Załącznik nr 1
do Zarządzenia Nr 26/2017/2018
z dnia 21.06.2018 r.

# Procedura ochrony danych osobowych w Zespole Szkolno-Przedszkolnym nr 3 w Skidziniu

## Postanowienia ogólne

### § 1

1. „Procedura ochrony danych osobowych”, zwana dalej Procedurą ochrony, opracowana została zgodnie z wymogami określonymi w Rozporządzeniu 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), zwanego dalej „Rozporządzeniem”.
2. Niniejsza Procedura ochrony, jest wewnętrznym dokumentem wydanym przez Dyrektora Szkoły, dalej zwanego „Dyrektorem” i stanowi najwyższej rangi dokument w Zespole Szkolno-Przedszkolnym nr 3 w Skidziniu (zwanej dalej Szkołą), dotyczące ochrony danych osobowych. Obowiązek stosowania zasad opisanych w tych dokumentach obejmuje wszystkich pracowników oraz podmioty zewnętrzne świadczące usługi na rzecz Szkoły.
3. Procedura ochrony nie może być udostępniania osobom nieupoważnionym w żadnej formie.
4. Celem Procedury ochrony jest wskazanie działań, jakie należy podejmować oraz ustanowienie zasad postępowania w celu zapewnienia standardów bezpieczeństwa danych osobowych, aby prawidłowo były realizowane obowiązki administratora danych w zakresie zabezpieczenia danych osobowych.
5. Wszyscy pracownicy zobowiązani są do bezwzględnego stosowania przy przetwarzaniu danych osobowych procedur i zasad zawartych w niniejszej dokumentacji.
6. Każdy pracownik Szkoły przyjmuje na siebie obowiązek ochrony zasobów Szkoły w zakresie uzyskanych uprawnień. Obowiązek ochrony zasobów nie kończy się z chwilą ustania stosunku pracy lub innego stosunku prawnego stanowiącego podstawę wykonywania pracy na rzecz Szkoły w takim zakresie, jaki ustanawiają przepisy prawa.
7. Obowiązek ochrony zasobów w przypadku współpracy z Podmiotami zewnętrznymi określany jest w ramach zawartych z nimi umów.

### § 2

Podstawowe definicje pojęć:

1) **Administrator Danych Osobowych (Administrator)** – Szkoła, w której imieniu działa Dyrektor Szkoły, który ustala cele i sposoby przetwarzania danych osobowych w Szkole.
2) **Administrator Systemu Informatycznego** (ASI) – należy przez to rozumieć wyznaczoną przez Administratora osobę realizującą zadania związane z utrzymaniem systemu teleinformatycznego, a w szczególności odpowiedzialną za utrzymywanie zabezpieczeń w tym systemie. W razie braku wyznaczenia ASI - jego zadania realizuje Administrator.
3) **Autentyczność** – właściwość polegająca na tym, że pochodzenie lub zawartość obiektu informatycznego są takie jak deklarowane. Autentyczność dotyczy takich podmiotów jak użytkownicy, procesy, systemy i informacja.

4) **Bezpieczeństwo informacji** - zachowanie poufności, integralności i dostępności informacji; dodatkowo, mogą być brane pod uwagę inne właściwości informacji, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.
5) **Dane osobowe** – oznaczają informacje o zidentyfikowanej lub możliwej do identyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.
6) **Dostępność** – właściwość bycia dostępnym i możliwym do wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot.
7) **Hasło** - ciąg znaków literowych, cyfrowych lub innych znany jedynie użytkownikowi, wykorzystywany w procesie uwierzytelniania użytkownika przy uzyskiwaniu dostępu do systemu informatycznego, lub urządzenia.
8) **Identyfikator użytkownika**, zwany zamiennie „loginem" - ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę, która jest użytkownikiem systemu informatycznego, lub urządzenia.
9) **Incydent związany z bezpieczeństwem informacji** – pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń, związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań i zagrażają bezpieczeństwu informacji.
10) **Inspektor ochrony danych** (IOD) – osoba, której Administrator powierzył zadania określone w Rozporządzeniu.
11) **Integralność** (spójność) **danych -** właściwość zapewniająca, że dane nie zostały zmodyfikowane lub zniszczone w sposób nieuprawniony.
12) **Integralność systemu -** właściwość polegająca na tym, że system realizuje swoją zamierzoną funkcję w nienaruszony sposób, wolny od nieautoryzowanej manipulacji, celowej lub przypadkowej.
13) **Klient** - osoba fizyczna, podmiot publiczny, osoba prawna, lub jednostka organizacyjna nie posiadająca osobowości prawnej korzystająca z usług systemu Szkoły.
14) **Monitorowanie** – proces weryfikacji stosowanych metod i zasad bezpieczeństwa oraz kontrolę ich przestrzegania.
15) **Naruszenie ochrony danych osobowych** - oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
16) **Niezaprzeczalność** - możliwość przeprowadzenia dowodu, że działanie lub zdarzenie miało miejsce, w taki sposób, że nie można temu działaniu lub zdarzeniu później zaprzeczyć.
17) **Niezawodność** - właściwość oznaczająca spójne, zamierzone zachowanie i skutki.
18) **Podatność** - słabość aktywu lub grupy aktywów, która może być wykorzystana przez jedno lub więcej zagrożeń.
19) **Podmiot zewnętrzny** - osoba fizyczna, osoba prawna, jednostka organizacyjna nie posiadająca osobowości prawnej lub organ współpracujący ze Szkołą bądź świadczący na jej rzecz usługi.

20) **Poufność** - właściwość zapewniająca, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom.
21) **Przetwarzanie danych osobowych** – oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
22) **PUODO** – Prezes Urzędu Ochrony Danych Osobowych.
23) **Rozliczalność** - właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
24) **Ryzyko związane z bezpieczeństwem informacji** - potencjalna sytuacja, w której dane zagrożenie wykorzysta podatności aktywów lub grupy aktywów, co spowoduje szkodę dla organizacji. Ryzyko jest funkcją prawdopodobieństwa zdarzenia i jego konsekwencji.
25) **Sieć publiczna** - rozumie się przez to sieć publiczną w rozumieniu ustawy Prawo telekomunikacyjne.
26) **Sieć telekomunikacyjna** - rozumie się przez to sieć telekomunikacyjną w rozumieniu ustawy Prawo telekomunikacyjne.
27) **Stacja robocza** – stacjonarny lub przenośny komputer lub inne urządzenie wchodzące w skład systemu informatycznego umożliwiające użytkownikom systemu dostęp do danych osobowych znajdujących się w systemie.
28) **System** – system informacyjny, w którym w trakcie zachodzących w nim procesów gromadzi się, przetwarza, przechowuje i udostępnia informacje, niezależnie od formy realizacji tych procesów.
29) **System teleinformatyczny** - zespół współpracujących ze sobą według określonych reguł urządzeń i oprogramowania.
30) **Teletransmisja** - rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej.
31) **Umowa powierzenia –** należy przez to rozumieć umowę z podmiotem zewnętrznym, której przedmiotem jest świadczenie usługi przetwarzania danych osobowych, na warunkach określonych w umowie.
32) **Uwierzytelnianie** - rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości użytkownika.
33) **Użytkownik systemu** —osoba uprawniona do przetwarzania danych, która uzyskała dostęp i korzysta z zasobów systemów informatycznych Szkoły.
34) **Właściciel Zasobu** – osoba kierująca komórką organizacyjną Szkoły, nadzorująca eksploatację, rozwój, utrzymanie, korzystanie, bezpieczeństwo i dostęp do Zasobu.
35) **Zagrożenie** - potencjalna przyczyna incydentu, który może spowodować stratę w systemie lub dla organizacji.
36) **Zarządzanie ryzykiem** - skoordynowane działania kierowania i kontrolowania organizacji z uwzględnieniem ryzyka.
37) **Zasoby** - wszystko to, co ma wartość dla Szkoły, w szczególności informacje przetwarzane w Szkole oraz mienie wykorzystywane przez Szkołę (równoważnie - aktywa (informacyjne)).

