POLITYKA BEZPIECZEŃSTWA
OCHRONY I PRZETWARZANIA DANYCH OSOBOWYCH
W GIMNAZJUM Z ODDZIAŁAMI INTEGRACYJNYMI nr 7
im. CZESŁAWA MIŁOSZA w RYBNIKU
wydana dnia 01.01.2015r.
przez DYREKTORA SZKOŁY

ROZDZIAŁ I
Postanowienia ogólne

§ 1

Użyte w Polityce bezpieczeństwa określenia oznaczają:

1. **Zbiór danych osobowych** - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
2. **Administrator Danych Osobowych** - rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, o których mowa w art. 3, decydujące o celach i środkach przetwarzania danych osobowych.
3. **Administrator Bezpieczeństwa Informacji** - osoba wyznaczona przez administratora danych osobowych, odpowiedzialna za bezpieczeństwo danych osobowych, przetwarzanych zarówno w formie tradycyjnej jak i za pomocą systemów informatycznych.
4. **Administrator Systemu Informatycznego** - osoba odpowiedzialna za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego do przetwarzania danych osobowych (może to być administrator sieci lokalnej, systemu operacyjnego, bazy danych itp.).
5. **System informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
6. **Stacja robocza** – stacjonarny lub przenośny komputer wchodzący w skład systemu informatycznego umożliwiający użytkownikom systemu dostęp do danych osobowych znajdujących się w systemie.
7. **Bezpieczeństwo systemu informatycznego** - wdrożenie przez administratora danych osobowych lub osobę przez niego uprawnioną środków organizacyjnych i technicznych w celu zabezpieczenia oraz ochrony danych przed dostępem, modyfikacją, ujawnieniem, pozyskaniem lub zniszczeniem.
8. **Przetwarzanie danych osobowych** - wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie.
9. **Osoba upoważniona** - osoba posiadająca upoważnienie wydane przez Administratora Danych Osobowych (lub osobę uprawnioną przez niego) i dopuszczona jako użytkownik do przetwarzania danych osobowych w systemie informatycznym danej komórki organizacyjnej w zakresie wskazanym w upoważnieniu (listę osób

upoważnionych do przetwarzania danych osobowych posiada administrator bezpieczeństwa informacji w sytuacji kiedy zostanie powołany).

10. **Użytkownik systemu** - osoba posiadająca uprawnienia do przetwarzania danych osobowych w systemie informatycznym.
11. **Osoba uprawniona** - osoba posiadająca upoważnienie wydane przez administratora danych osobowych do wykonywania w jego imieniu określonych czynności.
12. **Ustawa** – ustawa z dnia 29 sierpnia 1997 r. o ochronie danych..
13. **Rozporządzenie** - rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

§ 2

1. Realizując Politykę bezpieczeństwa informacji zapewnia się ich:
    1. Poufność – informacja nie jest udostępniana lub ujawniana nieupoważnionym osobom, podmiotom i procesom.
    2. Integralność – dane nie zostają zmienione lub zniszczone w sposób nieautoryzowany.
    3. Dostępność – istnieje możliwość wykorzystania ich na żądanie, w założonym czasie, przez autoryzowany podmiot.
    4. Rozliczalność – możliwość jednoznacznego przypisania działań poszczególnym osobom.
    5. Autentyczność – zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana.
    6. Niezaprzeczalność – uczestnictwo w całości lub części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie jest niepodważalne.
    7. Niezawodność – zamierzone zachowania i skutku są spójne.

2. Polityka bezpieczeństwa i ochrony przetwarzania danych osobowych ma na celu zredukowanie możliwości wystąpienia negatywnych konsekwencji naruszeń w tym zakresie, tj.:
    1. Naruszeń danych osobowych rozumianych jako prywatne dobro powierzone podmiotowi.
    2. Naruszeń przepisów prawa oraz innych regulacji.
    3. Utraty lub obniżenia reputacji podmiotu.
    4. Strat finansowych ponoszonych w wyniku nałożonych kar.
    5. Zakłóceń organizacji pracy spowodowanych nieprawidłowym działaniem systemów.

§ 3

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, oprogramowanie systemowe, aplikacje oraz przez użytkowników.
2. Zastosowane zabezpieczenia gwarantują:
    1. poufność danych - rozumie się przez to właściwość zapewniającą, że dane nie są

udostępniane nieupoważnionym podmiotom,
2. integralność danych- rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
3. rozliczalność - rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,
4. integralność systemu- rozumie się przez to nienaruszalność systemu, niemożność jakiejkolwiek manipulacji,
5. uwierzytelnianie - rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

§ 4

Realizację zamierzeń określonych w § 3 ust. 2 powinny zagwarantować następujące założenia:

