ZATWIERDZAM

Administrator Danych Osobowych

INSTRUKCJA

ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

SZKOŁA PODSTAWOWA NR 1 IM. STANISŁAWY ŁAKOMIK W CZELADZI

UL. REYMONTA 80

41-250 CZELADŹ

(IZSI)

Czeladź, 03.11.2023 r.

METRYKA DOKUMENTU

Nazwa	Szkoła Podstawowa nr 1 im. Stanisławy Łakomik w Czeladzi		
Tytuł dokumentu	Instrukcja Zarządzania Systemem Informatycznym w Szkole Podstawowej nr 1 im. Stanisławy Łakomik w Czeladzi, ul. Reymonta 80, 41-250 Czeladź (IZSI)		
System	System Ochrony Danych Osobowych		
Rodzaj	Dokument wykonawczy		
Zastosowanie	Pracownicy i współpracownicy		
Plik	*IZSI*		
Status	Dokument finalny	Liczba stron	55

HISTORIA ZMIAN

Wersja	Data wersji	Opis zmiany	Akcja	Rozdział	Autor	Zatwierdził

Spis treści

ROZDZIAŁ I.

POSTANOWIENIA OGÓLNE

1. Niniejsza Instrukcja jest dokumentem eksploatacyjnym regulującym zasady oraz procedury zarządzania i administrowania systemami informatycznymi służącymi do przetwarzania danych osobowych w Szkole Podstawowej nr 1 im. Stanisławy Łakomik w Czeladzi opisującym zasady zapewnienia bezpieczeństwa danych osobowych w systemach informatycznych.

   Instrukcja została opracowana na podstawie:

   1.1 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 (ogólne rozporządzenie o ochronie danych – dalej RODO)

   1.2 Ustawy z dnia 10 maja 2018 r o ochronie danych osobowych

   1.3 Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne

   1.4 Rozporządzenie rady ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych
   i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych

   1.5 Tak zwanych „dobrych praktyk” wynikających między innymi z przepisów i norm branżowych dotyczących bezpieczeństwa informacji.

   1.6 Wytycznych Normy PN ISO/IEC 27001

2. Instrukcja obejmuje swoim zakresem komórki organizacyjne w Szkole Podstawowej nr 1 im. Stanisławy Łakomik w Czeladzi, w tym pracowników na samodzielnych stanowiskach pracy, osoby biorące udział w procesie przetwarzania danych osobowych zarówno w systemach informatycznych, jak i w systemach tradycyjnych (papierowych) oraz usługobiorców realizujących zadania na rzecz Szkoły Podstawowej nr 1 im. Stanisławy Łakomik w Czeladzi wymagające dostępu do danych osobowych, których administratorem jest Szkoła Podstawowa nr 1 im. Stanisławy Łakomik w Czeladzi W szczególności instrukcja odnosi się do osób takich jak:

2.1 Inspektor Ochrony Danych, który w jego imieniu, realizuje obowiązki związane z ochroną danych osobowych;
2.2 Administrator Systemów Informatycznych (ASI) – jeśli został powołany lub Informatyk
2.3 Zarządzający poszczególnymi procesami przetwarzania danych osobowych dalej również zbiorami danych osobowych (osoby odpowiedzialne z racji zajmowanego stanowiska służbowego za przetwarzanie i bezpieczeństwo danych w podległych im procesie przetwarzania - zbiorze danych);
2.4 Osoby przetwarzające dane osobowe;
2.5 Inne osoby wskazane przez Administratora Danych Osobowych.

ROZDZIAŁ II.

DEFINICJE I SKRÓTY UŻYTE W INSTRUKCJI

W niniejszej Instrukcji następujące wyrażenia i określenia mają znaczenie zgodnie z podanymi poniżej definicjami:

1. **Administrator Danych Osobowych (ADO)** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych, o których mowa w art. 4 pkt.7 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 (ogólne rozporządzenie o ochronie danych – dalej RODO) - w tym przypadku ADO jest Szkoła Podstawowa nr 1 im. Stanisławy Łakomik w Czeladzi

2. **Inspektor ochrony danych (IOD)** – rozumie się przez to osobę, która w imieniu i z upoważnienia Administratora Danych zapewnia przestrzeganie przepisów o ochronie danych osobowych. Inspektor Ochrony Danych musi zostać powołany obligatoryjnie w Podmiocie, w przypadku o którym mowa w art. 37 ust.1 lit.a RODO.

3. **Administrator Systemów Informatycznych (ASI)** / **Informatyk** – osoba/osoby odpowiedzialna/e za funkcjonowanie systemów informatycznych oraz stosowanie technicznych i organizacyjnych środków ochrony przewidzianych w systemach informatycznych.

4. **Bezpieczeństwo informacji** – zachowanie poufności, integralności i dostępności informacji; dodatkowo, mogą być brane pod uwagę inne własności takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

5. **Dostępność danych** – właściwość danych polegająca na tym, że są one dostępne i mogą być wykorzystywane na żądanie w założonym czasie przez uprawniony podmiot.

6. **Hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

7. **Identyfikator użytkownika** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.

8. **Incydent bezpieczeństwa informacji** - pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń, które związane są z naruszeniem przyjętych zasad bezpieczeństwa i zagrażają bezpieczeństwu informacji, w tym danych osobowych.

9. **Instrukcja** – rozumie się przez to Instrukcję Zarządzania Systemem Informatycznym w Szkole Podstawowej nr 1 im. Stanisławy Łakomik w Czeladzi
10. **Integralność danych** – właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany**.**
11. **Poufność danych** – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom.
12. **Rozliczalność** – właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
13. **RODO** – Rozporządzenie 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
14. **Sieć LAN / WAN** – sieć lokalna / rozległa umożliwiająca połączenie systemów informatycznych u ADO przy wykorzystaniu specjalistycznych, dedykowanych urządzeń i sieci telekomunikacyjnych w rozumieniu ustawy z dnia 16 lipca 2004 r. Prawo Telekomunikacyjne
15. **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych
16. **Ustawa / UODO** – ustawa z dnia 10 maja 2018r. 2018 r. o ochronie danych osobowych .
17. **Uwierzytelnianie** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości użytkownika
18. **Zagrożenie –** potencjalna przyczyna niepożądanego incydentu, który może wywołać szkodę w systemie lub organizacji.

ROZDZIAŁ III.

POZIOMY BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH W SYSTEMACH INFORMATYCZNYCH

1. Szkoła Podstawowa nr 1 im. Stanisławy Łakomik w Czeladzi wprowadza trzy poziomy bezpieczeństwa przetwarzanych danych osobowych. To, jaki poziom zabezpieczenia należy stosować zależy od tego, czy w systemie informatycznym są przetwarzane dane „wrażliwe społecznie” (czyli dane osobowe o których mowa w art. 9 ust. 1 RODO, ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, dane o stanie zdrowia, kodzie genetycznym, nałogach, życiu seksualnym, oraz danych o których mowa w Art. 10 RODO dotyczących wyroków skazujących, oraz naruszeń prawa, oraz czy urządzenia systemu informatycznego, służącego do przetwarzania danych osobowych nie są połączone z siecią publiczną.

2. Zabezpieczenia na poziomie, co najmniej podstawowym należy stosować, gdy:

   2.1 W systemie informatycznym nie są przetwarzane dane osobowe „wrażliwe”;

   2.2 Żadne z urządzeń systemu informatycznego, służącego do przetwarzania danych osobowych nie jest połączone z siecią publiczną.

3. Zabezpieczenia na poziomie, co najmniej podwyższonym należy stosować, gdy:

   3.1 W systemie informatycznym są przetwarzane dane osobowe „wrażliwe społecznie”;

   3.2 Żadne z urządzeń systemu informatycznego, służącego do przetwarzania danych osobowych nie jest połączone z siecią publiczną.

4. Zabezpieczenia na poziomie, wysokim należy stosować, gdy:

   4.1 Przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, połączone jest z siecią publiczną.

5. W związku z faktem, że zadania Szkoły Podstawowej nr 1 im. Stanisławy Łakomik w Czeladzi powodują konieczność przetwarzania danych wrażliwych, oraz że dane osobowe przetwarzane są w systemach informatycznych podłączonych do sieci publicznej, w Podmiocie obowiązuje **wysoki poziom bezpieczeństwa systemów informatycznych**.

ROZDZIAŁ IV.

OPIS OGÓLNYCH WYMAGAŃ BEZPIECZEŃSTWA SYSTEMU INFORMATYCZNEGO, W KTÓRYM SĄ PRZETWARZANE DANE OSOBOWE I ZASTOSOWANYCH ROZWIĄZAŃ

1. Środki bezpieczeństwa na poziomie podstawowym:

   1.1 W systemach informatycznych służących do przetwarzania danych osobowych stosuje się mechanizmy kontroli dostępu do tych danych;

   1.2 W przypadku dostępu do danych przetwarzanych w systemie informatycznym, przez co najmniej dwie osoby zapewnia się, aby w systemie dla każdego użytkownika rejestrowany był oddzielny identyfikator;

   1.3 Dostęp do danych przetwarzanych w tym systemie jest możliwy tylko i wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia;

   1.4 W celu ochrony systemów informatycznych służących do przetwarzania danych osobowych przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemów zastosowano oprogramowanie antywirusowe, bieżąco aktualizowane;

   1.5 Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych osobowych nie może zostać przydzielony innej osobie;

   1.6 Dane osobowe przetwarzane w systemach informatycznych zabezpiecza się poprzez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych zgodnie z procedurą tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi służących do ich przetwarzania (Rozdział V, procedura D);

   1.7 Kopie zapasowe są przechowywane w miejscu zabezpieczającym je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem;

   1.8 Kopie zapasowe zbiorów danych osobowych oraz programów służących do ich przetwarzania usuwa się niezwłocznie po ustaniu ich użyteczności;

   1.9 Osoby użytkujące komputery przenośne stanowiące własność Szkoły Podstawowej nr 1 im. Stanisławy Łakomik w Czeladzi zawierające dane osobowe, zachowują szczególną ostrożność jego podczas transportu, przechowywania i użytkowania poza obszarem przetwarzania danych osobowych oraz stosują środki ochrony kryptograficznej wobec przetwarzanych danych osobowych. Osoby użytkujące komputery przenośne zobowiązane są przestrzegać Regulaminu użytkowania komputerów przenośnych, wprowadzonego przez ADO. ADO każdej osobie upoważnionej do pracy na komputerze przenośnym wydaje stosowne upoważnienie oraz prowadzi ewidencję osób upoważnionych do przetwarzania danych za pomocą komputerów przenośnych;

1.10 Urządzenia, dyski lub inne elektroniczne nośniki informacji stanowiące własność Szkoły Podstawowej nr 1 im. Stanisławy Łakomik w Czeladzi, zawierające dane osobowe, przeznaczone do likwidacji pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;

1.11 Urządzenia, dyski lub inne elektroniczne nośniki informacji stanowiące własność Podmiotu, zawierające dane osobowe, przeznaczone do przekazania podmiotowi nieuprawnionemu do przetwarzania danych pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;

1.12 Urządzenia, dyski lub inne elektroniczne nośniki informacji stanowiące własność Podmiotu, zawierające dane osobowe, przeznaczone do naprawy pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych. W przypadku konieczności przeprowadzenia naprawy poza siedzibą Podmiotu, oraz bez możliwości sprawowania nadzoru przez osobę upoważnioną przez ADO, z podmiotem świadczącym usługi serwisowe zawierana jest umowa powierzenia przetwarzania danych zgodnie z art.28 ust.3 RODO .