38) **Zbiór danych osobowych** – oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.
39) **Zdarzenie związane z bezpieczeństwem informacji -** określony stan systemu, usługi lub sieci, który wskazuje na możliwe przełamanie bezpieczeństwa informacji, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem.

**Naruszenie ochrony danych osobowych**
**§ 3**

1. Za naruszenie ochrony danych osobowych uważa się w szczególności:
   a) nieuprawniony dostęp lub próbę dostępu do danych osobowych lub pomieszczeń, w których się one znajdują,
   b) wszelkie modyfikacje danych osobowych lub próby ich dokonania przez osoby nieuprawnione (np. zmiana zawartości danych, utrata bądź przejęcie całości lub części danych),
   c) naruszenie lub próby naruszenia integralności systemu,
   d) zmianę lub utratę danych zapisanych na kopiach zapasowych,
   e) naruszenie lub próby naruszenia poufności danych lub ich części,
   f) nieuprawniony dostęp (sygnał o nielegalnym logowaniu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu),
   g) udostępnienie osobom nieupoważnionym danych osobowych lub ich części,
   h) zniszczenie, uszkodzenie lub wszelkie próby nieuprawnionej ingerencji zmierzające do zakłócenia działania bądź pozyskania w sposób niedozwolony (lub w celach niezgodnych z przeznaczeniem) danych zawartych w systemach informatycznych lub kartotekach,
   i) inny stan systemu informatycznego lub pomieszczeń niż pozostawiony przez użytkownika po zakończeniu pracy.

**Wykaz osób odpowiedzialnych**
**§ 4**

1. Osobami odpowiedzialnymi za tworzenie Procedury ochrony są:
   a) Administrator,
   b) ASI - jeśli nie został powołany, to jego zadania wykonuje Administrator,
   c) IOD.
2. Osobami odpowiedzialnymi za realizację Procedury ochrony są:
   a) Administrator:
      - samodzielnie ustala cele i sposoby przetwarzania danych osobowych,
      - formułuje i wdraża warunki techniczne i organizacyjne służące ochronie danych osobowych;
      - prowadzi i przechowuje niezbędną dokumentację, w celu umożliwienia spełnienia zasady rozliczalności;
      - zarządza ryzykiem związanym z przetwarzaniem danych osobowych, w tym w razie potrzeby podejmuje działania minimalizujące jego poziom;
      - odpowiada w szczególności za nadzorowanie i monitorowanie przestrzegania zasad ochrony danych osobowych przetwarzanych w Szkole;

- podejmuje niezbędne działania w celu likwidacji słabych ogniw w systemie zabezpieczeń, wdraża nowe narzędzia i metody pracy mające na celu zwiększenie ochrony danych osobowych.

b) ASI:
- odpowiada w szczególności za właściwą konfigurację i administrowanie elementami Systemu informatycznego Szkoły, w szczególności za zapewnienie bezpieczeństwa danych osobowych,
- odpowiada za bieżące monitorowanie elementów Systemu informatycznego Szkoły, w szczególności pod kątem prób nieautoryzowanego dostępu do danych osobowych,
- przeciwdziała próbom włamania, zniszczenia oraz nieautoryzowanego dostępu do elementów Systemu Informatycznego, w tym także do danych osobowych,
- zabezpiecza dane osobowe przed ich nieuprawnionym przetwarzaniem, a w szczególności przeciwdziała dostępowi osób trzecich do systemu,
- konserwuje i wdraża techniczne zabezpieczenia systemu informatycznego oraz rejestruje i wyrejestrowuje użytkowników z systemu.

c) Inspektor ochrony danych (IOD) – pracownik Szkoły lub podmiot zewnętrzny:
- realizuje zadania określone w ww. Rozporządzeniu;
- zapoznaje osoby upoważnione do przetwarzania danych osobowych z przepisami o ochronie danych osobowych;
- doradza przy realizacji ochrony danych osobowych;
- pomaga ustalić odpowiednie warunki techniczne i organizacyjne służące ochronie danych osobowych;
- szkoli pracowników Szkoły w zakresie ochrony danych osobowych;
- dokonuje okresowych sprawdzeń i oceny funkcjonowania mechanizmów zabezpieczeń oraz przestrzegania zasad postępowania.

d) Wszyscy pracownicy Szkoły oraz podmioty zewnętrzne świadczące usługi na rzecz Szkoły - zobowiązani są do:
- Zapoznania się z zasadami określonymi w przepisach prawa (w szczególności z Rozporządzeniem) oraz niniejszej Procedurze ochrony oraz złożenia oświadczenia o znajomości zawartych w nich przepisów.
- Chronienia prawa do prywatności osób powierzających swoje dane osobowe poprzez przetwarzanie ich zgodnie z przepisami prawa oraz zasadami określonymi w Procedurze ochrony.
- Przestrzegania przepisów o ochronie danych osobowych, a także ścisłej współpracy z Administratorem. W tym celu zobowiązani jest do: informowania Administratora o wszystkich zauważonych nieprawidłowościach, zgłaszania powstania nowych zbiorów danych osobowych, występowania z wnioskami w sprawie wprowadzenia niezbędnych zmian w zakresie ochrony danych osobowych.

3. ADO, ASI i IOD na bieżąco dokonują oceny realizowania Procedury ochrony i w razie konieczności wprowadzają zmiany do jej treści.

**Dokumentacja dotycząca przetwarzania danych osobowych**

**§ 5**

W związku z ochroną przetwarzania danych osobowych w Szkole prowadzona jest następująca dokumentacja:

1. Rejestr czynności przetwarzania określony w zał. nr 1a. W przypadku zaistnienia zmian Rejestr czynności aktualizowany jest niezwłocznie.

2. Rejestr kategorii czynności przetwarzania określony w zał. nr 1b. W przypadku zaistnienia zmian Rejestr kategorii czynności aktualizowany jest niezwłocznie.
3. Analiza ryzyka dot. możliwości naruszenia praw lub wolności osoby, której dane dotyczą, zgodnie z metodologią stanowiącą zał. nr 2. W przypadku zaistnienia zmian Analiza ryzyka aktualizowana jest niezwłocznie.
4. Rejestr zasobów informatycznych – ujmowane są w nim (zał. nr 3) zidentyfikowane zasoby systemu informatycznego.
5. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe określono w zał. nr 4.
6. Wykaz osób upoważnionych do przetwarzania danych osobowych określono w zał. nr 5, wzór upoważnienia i oświadczenia w zał. nr 6, a odwołania upoważnienia w zał. nr 7.