1. wdrożenie procedur określających postępowanie osób zatrudnionych przy przetwarzaniu danych osobowych oraz ich odpowiedzialność za bezpieczeństwo tych danych,
2. przeszkolenie użytkowników w zakresie bezpieczeństwa i ochrony danych osobowych,
3. przypisanie użytkownikom określonych atrybutów pozwalających na ich identyfikację (hasła, identyfikatory), zapewniających im dostęp do różnych poziomów baz danych osobowych – stosownie do indywidualnego zakresu upoważnienia,
4. podejmowanie niezbędnych działań w celu likwidacji słabych ogniw w systemie zabezpieczeń,
5. okresowe sprawdzanie przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych osobowych,
6. opracowanie procedur odtwarzania systemu w przypadku wystąpienia awarii,
7. śledzenie osiągnięć w dziedzinie bezpieczeństwa systemów informatycznych:
   - w miarę możliwości organizacyjnych i techniczno - finansowych,
   - wdrażanie nowych narzędzi i metod pracy oraz sposobów zarządzania systemami informatycznymi, które będą służyły wzmocnieniu bezpieczeństwa danych osobowych.

§ 5

1. Za naruszenie ochrony danych osobowych uważa się w szczególności:
   1. nieuprawniony dostęp lub próbę dostępu do danych osobowych lub pomieszczeń, w których się one znajdują,
   2. wszelkie modyfikacje danych osobowych lub próby ich dokonania przez osoby nieuprawnione (np. zmian zawartości danych, utrat całości lub części danych),
   3. naruszenie lub próby naruszenia integralności systemu,
   4. zmianę lub utratę danych zapisanych na kopiach zapasowych,
   5. naruszenie lub próby naruszenia poufności danych lub ich części,
   6. nieuprawniony dostęp (sygnał o nielegalnym logowaniu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu),
   7. udostępnienie osobom nieupoważnionym danych osobowych lub ich części,
   8. zniszczenie, uszkodzenie lub wszelkie próby nieuprawnionej ingerencji w systemy informatyczne zmierzające do zakłócenia ich działania bądź pozyskania w sposób

niedozwolony (lub w celach niezgodnych z przeznaczeniem) danych zawartych w systemach informatycznych lub kartotekach,

9. inny stan systemu informatycznego lub pomieszczeń niż pozostawiony przez użytkownika po zakończeniu pracy.

2. Za naruszenie ochrony danych osobowych uważa się również włamanie do budynku lub pomieszczeń, w których przetwarzane są dane osobowe lub próby takich działań.

ROZDZIAŁ II
Kompetencje i odpowiedzialność w zarządzaniu bezpieczeństwem danych osobowych

§ 6

Za przetwarzanie danych osobowych niezgodne z prawem, celami przetwarzania lub przechowywanie ich w sposób niezapewniający ochrony interesów osób, których te dane dotyczą grozi odpowiedzialność karna wynikająca z przepisów ustawy o ochronie danych osobowych lub pracownicza na zasadach określonych w Kodeksie pracy.

Administrator Danych Osobowych (ADO):

1. Formułuje i wdraża warunki techniczne i organizacyjne służące ochronie danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
2. Decyduje o zakresie, celach oraz metodach przetwarzania i ochrony danych osobowych.
3. Odpowiada za zgodne z prawem przetwarzanie danych osobowych.

Administrator Bezpieczeństwa Informacji (ABI):

1. Egzekwuje zgodnie z prawem przetwarzanie danych osobowych w imieniu ADO.
2. Wydaje upoważnienie do przetwarzania danych osobowych określając w nich zakres i termin ważności – wzór upoważnienia określa załącznik.
3. Prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych – wzór ewidencji określa załącznik.
4. Ewidencjonuje oświadczenia osób upoważnionych o zaznajomieniu się z zasadami zachowania bezpieczeństwa danych – wzór oświadczenia określa załącznik.
5. Określa potrzeby w zakresie stosowanych zabezpieczeń, wnioskuje do ADO o zatwierdzenie proponowanych rozwiązań i nadzoruje prawidłowość ich wdrożenia.
6. Bierze udział w podnoszeniu świadomości i kwalifikacji osób przetwarzających dane osobowe i zapewnia odpowiedni poziom przeszkolenia w tym zakresie.

Administrator Systemu Informatycznego (ASI):

1. Zarządza bezpieczeństwem przetwarzania danych osobowych w systemach informatycznych zgodnie z wymogami prawa i wskazówkami ABI.
2. Doskonali i rozwija metody zabezpieczenia danych przed zagrożeniami związanymi z ich przetwarzaniem.
3. Przydziela identyfikatory użytkownikom systemów informatycznych oraz zaznajamia ich z procedurami ustalania i zmiany haseł dostępu.
4. Nadzoruje prace związane z rozwojem, modyfikacją, serwisowaniem i konserwacją

systemu.

5. Zapewnia bezpieczeństwo wewnętrznego i zewnętrznego obiegu informacji w sieci i zabezpieczenie łączy zewnętrznych.
6. Prowadzi nadzór nad archiwizacją zbiorów danych oraz zabezpiecza elektroniczne nośniki informacji zawierających dane osobowe.

