy należy się wylogować (przełączenie użytkownika)

12.6. Dyrektor lub pracownik wyznaczony przez Administratora Danych Osobowych przeprowadza po godzinach pracy okresowe przeglądy z zakresu stosowania postanowień czystego pulpitu oraz wylogowania się z sieci w przypadku opuszczenia stanowiska pracy

13. Zapewnienie poufności danych osobowych

13.1. Przetwarzający dane osobowe zobowiązany jest do zachowania w tajemnicy danych osobowych, do których ma lub będzie miał dostęp w związku z wykonywaniem zadań służbowych lub zadań zleconych przez przełożonego,

13.2. Użytkownik zobowiązany jest do niewykorzystywania danych osobowych w celach pozasłużbowych bądź niezgodnych ze świadczoną pracą, o ile nie są one jawne,

13.3. Użytkownik zobowiązany jest do zachowania w tajemnicy sposobów zabezpieczenia danych osobowych, o ile nie są one jawne,

13.4. Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieuprawnionym do ich poznania.

14. Skrócona instrukcja postępowania w przypadku naruszenia ochrony danych osobowych

14.1. W przypadku, gdy stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci mogą wskazywać na naruszenie zabezpieczeń tych danych, każdy pracownik niezależnie do formy zatrudnienia przy przetwarzaniu danych osobowych, zobowiązany jest niezwłocznie powiadomić o tym ADO,

14.2. Administrator wprowadza procedurę postępowania w przypadku naruszenia ochrony danych, którą osoba upoważniona przez Administratora do przetwarzania danych osobowych powinna bezwzględnie przestrzegać.

14.3. Niektóre typowe sytuacje, które wskazują na możliwość zaistnienia incydentu:

- utrata lub przejęcie przez osoby nieuprawnione danych chronionych takich jak: dane osobowe pracowników, klientów, kontrahentów, danych powierzonych organizacji związanych z jej działalnością lub stanowiących tajemnicę przedsiębiorstwa;
- nieautoryzowany dostęp do informacji chronionych oraz ich modyfikacja;
- zagubienie lub zniszczenie informacji chronionej;
- ślady na drzwiach, oknach i szafach wskazujące na próbę włamania;
- dokumentacja jest niszczona bez użycia niszczarki;
- przebywanie osób bez nadzoru w budynku lub pomieszczeniach obszaru przetwarzania, zachowujących się podejrzanie, zwłaszcza jeśli nie towarzyszy im przedstawiciel – pracownik organizacji;
- otwarte drzwi do pomieszczeń, gdzie przechowywane są dokumenty, nieobecność pracownika na stanowisku pracy, gdy dokumenty są dostępne w zasięgu ręki, po zakończeniu pracy nie zamknięte szafy i nie wylogowany komputer;
- ustawienie monitorów komputerów pozwala na wgląd w ich zawartość przez osoby postronne;
- wynoszenie dokumentów zawierających dane osobowe w wersji papierowej lub elektronicznej na zewnątrz firmy bez upoważnienia przełożonego;
- próba skopiowania bazy danych (np. pracowników, klientów, kontrahentów) i przekazania ich podmiotowi nieuprawnionemu;
- ustne przekazywanie informacji mających znamiona informacji osobowych osobom nieuprawnionym;

- telefoniczne próby wyłudzenia danych osobowych;
- kradzież komputerów lub innych urządzeń stanowiących zasób informatyczny organizacji;
- maile zachęcające do ujawnienia identyfikatora i/lub hasła;
- pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów;
- hasła do systemów przyklejone są w post-it lub dostępne w innym miejscu w pobliżu komputera;
- logowanie się kilku pracowników do jednej stacji roboczej przy użyciu ogólnie dostępnego hasła.

15. Ciągłość działania

Zapewnienie ciągłości działania i ochrona procesów przed skutkami zdarzeń losowych i sytuacji kryzysowych.

15.1 Szkoła Podstawowa nr 1 w Porębie posiada Plan Ochrony ppoż. i ustalony sposób komunikacji na wypadek klęsk żywiołowych zalanie, pożar itp.;

15.2 W zakresie ciągłości funkcjonowania Jednostka wykonuje kopie zapasowe w wersji elektronicznej wszystkich istotnych danych dotyczących działalności Szkoły Podstawowej nr 1 w Porębie;

15.3 Archiwizowane dane elektroniczne przechowane są w szafie pancernej;

15.4 Dokumenty papierowe archiwizowane są w archiwum – nie wykonuje się kopii zapasowej tych dokumentów;

15.5 Pomieszczenie zabezpieczone jest odpowiednim zamkiem oraz systemem alarmowym i ppoż.,

15.6 Instrukcja ppoż. jest opracowywana i aktualizowana przez inspektora BHP, który odpowiedzialny jest za jej dostępność oraz przeszkolenie pracowników szkoły;

15.7 Instrukcje ppoż. przeglądane są pod kątem ich adekwatności i aktualności przez Inspektora BHP;

15.8 Dyrektor odpowiada za bezpieczeństwo pracy użytkowanych pomieszczeń i aktualną instrukcje ppoż., by była dostępna w miejscu jej stosowania oraz za organizację szkoleń pracowników w tym zakresie.

15.9 w przypadku utraty danych elektronicznych dane te są odtwarzane z kopii zapasowych;

15.10 Dyrektor odpowiada za organizację, wyznaczenie osób odpowiedzialnych za ewakuację z pomieszczeń szkoły dokumentów, danych i sprzętu w przypadku pożaru lub zalania użytkowanych pomieszczeń.

15.11 W przypadku stwierdzenia awarii łącza zapewniającego dostęp do Internetu, należy niezwłocznie skontaktować się z dostawca usługi i ustalić przyczynę awarii oraz uzyskać informacje o planowanym terminie przywrócenia poprawnego działania łącza;

15.12 w przypadku przerwa w dostawie zasilania prądu należy powiadomić Administratora Danych Osobowych o awarii, zlokalizować w miarę swoich możliwości powód wystąpienia awarii zgłosić fakt wystąpienia awarii do pogotowia energetycznego zamknięcia wszystkie maszyn i urządzania , wliczając oraz urządzenia sieciowe i telekomunikacyjne.

16. Postępowanie dyscyplinarne

16.1. W przypadku naruszeń zasad bezpieczeństwa w procesie przetwarzania danych osobowych pracownik ponosi odpowiedzialność porządkową, dyscyplinarną lub karną w

zależności od wagi naruszenia, z zastosowaniem właściwych przepisów prawa.

16.2. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub domniemania takiego naruszenia, nie podjęła działania określonego w niniejszym opracowaniu zasad, a w szczególności nie powiadomiła przełożonego , a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, mogą mieć zastosowanie przepisy odpowiedzialności porządkowej i materialnej.

.....

Podpis ADO

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

(data i podpis pracowników)