**Środki techniczne i organizacyjne służące zapewnieniu poufności i integralności przetwarzania danych**

**§ 6**

1. W celu zwiększenia efektywności ochrony danych osobowych dokonano połączenia różnych zabezpieczeń w sposób umożliwiający stworzenie kilku warstw ochronnych. Ochrona danych osobowych jest realizowana poprzez: zabezpieczenia fizyczne, procedury organizacyjne, uprawnionych użytkowników oraz oprogramowanie systemowe i aplikacje (w przypadku przetwarzania danych za pomocą systemu informatycznego).
2. Tradycyjne przetwarzanie danych osobowych oraz w systemach informatycznych odbywa się wyłącznie na obszarze wyznaczonym przez Administratora.
3. Przetwarzanie danych osobowych za pomocą urządzeń przenośnych może odbywać się poza obszarem przetwarzania danych wyłącznie za zgodą Administratora.
4. W celu ograniczenia dostępu osób postronnych do pomieszczeń, w których zlokalizowano przetwarzanie danych osobowych określona jest w Szkole procedura wydawania kluczy do pomieszczeń.
5. Pracownicy Szkoły są zobowiązani do przestrzegania zasad określających dopuszczalne sposoby przemieszczania się osób trzecich w obrębie pomieszczeń, w których przetwarzane są dane osobowe, tzn.:
   - stały dostęp do pomieszczeń, w których przetwarzane są dane osobowe mają tylko osoby upoważnione,
   - dostęp do pomieszczeń, w których przetwarzane są dane osobowe osób nie upoważnionych jest możliwy wyłącznie za zgodą Administratora,
   - przebywanie osób upoważnionych po godzinach pracy w pomieszczeniach, w których przetwarzane są dane osobowe jest dopuszczalne jedynie za zgodą Administratora,
   - wszyscy pracownicy zobowiązani są do zwracania uwagi na zachowanie osób wchodzących i wychodzących z jednostki.
6. Przebywanie osób trzecich w pomieszczeniach może odbywać się wyłącznie w obecności osób upoważnionych lub za zgodą Administratora.
7. Pracownicy zobowiązani są każdorazowo zamykać pomieszczenia w przypadku ich opuszczania - zabrania się pozostawiania pomieszczeń bez nadzoru oraz pozostawiania kluczy w zamkach po zewnętrznej stronie drzwi.
8. Po zakończeniu pracy wszystkie dokumenty zawierające dane osobowe należy odłożyć do zamykanej szafy.
9. Pracownicy zobowiązani są do zamknięcia okien, wyłączenia wszystkich urządzeń elektrycznych (w tym również komputerowych) oraz zgaszenia światła w pomieszczeniach

po zakończeniu pracy.

10. Środki ochrony fizycznej:
    a) po zakończeniu pracy wszystkie pomieszczenia, w których przetwarza się dane są zamykane,
    b) klucze do pomieszczeń przechowuje się zgodnie z obowiązującymi w Szkoły zasadami.
    c) budynek Szkoły, poza godzinami pracy jest zamykany,
    d) urządzenia służące do przetwarzania danych osobowych znajdują się w pomieszczeniach zabezpieczonych zamkami.
11. Szczegółowy opis zabezpieczeń fizycznych, logicznych, systemowych zawarto w zał. nr 8.
12. Administrator upoważnia osoby do przetwarzania danych osobowych i prowadzi ewidencję osób upoważnionych, w tym pracowników, którzy otrzymali karty mikroprocesorowe do podpisu przelewów, do podpisu elektronicznego. Zasady posługiwania się kartami mikroprocesorowymi do podpisu przelewów, do podpisu elektronicznego (kwalifikowanego i niekwalifikowanego) zawarte są w odrębnych przepisach.
13. Osoby upoważnione do przetwarzania danych osobowych są szkolone w zakresie obowiązujących przepisów o ochronie danych osobowych oraz procedur przetwarzania danych w momencie wydawania upoważnień i podpisywania oświadczeń.
14. Zasady postępowania z dziennikiem lekcyjnym oraz innymi dokumentami zawierającymi dane osobowe:
    a) Dzienniki lekcyjne są przechowywane w pokoju nauczycielskim w specjalnie do tego wyznaczonym miejscu – szafie zamykanej na klucz.
    b) Pokój nauczycielski jest miejscem szczególnie chronionym, nie może w nim przebywać osoba postronna bez nadzoru przynajmniej jednej osoby posiadającej upoważnienie do przetwarzania danych osobowych.
    c) Przenoszenie dzienników lekcyjnych przez uczniów, bądź inne osoby, które nie są upoważnione do przetwarzania danych osobowych jest bezwzględnie zakazane. Obowiązkiem nauczyciela jest pobranie i odłożenie dziennika na wyznaczone miejsce osobiście. Dopuszczalne jest przekazanie dziennika przez inną osobę, o ile posiada ona upoważnienie do przetwarzania danych osobowych obejmujące zakres danych przetwarzanych w dziennikach lekcyjnych.
    d) Szczególnej ochronie podlegają również wszelkie inne dokumenty zawierające dane osobowe uczniów, m.in. arkusze ocen, opinie z poradni psychologiczno-pedagogicznej, klasówki, sprawdziany, listy uczniów tworzone doraźnie, dane o stanie zdrowia itp. Przekazywanie w/w dokumentów osobom nieuprawnionym jest zabronione.
    e) Wynoszenie dzienników lekcyjnych oraz innych dokumentów poza placówkę jest zakazane.
    f) Wynoszenie dokumentów zawierających dane osobowe pracowników (pobieranie akt pracowniczych bądź kopii dokumentów z sekretariatu) jest zakazane.
15. W celu zapewnienia bezpieczeństwa informacji stosuje się następujące ogólne zasady:
    a) „przywilejów koniecznych” - każdy pracownik, współpracownik ma dostęp do Zasobów ograniczony wyłącznie do tego, który jest niezbędny do wykonywania powierzonych mu obowiązków;
    b) rozliczalności - Szkoła dąży do zapewnienia jednoznacznej odpowiedzialności pracowników za Zasoby im powierzone; wszyscy użytkownicy Zasobów muszą być świadomi swej odpowiedzialności i konsekwencji, które poniosą, jeżeli zaniedbają swoje obowiązki; przekazywanie własnych praw dostępu do Zasobów innym osobom jest

zabronione; odstępstwo od zasady rozliczalności musi być uzasadnione, odnotowane oraz zatwierdzone przez osoby odpowiedzialne za bezpieczeństwo;

c) „czystego biurka i ekranu" – polegającej na ograniczeniu ryzyka nieautoryzowanego dostępu, utraty, zniszczenia danych osobowych, poprzez przechowywanie papierowych i elektronicznych nośników pod zamknięciem, zamykanie sesji / blokowanie komputerów, usuwanie z drukarek wydruków zawierających dane osobowe.

d) „separacji obowiązków", polegającej na tym, że zadania krytyczne z punktu widzenia bezpieczeństwa informacji nie mogą być realizowane przez jedną osobę. Zadania krytyczne są wskazane w politykach szczegółowych i regulaminach.

**§ 7**

1. **Dostęp do systemu** informacyjnego Szkoły mogą posiadać:
   a) pracownicy Szkoły, praktykanci, stażyści, pracownicy zatrudnieni na umowę cywilno-prawną,
   b) pracownicy podmiotów nieujętych powyżej na podstawie odrębnej umowy (np. umowy o świadczenie usługi wsparcia technicznego),
   c) inne osoby spoza jednostki.
2. Użytkownicy posiadający nieograniczony dostęp do Systemu (Administrator, ASI), mają uprawnienia administratorów systemu. Hasła do systemów i zmiany tych haseł użytkownicy uprzywilejowani przechowują w sejfie Szkoły – sekretariat.
3. Osoby nie będące ASI są użytkownikami zwykłymi. Posiadają oni dostęp do Sytemu w ograniczonym zakresie, związanym wyłącznie z zakresem obowiązków służbowych, zakresem realizowanej umowy, porozumienia lub wniosku o dostęp do Systemu.
4. Dostęp użytkownika zwykłego do Systemu jest zapewniany przez ASI według następujących zasad:
   a) dostęp do Systemu może uzyskać wyłącznie osoba zarejestrowana,
   b) rejestracja, o której mowa w pkt. 1, polega na nadaniu identyfikatora i przydziale hasła pierwszego logowania,
   c) rejestr osób uprawnionych do przetwarzania danych, jak również rejestr osób uprawnionych do przetwarzania danych do których wymagana jest karta mikroprocesorowa (lub inna dodatkowa certyfikacja) stanowią załącznik do Procedury ochrony,
5. ASI blokuje konto użytkownika, który niewłaściwie chroni swoje hasło lub wykorzystuje je niezgodnie z postanowieniami niniejszej Procedury, a następnie postępuje zgodnie z procedurą zarządzania incydentami bezpieczeństwa informacji.
6. Co najmniej raz do roku ASI przeprowadza weryfikację kont w Systemie.