Pracownik przetwarzający dane:

1. Chroni prawo do prywatności osób fizycznych powierzających swoje dane osobowe poprzez przetwarzanie ich zgodnie z przepisami prawa oraz zasadami określonymi w polityce bezpieczeństwa i ochrony przetwarzania danych osobowych i instrukcji zarządzania systemem informatycznym.
2. Zapoznaje się z zasadami określonymi w polityce bezpieczeństwa i ochrony przetwarzania danych osobowych i instrukcji zarządzania systemem informatycznym oraz składa oświadczenie o znajomości zawartych w nich przepisów.

W przypadku, kiedy ADO nie powołuje ABI bądź ASI, wszystkie zapisy w dokumentacji, które odwołują się do ABI bądź ASI dotyczą ADO.

ROZDZIAŁ III
Zagrożenia bezpieczeństwa

§ 7

1. Charakterystyka możliwych zagrożeń:
   - **Zagrożenia losowe zewnętrzne** (np. klęski żywiołowe, przerwy w zasilaniu), których występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu.
   - **Zagrożenia losowe wewnętrzne** (np. niezamierzone pomyłki przetwarzających dane, pozostawienie danych lub pomieszczeń bez nadzoru, błędy operatorów systemu, awarie sprzętowe, błędy oprogramowania), przy których może dojść do zniszczenia danych lub naruszenia ich poufności.
   - **Zagrożenia zamierzone, świadome i celowe** - najpoważniejsze zagrożenia, gdzie występuje naruszenia poufności danych. Zagrożenia te możemy podzielić na: nieuprawniony dostęp z zewnątrz (włamanie), nieuprawniony dostęp do danych w wewnątrz (przez osoby nieuprawnione).

§ 8

1. Lista potencjalnych zagrożeń bezpieczeństwa danych:

Poniżej przedstawiono listy potencjalnych zagrożeń bezpieczeństwa danych z podziałem na zagrożenia miejsc przetwarzania oraz rodzajów danych, tj. zbiorów przetwarzanych tradycyjnie (papierowo) oraz z wykorzystaniem systemów informatycznych.

W każdym przypadku, w sytuacji stwierdzenia wystąpienia któregokolwiek z zagrożeń należy niezwłocznie powiadomić Administratora danych.

1. **Zagrożenia miejsc przetwarzania danych:**

   - Włamania od strony okien – wybite szyby, niedomknięte skrzydła.
   - Włamania od strony drzwi – zerwane plomby, uszkodzone klamki, źle działające zamki, niedomknięte drzwi, ślady po narzędziach.
   - Oddziaływanie czynników zewnętrznych – wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana.
   - Pozostawienie niezamkniętych drzwi lub okien –w pomieszczeniu nie pozostają osoby uprawnione do przetwarzania danych.
   - Pozostawienie bez nadzoru osób nieuprawnionych do przebywania w pomieszczeniach.

2. **Zagrożenia związane z tradycyjnym przetwarzaniem danych:**

   - Pozostawienie danych na biurkach, półkach, regałach, itp. po zakończeniu pracy.
   - Pozostawienie dokumentów zawierających dane osobowe w kserokopiarce lub skanerze.
   - Pozostawienie po zakończeniu pracy otwartych szaf, w których gromadzone są dane osobowe.
   - Przechowywanie dokumentów w miejscach do tego nieprzeznaczonych.
   - Wyrzucanie dokumentów w stopniu zniszczenia umożliwiającym ich odczytanie.
   - Przetwarzanie danych przez osoby nieuprawione.
   - Nieuzasadnione sporządzanie kserokopii danych.

3. **Zagrożenia związane z przetwarzaniem danych za pomocą systemów informatycznych:**

   - Dopuszczenie zapisywania na nośniki zewnętrzne wynoszone poza obszar przetwarzania lub przesyłanie poprzez Internet danych niezaszyfrowanych.
   - Dopuszczanie do nieuzasadnionego kopiowania dokumentów i utraty kontroli nad kopią.
   - Sporządzanie kopii danych w sytuacjach nieprzewidzianych procedurą.
   - Utrata kontroli nad kopią danych osobowych.
   - Podmiana lub zniszczenie nośników z danymi osobowymi.
   - Pozostawienie zapisanego hasła dostępu do bazy danych.
   - Samodzielne instalowanie jakiegokolwiek oprogramowania.
   - Obecność nowych programów w komputerze lub inne zmiany w konfiguracji oprogramowania.
   - Opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji umożliwiającej dostęp do bazy danych osobowych.
   - Odczytywanie dyskietek i innych nośników przed sprawdzeniem ich programem antywirusowym.
   - Niezabezpieczenie komputera zasilaczem awaryjnym podtrzymującym napięcie na wypadek braku zasilania.
   - Dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania osób nieuprawnionych.