2. Środki bezpieczeństwa na poziomie podwyższonym.

   Na poziomie podwyższonym obowiązują również środki bezpieczeństwa na poziomie podstawowym, o ile zasady na poziomie podwyższonym nie stanowią inaczej.

   2.1 Hasła użytkowników wykorzystywane do uwierzytelniania składają się, z co najmniej 8 znaków, zawierają małe i wielkie litery oraz cyfry lub znaki specjalne, a ich zmiana następują nie rzadziej, niż co 30 dni;

   2.2 Urządzenia i nośniki zawierające dane osobowe, przekazywane poza obszar przetwarzania danych osobowych, zabezpiecza się w sposób zapewniający poufność i integralność tych danych.

3. Środki bezpieczeństwa na poziomie wysokim. Obowiązujące środki bezpieczeństwa dotyczące poziomu wysokiego obejmują swym zakresem również systemy poziomu podstawowego i podwyższonego.

   3.1 Systemy informatyczne służące do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej z wykorzystaniem wysokiej klasy ścian ogniowych (ang. firewall)

   3.2 Wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane za pomocą sieci publicznej stosuje się środki kryptograficznej ochrony (między innymi poprzez wykorzystanie protokołu szyfrującego SSL);

4. Zastosowane środki ochrony danych w ramach infrastruktury technicznej oraz narzędzi programowych i baz danych.

4.1 Rozmieszczenie urządzeń teleinformatycznych (komputery, drukarki) uniemożliwia osobom niepowołanym dostęp do nich;

4.2 Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelniania z wykorzystaniem identyfikatora i hasła;

4.3 Zastosowano systemowe mechanizmy wymuszające okresową zmianę hasła dostępu do systemów informatycznych w przypadku kiedy taka funkcjonalność w rozwiązaniach konfiguracyjnych systemu występuje, w innym przypadku użytkownik systemów informatycznych zobowiązany jest samodzielnie kontrolować terminowość zmiany hasła;

4.4 Zainstalowano wygaszacze ekranów na stanowiskach powodujące zablokowanie systemów, na których są przetwarzane dane osobowe po 5 min. bezczynności ;

4.5 W przypadki korzystania z serwerów bazodanowych/komputerów centralnych zostały one zabezpieczone centralnym urządzeniem UPS;

4.6 Konta administracyjne w systemach przetwarzających dane osobowe zostały zabezpieczone minimum 8-znakowym hasłem. Dostęp do tych kont posiada ASI – jeśli został powołany, lub wyznaczony przez ADO informatyk ;

4.7 ADO przechowuje metrykę haseł dostępowych na poziomie administratora do wszystkich systemów informatycznych oraz urządzeń aktywnych sieci informatycznej w miejscu niedostępnym dla osób nieupoważnionych. Metryki haseł przechowywane są w sejfie lub innym zabezpieczonym miejscu w zamkniętej kopercie. Dostęp do Metryki haseł posiada wyłącznie ADO i ASI/Informatyk administrujący systemami, oraz w uzasadnionych przypadkach Inspektor Ochrony Danych

4.8 ADO jeśli posiada takie możliwości organizacyjno-techniczne, dąży aby kluczowe systemy służące do przetwarzania danych osobowych posiadały architekturę klient-serwer, przez co możliwe jest lepsze zabezpieczenie danych. Serwer decyduje, kto ma prawo do odczytywania, kopiowania i zmiany danych. W przypadku braku serwera, każdy z użytkowników posiada lokalnie skonfigurowany komputer w sposób umożliwiający prawidłowe katalogowanie danych przetwarzanych w systemach informatycznych .

ROZDZIAŁ V.

PROCEDURY BEZPIECZNEJ EKSPLOATACJI SYSTEMÓW INFORMATYCZNYCH PRZETWARZAJĄCYCH DANE OSOBOWE

A. PROCEDURA NADAWANIA UPOWAŻNIEŃ DO PRZETWARZANIA DANYCH i REJESTROWANIA TYCH UPOWAŻNIEŃ w SYSTEMIE INFORMATYCZNYM ORAZ WSKAZANIE OSOBY ODPOWIEDZIALNEJ ZA TE CZYNNOŚCI

1. Odpowiedzialność

1.1 Za wykonanie czynności zawartych w niniejszej procedurze odpowiadają Administrator Danych Osobowych (ADO), Administrator Systemów Informatycznych (ASI) jeśli został powołany lub wyznaczony Informatyk, kierownicy komórek organizacyjnych jeśli funkcjonują w strukturze organizacyjnej Podmiotu, oraz pracownicy na samodzielnych stanowiskach pracy.

1.2 Czynności administracyjne i formalne związane z nadawaniem, zmianą lub odebraniem upoważnień do pracy w systemach informatycznych oraz ich zakres realizuje Administrator Danych Osobowych (ADO). Za prawidłowe nadanie uprawnień w systemie odpowiada Administrator Systemów Informatycznych (ASI) jeśli został powołany lub wyznaczony przez ADO Informatyk.–

1.3 Nadzór nad właściwą i terminową realizacją postanowień niniejszej procedury pełni Administrator Danych Osobowych (ADO).

2. Zasady bezpieczeństwa

Niniejsza procedura spełnia następujące zasady bezpieczeństwa w systemach informatycznych Szkoły Podstawowej nr 1 im. Stanisławy Łakomik w Czeladzi:

2.1 Dostęp do systemów informatycznych posiadają jedynie pracownicy, którym nadano w sposób formalny upoważnienia.

2.2 Zakres nadanych uprawnień użytkownikom do korzystania z systemów informatycznych uwidoczniony w nadanym upoważnieniu, opiera się o zasadę „wiedzy koniecznej” i zasadę „minimalnych uprawnień”. Użytkownik ma dostęp tylko do tych systemów informatycznych, które są mu potrzebne do realizacji zadań.

2.3 Za określenie uprawnień do poszczególnych systemów informatycznych odpowiedzialni są zarządzający danym procesem – ADO lub inna wyznaczona przez ADO osoba, definiując typy użytkowników w oparciu o zakresy obowiązków podległych pracowników.

2.4 Formalne nadawanie, zmiana i odbieranie upoważnień użytkownikom do systemów informatycznych leży w gestii Administratora Danych Osobowych (ADO)

3. **Opis postępowania**

3.1 Podstawowe zasady nadawania uprawnień w systemie:

a. Przed dopuszczeniem do pracy przy przetwarzaniu danych osobowych każdy pracownik Szkoły Podstawowej nr 1 im. Stanisławy Łakomik w Czeladzi, z którego zakresu obowiązków i uprawnień wynika konieczność przetwarzania danych osobowych, powinien zostać zapoznany przez Inspektora Ochrony Danych (IOD) lub bezpośredniego przełożonego, lub też inną osobę wyznaczoną przez Administratora Danych Osobowych (ADO), z przepisami dotyczącymi ochrony danych osobowych.

b. Administrator Danych Osobowych (ADO) włącza do indywidualnych zakresów obowiązków służbowych każdego pracownika zatrudnionego przy przetwarzaniu danych osobowych obowiązek ochrony danych osobowych oraz odpowiedzialności za nieuzasadnioną ich modyfikację lub zniszczenie bądź nielegalne ujawnienie lub pozyskanie.

3.2 Sposoby nadawania upoważnień:

a. Administrator Danych Osobowych nadaje upoważnienia do każdego programu w systemie informatycznym, do którego pracownik ma uzyskać dostęp. Wzór nadania upoważnienia stanowi **załącznik nr 1** do niniejszej procedury.

b. Zakres uprawnień w systemach informatycznych nadawany jest na poziomie „użytkownik". Nie jest dopuszczalne nadanie uprawnień na poziomie „Administratora" w przypadku kiedy osoba upoważniona nie pełni funkcji ASI / Informatyka, chyba że poziom „Administratora" w danym systemie jest niezbędny, aby możliwe było prawidłowe wykonanie czynności powierzonych pracownikowi. Zakres uprawnień w systemie odzwierciedlać powinien zakres czynności na danym stanowisku pracy i wynikać z opisu stanowiskowego pracownika, znajdującego się w teczce akt osobowych pracownika.

c. Administrator Danych Osobowych, przy wsparciu ASI/Informatyka okresowo weryfikuje zasadność nadanych upoważnień i w zależności od dokonanych ustaleń podejmuje decyzję o pozostawieniu lub modyfikacji zakresu wydanego upoważnienia do pracy w systemach

d. W celu nadania upoważnienia / modyfikacji / odbioru uprawnień do pracy w systemach informatycznych osoba wyznaczona przez Administratora Danych Osobowych kieruje odpowiednio wypełniony wniosek o założenie kont i nadanie uprawnień dla użytkownika w systemie informatycznym (**załącznik nr 2** do niniejszej procedury) do Administratora Systemów Informatycznych jeśli został powołany lub wyznaczonego informatyka,

który nadaje uprawnienia w systemach informatycznych zgodnie z otrzymaną dyspozycją.

e. Przed nadaniem upoważnienia Administrator Danych Osobowych (ADO) lub osoba przez niego wyznaczona informuje o terminie szkolenia z zakresu bezpieczeństwa informacji i ochrony danych osobowych.