**§ 8**

1. **Odebranie dostępu** do systemu dokonuje ASI.
2. Odebranie dostępu, o którym mowa w ust. 1, może mieć charakter czasowy lub trwały i polega na zablokowaniu wszystkich kont użytkownika w Systemie, natomiast identyfikator użytkownika nie może zostać usunięty z ewidencji (bazy) użytkowników nawet po wyrejestrowaniu takiego użytkownika.
3. Przyczyną czasowego odebrania dostępu do systemu informatycznego jest:
   a) nieobecność w pracy trwająca dłużej niż 30 dni kalendarzowych,
   b) zawieszenie w pełnieniu obowiązków służbowych,
   c) zwolnienie z pełnienia obowiązków służbowych,

d) naruszenie zasad bezpieczeństwa informacji określonych w niniejszej Procedurze ochrony.

4. Przyczyną trwałego odebrania dostępu do systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy użytkownika.

**§ 9**

1. Dostęp do Systemu (konto użytkownika) może być wykorzystywane przez użytkownika wyłącznie do zadań związanych z pełnionym stanowiskiem lub realizacją umów. W szczególności nie może być ono wykorzystywane do rozpowszechniania treści i obrazów wulgarnych, obrażających osoby trzecie, naruszających czyjekolwiek dobra osobiste lub niezgodnych z prawem.
2. Zabrania się użytkownikom pracującym w systemie:
   a) udostępniania stacji roboczej osobom niezarejestrowanym w systemie,
   b) udostępniania stacji roboczej do konserwacji lub naprawy bez porozumienia z ASI,
   c) instalowania samodzielnie, bez zgody ASI oprogramowania systemowego i aplikacji (programów),
   d) uruchamiania aplikacji (programów), które mogą zakłócić i destabilizować pracę Systemu, bądź naruszyć bezpieczeństwo danych w nim przetwarzanych,
   e) pobierać z sieci, kopiować, przechowywać lub rozprowadzać oprogramowania, dane multimedialnych (filmy, muzyka) oraz inne pliki, których używanie może powodować naruszenie praw do własności intelektualnej,
   f) udostępniania osobom trzecim informacji na temat struktury Systemu, również po ustaniu okresu zatrudnienia lub po odebraniu dostępu do Systemu,
   g) używania Systemu do celów prywatnych, co w szczególności oznacza, że wszelkie dane przetwarzane w Systemie nie oznaczone jako własność osób trzecich, są własnością Szkoły – w tym także korespondencja elektroniczna.
3. Należy chronić **sprzęt komputerowy** przed kradzieżą, zniszczeniem lub niewłaściwym użytkowaniem oraz zagrożeniami ze strony otoczenia (kurz, promieniowanie słoneczne, ogień, woda itp.). Sprzęt komputerowy będący własnością Szkoły nie może być wynoszony z siedziby Szkoły, a w przypadku sprzętu stacjonarnego, przenoszony w inne miejsce Szkoły bez wcześniejszej zgody ASI.
4. Utrata lub kradzież powierzonego Pracownikowi sprzętu powinna być niezwłocznie zgłaszana do Administratora.
5. Zabrania się używania jakichkolwiek prywatnych nośników danych (magnetycznych, optycznych oraz pamięci przenośnych) na stanowiskach komputerowych (w tym komputerach przenośnych) będących własnością Szkoły bez zgody ASI.
6. Wszelkie osoby korzystające z Systemu są zobowiązane do przestrzegania prawa, zasad współżycia społecznego oraz zasad etyki. Zabrania się podejmowania działań, które naruszałyby dobra osobiste innych osób lub narażały te osoby na straty moralne lub materialne.

**§ 10**

1. Każdy użytkownik może posiadać tylko jeden **identyfikator użytkownika** do jednego programu. Nie można zmieniać tego identyfikatora lub przyznawać takiego samego identyfikatora innemu użytkownikowi.
2. ASI może posiadać więcej niż jeden identyfikator, pod warunkiem, iż żaden z używanych przez niego identyfikatorów nie jest używany przez innego użytkownika Systemu.

3. Administrator nadzoruje ewidencję wszystkich identyfikatorów użytkowników (w tym także ASI) prowadzoną przez ASI.
4. Identyfikator użytkownika składa się z takiej liczby znaków, jaka jest wymagana przez dany program/aplikację.
5. W przypadku zbieżności nadawanego identyfikatora z identyfikatorem wcześniej zarejestrowanego użytkownika nadaje się inny identyfikator dodając na końcu kolejną liczbę.

**§ 11**

1. **Hasło** powinno składać się z unikalnego zestawu co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.
2. Hasło nie może być identyczne z identyfikatorem użytkownika, ani z jego imieniem lub nazwiskiem.
3. Zmiana hasła następuje nie rzadziej niż co 30 dni. Odpowiedzialny za to jest każdy z użytkowników.
4. Przy pierwszym logowaniu do systemu użytkownik ma obowiązek zmienić hasło nadane przez ASI, czy też firmy obsługującej dany program/aplikację.
5. Zabrania się użytkownikom systemu udostępniania swojego identyfikatora i hasła innym osobom.
6. W przypadku utraty hasła użytkownik zobowiązany jest zgłosić się niezwłocznie do ASI w celu zmiany hasła.
7. Hasła użytkownika utrzymuje się w tajemnicy (nie powinny być nigdzie zapisywane), również po upływie ich ważności. Użytkownicy odpowiedzialni są za poufność swoich haseł.
8. Zabrania się zapamiętywania w programach mających taką możliwość (np. przeglądarki www) nazw użytkowników i haseł.
9. Jeśli występuje podejrzenie, że hasło zostało ujawnione, należy niezwłocznie je zmienić.
10. Jeśli użytkowany program/aplikacja określa bardziej rygorystyczne wymogi, aniżeli powyżej określone, to należy je zastosować.

**§ 12**

1. **Rozpoczęcie pracy w systemie** odbywa się poprzez:
   1) przygotowanie stanowiska pracy,
   2) włączenie stacji roboczej,
   3) wprowadzenie swojego identyfikatora i hasła.
2. Przed rozpoczęciem pracy na danym stanowisku komputerowym użytkownik zobowiązany jest do jego zweryfikowania w celu sprawdzenia, czy nie zostało ono naruszone lub wykorzystane przez osobę nie będącą jego użytkownikiem. W przypadku pojawienia się trudności w autoryzacji (logowaniu), pomimo prawidłowo podanej nazwy użytkownika i hasła, użytkownik zobowiązany jest skontaktować się z ASI. Jeżeli proces autoryzacji przebiegł prawidłowo, użytkownik może przystąpić do pracy.

**§ 13**

**Zawieszenie pracy w systemie** - w przypadku konieczności czasowego opuszczenia stanowiska pracy użytkownik jest zobowiązany zastosować zasady czystego biurka oraz czystego ekranu, blokując komputer poprzez wciśnięcie kombinacji klawiszy WIN+L lub Ctrl+Alt+Delete i wybranie opcji „Zablokuj ten komputer”.