- Ujawnianie sposobu działania aplikacji oraz jej zabezpieczeń osobom niepowołanym.
- Ujawnianie informacji o sprzęcie i pozostałej infrastrukturze informatycznej.
- Dopuszczenie, aby inne osoby odczytywały zawartość ekranu monitora, na którym wyświetlane są dane osobowe.
- Pojawianie się komunikatów alarmowych.
- Awarie sprzętu i oprogramowania, które mogą wskazywać na działanie osób trzecich.
- Nieoczekiwane, nie dające się wyjaśnić, zmiany zawartości bazy danych.
- Niezapowiedziane zmiany w wyglądzie lub zachowaniu aplikacji służącej do przetwarzania danych osobowych.
- Próba nieuzasadnionego przeglądania danych w ramach pomocy technicznej.
- Dopuszczanie, aby osoby inne niż ASI lub osoby przez ASI uprawnione, podłączały jakikolwiek urządzenia, demontowały elementy sieci lub dokonywały innych manipulacji.
- Ślady manipulacji przy układach sieci komputerowej lub komputerach.
- Obecność nowych urządzeń i kabli o nieznanym przeznaczeniu i pochodzeniu.
- Naruszenie dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji.

§ 9

1. Przedsięwzięcia zabezpieczające przed naruszeniem ochrony danych osobowych:

Na podstawie przeprowadzonej charakterystyki możliwych zagrożeń podjęto zabezpieczenia, które powinny bezpośrednio oddziaływać na procesy przetwarzania danych, Administrator danych wprowadza określone poniżej środki organizacyjne:

- Przetwarzanie danych osobowych w placówce może odbywać się wyłącznie w ramach wykonywania zadań służbowych. Zakres uprawnień wynika z zakresu tych zadań.
- Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych.
- Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające stosowne upoważnienie. Wzór upoważnienia stanowi do niniejszej dokumentacji.
- Unieważnienie upoważnienia następuje na piśmie.
- Każdy pracownik placówki musi odbyć szkolenie z zakresu ochrony danych osobowych. Nowo przyjęty pracownik odbywa szkolenie przed przystąpieniem do przetwarzania danych.
- Ponadto każdy upoważniony do przetwarzania danych potwierdza pisemnie fakt zapoznania się z niniejszą dokumentacją i zrozumieniem wszystkich zasad bezpieczeństwa.
- Nie należy gromadzić w podręcznej dokumentacji danych osobowych. W wszystkie dane niezbędne do prawidłowej pracy powinny znajdować się w zbiorach. Jeżeli posiadane druki lub zestawienia są niezbędne należy je zanonimizować (usunąć dane osobowe, np. adres, pesel, pozostawiając tylko nazwiska, imiona itd.).

- Dokumenty zawierające dane osobowe należy niszczyć w specjalistycznych niszczarkach.

- Każdorazowe zbieranie danych zgodnie z art. 24 oraz 25 ustawy o ochronie danych osobowych rodzi obowiązek informacyjny. Obowiązek należy realizować umieszczając odpowiednią treść informacyjną pod formularzem z danymi.
- Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.
- Dokumenty w wersji elektronicznej, które zapisywane są na nośniki zewnętrzne, przenoszone poza Placówkę lub przesyłane pocztą elektroniczną, należy zabezpieczyć poprzez nadanie im haseł odczytu.
- Zbiory osobowe przetwarzane elektronicznie należy zabezpieczać poprzez wykonywanie kopii bezpieczeństwa, zapisywanych na zewnętrznych nośnikach i przechowywanych pod zamknięciem.
- Pliki edytorów tekstu lub arkuszy kalkulacyjnych należy traktować jak kopie zbiorów, z których pochodzą przetwarzane w nich dane i odpowiednio zabezpieczać stosując wytyczne zawarte w Instrukcji zarządzania systemem informatycznym będącej częścią niniejszej dokumentacji.

§ 10

Wykaz potencjalnych środków technicznych stosowanych w celu ochrony danych osobowych.

1. **Ogólna ochrona budynku** – alarm antywłamaniowy, całodobowy dozór służb ochrony, gaśnice lub systemy p-poż.
2. **Zabezpieczenia okien** – pomieszczenia zlokalizowane na parterze lub wyższych kondygnacjach można dodatkowo zabezpieczyć poprzez montaż krat, rolet lub szyb antywłamaniowych, zwłaszcza, jeśli istnieje do nich dostęp przez tarasy, dachy niższych budynków, drabiny p-poż, itp.
3. **Zabezpieczenie drzwi** – w zależności od kategorii danych i zagrożeń można stosować drzwi tradycyjne zamykane na klucz lub p-pożarowe, zaś w miejscach szczególnie narażonych na zagrożenia (drzwi wejściowe, sekretariaty, księgowość, archiwa, itp.) **można** stosować drzwi antywłamaniowe.
4. **Zabezpieczenia zbiorów tradycyjnych (papierowych)** – w zależności od kategorii danych i zagrożeń do przechowywania danych można stosować szafy tradycyjne zamykane na klucz, szafy metalowe lub sejfy (dla danych szczególnie ważnych). Dane przeznaczone do zniszczenia **należy** niszczyć w specjalistycznych niszczarkach.
5. **Zabezpieczenia zbiorów elektronicznych** – dane elektroniczne **należy** zabezpieczyć poprzez wyposażenie komputerów w zasilacze awaryjne podtrzymujące napięcie na wypadek braku zasilania oraz w systemy antywirusowe. Kopie danych **należy** gromadzić w szafach metalowych lub sejfach ognioodpornych.