Szkolenie może odbywać się w formie stacjonarnej, zdalnej lub e-learningowej.

f. ASI jeśli został powołany lub informatyk weryfikują czy nie doszło do przyznania zbyt szerokich uprawnień w stosunku do realizowanych przez pracownika zadań, zwłaszcza, jeżeli w związku z tym doszło do incydentu/naruszenia bezpieczeństwa danych osobowych.

g. Zakres nadanych pracownikowi uprawnień w ramach upoważnienia, może ulegać zmianie (rozszerzeniu bądź zawężeniu) w związku z pełnieniem przez niego zadań w określonym przedziale czasu. W takim przypadku tryb wskazany do nadawania uprawnień określony w pkt. 3.2 a-f niniejszej procedury jest właściwy również w razie zmiany zakresu uprawnień pracownika.

h. Utrata prawa do przetwarzania w programach określonych w upoważnieniu następuje w szczególności w przypadku: zmiany stanowiska pracy w Szkole Podstawowej nr 1 im. Stanisławy Łakomik w Czeladzi, na którym nie ma konieczności posiadania dostępu do systemów informatycznych lub w szczególności, gdy:

- ustaje zasadność i celowość dalszego wykonywania prawa do przetwarzania w systemach informatycznych w związku ze zmianą realizowanych przez pracownika zadań wynikających z jego indywidualnego zakresu czynności;
- rozwiązania stosunku pracy.

i. W przypadkach określonych w pkt. 3.2 h Administrator Danych Osobowych niezwłocznie cofa upoważnienia w systemie informatycznym, do którego miał dostęp pracownik na formularzu Upoważnienie (**Załącznik nr 1** do niniejszej procedury).

j. W przypadku założenia nowego konta użytkownika w systemie, Administrator Systemów Informatycznych, jeśli został powołany lub informatyk wyznaczony przez ADO dodatkowo powiadamia użytkownika o identyfikatorze przydzielonego konta i haśle początkowym, bądź innej stosowanej formie uwierzytelniania użytkownika w systemie informatycznym.

k. ADO przed nadaniem/ modyfikacją uprawnień dokonuje:

- sprawdzenia, czy przyznawany poziom dostępu nie zagraża obowiązującej zasadzie podziału obowiązków polegającej na

niełączeniu działań wykonawczych z funkcjami kontrolnymi i decyzyjnymi w celu zapobiegania nadużyciom uprawnień;

- szczególnie wnikliwej weryfikacji podlegają przyznawane uprawnienia dotyczące tworzenia oraz dostępu do kont uprzywilejowanych związanych z realizacją przywilejów administracyjnych w systemie informatycznym, dających nieograniczone lub duże uprawnienia dostępu, w stosunku do tego systemu.

l. W przypadku utraty przez użytkownika upoważnienia do przetwarzania danych osobowych (np. rozwiązanie stosunku pracy, nie obsługiwanie systemu z powodu zmiany stanowiska pracy) Administratora Danych Osobowych niezwłocznie odbiera upoważnienia do przetwarzania danych osobowych zgodnie z **załącznikiem nr 1** do niniejszej procedury tak aby nie było możliwe wykonanie przez tego pracownika jakichkolwiek operacji które mogłyby przyczynić się do ingerencji w zakres przetwarzanych w systemach informacji.

m. W przypadku zmiany upoważnienia do przetwarzania danych osobowych (np. zmiana stanowiska pracy wiążąca się ze zmianą dostępu do procesów - zbiorów oraz systemów) czynności związane z tą zmianą odbywają się w takim samym zakresie jak przy odbiorze upoważnienia.

n. W przypadku wycofania użytkownikowi uprawnień do przetwarzania danych osobowych zawartych w zbiorze danych lub dostępu do systemu informatycznego przetwarzającego te dane, konto użytkownika nie podlega usunięciu z systemu, ale skutecznemu zablokowaniu przez Administratora Systemów Informatycznych jeśli został powołany lub przez Informatyka wyznaczonego przez ADO.

o. Proces okresowego sprawdzania uprawnień logicznego dostępu użytkowników do zasobów systemu informatycznego realizowany jest bezpośrednio przez Administratora Systemów Informatycznych jeśli został powołany, lub przez Informatyka wyznaczonego przez ADO bądź przy jego udziale i odbywa się na wyłączne polecenie wydane przez Administratora Danych Osobowych (ADO), w związku z prowadzeniem sprawdzeń kontrolnych dostępu do danego zbioru danych osobowych w systemie informatycznym.

4. Spis załączników

4.1 Wzór formularza nadania/modyfikacji uprawnień dla użytkownika do systemu informatycznego w Szkole Podstawowej nr 1 im. Stanisławy Łakomik w Czeladzi

4.2 wniosek o założenie kont i nadanie uprawnień dla użytkownika w systemie informatycznym

ZAŁĄCZNIK NR 1

Upoważnienie

Administrator: **Szkoła Podstawowa nr 1 im. Stanisławy Łakomik w Czeladzi, ul. Reymonta 80, 41-250 Czeladź**

Nazwiska i imię pracownika: ……..
Stanowisko: ……

Nazwa konta mailowego: ……..

Identyfikator użytkownika w aplikacjach:

a) …… **…**
nazwa aplikacji (bazy danych) identyfikator

b) …… **…**
nazwa aplikacji (bazy danych) identyfikator

c) …… **…**
nazwa aplikacji (bazy danych) identyfikator

d) …… **…**
nazwa aplikacji (bazy danych) identyfikator

e) …… **…**
nazwa aplikacji (bazy danych) identyfikator

Uwagi .....

.....

.....

Data nadania upoważnienia w systemach: **……**

Data wyrejestrowania z systemów: .....

Czasowe ograniczenia dostępu: od ..... do .....

.....
Podpis ASI

Potwierdzam otrzymanie uprawnień.

……..
data i podpis użytkownika

ZAŁĄCZNIK NR 2

Wniosek o założenie kont i nadanie uprawnień dla użytkownika w systemie informatycznym

Imię i nazwisko użytkownika **……..**	**Dział/Stanowisko** **……..** **……..**
Rodzaj umowy (na czas określony lub na czas nieokreślony)- jeśli umowa zawarta na czas określony proszę podać dokładną datę zakończenia umowy	Rodzaj umowy …….. Data zakończenia umowy ……..

☐ Nadanie uprawnień	☐ Odebranie uprawnień
Data wniosku: **……..**	Data wniosku: ……

1. Konto dostępu do stacji roboczej ☐ TAK ☐ NIE
2. Konto pocztowe ☐ TAK ☐ NIE
3. Aplikacje

APLIKACJE/PROGRAMY	MODYFIKCJA	DATA

4. Czasowe zawieszenie użytkownika **od …… do……..**

……

data i podpis wnioskodawcy

B. PROCEDURA ZARZĄDZANIA I UŻYTKOWANIA METODAMI I ŚRODKAMI UWIERZYTELNIENIA

1. **Zakres obowiązywania**

Procedura obowiązuje wszystkich użytkowników przetwarzających dane osobowe w Szkole Podstawowej nr 1 im. Stanisławy Łakomik w Czeladzi

Odpowiedzialność

1.1 Osoba wyznaczona przez ADO lub Administrator Systemów Informatycznych / jeśli został powołany lub Informatyk jest odpowiedzialny za zarządzanie hasłami.

1.2 Osoba odpowiedzialna za realizację zadań nadzoruje proces zarządzania hasłami i za przestrzeganie przez użytkowników zasad bezpieczeństwa przy posługiwaniu się hasłami.

1.3 Użytkownicy systemu informatycznego są odpowiedzialni za terminowe zmienianie haseł oraz za przestrzeganie zasad bezpieczeństwa przy stosowaniu haseł.

2. **Zasady bezpieczeństwa**

2.1 Wszystkie osoby posiadające dostęp do danych osobowych w szczególności przetwarzanych w systemach informatycznych są zobowiązane do uwierzytelniania się (logowania) do tych systemów przy użyciu identyfikatora i hasła.

2.2 Szczegółowe wymagania dotyczące budowy oraz ochrony haseł:

a. Bezpośredni dostęp do danych przetwarzanych w systemie informatycznym może mieć miejsce tylko po podaniu przez użytkownika swego identyfikatora oraz właściwego hasła do dostępu do zasobów;

b. Hasła użytkownika są poufne – użytkownikowi nie wolno przekazywać własnego hasła innym osobom;

c. Identyfikator oraz pierwsze hasło użytkownika nadaje użytkownikowi Administrator Systemów Informatycznych lub informatyk wyznaczony przez ADO, lub inna osoba upoważniona przez ADO.

2.3 Identyfikator użytkownika nie może być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego nie może być przydzielony innej osobie.

2.4 ASI jeśli został powołany lub Informatyk wyznaczony przez ADO wyrejestrowuje użytkownika z systemu informatycznego i unieważnia jego identyfikator bądź podejmuje inne stosowne czynności mające na celu uniemożliwienie dalszego

dostępu do systemu i jego zasobów użytkownikowi, który utracił uprawnienia do dostępu.

2.5 Hasło użytkownika składa się, co najmniej z 8 znaków, przy czym zawiera duże i małe litery, cyfry lub znaki specjalne. Hasło nie może kojarzyć się w łatwy sposób z innymi danymi pracownika.

2.6 Użytkownik zmienia je nie rzadziej niż co 30 dni.

2.7 Hasło stanowiące element uwierzytelniający użytkownika powinno być przechowywane w sposób bezpieczny i wprowadzane w sposób uniemożliwiający osobom trzecim poznanie jego treści. Jeśli zachodzi jakiekolwiek podejrzenie, że hasło zostało ujawnione, należy bezzwłocznie dokonać jego zmiany i powiadomić o zdarzeniu ADO lub ASI / Informatyka.

3. **Zasady zarządzania kontami i uprawnieniami**

3.1 Zarządzanie przywilejami odbywa się zgodnie z zasadą minimalnych uprawnień. Jedynie ASI jeśli został powołany lub informatyk wyznaczony przez ADO jest upoważniony do posiadania kont uprzywilejowanych – administracyjnych. Konta użytkowników o częściowo rozszerzonych przywilejach na komputerach stacjonarnych oraz komputerach przenośnych mogą być utworzone wyłącznie, jeżeli jest to konieczne do wykonywania zadań wynikających z zakresu obowiązków danego pracownika.

3.2 Pozostałym użytkownikom należy przydzielać konta z ograniczonymi uprawnieniami.

C. PROCEDURA ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY PRZEZ UŻYTKOWNIKÓW SYSTEMU

1. **Zakres obowiązywania**

Procedura obowiązuje wszystkich użytkowników przetwarzających dane osobowe w Szkole Podstawowej nr 1 im. Stanisławy Łakomik w Czeladzi oraz Administratora Systemów Informatycznych (ASI) jeśli został powołany lub informatyka wyznaczonego przez ADO.

2. **Odpowiedzialność**

2.1 Za wykonanie czynności zawartych w niniejszej procedurze odpowiadają użytkownicy oraz Administrator Systemów Informatycznych (ASI) jeśli został powołany lub informatyk wyznaczony przez ADO.

2.2 Nadzór nad właściwą i terminową realizacją postanowień niniejszej procedury pełni Administrator Systemów Informatycznych (ASI) jeśli został powołany lub informatyk wyznaczony przez ADO, który w jego imieniu, realizuje obowiązki w tym zakresie wobec wszystkich pracowników mających dostęp do danych osobowych.

3. **Zasady bezpieczeństwa**

3.1 Przed rozpoczęciem pracy użytkownik zobowiązany jest sprawdzić czy urządzenie komputerowe nie nosi śladów uszkodzeń lub ingerencji osób trzecich. W przypadku stwierdzenia nieprawidłowości użytkownik zgłasza wystąpienie incydentu bezpieczeństwa.