**§ 14**

**Kończąc pracę**, użytkownik zobowiązany jest do:

1) zapisania danych w aplikacji i zamknięcia aplikacji,
2) wylogowania się z systemu i poczekania na jego wyłączenie, a następnie odłączenie urządzenia od zasilania,
3) sprawdzenia czy w drukarce nie pozostały wydruki,
4) umieszczenia w zamykanych na klucz szafach informatycznych nośników danych oraz dokumentów zawierających dane osobowe,
5) zamknięcia okien, wyłączenia wszystkich urządzeń elektrycznych (w tym również komputerowych), zgaszenia światła w pomieszczeniach oraz zamknięcia drzwi opuszczanego pomieszczenia.

**§ 15**

1. **Kopie zapasowe** tworzy się są na zewnętrznych dyskach lub płytach CD z następującą częstotliwością: jeden raz na miesiąc. Kopie roczne przechowywane są przez 5 lat.
2. ASI przegląda okresowo kopie awaryjne i ocenia ich przydatność do odtworzenia zasobów systemu w przypadku jego awarii.
3. Stwierdzenie utraty przez kopie awaryjne waloru przydatności do celu, o którym mowa w ust. 1 upoważnia ASI do ich zniszczenia.
4. Niszczenie kopii zawierających dane, jak również wszelkich innych nośników zawierających zapis cyfrowy dokonuje się w sposób uniemożliwiający ich odzyskanie.
5. Kopie zapasowe przechowywane są w pomieszczeniach innych aniżeli pomieszczenia przeznaczone do przechowywania zbiorów danych pozostających w bieżącym użytkowaniu. Kopie zapasowe przechowane są w zamykanych na klucz szafach w wyznaczonym obszarze przetwarzania. W miarę możliwości organizacyjnych kopie zapasowe przechowywane są w innym budynku.

**§ 16**

1. **Nośniki informatyczne** przechowywane są w miejscach, do których dostęp mają wyłącznie osoby upoważnione.
2. Nośniki z informacjami powinny być fizycznie chronione przed kradzieżą, zniszczeniem lub niewłaściwym używaniem.
3. Nośniki informatyczne zawierające dane osobowe powinny być opisane w sposób czytelny i zrozumiały dla użytkownika, a zarazem nie powinny ułatwiać rozpoznania zawartości przez osoby nieupoważnione.

**§ 17**

1. W pomieszczeniach, gdzie nie jest możliwe ograniczenie dostępu osób postronnych, **monitory stanowisk** dostępu do danych osobowych ustawia się w taki sposób, aby uniemożliwić tym osobom wgląd w dane.
2. Ekrany monitorów stanowisk dostępu do danych osobowych są zaopatrzone w wygaszacze z ustawioną opcją wymagania hasła, które po upływie maksymalnie 10 minut nieaktywności użytkownika automatycznie wyłączają funkcje eksploatacji ekranu.

**§ 18**

1. **Sprawdzanie obecności wirusów** komputerowych w systemie oraz ich usuwanie odbywa się przy wykorzystaniu licencjonowanego oprogramowania w oparciu o aktualną wersję oprogramowania.
2. Oprogramowanie, o którym mowa w ust. 1, sprawuje ciągły nadzór (ciągła praca w tle) nad pracą systemu i jego zasobami oraz serwerami i stacjami roboczymi.
3. Do obowiązków ASI należy poprawna konfiguracja automatycznej aktualizacji oprogramowania służącego do sprawdzania w systemie obecności wirusów komputerowych.
4. Na każdym stanowisku komputerowym musi być zainstalowane oprogramowanie antywirusowe.
5. Każdy e-mail wpływający do Szkoły musi być sprawdzony pod kątem występowania wirusów.
6. Zabrania się używania nośników niewiadomego pochodzenia bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje użytkownik, który nośnik zamierza użyć.
7. Zabrania się pobierania z Internetu plików niewiadomego pochodzenia. Każdy plik pobrany z Internetu musi być sprawdzony programem antywirusowym. Sprawdzenia dokonuje użytkownik, który pobrał plik.
8. Zabrania się odczytywania załączników poczty elektronicznej bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje pracownik, który pocztę otrzymał.
9. Kontrola antywirusowa przeprowadzana jest również na wybranych komputerach w przypadku zgłoszenia nieprawidłowości w funkcjonowaniu sprzętu komputerowego lub oprogramowania.
10. W przypadku wykrycia wirusów komputerowych sprawdzane jest stanowisko komputerowe, na którym wirusa wykryto.

**§ 19**

1. System i urządzenia informatyczne służące do przetwarzania danych osobowych, zasilane energią elektryczną, zabezpiecza się za pomocą odpowiednich urządzeń przed utratą danych osobowych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.
2. Minimalne zabezpieczenie systemu i urządzeń informatycznych, o których mowa w ust. 1, polega na wyposażeniu serwera oraz stacji roboczych w zasilacze awaryjne (UPS).

**§ 20**

1. Urządzenia informatyczne służące do przetwarzania danych osobowych dopiero po prawidłowym usunięciu tych danych oraz po uprzednim uzyskaniu zgody ASI lub Administratora można przekazać:
   a) do naprawy,
   b) do likwidacji,
   c) innemu podmiotowi.
2. Urządzenia, o których mowa w ust. 1, przed ich przekazaniem pozbawia się zapisu danych osobowych.
3. Jeżeli nie jest to możliwe, urządzenie to może być naprawiane wyłącznie pod nadzorem ASI lub osoby pisemnie upoważnionej przez Administratora.

4. Jeżeli nie jest możliwe pozbawienie urządzenia przekazywanego do likwidacji zapisu danych osobowych, urządzenie - przed przekazaniem - uszkadza się w sposób uniemożliwiający odczytanie tych danych.
5. Niesprawne urządzenia komputerowe, do czasu ich naprawienia lub zbycia, powierza się ASI zgodnie z przepisami o odpowiedzialności za mienie powierzone pracownikowi. Urządzenia te mają być przechowywane na terenie Szkoły.

**§ 21**

1. Przeglądu i konserwacji urządzeń dokonuje ASI doraźnie.
2. Przeglądu i sprawdzenia poprawności zbiorów danych zawierających dane osobowe dokonuje użytkownik przy współudziale ASI w miarę potrzeb.

**§ 22**

1. Przekazania i odbioru sprzętu komputerowego do i z serwisu może dokonywać wyłącznie ASI lub osoba przez niego upoważniona.
2. W przypadku przekazywania wraz z komputerem dokumentacji licencyjnej należy sporządzić protokół oddania do serwisu komputera wraz z dokumentacją. W protokole musi zostać wyszczególniona cała dokumentacja licencyjna przekazywana razem z komputerem. Protokół podpisuje osoba przekazująca i osoba przyjmująca do serwisu komputer wraz z dokumentacją. Na podstawie protokołu serwis bierze całkowitą odpowiedzialność za tę dokumentację. Z obowiązku sporządzenia dodatkowego protokołu obioru zwolnione jest oprogramowanie na licencji OEM.
3. W przypadku, kiedy na danym sprzęcie komputerowym przechowywane są istotne dla Szkoły dane, ASI dokonuje wymontowania stacjonarnego nośnika danych (dysk twardy), który nie jest przekazywany wraz ze sprzętem.
4. Serwis odpowiada w całości za ewentualną instalację oprogramowania dokonaną w ramach prac serwisowych.
5. Po odebraniu komputera z serwisu należy sprawdzić stan dokumentacji licencyjnej i zainstalowanego na nim oprogramowania ze stanem z momentu przed oddaniem do serwisu. Osobą odpowiedzialną za wykonanie powyższego zadania jest ASI. W przypadku stwierdzenia rozbieżności należy przywrócić stan z momentu przed oddaniem do serwisu.
6. Każde przeprowadzenie napraw serwisowych musi być dokumentowane.