Lista zastosowanych w placówce środków technicznych, dobrana odpowiednio do istniejących zagrożeń znajduje się w załączniku do niniejszego dokumentu.

ROZDZIAŁ IV
Przetwarzanie danych osobowych

§ 11

1. Przetwarzanie danych osobowych z użyciem stacjonarnego sprzętu komputerowego oraz kartotek odbywa się wyłącznie na obszarze wyznaczonym przez Administratora Danych Osobowych.
2. Przetwarzanie danych osobowych za pomocą urządzeń przenośnych może odbywać się poza obszarem przetwarzania danych wyłącznie za zgodą Administratora Danych Osobowych czy też Administratora Bezpieczeństwa Informacji w przypadku, gdy został powołany.
3. Szczegółowy wykaz pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe określa załącznik Nr 1 do Polityki bezpieczeństwa.

§ 12

W celu ograniczenia dostępu osób postronnych do pomieszczeń, w których zlokalizowano przetwarzanie danych osobowych, należy zapewnić, aby:

1. Pomieszczenia, w których znajdują się serwery były wyposażone w sprawne systemy ochrony przeciwwłamaniowej.
2. Pracownicy Administratora Danych Osobowych oraz pracownicy ochrony są zobowiązani do przestrzegania zasad określających dopuszczalne sposoby przemieszczania się osób trzecich w obrębie pomieszczeń, w których przetwarzane są dane osobowe.
3. Przebywanie osób trzecich w pomieszczeniach może odbywać się wyłącznie w obecności użytkowników lub za zgodą Administratora Danych Osobowych.

§ 13

1. Stały dostęp do pomieszczeń, w których przetwarzane są dane osobowe, mają tylko użytkownicy oraz informatyk.
2. Dostęp do pomieszczeń, w których przetwarzane są dane osobowe, osób innych, niż wymienione w ust. 1, jest możliwy wyłącznie w obecności, co najmniej jednego użytkownika lub za zgodą Administratora Danych Osobowych.
3. Zakaz wyrażony w ust. 2 dotyczy innych, niż określeni w ust. 1, pracowników Administratora Danych Osobowych oraz pracowników służb technicznych, porządkowych, itp.
4. Przebywanie użytkownika po godzinach pracy w pomieszczeniach, w których przetwarzane są dane osobowe jest dopuszczalne jedynie za zgodą dyrektora szkoły.

§ 14

W trakcie prac technicznych wykonywanych przez osoby trzecie w pomieszczeniach, przetwarzanie danych jest zabronione.

§ 15

1. Administrator Danych Osobowych czy też Administrator Bezpieczeństwa Informacji

w przypadku, gdy został wyznaczony, jest odpowiedzialny za całość zagadnień dotyczących ochrony i bezpieczeństwa danych osobowych.

2. W celu sprawnego wykonywania swoich zadań Administrator Bezpieczeństwa Informacji jest uprawniony do wnioskowania do Administratora Danych Osobowych w celu wyznaczania użytkownikom wykonywania określonych zadań.
3. Użytkownicy zobowiązani są do przestrzegania przepisów o ochronie danych osobowych na terenie szkoły, a także do ścisłej współpracy z Administratorem Danych Osobowych czy też Administratorem Bezpieczeństwa Informacji w przypadku, gdy został wyznaczony. W tym celu zobowiązani są do:
   1. pisemnego wnioskowania o rejestrację nowych zbiorów danych osobowych,
   2. okresowego składania pisemnej informacji z przebiegu bieżącej kontroli i oceny funkcjonowania mechanizmów zabezpieczeń i ochrony,
   3. występowania z wnioskami w sprawie wprowadzenia niezbędnych zmian w zakresie ochrony danych osobowych.

§ 16

Szczegółowy wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do ich przetwarzania określa załącznik Polityki.

§ 17

Opis struktury zbiorów danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych określa załącznik Polityki.