3.2 Logowanie do systemu powinno być przeprowadzone w sposób zapewniający poufność wprowadzanego hasła użytkownika (tj. uniemożliwić jego podejrzenie etc.). W przypadku domniemania, że hasło utraciło atrybut poufności należy niezwłocznie powiadomić o tym fakcie ADO.

3.3 Zawieszenie pracy:

a. W momencie pozostawiania komputera bez nadzoru lub opuszczaniu pomieszczania biurowego, w którym jest komputer, osoba za niego odpowiedzialna zobowiązana jest do zablokowania urządzenia komputerowego (naciśnięcie klawiszy „Windows + L" lub „CTRL + ALT + Delete", a następnie ENTER – w systemach operacyjnych Microsoft Windows);

b. Wymaga się stosowania wygaszacza ekranu chronionego hasłem, który aktywuje się po czasie bezczynności nie dłuższym niż 5 minut.

c. Po poprawnym zakończeniu pracy w systemie informatycznym, użytkownik ma obowiązek wylogować się z systemu oraz upewnić się, że urządzenie komputerowe zostało wyłączone.

3.4 Wszystkie zasoby informatyczne – sprzęt, oprogramowanie i usługi informatyczne, wykorzystywane są w celach służbowych i nie mogą być używane w celach prywatnych.

3.5 Urządzenie komputerowe (stacja robocza, urządzenia peryferyjne) przydzielane jest użytkownikowi wyłącznie:

a. W celach związanych z realizacją zadań o charakterze służbowym.

b. W zakresie przyznanych uprawnień.

3.6 Korzystając ze sprzętu komputerowego, użytkownik musi przestrzegać ograniczeń, mających na celu:

a. Zapewnienie zgodności sprzętu i oprogramowania ze standardami dotyczącymi sprzętu komputerowego i dopuszczonego oprogramowania.

b. Zapewnienie legalności zainstalowanego oprogramowania i sprzętu wchodzącego w skład urządzenia komputerowego.

c. Zapewnienie właściwej ochrony informacjom przetwarzanym na urządzeniu komputerowym.

d. Ograniczenie dostępu do oprogramowania zainstalowanego na komputerze.

3.7 Użytkownikom korzystającym z urządzeń komputerowych zabrania się:

a. Używania modemów na stanowiskach komputerowych podłączonych do sieci LAN, bez pisemnego zezwolenia ADO.

b. Używania modemów podczas korzystania z sieci LAN. Urządzenia te powinny być wtedy wyłączone lub zablokowane.

c. Udostępniania osobom trzecim haseł oraz szczegółów technicznych dotyczących konfiguracji posiadanych usług (np. dane konfiguracyjne zdalnego dostępu).

d. Samodzielnego uruchamiania, instalowania i usuwania jakiegokolwiek dodatkowego oprogramowania bez zgody Administratora.

e. Samodzielnej instalacji, wymiany i usuwania jakichkolwiek komponentów oraz wyposażenia urządzenia komputerowego (napędy i nagrywarki CD i DVD, dodatkowe dyski twarde, rozszerzenia pamięci operacyjnej, itp.) bez zgody Administratora.

f. Samodzielnego uruchamiania urządzenia komputerowego z nośników zewnętrznych (karty pamięci, pendrive, CD-ROM, DVD-ROM, HDD itp.).

g. Przechowywania danych osobowych na prywatnych komputerach lub prywatnych przenośnych nośnikach informacji.

h. Instalowania lub używania prywatnego sprzętu na terenie Jednostki za wyjątkiem prywatnych telefonów komórkowych, odtwarzaczy mp3 i smartfonów, z zastrzeżeniem, że wykorzystywane urządzenia prywatne nie mogą być podłączane do urządzeń i sieci Jednostki. Zakazuje się także przenoszenia pomiędzy nimi danych (np. na kartach pamięci).

i. Modyfikowania logów i plików systemowych.

j. Dokonywania prób obejścia zabezpieczeń narzucanych przez systemy informatyczne.

D. PROCEDURA TWORZENIA KOPII ZAPASOWYCH ZBIORÓW DANYCH ORAZ PROGRAMÓW I NARZĘDZI SŁUŻĄCYCH DO ICH PRZETWARZANIA

1. Zakres obowiązywania

Procedura ma zastosowanie do systemów informatycznych Szkoły Podstawowej nr 1 im. Stanisławy Łakomik w Czeladzi, w których przetwarzane są dane osobowe, wymagające zabezpieczenia atrybutu dostępności w wymaganym czasie.

2. Odpowiedzialność

2.1 Za przestrzeganie zasad wymienionych w niniejszej procedurze odpowiada Administrator Systemów Informatycznych / Informatyk wyznaczony przez ADO.

2.2 Za nadzór nad realizacją zasad wymienionych w niniejszej procedurze odpowiada ADO lub IOD.

3. Zasady bezpieczeństwa

3.1 Dla wszystkich systemów informatycznych wykorzystywanych w działalności Podmiotu, w których są przetwarzane dane osobowe Administrator Systemów Informatycznych/ Informatyk jest zobowiązany do opracowania, przyjęcia i stosowania harmonogramu wykonywania kopii zapasowych i planu wykonywania kopii zapasowych. Harmonogram oraz plan powinny zostać stworzone w formie pisemnej i przechowywane w bezpiecznym miejscu. Harmonogram i plan powinny być zgodne lub zbliżone do wzorów zamieszczonych w załączniku nr 1 oraz w załączniku nr 2 do niniejszej procedury.

3.2 Za przestrzeganie przyjętego planu wykonywania kopii zapasowych odpowiada Administrator Systemów Informatycznych, lub informatyk wyznaczony przez ADO lub też inna osoba wyznaczona do realizacji tego zadania.

3.3 ASI jeśli został powołany lub informatyk wyznaczony przez ADO lub też osoba wyznaczona do tego zadania są zobowiązani do wykonywania oraz przechowywania kopii zapasowych konfiguracji urządzeń sieciowych.

3.4 ASI lub osoba wyznaczona zobowiązani są do prowadzenia dokumentacji z wykonywanych kopii na nośnik wydzielony z infrastruktury sieciowej (zewnętrzny), która powinna zawierać, co najmniej:

a. Datę i godzinę rozpoczęcia wykonywania kopii zapasowej.

b. Jednoznaczne oznaczenie nośnika, na którym została wykonana kopia.

c. Dane osoby wykonującej kopię oraz jej podpis

3.5 Fakt wykonania kopii zapasowej należy odnotować w dzienniku kopii zapasowych (załącznik nr 3 do niniejszej procedury).

3.6 Dopuszcza się prowadzenie dokumentacji w formie elektronicznej (np. w aplikacji służącej do wykonywania backupów).

3.7 Na ASI lub informatyku wyznaczonym przez ADO spoczywa obowiązek okresowego weryfikowania poprawności wykonania kopii zapasowej. W przypadku niepoprawnego zapisu kopii zapasowej obowiązkowo sprawdzany jest stan techniczny nośnika, na którym zapisywana jest kopia oraz ponownie przeprowadzany proces wykonywania kopii zapasowej na nieuszkodzonym nośniku.

3.8 ASI lub informatyk wyznaczony przez ADO ma obowiązek okresowo przeprowadzać operację testowego odzyskiwania z kopii zapasowych losowo wybranych danych w celu weryfikacji możliwości odzyskania danych. Podczas odtwarzania danych należy odnotować zakres przywracanych danych, identyfikator nośnika, z którego przywracano dane oraz wynik testu.

3.9 Nośniki informacji należy przechowywać w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem (np. szafy pancerne, szafy ogniotrwałe, sejf, zamykane szafy o ustalonym jako najwyższy stopień bezpieczeństwa).

3.10 Dopuszcza się możliwość przechowywania dodatkowych kopii zapasowych w obszarze przetwarzania danych (np. serwerowniach), gdy konieczność ich utworzenia i przechowywania wynika z zastosowanych narzędzi i metod archiwizacji, pod warunkiem zastosowania zabezpieczeń technicznych, uniemożliwiających dostęp do danych osobom nieuprawnionym, oraz pod warunkiem sporządzenia dodatkowej kopii danych przechowywanej na nośniku zewnętrznym w innym bezpiecznym pomieszczeniu, oddalonym od docelowego miejsca przetwarzania danych (np. serwera)

3.11 W przypadku transportowania nośników z kopiami zapasowymi poza obszar Jednostki, należy zapewnić bezpieczne warunki transportu poprzez:

a. Zapewnienie poufności danych przez zaszyfrowanie informacji na nośniku.

b. Przewożenie kopii bezpieczeństwa w postaci niezaszyfrowanej wyłącznie w obecności dwóch pracowników Jednostki.

c. Nie pozostawianie kopii zapasowych bez nadzoru.

d. Umieszczanie nośników w bezpiecznych pojemnikach zabezpieczających je przed zniszczeniem lub skopiowaniem.

3.12 Nośniki kopii zapasowych, które zawierają nieaktualne dane, są uszkodzone lub nie można ich ponownie wykorzystać, muszą być niezwłocznie zniszczone przez ASI lub osobę wyznaczoną przez ADO w sposób uniemożliwiający odtworzenie zapisanych na nich danych.

ZAŁĄCZNIK NR 1

HARMONOGRAM WYKONYWANIA KOPII ZAPASOWYCH

Nazwa systemu informatycznego	Typ bazy danych	Lokalizacja	Metody i narzędzia tworzenia kopii zapasowych	Częstotliwość tworzenia kopii zapasowych	Nośniki kopii zapasowych	Miejsce przechowywania kopii zapasowych
			Automatycznie	*Codziennie od poniedziałku do piątku*	*Dysk serwera/ Dysk zewnętrzny*	
			Ręcznie	*Raz w tygodniu*	*Płyta CD-R/DVD/ Dysk zewnętrzny*	

ZAŁĄCZNIK NR 2

WZÓR PLANU KOPII ZAPASOWYCH

1. Odpowiedzialność za wykonywanie kopii zapasowych.

Za wykonywanie kopii zapasowych odpowiedzialny jest każdy pracownik upoważniony do przetwarzania danych osobowych we własnym zakresie.

2. Rodzaje wykonywanych kopii zapasowych.

W Szkole Podstawowej nr 1 im. Stanisławy Łakomik w Czeladzi wykonuje się pełne kopie systemów informatycznych, oraz dokumentów wytworzonych przez użytkowników.

3. Częstotliwość wykonywania kopii zapasowych.

Kopie zapasowe dokumentów wytworzonych przez użytkowników wykonują użytkownicy we własnym zakresie raz w miesiącu lub w każdym przypadku gdy wprowadzone dane do systemu tego wymagają.

4. Weryfikowanie kopii zapasowych.

Próbne odtworzenie kopii zapasowej i sprawdzanie poprawności odtworzonych danych realizowane jest raz na pół roku.