**§ 23**

Do **przesyłania danych** przy połączeniach w sieci publicznej (Internet), z uwagi na przekazywane dane osobowe, powinny być wykorzystywane tylko kanały transmisji udostępniane przez ASI oraz dane osobowe muszą być szyfrowane.

**§ 24**

1. Osoby użytkujące **przenośne nośniki informatyczne**, służące do przetwarzania danych osobowych, obowiązane są niezwłocznie informować ASI o zakresie, rodzaju zbieranych danych osobowych oraz celu ich przetwarzania. ASI może żądać usunięcia danych, co do których zachodzi uzasadnione podejrzenie, że nie są przetwarzane zgodnie z zasadami określonymi w przepisach o ochronie danych osobowych lub niniejszej Procedury.
2. Zakazuje się przetwarzania danych osobowych na zewnętrznych nośnikach danych oraz ich przesyłania pocztą elektroniczną bez uprzedniego zaszyfrowania.

3. Na nośnikach, o których mowa w pkt 2, dopuszczalne jest przetwarzanie jedynie jednostkowych danych osobowych.
4. W przypadku posługiwania się nośnikami danych pochodzącymi od podmiotu zewnętrznego użytkownik jest zobowiązany do sprawdzenia go programem antywirusowym na wyznaczonym w tym celu stanowisku komputerowym oraz do oznakowania tego nośnika.
5. Nośniki magnetyczne raz użyte do przetwarzania danych osobowych nie mogą być wykorzystywane do innych celów mimo usunięcia danych.
6. Nośniki magnetyczne z zaszyfrowanymi jednostkowymi danymi osobowymi są na czas ich użyteczności przechowywane w zamkniętych na klucz szafach, a po wykorzystaniu dane na nich zawarte są trwale usuwane lub nośniki te są niszczone.

**§ 25**

1. **Przenośne stacje robocze** podlegają szczególnej ochronie. Ich używanie poza siedzibą Szkoły musi mieć uzasadnienie w realizowanych przez użytkownika zadaniach. Do przenośnych stacji roboczych zalicza się także telefon komórkowy, przy czym nie dotyczą go ograniczenia odnośnie użycia poza siedzibą Szkoły.
2. Przetwarzanie danych osobowych na przenośnych stacjach roboczych poza obszarem przetwarzania danych powinno być ograniczone do niezbędnych przypadków mających uzasadnienie w realizowanych przez użytkownika zadaniach i należy zapewnić szyfrowanie danych osobowych przetwarzanych na tych urządzeniach.
3. Każdy użytkownik, któremu powierzono urządzenie przenośne, przed rozpoczęciem użytkowania go poza siedzibą Szkoły, obowiązany jest do wystąpienia do ASI z prośbą o zapewnienie odpowiednich środków techniczno-organizacyjnych gwarantujących poufność i integralność przetwarzanych informacji. Do środków tych zalicza się np. zabezpieczenia kryptograficzne, ochronę antywirusową, a w przypadku telefonów komórkowych z dostępem do systemu informatycznego Szkoły - przynajmniej 4. znakowy kod PIN odblokowujący funkcje klawiszy i ekranu.
4. Osoba użytkująca przenośną stację roboczą, a w szczególności użytkująca przenośny komputer, służący do przetwarzania danych osobowych - obowiązana jest do ochrony urządzenia oraz zachowania szczególnej ostrożności podczas użytkowania, transportu lub przechowywania tego urządzenia poza Szkoły lub poza obszarem przetwarzania danych osobowych, a w szczególności zobowiązana jest do:
   - wykorzystywanie metod i środków uwierzytelniania w systemach informatycznych określonych w niniejszej Procedurze,
   - transportu urządzenia w sposób ograniczający powstanie ryzyka kradzieży lub zniszczenia,
   - korzystania z urządzenia w sposób uniemożliwiający osobom nieupoważnionym do wglądu w przetwarzane dane,
   - nie pozostawianie włączonego urządzenia bez uprzedniego zablokowania ekranu,
   - stosowania się do zakazu podłączania urządzeń poza służbowych do stacji roboczej bez wcześniejszego uzgodnienia z ASI,
   - bezwzględnego przestrzegania zakazu udostępniania takiego komputera osobom nieupoważnionym,
   - zabezpieczenia komputera w trakcie i po zakończeniu użytkowania przed negatywnym działaniem czynników zewnętrznych mogących spowodować uszkodzenie komputera lub utratę danych (wilgoć, wysoka temperatura, silne pole elektromagnetyczne),

- przechowywania komputera w sposób eliminujący powstanie ewentualnego incydentu bezpieczeństwa.

5. Użytkowanie takiego komputera poza obszarem przetwarzania danych może odbywać się wyłącznie przy zachowaniu zasad określonych w niniejszej Procedurze.
6. W razie utraty urządzenia (zagubienia, zniszczenia, kradzieży itp.) użytkownik, któremu powierzono komputer zobowiązany jest do natychmiastowego powiadomienia Administratora lub osoby uprawnionej zgodnie z zasadami zgłaszania naruszenia ochrony danych osobowych.
7. Zabrania się wykorzystywania przenośnych urządzeń do celów prywatnych.

**Zasady postępowania z przenośnymi pamięciami**

**§ 26**

1. Zapis danych osobowych na przenośnej pamięci (np. nośników typu „flash", pamięć typu „USB", przenośne dyski SSD lub HDD) jest dopuszczalny tylko w celu:
   - sporządzenia kopii zapasowej zgodnie z zasadami sporządzania kopii zapasowych,
   - wykonania obowiązku udostępnienia danych osobowych wynikającego z przepisów prawa lub umowy zawartej przez Administratora.
2. Osoba, której przydzielono przenośną pamięć lub przenośne urządzenie, obowiązana jest chronić je przed uszkodzeniem, utratą, kradzieżą oraz korzystaniem z niego przez osoby nieupoważnione, w tym także przez domowników.
3. Podczas korzystania z przenośnych pamięci w celu zapewnienia bezpieczeństwa ochrony danych należy stosować aplikację umożliwiającą szyfrowanie danych zawartych na przenośnej pamięci. Dostęp do zaszyfrowanych danych jest możliwy jedynie po wprowadzeniu wcześniej określonego hasła.
4. Jeżeli dane osobowe zapisane na przenośnej pamięci utracą przydatność do celu, w którym zostały zapisane, osoba, której przydzielono nośnik, niezwłocznie usuwa albo przekazuje w tym celu przenośną pamięć do Administratora.
5. Zasady przetwarzania danych osobowych na przenośnej pamięci: dane z przenośnej pamięci niebędących kopiami zapasowymi po wprowadzeniu do systemu informatycznego administratora powinny być trwale usuwane z tych nośników przez fizyczne zniszczenie (np. płyty CD-ROM) lub usunięcie danych programem trwale usuwającym pliki; uszkodzone nośniki przed ich wyrzuceniem należy zniszczyć fizycznie w niszczarce służącej do niszczenia nośników
6. Urządzenia przenośne oraz nośniki danych nie powinny być pozostawione bez nadzoru zarówno w Szkole, jak i w innych miejscach.
7. Nie należy pozostawiać bez kontroli dokumentów, nośników danych i urządzeń przenośnych zarówno w Szkole jak i w innych miejscach (w tym np. w samochodach).
8. Użytkownik przenośnego urządzenia zobowiązany jest do:
   1) sporządzania kopii zapasowych danych przetwarzanych na tym urządzeniu,
   2) niezwłocznego udostępnienia sprzętu do kontroli na wezwanie Administratora,
   3) niezwłocznego zwrotu sprzętu w razie zakończenia pracy u Administratora lub na żądanie Administratora.