Rozdział V
Kontrola przestrzegania zasad zabezpieczenia ochrony danych osobowych

§ 18

1. Administrator Danych Osobowych, który może zlecić Administrator Bezpieczeństwa Informacji sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych.
2. Administrator Danych Osobowych lub Administrator Bezpieczeństwa Informacji, czyli osoba przez niego wyznaczona dokonuje okresowych kontroli i oceny funkcjonowania mechanizmów zabezpieczeń oraz przestrzegania zasad postępowania w przypadku naruszenia ochrony danych osobowych.
3. Przedmiotem kontroli, o których mowa w ust. 2 powinno być w szczególności:
   1. Funkcjonowanie zabezpieczeń systemowych.
   2. Prawidłowość funkcjonowania mechanizmów kontroli dostępu do zbioru danych.
   3. Funkcjonowanie zastosowanych zabezpieczeń fizycznych.
   4. Zasady przechowywania kartotek.
   5. Zasady i sposoby likwidacji oraz archiwizowania zbiorów archiwalnych.
   6. Realizacja procedur wdrożonych przez Administratora Danych Osobowych w zakresie ochrony danych.

4. Administrator Danych Osobowych, który może zlecić to Administratorowi Bezpieczeństwa Informacji prowadzi rejestr dokonywanych kontroli oraz ustaleń, wniosków i zaleceń z nich wynikających, a także nadzoruje ich wykonywanie.
5. Z kontroli, o których mowa w ust. 2 należy sporządzać protokoły, które przechowuje

Administrator Danych Osobowych lub Administrator Bezpieczeństwa Informacji w przypadku, gdy został powołany.

Rozdział VI
Postępowanie w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych

§ 19

1. Przed przystąpieniem do pracy użytkownik obowiązany 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 Danych Osobowych lub Administratora Bezpieczeństwa Informacji, jeżeli został powołany.
3. Obowiązek określony w ust. 2 ciąży równie na pozostałych pracownikach Administratora Danych Osobowych.
4. Postanowienia ust. 2 i 3 mają zastosowanie zarówno w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych gromadzonych w systemach informatycznych, jak i w kartotekach.

§ 20

1. Do czasu przybycia Administratora Danych Osobowych czy też Administrator Bezpieczeństwa Informacji (w sytuacji, gdy został powołany), zgłaszający:
   1. Powstrzymuje się od rozpoczęcia lub kontynuowania pracy, jak również od podejmowania jakichkolwiek czynności, mogących spowodować zatarcie śladów naruszenia bądź innych dowodów.
   2. Zabezpiecza elementy systemu informatycznego lub kartotek, przede wszystkim poprzez uniemożliwienie dostępu do nich osób nieupoważnionych.
   3. Podejmuje, stosownie do zaistniałej sytuacji, wszelkie niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych.

2. Postanowienia ust. 1 mają zastosowanie zarówno w przypadku naruszenia, jak i w przypadku podejrzenia naruszenia ochrony danych.

§ 21

W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych, Administrator Danych Osobowych lub Administrator Bezpieczeństwa Informacji w przypadku, gdy został powołany, po przybyciu na miejsce:

1. 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.
2. Wysłuchuje relacji osoby, która dokonała powiadomienia.
3. Podejmuje decyzje o toku dalszego postępowania, stosownie do zakresu naruszenia

lub zasadności podejrzenia naruszenia ochrony danych osobowych.

W uzasadnionych przypadkach niezwłocznie powiadamia Administratora Danych Osobowych.

§ 22

1. Administrator Danych Osobowych lub Administrator Bezpieczeństwa Informacji w przypadku, gdy został wyznaczony sporządza z przebiegu zdarzenia raport, w którym powinny się znaleźć w szczególności informacje o:
   1. Dacie i godzinie powiadomienia.
   2. Godzinie pojawienia się w pomieszczeniach, w których przetwarzane są dane.
   3. Sytuacji, jaką zastał.
   4. Podjętych działaniach i ich uzasadnieniu.

2. Kopia raportu przekazywana jest bezzwłocznie Administratora Danych Osobowych tylko w przypadku, gdy raport sporządził Administrator Bezpieczeństwa Informacji.

§ 23

1. Administrator Danych Osobowych lub osoba przez niego wyznaczona, czyli Administrator Bezpieczeństwa Informacji podejmuje kroki zmierzające do likwidacji naruszeń zabezpieczeń danych osobowych i zapobieżenia wystąpieniu ich w przyszłości. W tym celu:
   1. W miarę możliwości przywraca stan zgodny z zasadami zabezpieczenia systemu.
   2. W przypadku, gdy na miejscu zdarzenia znajduje się Administrator Bezpieczeństwa Informacji, zobowiązany jest przekazać raport o zaistniałej sytuacji do Administratora Danych Osobowych.
   3. O ile taka potrzeba zachodzi, postuluje wprowadzenie nowych form zabezpieczenia, a w razie ich wprowadzenia nadzoruje zaznajamianie z nimi osób zatrudnionych przy przetwarzaniu danych osobowych.

2. W przypadku, gdy naruszenie ochrony danych osobowych jest wynikiem uchybienia obowiązującej u Administratora Danych Osobowych dyscypliny pracy, Administrator Bezpieczeństwa Informacji, jeżeli został powołany wnioskuje do Administratora Danych Osobowych o wyjaśnienie wszystkich okoliczności incydentu i o podjęcie stosownych działań wobec osób, które dopuściły się tego uchybienia.