5. Przechowywanie kopii zapasowych.

Kopie wykonywane w Szkole Podstawowej nr 1 im. Stanisławy Łakomik w Czeladzi przechowywane są w pomieszczeniu Sekretariatu w szafie pancernej.

Wykonał	Zatwierdził
Data	Data
Podpis	Podpis

ZAŁĄCZNIK NR 3

DZIENNIK KOPII ZAPASOWYCH

Lp.	Data i godzina	Opis nośnika	Osoba wykonująca	Podpis osoby wykonującej	Uwagi

E. PROCEDURA WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMÓW ORAZ NOŚNIKÓW INFORMACJI SŁUŻĄCYCH DO PRZETWARZANIA DANYCH

1. **Zakres obowiązywania**

Procedura ma zastosowanie w całym systemie informacyjnym Szkoły Podstawowej nr 1 im. Stanisławy Łakomik w Czeladzi, szczególnie w sytuacjach:

1.1 Konieczności udostepnienia systemu, sprzętu, nośników służących do przetwarzania danych osobowych podmiotom zewnętrznym celem wykonania na nim przeglądu, czynności serwisowych, wykonywania przeglądów i konserwacji na podstawie zawartej umowy.

1.2 Obowiązku przekazania systemu, sprzętu, nośników służących do przetwarzania danych osobowych, na podstawie przepisów prawa podmiotom uprawnionym w wymaganym zakresie (policja, prokuratura, sądy, inne uprawnione urzędy państwowe).

1.3 Wspólnej realizacji projektów wymagających przekazania danych osobowych, których Administratorem jest Szkoła Podstawowa nr 1 im. Stanisławy Łakomik w Czeladzi podmiotowi zewnętrznemu na podstawie umowy o zachowaniu poufności.

2. **Odpowiedzialność**

2.1 Zgodę na przekazywanie systemu, sprzętu, nośników służących do przetwarzania danych osobowych podmiotowi zewnętrznemu w zakresie określonym przepisami prawa lub umową wydaje Dyrektor Szkoły Podstawowej nr 1 im. Stanisławy Łakomik w Czeladzi

2.2 Administrator Danych Osobowych (ADO), określa środki bezpieczeństwa wymagane przy współpracy z podmiotami zewnętrznymi oraz ogólny nadzór nad ich przestrzeganiem.

2.3 Administrator Systemów Informatycznych (ASI) / informatyk lub inny pracownik wyznaczony przez ADO odpowiadają za zapewnienie kontrolowanego dostępu pracowników serwisu do danych osobowych oraz za prowadzenie działań serwisowych mających na celu niedopuszczenie do awarii, jak również szybkie przywrócenie działania infrastruktury informatycznej po zaistniałej awarii lub usterce.

2.4 Pracownicy Szkoły Podstawowej nr 1 im. Stanisławy Łakomik w Czeladzi zaangażowani do bezpośredniej współpracy z podmiotami zewnętrznymi odpowiadają za zachowanie wymaganych środków bezpieczeństwa oraz zgodną z zapisami umów współpracę z przedstawicielami tych podmiotów.

3. **Zasady bezpieczeństwa**

3.1 Podmiot zewnętrzny realizujący zadania na rzecz Jednostki winien być zobowiązany umową o poufności do zachowania w tajemnicy informacji pozyskiwanych w czasie realizacji swoich zadań, chyba że zawarta została przez ADO z danym podmiotem zewnętrznym pisemna umowa powierzenia przetwarzania danych osobowych.

3.2 Zaleca się, aby podmiot zewnętrzny świadczący usługi na rzecz Jednostki posiadał wdrożony system ochrony informacji, którego skuteczność może być potwierdzona odpowiednim certyfikatem branżowym, bądź też stosowną pisemną deklaracją o posiadaniu przez podmiot zewnętrzny odpowiedniego systemu ochrony danych .

3.3 Pracownicy podmiotu zewnętrznego powinni zostać zobowiązani do zachowania w poufności pozyskanych w trakcie realizacji projektu informacji na określony czas ich ochrony oraz winni być poinformowani pisemnie o karach wynikających z przepisów prawa za nieuprawnione ich ujawnienie.

3.4 Administratora Danych Osobowych (ADO), wraz z ASI / Informatykiem określa zakres dostępu do danych osobowych i innych informacji chronionych niezbędny do udostępnienia pracownikom podmiotu zewnętrznego w ramach realizacji prac serwisowych, przeglądów i konserwacji lub wspólnej realizacji projektu. Zakres ten powinien zostać określony w zapisach umowy (o współpracy, o poufności, umowie serwisowej).

4. **Opis postępowania**

4.1 Konserwacja i serwisowanie urządzeń ma na celu zapewnienie nieprzerwanej i bezpiecznej pracy systemów, zapobieganie utratom, uszkodzeniom lub innym naruszeniom bezpieczeństwa informacji.

4.2 Sprzęt podlega konserwacji zgodnie z ustalonym harmonogramem, wynikającym z zaleceń producentów.

4.3 W przypadku, gdy na nośnikach stanowiących integralną część sprzętu przekazywanego do naprawy, znajdują się dane osobowe, ASI/ Informatyk lub użytkownik ma obowiązek zgłosić ten fakt przy przekazywaniu urządzenia do serwisu. Sprzęt taki naprawiany jest pod nadzorem osoby wyznaczonej przez ADO. Jeżeli zaś taki nadzór nie jest możliwy, to informacje te muszą być uprzednio skutecznie usunięte, przy zapewnieniu możliwości ich późniejszego odtworzenia, bądź, jeśli istnieje możliwość wymontowania nośnika danych (np. dysku twardego z komputera, serwera), urządzenie należy przekazać do naprawy po uprzednim wymontowaniu nośnika.

4.4 Sprzęt przekazywany do naprawy poza siedzibę Jednostki powinien być transportowany w sposób minimalizujący ryzyko kradzieży, uszkodzenia, zniszczenia lub kompromitacji danych na nim zapisanych.

4.5 Przeglądy, konserwacje i serwis sprzętu wymagające zaangażowania firm zewnętrznych powinny być wykonywane pod nadzorem Administratora Systemu Informatycznego jeśli został powołany lub informatyka wyznaczonego przez ADO lub też upoważnionego przedstawiciela Szkoły Podstawowej nr 1 im. Stanisławy Łakomik w Czeladzi. Niedopuszczalny jest samodzielny serwis urządzenia komputerowego lub jego rozmontowywanie przez użytkownika.

ROZDZIAŁ VI.

SPOSÓB, MIEJSCE I OKRES PRZECHOWYWANIA ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI, KOPII ZAPASOWYCH I WYDRUKÓW

A. ELEKTRONICZNE NOŚNIKI INFORMACJI

1. **Zakres obowiązywania**

Procedura obowiązuje wszystkich użytkowników wykorzystujących elektroniczne nośniki informacji do przetwarzania danych osobowych w Szkole Podstawowej nr 1 im. Stanisławy Łakomik w Czeladzi

Odpowiedzialność

1.1 Za wykonanie czynności zawartych w niniejszej procedurze odpowiadają użytkownicy oraz Administrator Systemów Informatycznych (ASI) lub informatyk wyznaczony przez ADO

1.2 Nadzór nad właściwą i terminową realizacją postanowień niniejszej procedury pełni ADO lub osoba wyznaczona przez Administratora Danych Osobowych (ADO), która w jego imieniu, realizuje niniejsze obowiązki

2. **Zasady postępowania**

2.1 Elektroniczne nośniki informacji służące do przetwarzania danych osobowych są przechowywane w pomieszczeniach stanowiących obszar przetwarzania danych osobowych.

2.2 Elektroniczne nośniki informacji zawierające dane osobowe można przekazywać tylko podmiotom lub osobom uprawnionym na podstawie przepisów prawa, za zgodą ADO lub IOD lub osoby wyznaczonej przez Administratora Danych Osobowych (ADO), do podejmowania decyzji w tym zakresie.

2.3 Nośniki danych są przechowywane w sposób uniemożliwiający dostęp do nich osób nieupoważnionych, jak również zabezpieczający je przed zagrożeniami środowiskowymi (zalanie, pożar, wpływ pól elektromagnetycznych).

2.4 Wymaga się, aby dane osobowe znajdujące się na nośnikach przenośnych, wynoszonych poza obszar przetwarzania danych osobowych były szyfrowane.

2.5 Wszelkie zbędne nośniki – uszkodzone, zawierające niepotrzebne lub przeterminowane dane, których nie da się usunąć i ponownie wykorzystać nośnika – są fizycznie i trwale zniszczone w sposób uniemożliwiający odczytanie zapisanych na nich danych.

2.6 Niszczenia elektronicznych nośników informacji dokonuje ASI jeśli został powołany lub informatyk wyznaczony przez ADO, w związku, z czym użytkownik jest zobowiązany przekazać mu zbędny dysk twardy, przenośny dysk zewnętrzny, płytę CD-R, pendrive z backupem.

2.7 Zniszczenia dokonuje się komisyjnie, z udziałem przynajmniej 2 pracowników Jednostki.

2.8 Każdy przypadek zniszczenia jakiegokolwiek rodzaju nośnika podlega zaprotokołowaniu. Protokół (załącznik nr 1) zawiera skład komisji, rodzaj i numer niszczonego przedmiotu, datę, godzinę i sposób jego zniszczenia, a także podpisy wszystkich członków komisji. Protokół przechowywany jest przez Administratora Systemów Informatycznych jeśli został powołany, informatyka wyznaczonego przez ADO, lub inną osobę wyznaczoną przez Administratora Danych Osobowych (ADO), która w jego imieniu, realizuje obowiązki w tym zakresie.

2.9 W celu skutecznego zniszczenia nośnika można skorzystać z usług specjalistycznej Jednostki zewnętrznej. Odbywa się to zgodnie z zasadami określonymi w umowie z usługodawcą i potwierdzane jest odpowiednim dokumentem stwierdzającym fakt zniszczenia nośnika, wydawanym przez firmę zewnętrzną. Umowa z taką firmą musi zawierać odpowiednie klauzule bezpieczeństwa, zapewniające poufność pracowników.

2.10 Wszelki sprzęt zbywany, przekazywany podmiotowi zewnętrznemu do naprawy lub likwidacji zostaje pozbawiony nośników informacji, zgodnie z umową podpisywaną z dostawcą.

B. KOPIE ZAPASOWE

1. **Zakres obowiązywania**

   Procedura obowiązuje Administratora Systemów Informatycznych wykonującego kopie zapasowe.

2. **Odpowiedzialność**

   2.1 Za wykonanie czynności zawartych w niniejszej procedurze odpowiada Administrator Systemów Informatycznych (ASI) lub osoba wyznaczona przez ADO.