**§ 27**

Osoby posiadające **karty mikroprocesorowe** zobowiązane są:

1. zgłosić ten fakt Administratorowi z poinformowaniem do czego służy karta (do podpisu elektronicznego, do logowania się do systemu itp.),

2. zachować szczególną ostrożność przy posługiwaniu się kartą w tym:
   a) nieudostępniania i niepozostawiania na widocznym miejscu PIN-u do karty,
   b) starannego zabezpieczenia karty przed kradzieżą,
3. w przypadku utraty (zgubienia, kradzieży, zniszczenia itp.) karty osoby są zobowiązane do niezwłocznego poinformowania o tym fakcie Administratora.

**§ 28**

Osoby przetwarzające dane osobowe przy pomocy edytorów tekstu, arkuszy kalkulacyjnych, baz danych itp. zobowiązane są:

1) w uzasadnionych przypadkach chronić dostęp do plików hasłem,
2) w przypadku przesyłania plików mailem pliki powinny być zabezpieczone hasłem lub zaszyfrowane.

**§ 29**

1. Użytkownik sporządzający **wydruki**, które zawierają dane osobowe jest odpowiedzialny za zachowanie szczególnej ostrożności przy korzystaniu z nich, a zwłaszcza za zabezpieczenie ich przed dostępem osób nieupoważnionych.
2. Zabrania się powtórnego używania do sporządzania brudnopisów pism jednostronnie zadrukowanych kart.
3. Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie. Nie należy pozostawiać takich wydruków (również w czasie dnia pracy np. na biurku) bez nadzoru osoby upoważnionej do ich przetwarzania ani też wynosić poza siedzibę Szkoły.

**Zasady postępowania w przypadku naruszenia lub podejrzenia naruszenia ochrony**

**§ 30**

1. Przed przystąpieniem do pracy osoba upoważniona zobowiązana jest dokonać sprawdzenia stanu urządzeń komputerowych oraz oględzin swojego stanowiska pracy, w tym zwrócić szczególną uwagę, czy nie zaszły okoliczności wskazujące na naruszenie lub próby naruszenia ochrony danych osobowych.
2. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych, użytkownik zobowiązany jest do bezzwłocznego powiadomienia o tym fakcie Administratora. Powyższy obowiązek ciąży również na pozostałych pracownikach Administratora. Wzór raportu o incydencie zawiera zał. nr 9.
3. Postanowienia ust. 2 mają zastosowanie zarówno w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych gromadzonych w systemach informatycznych, jak i w formie tradycyjnej.
4. Do Administratora zgłasza się w szczególności przypadki:
   a) użytkowania stacji roboczej przez osobę nie będącą użytkownikiem systemu,
   b) usiłowania logowania się do Systemu (sieci) przez osobę nieuprawnioną,
   c) usuwania, dodawania lub modyfikowania bez wiedzy i zgody użytkownika jego dokumentów,
   d) przebywania osób nieuprawnionych w obszarze, w którym przetwarzane są dane osobowe, w trakcie nieobecności osoby zatrudnionej przy przetwarzaniu tych danych i bez zgody administratora danych,
   e) pozostawiania bez nadzoru otwartych pomieszczeń, w których przetwarzane są dane osobowe,

f) udostępniania osobom nieuprawnionym stacji roboczej (w tym przenośnej), służącej do przetwarzania danych osobowych,
g) niezabezpieczenia hasłem dostępu do urządzenia służącego do przetwarzania danych osobowych,
h) przechowywania nośników informacji oraz wydruków z danymi osobowymi, nieprzeznaczonymi do udostępniania, w warunkach umożliwiających do nich dostęp osobom nieuprawnionym,
i) zagubienia lub kradzieży nośnika danych osobowych, lub urządzenia na którym zapisane są dane osobowe,
j) zagubienia lub kradzieży kart mikroprocesorowych.

5. Do czasu przybycia Administratora zgłaszający (zarówno w przypadku naruszenia, jak i w przypadku podejrzenia naruszenia ochrony danych):
   a) powstrzymuje się od rozpoczęcia lub kontynuowania pracy, jak również od podejmowania jakichkolwiek czynności mogących spowodować zatarcie lub naruszenie śladów bądź innych dowodów,
   b) zabezpiecza elementy systemu informatycznego lub dokumentacji, przede wszystkim poprzez uniemożliwienie dostępu do nich osobom nieupoważnionym,
   c) podejmuje, stosownie do zaistniałej sytuacji, wszelkie niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych.
6. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych Administrator po przybyciu na miejsce:
   a) ocenia zastałą sytuację, biorąc pod uwagę w szczególności stan pomieszczeń, w których przetwarzane są dane oraz stan urządzeń, a także identyfikuje wielkość negatywnych następstw incydentu,
   b) wysłuchuje relacji osoby, która dokonała powiadomienia,
   c) podejmuje decyzje o toku dalszego postępowania, stosownie do zakresu naruszenia lub zasadności podejrzenia naruszenia ochrony danych osobowych.
7. Administrator dokumentuje zastaną sytuację.
8. W przypadku naruszenia integralności bezpieczeństwa sieciowego, obowiązkiem ASI jest natychmiastowe wstrzymanie udostępniania zasobów dla użytkowników i odłączenie serwerów od sieci. ASI w porozumieniu z Administratorem ustalają przyczyny naruszenia integralności bezpieczeństwa sieciowego. Przywrócenie udostępniania zasobów użytkownikom może nastąpić dopiero po ustaleniu i usunięciu przyczyny naruszenia integralności bezpieczeństwa sieciowego.
9. Administrator podejmuje kroki zmierzające do likwidacji naruszeń zabezpieczeń danych osobowych i zapobieżenia wystąpieniu ich w przyszłości. W tym celu:
   a) w miarę możliwości przywraca stan zgodny z zasadami zabezpieczenia systemu,
   b) ile taka potrzeba zachodzi, wprowadza nowe formy zabezpieczenia oraz nadzoruje zaznajamianie z nimi osób upoważnionych do przetwarzania danych osobowych.
10. W przypadku, gdy naruszenie ochrony danych osobowych jest wynikiem uchybienia obowiązującej dyscypliny pracy, Administrator podejmuje stosowne działania wobec osób, które dopuściły się tego uchybienia.
11. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych, użytkownik może kontynuować pracę dopiero po otrzymaniu pozwolenia od Administratora.

**§ 31**

1. W przypadku zaginięcia urządzenia lub nośników, na których były zgromadzone dane osobowe, użytkownik systemu niezwłocznie powiadamia Administratora, a w przypadku kradzieży występuje o powiadomienie jednostki policji.
2. W sytuacji, o której mowa w ust. 1 Administrator, podejmuje niezbędne kroki do wyjaśnienia okoliczności zdarzenia, sporządza protokół, który powinna podpisać także osoba, której skradziono lub której zaginął sprzęt.
3. W przypadku kradzieży urządzenia razem z nośnikiem magnetycznym lub elektronicznym Administrator podejmuje działania zmierzające do odzyskania utraconych danych oraz monitoruje proces przebiegu wyjaśnienia sprawy.

**§ 32**

Osoba upoważniona do przetwarzania danych osobowych odpowiedzialna za naruszenie obowiązków wynikających z niniejszej Procedury ochrony oraz przepisów o ochronie danych osobowych ponosi odpowiedzialność przewidzianą w przepisach wewnętrznych Szkoły oraz w odpowiednich przepisach prawa.

**§ 33**

1. Jeśli naruszenie skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych to Administrator zgłasza naruszenie do organu nadzorczego i zawiadamia osoby, których dane dotyczą, o naruszeniu - zgodnie z odrębnymi przepisami.
2. Administrator prowadzi rejestr naruszeń wg wzoru z zał. nr 10.

**Postępowanie w wypadku klęski żywiołowej**

**§ 34**

1. Klęską żywiołową jest katastrofą spowodowaną działaniem sił przyrody, takich jak ogień, huragan, woda lub ich przejawami.
2. W przypadku wystąpienia zagrożenia powodującego konieczność przeprowadzenia ewakuacji osób lub mienia z pomieszczeń, w których przetwarzane są dane osobowe mają zastosowanie przepisy niniejszej Procedury oraz innych przepisów szczególnych.
3. Każda osoba, która będzie świadkiem zbliżania się lub działania zagrożeń określonych powyżej zobowiązana jest powiadomić Administratora w każdy możliwy sposób.
4. Numer telefonu Administratora jest znany pracownikom i osobom współpracującym.
5. Osoby biorące udział w akcji ratunkowej, mają prawo wejść do pomieszczeń, w których przetwarzane są dane osobowe bez dopełniania obowiązku posiadania upoważnienia.
6. W przypadku ogłoszenia alarmu ewakuacyjnego użytkownicy przebywający w pomieszczeniach, w których przetwarzane są dane osobowe obowiązani są do przerwania pracy, a w miarę możliwości przed opuszczeniem tych pomieszczeń do:
   a) zamknięcia systemu informatycznego,
   b) zabezpieczenia danych osobowych przetwarzanych tradycyjnie.
7. W czasie trwania akcji ratunkowej i po jej zakończeniu Administrator oraz obecni użytkownicy powinni w miarę możliwości zabezpieczać dane osobowe przed nieuprawnionym do nich dostępem, o ile nie stoi to w sprzeczności z poleceniami wydanymi przez służby ratunkowe.
8. Obowiązek ten ciąży w równym stopniu na innych pracownikach Administratora obecnych przy akcji ratunkowej.

**Niszczenie danych osobowych**

**§ 35**

1. Usuwanie danych osobowych, polega na:
   a) trwałym, fizycznym ich zniszczeniu wraz z ich nośnikami w stopniu uniemożliwiającym ich odtworzenie przez osoby niepowołane przy zastosowaniu powszechnie dostępnych metod,
   b) anonimizacji zbiorów danych osobowych polegającej na pozbawieniu danych osobowych, ich zbiorów – cech umożliwiających identyfikację osób fizycznych, których dane dotyczą.
2. Procedura niszczenia danych osobowych:
   a) niszczenie danych osobowych następuje wyłącznie na wniosek Administratora i w zgodzie z odrębnymi przepisami,
   b) sposób zniszczenia danych osobowych musi być odpowiednio dobrany do rodzaju nośnika danych oraz ich kategorii,
   c) niszczenie danych osobowych musi odbywać się komisyjnie, przy czym w komisji musi znajdować się Administrator (lub jego przedstawiciel),
   d) zniszczenie danych osobowych musi zostać potwierdzone spisaniem protokołu.
3. Usuwanie danych osobowych jest zależne od rodzaju nośnika, na którym są przechowywane.
   a) Dokumentacja tradycyjna (wydruki, notatki, dokumenty itd.) – przy użyciu niszczarki,
   b) Nośniki optyczne (płyty CD/DVD) – za pomocą niszczarek.
   c) Nośniki elektroniczne (pendrive/karty pamięci/dyski twarde SSD) – korzystając z jednej z dwóch metod:
      - niszczenie programowe – polegające na wielokrotnym nadpisywaniu danych na nośniku, które uniemożliwiają odczytanie danych,
      - niszczenie sprzętowe – polegające na trwałym zniszczeniu nośnika za pomocą odpowiednich urządzeń.
   d) Nośniki magnetyczne (dyskietki/dyski twarde HDD) – korzystając z jednej z trzech metod:
      - niszczenie programowe – polegające na wielokrotnym nadpisywaniu danych na nośniku, które uniemożliwiają odczytanie danych,
      - niszczenie sprzętowe – polegające na trwałym zniszczeniu nośnika za pomocą odpowiednich urządzeń, oprócz sposobów niszczenia danych dostępnych dla nośników elektronicznych,
      - demagnetyzacji nośników.

**Obsługa żądań i wniosków o dostęp do swoich danych**

**§ 36**

1. W przypadku wpływu do jednostki żądania/wniosku osoby, której dane dotyczą, w zakresie jej danych osobowych (do którego ma prawo w oparciu o przepisy Rozporządzenia) należy je przekazać do Administratora.
2. Jeżeli osoba odbierająca żądanie/wniosek ma uzasadnione wątpliwości co do tożsamości osoby fizycznej składającej żądanie/wniosek, powinna zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą.
3. Po konsultacji z IOD Administrator podejmuje odpowiednie działania celem spełnienia żądania/wniosku osoby, której dane dotyczą, bądź poinformowania osoby o nie podejmowaniu żądanych działań (wraz z uzasadnieniem i informacją o możliwości

wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem).
4. Odpowiedź na żądanie/wniosek osoby dokonywana jest przez Administratora w formie, w jakiej wpłynęło żądanie/wniosek (papierowej, bądź elektronicznej).
5. W sytuacji żądania/wniosku złożonego w formie ustnej, w celu odpowiedniego udokumentowania działań, należy poprosić osobę o podanie adresu na jaki należy wysłać odpowiedź na żądanie/wniosek.
6. Administrator prowadzi ewidencję żądań/wniosków (zał. nr 11).

**Udostępnianie danych**

**§ 37**

1. Dane osobowe mogą być udostępniane wyłącznie osobom upoważnionym.
2. Udostępnianie danych osobowych, w jakiejkolwiek postaci, jednostkom/osobom nieuprawnionym wymaga pisemnego upoważnienia Administratora.
3. Udostępnienie danych osobowych osobom nie może być realizowane drogą telefoniczną.
4. Udostępnienie danych osobowych może nastąpić wyłącznie po przedstawieniu wniosku (zał. nr 12).
6. Aplikacje wykorzystane do obsługi baz danych osobowych powinny zapewniać odnotowanie informacji o udzielonych odbiorcom danych. Zakres informacji powinien obejmować co najmniej: dane odbiorcy, datę wydania, zakres udostępnionych danych.
7. Administrator prowadzi Ewidencję udostępnień (zał. nr 13).

**Szkolenia**

**§ 38**

1. Każdy nowo zatrudniony pracownik przed otrzymaniem dostępu do przetwarzania danych osobowych musi zostać przeszkolony w zakresie przepisów o ochronie danych osobowych wraz z wynikającymi z nich zadaniami i obowiązkami przez IOD.
2. IOD będzie sporządzać informacje odświerzające wiedzę nt. ochrony informacji zwane biuletynem bezpieczeństwa. Informacje te przesyłane będą za pośrednictwem e-maili do pracowników.

**Ciągłość działalności**

**§ 39**

1. Administrator zapewnia minimalizację zakłóceń w realizacji działalności statutowej w związku z dysfunkcją systemu informatycznego Szkoły.
2. W przypadku zaistnienia zdarzeń mających wpływ (również potencjalny) na bezpieczeństwo informacji oraz ciągłość działania Szkoły należy podjąć działania określone w Procedurze pn. Plan ciągłości działania (zał. nr 14).
3. Za opracowanie, realizację i utrzymanie planu ciągłości działania odpowiedzialny jest ASI. Za realizację działań przewidzianych w tym planie odpowiedzialne są osoby w nim wskazane.

**Postanowienia końcowe**

**§ 40**

Niniejszy dokument oraz dokumenty z nim powiązane podlegają, nie rzadziej niż raz w roku, przeglądowi i w razie potrzeby aktualizacji wraz ze zmieniającymi się przepisami prawa oraz modyfikowane w celu dostosowania do zmieniającego się otoczenia.

Dyrektor ZSP nr 3 w Skidziniu
Urszula Bandoła