§ 24

W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych, użytkownik może kontynuować pracę dopiero po otrzymaniu pozwolenia od Administratora Danych Osobowych lub Administratora Bezpieczeństwa Informacji w przypadku, gdy został wyznaczony.

§ 25

1. W przypadku zaginięcia komputera lub nośników magnetycznych, na których były zgromadzone dane osobowe, użytkownik posługujący się komputerem niezwłocznie powiadamia Administratora Danych Osobowych lub Administratora Bezpieczeństwa

Informacji, a w przypadku kradzieży występuje o powiadomienie jednostki policji.

2. W sytuacji, o której mowa w ust. 1 Administrator Danych Informacji lub upoważniona przez niego osoba, czyli Administrator Bezpieczeństwa Informacji podejmuje niezbędne kroki do wyjaśnienia okoliczności zdarzenia, sporządza protokół z zajęcia, który powinna podpisać także osoba, której skradziono lub, której zaginął sprzęt oraz powiadamia Administratora Danych Osobowych.
3. W przypadku kradzieży komputera razem z nośnikiem magnetycznym Administrator Danych Osobowych lub Administrator Bezpieczeństwa w przypadku, gdy został wyznaczony podejmuje działania zmierzające do odzyskania utraconych danych oraz nadzoruje proces przebiegu wyjaśnienia sprawy.

§ 26

Osoba zatrudniona przy przetwarzaniu danych osobowych za naruszenie obowiązków wynikających z niniejszej Polityki bezpieczeństwa oraz przepisów o ochronie danych osobowych ponosi odpowiedzialność przewidzianą w Regulaminie pracy, Kodeksie pracy oraz wynikając z ustawy o ochronie danych osobowych.

Rozdział VII
Postępowanie w wypadku klęski żywiołowej

§ 27

Klęską żywiołową jest katastrofa, spowodowana działaniem sił przyrody takich jak ogień, huragan, woda lub ich przejawami.

§ 28

W przypadku wystąpienia zagrożenia powodującego konieczność przeprowadzenia ewakuacji osób lub mienia z pomieszczeń, w których przetwarzane są dane osobowe, mają zastosowanie przepisy niniejszego rozdziału oraz innych przepisów szczególnych.

§ 29

1. O zagrożeniu, jego skali i podjętych krokach zaradczych pracownik ochrony zobowiązany jest niezwłocznie powiadomić Administratora Danych Osobowych w każdy możliwy sposób. W razie niemożności skontaktowania się z nim pracownik ochrony zawiadamia, co najmniej jedną z niej wymienionych osób:
    1. Administratora Bezpieczeństwa Informacji w przypadku, gdy został wyznaczony.
    2. Administratora Danych Osobowych.

2. Numery telefonów Administratora Danych Osobowych i Administratora Bezpieczeństwa Informacji w przypadku, gdy został wyznaczony, z którymi należy się kontaktować na wypadek klęski żywiołowej powinny być znane pracownikom.

§ 30

Osoby biorące udział w akcji ratunkowej, mają prawo wejść do pomieszczeń, w których przetwarzane są dane osobowe bez dopełniania obowiązku, o którym mowa w § 14 ust.2 Polityki.

§ 31

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:

1. Zamknięcia systemu informatycznego.
2. Zabezpieczenia danych osobowych gromadzonych w kartotekach.

§ 32

1. W czasie trwania akcji ratunkowej i po jej zakończeniu Administrator Danych Osobowych czy też Administrator Bezpieczeństwa Informacji, jeżeli został wyznaczony oraz obecni użytkownicy powinni, w miarę możliwości, zabezpieczać dane osobowe przed nieuprawnionym do nich dostępem.
2. Obowiązek ten ciąży w równym stopniu na innych pracownikach Administratora Danych Osobowych, obecnych przy akcji ratunkowej.

ROZDZIAŁ VIII
Niszczenie danych osobowych

§ 33

Ustawa o ochronie danych osobowych nakłada na podmioty zobowiązane do jej stosowania obowiązek należytego przetwarzania takich danych, tak, aby spełniony został podstawowy cel ustawy w postaci zapewnienia każdemu ochrony dotyczących go danych osobowych. **Jednym z obowiązków** administratora danych osobowych w zakresie ich przetwarzania **jest ich usuwanie w momencie, kiedy ustanie celowość ich przetwarzania zgodnie z wytycznymi wynikającymi z odrębnych ustaw.**

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 danych osobowych, zbiorów polegającej na pozbawieniu danych osobowych, ich zbiorów – cech umożliwiających identyfikację osób fizycznych, których dane dotyczą.