   2.2 Nadzór nad właściwą i terminową realizacją postanowień niniejszej procedury pełni osoba wyznaczona przez Administratora Danych Osobowych (ADO), która w jego imieniu, realizuje obowiązki związane z ochroną danych osobowych.

3. **Zasady postępowania**

   3.1 Nośniki informacji należy przechowywać w miejscach i urządzeniach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem (np. szafy pancerne, szafy ogniotrwałe, szafy metalowe na akta).

   3.2 Dopuszcza się możliwość przechowywania dodatkowych kopii zapasowych w obszarze przetwarzania danych (np. serwerowni), gdy konieczność ich utworzenia i przechowywania wynika z zastosowanych narzędzi i metod archiwizacji, pod warunkiem zastosowania zabezpieczeń technicznych, uniemożliwiających dostęp do danych osobom nieuprawnionym, oraz pod warunkiem sporządzenia dodatkowej kopii danych przechowywanej na nośniku zewnętrznym w innym bezpiecznym pomieszczeniu, oddalonym od docelowego miejsca przetwarzania danych (np. serwera)

   3.3 W przypadku transportowania nośników z kopiami zapasowymi poza obszar Jednostki, należy zapewnić bezpieczne warunki transportu poprzez:

   a. Zapewnienie poufności danych poprzez zaszyfrowanie informacji na nośniku.

   b. Przewożenie kopii bezpieczeństwa w postaci niezaszyfrowanej wyłącznie w obecności dwóch pracowników Jednostki.

   c. Nie pozostawianie kopii zapasowych bez nadzoru.

   d. Umieszczanie nośników w bezpiecznych pojemnikach zabezpieczających je przed zniszczeniem lub skopiowaniem.

C. WYDRUKI

1. **Zakres obowiązywania**

Procedura obowiązuje wszystkich użytkowników mających dostęp do wydruków, dokumentów zawierające dane osobowe w Szkole Podstawowej nr 1 im. Stanisławy Łakomik w Czeladzi

Odpowiedzialność

1.1 Za wykonanie czynności zawartych w niniejszej procedurze odpowiadają: ASI/Informatyk, zarządzający zbiorami oraz pracownicy upoważnieni do przetwarzania danych osobowych, mający dostęp do danych osobowych w formie tradycyjnej.

1.2 Nadzór nad właściwą i terminową realizacją postanowień niniejszej procedury pełni Administrator Danych Osobowych (ADO), lub osoba przez ADO wyznaczona do realizacji tego zadania.

2. **Zakres postępowania**

2.1 Wydruki/dokumenty (umowy, decyzje, faktury, pisma, orzeczenia itp.), zawierające dane osobowe, przechowuje się w pokojach stanowiących obszar przetwarzania danych osobowych, określony przez ADO w odrębnym dokumencie.

2.2 Wydruki/dokumenty, zawierające dane osobowe, należy niszczyć przez pocięcie w niszczarce. Niszczarki są dostępne dla wszystkich użytkowników przetwarzających dane osobowe.

2.3 Za bezpieczeństwo danych osobowych zapisanych w formie papierowej odpowiedzialne są osoby je przetwarzające oraz bezpośrednio zarządzający zbiorami danych osobowych.

ZAŁĄCZNIK NR 1

PROTOKÓŁ USUNIĘCIA DANYCH / ZNISZCZENIA NOŚNIKA DANYCH PRZECHOWUJĄCEGO DANE OSOBOWE

Szkoła Podstawowa nr 1 im. Stanisławy Łakomik w Czeladzi		Data (DD-MM-RRRR):	
PROTOKÓŁ USUNIĘCIA DANYCH / ZNISZCZENIA NOŚNIKA DANYCH PRZECHOWUJĄCEGO DANE OSOBOWE Niniejszym stwierdza się trwałe zniszczenie nośnika danych:			
Rodzaj:			
Typ:			
Model:			
Numer seryjny:			
Wykonujący:			
Imię i nazwisko:		Podpis:	
Zatwierdzający:			
Imię i nazwisko:		Podpis:	
Zatwierdzający:			
Imię i nazwisko:		Podpis:	

ROZDZIAŁ VII.

SPOSÓB ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO PRZED ZŁOŚLIWYM OPROGRAMOWANIEM I NIEAUTORYZOWANYM DOSTĘPEM

A. OCHRONA PRZED ZŁOŚLIWYM OPROGRAMOWANIEM

1. Za złośliwe oprogramowanie, którego celem jest nieuprawniony dostęp i zniszczenia w systemach informatycznych, uważa się:
   1.1 Wirusy, konie trojańskie, robaki internetowe;
   1.2 Programy mające na celu nieautoryzowane zdobycie, modyfikację lub destrukcję danych komputerowych;
   1.3 Programy umożliwiające zdobycie lub podniesienie uprawnień w systemach komputerowych;
   1.4 Programy, które mogą wpłynąć niekorzystnie na pracę systemów komputerowych poprzez utrudnienie lub sparaliżowanie ich pracy;
   1.5 Inne, które może spowodować destabilizację działania i fałszowanie danych.
2. Ochrona przed złośliwym oprogramowaniem jest realizowana poprzez zapobieganie, wykrywanie i usuwanie tego typu programów oraz uświadamianie użytkowników w zakresie zasad bezpiecznego korzystania z zasobów systemów informatycznych oraz bieżących zagrożeń występujących w sieci zewnętrznej.
3. W Szkole Podstawowej nr 1 im. Stanisławy Łakomik w Czeladzi wdrożono system ochrony antywirusowej na komputerach użytkowników oraz na serwerze (jeśli podmiot posiada serwer) . O ile jest to możliwe technicznie, wszystkie aktywa informatyczne objęte są ochroną przed złośliwym oprogramowaniem w czasie rzeczywistym, w sposób umożliwiający automatyzację wszystkich niezbędnych czynności, w tym np. umożliwiający automatyczne aktualizowanie baz wirusów dla oprogramowania antywirusowego.
4. Jednostka prowadzi edukację użytkowników w zakresie ochrony przed szkodliwym oprogramowaniem. W przypadku pojawienia się nowych zagrożeń związanych z działalnością złośliwego oprogramowania Administrator Systemów Informatycznych lub Informatyk wyznaczony przez ADO w miarę możliwości wysyła komunikaty do pracowników lub informuje ich osobiście.
5. W przypadku, gdy stacje robocze oraz serwery (jeśli występując w Podmiocie) nie są objęte ochroną w czasie rzeczywistym, ASI lub Informatyk wyznaczony przez ADO co najmniej raz w tygodniu dokonuje rutynowej kontroli pod kątem obecności złośliwego oprogramowania.

6. Za zarządzanie aplikacjami zabezpieczającymi przed złośliwym oprogramowaniem (w tym antywirusowym, filtrami i zaporami sieciowymi) odpowiada ASI / Informatyk lub osoba wyznaczona przez ADO.

7. Po każdej naprawie i konserwacji urządzenia, a przed ponownym włączeniem do sieci Jednostki, zawartość stałych nośników komputerowych jest sprawdzana za pomocą aktualnego oprogramowania antywirusowego zawierającego najnowsze bazy sygnatur.

8. W przypadku oznak zainfekowania komputera złośliwym oprogramowaniem należy:

   8.1 Powiadomić osobę odpowiedzialną za profilaktykę antywirusową w danym dziale (Administrator Systemów Informatycznych lub informatyk wyznaczony przez ADO);

   8.2 Odłączyć komputer od Internetu;

   8.3 Jeśli komputer podłączony jest do sieci lokalnej, należy ją odłączyć;

   8.4 Jeśli nie można uruchomić komputera z dysku twardego (błąd przy starcie), należy spróbować uruchomić system w trybie awaryjnym lub przy użyciu dysku startowego systemu Windows;

   8.5 Wykonać pełne skanowanie systemu.

9. W przypadku wykrycia infekcji należy z wykorzystaniem zainstalowanej aplikacji antywirusowej usunąć złośliwe oprogramowanie.

10. Wszystkie zdarzenia typu zdiagnozowanie i usunięcie złośliwego oprogramowania są regularnie raportowane do ADO i IOD lub innej osoby wyznaczonej przez Administratora Danych Osobowych (ADO), która w jego imieniu, realizuje obowiązki w tym zakresie.

11. W przypadku uszkodzenia danych lub oprogramowania należy przywrócić sprawność systemu wykorzystując kopie zapasowe.

B. OCHRONA PRZED NIEAUTORYZOWANYM DOSTĘPEM DO SIECI LOKALNEJ

1. Systemy informatyczne służące do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej z wykorzystaniem firewalla wbudowanego w router, który realizuje następujące zadania:

   a. Bazująca na politykach kontrola dostępu na podstawie aplikacji, kategorii aplikacji, podkategorii, technologii, czynnika ryzyka lub charakterystyki;
   b. Filtrowanie danych;
   c. Filtrowanie URL;
   d. Strumieniowa ochrona przed wirusami, oprogramowaniem spyware oraz robakami.

ROZDZIAŁ VIII. PO
NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. **Postanowienia ogólne**

1.1 Celem procedury jest zapewnienie szybkiej, skutecznej i uporządkowanej reakcji na incydenty związane z bezpieczeństwem informacji, w szczególności awarii i przeciążeń systemów informatycznych, utraty urządzeń lub danych, błędów ludzkich skutkujących zagrożeniem dla bezpieczeństwa środowiska teleinformatycznego, naruszeń lub prób naruszeń zabezpieczeń czy niekontrolowanych zmian w systemach.

1.2 Za podejmowanie działań wyjaśniających, korygujących, zaradczych oraz zbieranie materiałów dowodowych, odpowiedzialne jest kierownictwo Jednostki, przy wsparciu Inspektora Danych Osobowych (IOD), który realizuje obowiązki związane z ochroną danych osobowych.

1.3 Procedura zapewnia jak najszybsze raportowanie wszelkich symptomów świadczących lub mogących świadczyć o naruszeniu bezpieczeństwa informacji, w celu jak najszybszej reakcji na te zdarzenia i podjęcie działań zaradczych.

2. Opis postępowania – zgłaszanie incydentów / zagrożeń

2.1 Każdy pracownik Jednostki, oraz osoby świadczące usługi na rzecz Jednostki zobowiązane są do niezwłocznego zgłaszania wszelkich incydentów, oraz możliwości zaistnienia incydentów, bez zbędnej zwłoki, bezpośrednio do osób odpowiedzialnych za bezpieczeństwo teleinformatyczne i fizyczne Jednostki.

2.2 Pracownicy Jednostki i osoby świadczące usługi na rzecz Jednostki, zobowiązani są do powstrzymania się od kontynuowania jakiejkolwiek czynności mogącej spowodować zatarcie śladów bądź dowodów naruszenia bezpieczeństwa informacji, oraz niepodejmowania żadnych kroków własnych, w celu zaradzenia incydentowi – aż do czasu reakcji przedstawiciela Jednostki zewnętrznej wykonującego obsługę informatyczną na zaistniałe zdarzenia/incydenty naruszające bezpieczeństwo informacji.

2.3 Zgłaszanie incydentów oraz możliwości zaistnienia incydentów, odbywa się w formie pisemnej (poprzez wypełnienie formularza zgłoszenia incydentu stanowiącego załącznik nr 1 do niniejszej procedury), telefonicznej lub za pośrednictwem poczty elektronicznej. W przypadku zgłoszenia dokonanego telefonicznie, pracownik Jednostki lub pracownik usługodawcy zewnętrznego, zobowiązany jest niezwłocznie po dokonaniu zgłoszenia w formie telefonicznej, wypełnić i przesłać do ADO formularz zgłoszenia incydentu bezpieczeństwa.

2.4 O zaistnieniu incydentu/zagrożenia lub możliwości wystąpienia incydentu bezpieczeństwa informacji mogą świadczyć:

a. Utrata usługi, urządzenia lub funkcjonalności,

b. Przeciążenie lub niepoprawne działanie systemu,
c. Błędy ludzkie,
d. Niezgodność z politykami lub zaleceniami,
e. Naruszenia ustaleń związanych z bezpieczeństwem fizycznym,
f. Niepoprawne działanie oprogramowania lub sprzętu,
g. Naruszenie dostępu.

Ponadto szczegółowy wykaz potencjalnych zagrożeń dla bezpieczeństwa informacji został wykazany w załączniku nr 2 do niniejszej Rozdziału.

2.5 Za odbieranie zgłoszeń incydentów oraz rozpoznawanie ich i reakcję na zaistnienie incydentu/zagrożenia bezpieczeństwa (w tym zbieranie materiałów dowodowych) odpowiedzialny jest IOD, który powinien otrzymać raport z podjętych działań i zebranych materiałów dowodowych.

2.6 W celu umożliwienia podejmowania działań zapobiegawczych w odniesieniu do identyfikowanych problemów, zaprowadza się rejestr incydentów naruszenia bezpieczeństwa środowiska teleinformatycznego, który stanowi załącznik nr 2 do niniejszej procedury, w którym to rejestrze należy odnotowywać wszelkie incydenty bezpieczeństwa wraz z podjętymi działaniami zaradczymi.

2.7 ASI lub wyznaczony przez ADO informatyk lub inny pracownik wyznaczony przez ADO tworząc dla IOD raport z zaistnienia incydentu oraz zbierając materiał dowodowy, w szczególności bierze pod uwagę:

a. Przyczyny incydentu,
b. Zasięg naruszenia,
c. Działania naprawcze w celu uniknięcia ponownego wystąpienia incydentu,
d. Sposób komunikacji z podmiotami dotkniętymi incydentem i zaangażowanymi w jego usunięcie.

2.8 Wszelkie działania zaradcze podejmowane po zaistnieniu incydentu, leżą w gestii jedynie ASI lub informatyka wyznaczonego przez ADO, która dokonuje szczegółowej dokumentacji każdego działania.

3. Wyciąganie wniosków z incydentów/zagrożeń związanych z bezpieczeństwem informacji oraz gromadzenie materiału dowodowego.

3.1 Incydenty występujące w ramach działalności Jednostki, oraz związane z wykonywaniem usług na rzecz Jednostki, przez podmioty zewnętrzne, należy odnotowywać w rejestrze naruszeń/incydentów, który stanowi część integralną **Załącznika J** do Wewnętrznej Polityki Bezpieczeństwa Danych osobowych.

3.2 Regularnie, przynajmniej raz za kwartał ASI lub osoba wyznaczona przez ADO zobowiązana jest do przeprowadzenia na podstawie rejestru incydentów, analizę zaistniałych incydentów, biorąc pod uwagę:

a. Określenie liczby incydentów,
b. Określenie incydentów powtarzających się,
c. Określenie trendów związanych z incydentami bezpieczeństwa,
d. Określenie kosztów (straty oraz nakłady finansowe), związanych z incydentami bezpieczeństwa.

3.4 W przypadku podejmowania kroków prawnych, po wystąpieniu incydentu związanego z bezpieczeństwem informacji, należy zgromadzić, zachować i przedstawić materiał dowodowy, zgodnie z obowiązującymi wymogami prawnymi .

3.5 Materiał dowodowy winien być zabezpieczony w formie uniemożliwiającej jego utratę, lub niekontrolowaną modyfikację, przed dostarczeniem go odpowiednim organom. Dokonywać tego można poprzez:

a. Bezpiecznie przechowywać dokument papierowy wraz z informacją, kto znalazł dokument, gdzie, kiedy i kto był świadkiem zdarzenia;
b. Utworzenie obrazu lub kopii wszelkich nośników wymiennych (dla dokumentów na nośnikach komputerowych);
c. Zapisanie informacji znajdujących się na dyskach twardych lub w pamięci komputera w celu zapewnienia dostępności materiału;
d. Zapisanie wszelkich działań podczas procesu kopiowania wraz z określeniem świadków tego procesu;
e. Przechowywanie oryginalnego nośnika i dziennika zdarzeń w sposób bezpieczny i nienaruszony (co najmniej jeden obraz lustrzany lub kopia).

3.6 W celu realizacji obowiązku wynikającego z art. 33 RODO a tym samym konieczności szybkiego rozważenia działań prawnych oraz wyboru materiału dowodowego do zabezpieczenia, należy w możliwie najszybszym czasie nie dłuższym niż 24 godziny od powzięcia wiedzy o zaistniałym incydencie skonsultować wagę zgromadzonego materiału dowodowego z IOD, oraz z pracownikami innych organów, w tym Policji jeśli rodzaj incydentu tego wymaga.

4. Zgłoszenie naruszenia ochrony danych organowi nadzorczemu

Procedurę zgłaszania naruszeń organowi nadzorczemu reguluje **Załącznik nr J** do Wewnętrznej Polityki Bezpieczeństwa Danych osobowych

ZAŁĄCZNIK NR 1

FORMULARZ ZGŁOSZENIA INCYDENTU/ZAGROŻENIA

FORMULARZ ZGŁOSZENIA INCYDENTU/ZAGROŻENIA	
Imię i nazwisko zgłaszającego:	
Komórka organizacyjna /stanowisko :	
Data oraz godzina stwierdzenia zdarzenia związanego z bezpieczeństwem informacji:	
Opis informacji i aktywów, których dotyczy zdarzenie:	
Opis okoliczności, w jakich stwierdzono wystąpienie zdarzenia związanego z bezpieczeństwem informacji:	
Data i podpis Zgłaszającego:	Data i podpis Przyjmującego:

Załącznik nr 2
PRZYKŁADY ZAGROŻEŃ DLA BEZPIECZEŃSTWA INFORMACJI

Grupa Zasobu	Zagrożenie
Bazy danych	Kradzież
	Modyfikacja lub usunięcie danych
	Nieuprawniony dostęp
	Uszkodzenie
Pliki w postaci elektronicznej	Kradzież
	Ujawnienie danych osobom nieupoważnionym
	Nieuprawniony dostęp
	Uszkodzenie
Dane w postaci papierowej	Kradzież
	Nieuprawniony dostęp
	Uszkodzenie lub zniszczenie
	Wyciek wrażliwych danych
	Zagubienie
Systemy wspomagające	Awaria urządzenia
	Brak klimatyzacji
	Brak zasilania
	Niedziałanie urządzenia
	Zniszczenie instalacji
Sieci	Awaria urządzenia
	Nieuprawniony dostęp fizyczny
	Niezabezpieczona sieć
	Podsłuch
	Przeciążenie ruchu
	Uszkodzenie sieci
Oprogramowanie	Wadliwe działanie lub brak działania
	Rozprzestrzenianie wirusów itp.
Sprzęt i nośniki danych	Awaria sprzętu
	Awaria urządzenia lub jego podzespołów
	Awarie prądowe
	Awarie przez kurz
	Awarie ze względu na temperaturę
	Błędy działania

Grupa Zasobu	Zagrożenie
	Błędy konserwacji
	Błędy personelu obsługującego
	Kradzież
	Nieautoryzowane kopiowane/zmiana/usunięcie
	Nieprawdziwa informacja lub funkcjonowanie strony intranetowej
	Niewłaściwe wykorzystanie
	Zniszczenie
	Zużycie części
	Zużycie nośników
Budynki/Pomieszczenia	Awaria ze względu na temperaturę lub wilgotność
	Kradzież lub nieupoważniony dostęp do informacji
	Pożar
	Umyślna szkoda
	Wahania napięcia prądu
	Zalanie
Personel zewnętrzny - Jednostki współpracujące	Błąd personelu obsługującego
	Kradzież
	Nieautoryzowany dostęp
	Niedobór (brak) personelu
	Niemożliwość respektowania swoich potrzeb
	Podsłuch lub szpiegostwo
	Szkoda umyślna lub nieumyślna
	Ujawnienie informacji chronionych
	Użycie oprogramowania w niewłaściwy sposób
Personel własny (pracownicy)	Błąd personelu obsługującego
	Kradzież
	Nieautoryzowany dostęp
	Niedobór (brak) personelu
	Podsłuch lub szpiegostwo
	Szkoda umyślna lub nieumyślna
	Ujawnienie informacji chronionych
	Użycie oprogramowania w niewłaściwy sposób

WYKAZ NAJCZĘŚCIEJ WYSTĘPUJACYCH INCYDENTÓW BEZPIECZEŃSTWA ZWIĄZANYCH Z PRZETWARZANIEM DANYCH OSOBOWYCH

Rodzaj incydentu bezpieczeństwa	Podjęte działania zapobiegawcze i naprawcze
Ujawnienie danych osobowych osobom nieupoważnionym	
Nieodwracalne uszkodzenie nośnika z danymi osobowymi	
Kradzież nośnika z danymi osobowymi (np. komputera przenośnego, nośników zewnętrznych, dokumentów papierowych itp.)	
Usunięcie lub przekłamanie (zmiana) danych osobowych zapisanych na nośnikach danych w formie elektronicznej	
Brak dostępu do danych osobowych dla osób upoważnionych (posiadających upoważnienia i uprawnienia do pracy w systemach IT)	
Przełamanie lub próby przełamania zabezpieczeń systemów informatycznych służących do przetwarzania danych osobowych	
Nieprawidłowe działania lub awarie systemów informatycznych wykorzystywanych do przetwarzania danych osobowych	
Działania szkodliwego oprogramowania w postaci wirusów, trojanów, robaków, programów szpiegujących, keyloggerów itp.	
Pozyskanie lub próby nieuprawnionego pozyskania danych osobowych oraz sposobów zabezpieczeń tych danych za pomocą ataków socjotechnicznych	
Nie wykonywanie lub utrata kopii zapasowych znajdujących się na nośnikach	
Dopuszczenie osób nieuprawnionych (lub wtargnięcie osób nieupoważnionych) do obszaru w którym są przetwarzane dane osobowe	
Utrata sprzętu komputerowego lub nośnika z danymi osobowymi wskutek klęski żywiołowej (pożar, powódź, zalanie itp.)	
Wykorzystywanie danych osobowych niezgodnie z celem ich przetwarzania	
Brak zastosowania zabezpieczeń organizacyjnych i technicznych wymaganych ustawą o ochronie danych osobowych i przepisami wykonawczymi do tej ustawy	

ROZDZIAŁ IX. ZAS
INFORMACJI O UDOSTĘPNIENIU DANYCH OSOBOWYCH

1. Odbiorcą danych osobowych jest każdy, komu udostępnia się dane osobowe, z wyłączeniem:

   1.1 Osoby, której dane dotyczą;
   1.2 Osoby, użytkownika systemu lub innej osoby upoważnionej do przetwarzania danych osobowych w Szkole Podstawowej nr 1 im. Stanisławy Łakomik w Czeladzi;
   1.3 Podmiotu, któremu powierzono przetwarzanie danych;
   1.4 Organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

2. Dane osobowe administrowane przez Szkoła Podstawowa nr 1 im. Stanisławy Łakomik w Czeladzi mogą być udostępnione osobom lub podmiotom:

   2.1 Uprawnionym na mocy RODO oraz innych przepisów obowiązujących w działalności Jednostki w celu włączenia ich do procesu - zbioru;

   2.2 Osobie fizycznej w przypadku nie włączenia do procesu - zbioru, gdy uzasadni potrzebę uzyskania danych osobowych.

3. Dane udostępnione przez inny podmiot można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

4. ADO lub osoba wyznaczona przez Administratora Danych Osobowych (ADO), która w jego imieniu, realizuje ten zakres obowiązków prowadzi ewidencję udostępnień danych. Odnotowanie obejmuje informacje o:

   4.1 Dacie udostępnienia;
   4.2 Osobie/Podmiocie, któremu dane udostępniono (nazwa, adres);
   4.3 Podstawie prawnej udostępnienia danych osobowych;
   4.4 Celu i zakresie udostępnionych danych;
   4.5 Imię i nazwisko pracownika udostepniającego dane osobowe.

5. W przypadku występowania funkcjonalności w systemie informatycznym eksploatowanym w Podmiocie polegającej na możliwości odnotowania w nim informacji o udostępnieniu danych, obowiązek odnotowania w/w informacji w systemach informatycznych Jednostki spoczywa na każdym uprawnionym pracowniku. Kontrolę odnotowań udostępnień w systemie prowadzą ASI jeśli został wyznaczony/ Informatyk, lub inna osoba wyznaczona przez Administratora Danych Osobowych (ADO), która w jego imieniu, realizuje ten zakres obowiązków .

ROZDZIAŁ X.

WYMAGANIA FUNKCJONALNE SYSTEMÓW INFORMATYCZNYCH WYNIKAJĄCE Z OBOWIĄZKU INFORMACYJNEGO

1. Wymagania dotyczące obowiązku informacyjnego określają zakres danych, jakie powinny być rejestrowane w systemach informatycznych. Ich posiadanie stanowi element niezbędny dla wykonania obowiązku informacyjnego określonego w RODO
2. ADO dąży do korzystania z systemów które będą w stanie rejestrować następujące informacje:
   - 2.1 Daty pierwszego wprowadzenia danych do systemu;
   - 2.2 Identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba;
   - 2.3 Źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą;
   - 2.4 Informacji o odbiorcach, w rozumieniu RODO, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych;
   - 2.5 Sprzeciwu, złożonego przez osobę fizyczną której dane są przetwarzane.
3. W przypadku przetwarzania danych osobowych, w co najmniej dwóch systemach informatycznych, wymagania dotyczące udostępnień, mogą być realizowane w jednym z nich lub w odrębnym systemie informatycznym przeznaczonym do tego celu.

ROZDZIAŁ XI.

ZASADY KORZYSTANIA Z POCZTY ELEKTRONICZNEJ

Zasady korzystania z poczty elektronicznej

1. Osoby upoważnione do przetwarzania danych osobowych zobowiązane są do korzystania z poczty elektronicznej tylko w celach służbowych.
2. W przypadku przesyłania danych osobowych poza Jednostkę należy wykorzystywać mechanizmy kryptograficzne (hasłowanie wysyłanych dokumentów lub plików zzipowanych, podpis elektroniczny).
3. 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.
4. Każdy użytkownik przed wysłaniem poczty jest zobowiązany sprawdzić poprawność adresu odbiorcy dokumentu.
5. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.
6. W celu ochrony przed zainfekowaniem komputera użytkownika i komputerów pracujących w sieci (kryptowirusy) zabrania się otwierania załączników (plików) w mailach nawet od prawdopodobnie znanych użytkownikowi nadawców bez weryfikacji nadawcy.
7. 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.
8. Wszystkie przypadki e-maili budzących podejrzenie należy zgłaszać ASI/ Informatykowi.
9. Przy wysyłaniu maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW”. Zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości”.
10. Zabrania się rozsyłania maili z tzw. „ łańcuszkami szczęścia”. Adres mailowy służbowy służy wyłącznie do korespondencji służbowej.
11. Nakazuje się okresowe czyszczenie poczty z nieaktualnych e- mali i opróżnianie kosza.

12. Zakazuje się wysyłania korespondencji służbowej na prywatne skrzynki pocztowe pracowników lub innych osób.
13. Użytkownicy mają prawo korzystać z poczty mailowej dla celów prywatnych wyłącznie okazjonalnie i powinno być to ograniczone do niezbędnego minimum.
14. 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.
15. Użytkownicy nie mają prawa korzystać z poczty elektronicznej w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub nieetycznym i naruszającym cudzą godność i prywatność.
16. Zabrania się dokonywanie w sieci zakupów, rezerwacji usług lub świadczeń na rzecz użytkownika oraz dokonywania płatności bankowych z prywatnego konta.
17. Użytkownik bez zgody ADO nie ma prawa wysyłać wiadomości zawierających dane osobowe dotyczące Pracodawcy / Zleceniodawcy, jego pracowników, dzieci i ich rodziców/opiekunów prawnych, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej.
18. Wszelkie przesyłane dokumentów, opracowania, jak i innych treści przesyłane przez użytkownika podlegają zasadom ochrony prawa autorskiego i prawa własności przemysłowej, które użytkownik jest obowiązany przestrzegać.

ROZDZIAŁ XII.

ZASADY WYNOSZENIA NOŚNIKÓW Z DANYMI OSOBOWYMI POZA JEDNOSTKĘ

1. Użytkownicy nie mogą wynosić poza Jednostkę bez zgody Administratora danych żadnych wymiennych elektronicznych nośników informacji, tj. wymienne twarde dyski, pendrive, płyty CD, DVD, pamięci typu Flash.
2. W sytuacjach koniecznych, za zgodą Administratora danych, wynoszone nośniki wymienne muszą być zaszyfrowane, lub pliki opatrzone hasłem.
3. Zabrania się korzystania z nośników prywatnych, bądź niewiadomego pochodzenia. W celu wyniesienia danych poza obszar przetwarzania korzysta się wyłącznie z nośników służbowych
4. Zabrania się wynoszenia poza Jednostkę dokumentacji papierowej, zwierającej dane osobowe bez zgody ADO, jeśli nie wymaga tego zakres zadań służbowych. W przypadku takiej konieczności, należy ją przenosić w zamykanych teczkach lub w innej bezpiecznej formie.

ROZDZIAŁ XIII.

EWIDENCJA SPRZĘTU I OPROGRAMOWANIA

1. W celu zagwarantowania prawidłowej realizacji powierzonych Jednostce zadań, w tym zabezpieczenia ciągłości działania systemów informatycznych, ADO prowadzi ewidencję sprzętu informatycznego oraz oprogramowania wykorzystywanego w procesie przetwarzania danych osobowych oraz wspomagającego funkcjonowanie infrastruktury informatycznej.
2. Ewidencja służy następującym celom:
   a) Zagwarantowaniu kompletności sprzętu niezbędnego do realizacji zadań powierzonych Jednostce
   b) Monitorowaniu stanu technicznego sprzętu eksploatowanego w Jednostce oraz podzespołów niezbędnych do prawidłowego przepływu informacji w infrastrukturze informatycznej
   c) Ustalenia lokalizacji usytuowania sprzętu oraz poszczególnych elementów infrastruktury informatycznej
   d) Monitorowania legalności użytkowanego oprogramowania, poprzez sprawdzanie stanu ilościowego oraz ważności licencji oprogramowania
   e) Zdjęcia ze stanu posiadania programów/aplikacji , których użytkowanie w Jednostce zakończono, jak też eliminowanie zainstalowanych programów/aplikacji, których posiadanie jest nieuzasadnione (instalacje aplikacji w wersjach demo na potrzeby ich przetestowania, programy narzędziowe do diagnostyki sprzętu, oprogramowania, lub inne które nie są już wykorzystywane)
3. ADO zleca ASI/Informatykowi co najmniej raz w roku przeprowadzenie inwentaryzacji sprzętu informatycznego oraz oprogramowania użytkowanego w Jednostce według ustalonego formularza ewidencyjnego.
4. Wzór formularza ewidencji sprzętu i oprogramowania stanowi załącznik 1 do niniejszego rozdziału

Załącznik 1. Ewidencja sprzętu i oprogramowania

Zestawienie sprzętu i oprogramowania komputerowego											
Nr pomieszczenia/ lokalizacja i użytkownik	**Rodzaj Komputera**	**Nr inwent.**	**Monitor**	**Nr inwent.**	**Procesor**	**Pamięć RAM**	**Pojemność dysków**	**Drukarki**	**Nr inwent.**	**System operacyjny**	**Oprogramowanie**

Inwentaryzacja oprogramowania - informacje o licencjach			
Nazwa systemu/aplikacji	**Lokalizacja / miejsce instalacji**	**termin obowiązywania licencji**	**Ilość licencji**

ROZDZIAŁ XIV.

POSTANOWIENIA KOŃCOWE

1. Zasady przetwarzania danych osobowych, których Administratorem jest Szkoła Podstawowa nr 1 im. Stanisławy Łakomik w Czeladzi przez podmioty zewnętrzne regulują, na podstawie szczegółowych zasad określonych w niniejszej Instrukcji stosowne umowy zawarte w tym zakresie z tymi podmiotami.
2. W sprawach nieuregulowanych niniejszą Instrukcją zastosowanie znajdują przepisy obowiązującego prawa, oraz wytyczne dotyczące zasad przetwarzania danych w systemach informatycznych, realizowane przez podmioty publiczne, oraz Norma PN ISO/IEC 27001 i Norma PN-ISO/IEC 27002.