W zależności od nośnika, na którym przechowywane są dane osobowe, ich usuwanie polega na:

1. Dokumentacja tradycyjna (wydruki, notatki, dokumenty) – należy dokumentację zniszczyć bądź zanonimizować w sposób uniemożliwiający odczyt. Zgodnie z obowiązującą normą **DIN 66399** opracowaną przez *Standards Committee for Information Technology and Applications* (*Komitet Normalizacyjny ds. Technik Informacyjnych i ich Zastosowań*) niszczarki stosowane do niszczenia danych osobowych powinny spełniać poniższe wymagania:

- **Klasa B**: Ochrona przeznaczona dla danych poufnych, przeznaczonych dla wąskiego grona odbiorców.

    - ✓ **Stopień 3**: Nośniki z danymi chronionymi i poufnymi, a także danymi osobowymi, które wymagają większej ochrony - kategoria P-3 dla papieru.
    - ✓ **Stopień 4**: Nośniki z danymi szczególnie chronionymi i poufnymi, a także z danymi osobowymi, które podlegają większej ochronie, takie jak dane wrażliwe - kategoria P-4 dla papieru.

2. Nośniki optyczne (płyty CD/DVD/BLU-RAY – Analogicznie do dokumentacji tradycyjnej, należy w taki sposób zniszczyć nośnik, aby uniemożliwić odczytanie danych z płyty. W tym przypadku również zalecane jest wykorzystanie niszczarek spełniających wymagania:

    - **Klasa B**: Ochrona przeznaczona dla danych poufnych, przeznaczonych dla wąskiego grona odbiorców.

        - ✓ **Stopień 3**: Nośniki z danymi chronionymi i poufnymi, a także danymi osobowymi, które wymagają większej ochrony - kategoria O-3 dla płyt CD/DVD/BLU-RAY.
        - ✓ **Stopień 4**: Nośniki z danymi szczególnie chronionymi i poufnymi, a także z danymi osobowymi, które podlegają większej ochronie, takie jak dane wrażliwe - kategoria O-4 dla płyt CD/DVD/BLU-RAY.

3. Nośniki elektroniczne (pendrive/karty pamięci/dyski twarde SSD) – obecnie istniejące sposoby niszczenia danych można podzielić na dwie główne grupy metod:

    - niszczenie programowe – polegające na wielokrotnym nadpisywaniu danych na nośniku, które uniemożliwiają odczytanie danych. Istnieje specjalne oprogramowanie dostępne na rynku służące do nadpisywania (definitywnego usuwania) danych. Wadą tej metody jest możliwość częściowego odzyskania danych za pomocą specjalistycznego oprogramowania, zaletą natomiast możliwość ponownego wykorzystania nośnika,
    - niszczenie sprzętowe – polegające na trwałym zniszczeniu nośnika za pomocą odpowiednich urządzeń. Wadą tej metody jest brak możliwości ponownego wykorzystania nośnika, zaletą natomiast całkowity brak możliwości nawet częściowego odzyskania danych.

4. Nośniki magnetyczne (dyskietki/dyski twarde HDD) – oprócz sposobów niszczenia danych dostępnych dla nośników elektronicznych, istnieje również możliwość demagnetyzacji nośników, jako jednego z rodzajów niszczenia sprzętowego.

Niezależnie od nośnika, na którym są przechowywane dane osobowe przeznaczone do zniszczenia, samo ich zniszczenie powinno odbyć się komisyjnie, a z samej operacji powinien zostać sporządzony protokół.

§ 34

Procedura niszczenia danych osobowych:

1. Niszczenie danych osobowych ma na celu zniszczenie danych zawartych na nośniku, w celu uniemożliwienia identyfikacji osób, których dane osobowe będą niszczone.
2. Niszczenie danych osobowych następuje wyłącznie na wniosek Administratora Danych Osobowych lub Administratora Bezpieczeństwa Informacji.
3. Sposób zniszczenia danych osobowych musi być odpowiednio dobrany do rodzaju nośnika danych oraz ich kategorii.
4. Niszczenie danych osobowych musi odbywać się komisyjnie, przy czym w komisji musi znajdować się Administrator Danych Osobowych lub Administrator Bezpieczeństwa Informacji.
5. Zniszczenie danych osobowych musi zostać potwierdzone spisaniem protokołu.

ROZDZIAŁ IX
Postanowienia końcowe

§ 35

Polityka jest dokumentem wewnętrznym i nie może być udostępniania osobom nieupoważnionym w żadnej formie.

§ 36

1. Każda osoba przetwarzająca dane osobowe zobowiązane jest do zapoznania się z treścią Polityki bezpieczeństwa oraz Instrukcji zarządzania systemem Informatycznym.
2. Użytkownik zobowiązany jest złożyć oświadczenie, o tym, i został zaznajomiony z przepisami ustawy o ochronie danych osobowych, wydanymi na jej podstawie aktami wykonawczymi, obowiązującą Polityką bezpieczeństwa oraz Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.
3. Oświadczenia przechowywane są w aktach personalnych pracownika.

§ 37

1. W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie przepisy ustawy o ochronie danych osobowych oraz wydanych na jej podstawie aktów wykonawczych.
2. Użytkownicy zobowiązani są do bezwzględnego stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce.