Polityka bezpieczeństwa przetwarzania danych osobowych w Przedszkolu „Echa Leśne”

§1
Definicje

1. Użyte w niniejszym dokumencie pojęcia oznaczają:
   a) **Organizacja –** nazwa i siedziba Organizacji
   b) **Administrator danych osobowych (ADO)** – nazwa i siedziba Organizacji
   c) **Administrator Systemu Informatycznego (ASI)** – osoba odpowiedzialna za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego do przetwarzania danych osobowych.
   d) **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
   e) **Stacja robocza** – stacjonarny lub przenośny komputer wchodzący w skład systemu informatycznego umożliwiający Użytkownikom systemu dostęp do danych osobowych znajdujących się w systemie.
   f) **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.
   g) **Przetwarzanie danych osobowych** – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich 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.
   h) **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 w zakresie wskazanym w upoważnieniu (listę osób upoważnionych do przetwarzania danych osobowych posiada administrator danych osobowych).
   i) **Użytkownik systemu (Użytkownik)** – osoba posiadająca uprawnienia do przetwarzania danych osobowych w systemie informatycznym.
   j) **Osoba uprawniona** – osoba posiadająca upoważnienie wydane przez Administratora danych osobowych do wykonywania w jego imieniu określonych czynności.
   k) **RODO** - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem

danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

§2
Zasady ogólne

1. W celu zapewnienia ochrony przetwarzanych danych osobowych, zarówno za pomocą systemów informatycznych jak i w wersji papierowej, Administrator wdraża niniejszą politykę bezpieczeństwa.
2. Administrator dokłada należytej staranności w celu ochrony interesów osób, których dane osobowe dotyczą, w szczególności jest obowiązany zapewnić, aby dane były:
    a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą – zgodnie z zasadą zgodności z prawem, rzetelności i przejrzystości;
    b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami – zgodnie z zasadą ograniczenia celu;
    c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane – zgodnie z zasadą minimalizacji danych;
    d) prawidłowe i w razie potrzeby uaktualniane – zgodnie z zasadą prawidłowości;
    e) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane – zgodnie z zasadą ograniczenia przechowywania;
    f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem – zgodnie z zasadą integralności i poufności.
3. Administrator deklaruje pełne zaangażowanie i determinację celem zapewnienia bezpieczeństwa przetwarzanych danych osobowych, a także prawidłowego zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych.
4. Administrator nadzoruje jakie dane, kiedy i przez kogo zostały do zbiorów Administratora wprowadzone, bądź z tych zbiorów usunięte oraz komu są przekazywane.
5. Administrator w miarę uzasadnionych potrzeb dostosowuje systemy informatyczne służące do przetwarzania danych i wszelkie systemy zabezpieczeń przetwarzania danych osobowych do wymogów określonych w RODO.
6. Ochrona danych osobowych przetwarzanych w Organizacji obowiązuje wszystkie osoby, które mają dostęp do informacji zbieranych, przetwarzanych oraz przechowywanych w Organizacji, bez względu na zajmowane stanowisko oraz miejsce wykonywania jak również charakter stosunku pracy.
7. Zobowiązuje się wszystkie osoby posiadające upoważnienie do przetwarzania danych osobowych, nadane przez Administratora danych osobowych, do bezwzględnego przestrzegania podanych w niniejszym dokumencie reguł i zasad tworzących Politykę

bezpieczeństwa oraz stosowania niezbędnych środków zapobiegających ujawnieniu tych danych osobom nieupoważnionym.

8. Zachowanie tajemnicy obowiązuje zarówno podczas trwania stosunku pracy jak i po jego ustaniu.
9. Polityka bezpieczeństwa w zakresie ochrony danych osobowych w Organizacji odnosi się do danych osobowych przetwarzanych w zbiorach danych:
    a. tradycyjnych, w szczególności w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych,
    b. w systemach informatycznych, także w przypadku przetwarzania danych poza zbiorem danych osobowych.
10. Organizacja jest odpowiedzialna za tworzenie, wdrażanie, administrację i interpretację Polityki bezpieczeństwa informacji, standardów, zaleceń oraz procedur.
11. Organizacja deklaruje, że będzie stale doskonaliła i rozwijała organizacyjne, techniczne oraz informatyczne środki ochrony danych osobowych przetwarzanych zarówno metodami tradycyjnymi jak i elektronicznie tak, aby skutecznie zapobiegać ewentualnym zagrożeniom.

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe

1. Wykaz pomieszczeń przeznaczonych do przetwarzania danych:
    a) Siedziba Organizacji – wydzielone pomieszczenia, znajdujące się w budynku przy ul. Janowskiego 50 w Warszawie oraz w budynku przy ul. Świderskiej 109H w Warszawie
    b) Biuro Księgowe
2. W szczególnych przypadkach możliwe jest przetwarzanie danych osobowych poza wyznaczonym obszarem (np. na komputerach przenośnych), jednak wymaga to zgody indywidualnej ADO.

§4
Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

1. Wykaz zbiorów osobowych wraz ze wskazaniem programów komputerowych służących do ich przetwarzania:

    a) *Zbiór dzieci*
    b) *Zbiór przedstawicieli ustawowych dziecka*
    c) *Zbiór pracowników*

2. Z uwagi na połączenie komputerów z siecią Internet, dla zbiorów przetwarzanych elektronicznie stosuje się środki bezpieczeństwa na poziomie **WYSOKIM**.

§5

Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przy przetwarzaniu danych

1. Organizacja realizując Politykę w zakresie bezpieczeństwa ochrony danych osobowych stosuje odpowiednie środki informatyczne, techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności:

   a) w obszarze przetwarzania danych osobowych mogą przebywać wyłącznie pracownicy zatrudnieni przy przetwarzaniu danych, osoby zainteresowane przetwarzanymi danymi, Administrator Systemu Informatycznego oraz inne osoby indywidualnie upoważnione do tego przez Administratora danych osobowych. Przebywanie osób nieuprawnionych do dostępu do danych osobowych w pomieszczeniach znajdujących się wewnątrz obszaru przetwarzania tych danych, jest dopuszczalne tylko w obecności i pod nadzorem osoby upoważnionej do przetwarzania danych osobowych,
   b) dostęp do danych osobowych i ich przetwarzanie bez odrębnego upoważnienia ADO lub upoważnionej przezeń osoby może mieć miejsce wyłącznie w przypadku działań podmiotów upoważnionych na mocy odpowiednich przepisów prawa do dostępu i przetwarzania danych określonej kategorii,
   c) ADO prowadzi **ewidencję osób upoważnionych** i na jej podstawie przygotowuje **Upoważnienia do przetwarzania danych,**
   d) do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające stosowne **upoważnienie,**
   e) każdy pracownik Organizacji musi zapoznać się z zasadami ochrony danych osobowych przed przystąpieniem do przetwarzania danych, co potwierdza podpisując stosowne oświadczenie. Za powyższe działania odpowiedzialny jest ADO,
   f) zastosowano poniższe środki techniczne:
      - Sieć wewnętrzna podłączona jest do sieci Internet poprzez firewall typu UTM (firewall, IPS, IDS i antywirus), przez który dostęp do usług z wewnątrz sieci będzie kontrolowany na podstawie pochodzenia z danego fragmentu logicznego sieci oraz usługi, do której kierowane jest żądanie.
      - Użytkownicy końcowi korzystają z komputerów stacjonarnych lub laptopów z systemem Windows. Nie mają oni możliwości konfiguracji systemu (praw administracyjnych), instalacji aplikacji ani żadnej innej ingerencji w system

operacyjny mogącej wpłynąć na poziom bezpieczeństwa danych na nim przechowywanych. Wszystkie dane poza plikami systemowymi są przechowywane w folderach sieciowych, do których dostęp jest ograniczony tylko do użytkowników uprawnionych. W przypadku komputerów stacjonarnych nie ma możliwości logowania lokalnego do systemu operacyjnego poza siecią firmową. Na laptopach dane na dyskach są szyfrowane w celu uniknięcia ewentualnej utraty wrażliwych danych w przypadku straty urządzenia. Wszystkie systemy operacyjne są wyposażone w oprogramowanie antywirusowe, pakiet biurowy oraz oprogramowanie służące wykonywaniu tylko i wyłącznie czynności służbowych.

§6

Obowiązki Administratora Danych Osobowych

1. ADO zobowiązany jest do zapewnienia, aby dane osobowe były:
    a. przetwarzane zgodnie z prawem,
    b. zbierane dla oznaczonych, zgodnych z prawem celów,
    c. przetwarzane merytorycznie poprawne i adekwatne w stosunku do celów.
2. ADO odpowiada za bezpieczeństwo danych osobowych w systemie informatycznym, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe, oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń.
3. ADO opracowuje procedurę postępowania w przypadku naruszenia ochrony danych osobowych, przeznaczoną dla osób zatrudnionych przy przetwarzaniu tych danych.
4. ADO opracowuje procedurę obsługi praw osób, których dane dotyczą.
5. ADO określa budynki, pomieszczenia lub części pomieszczeń, tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego.
6. ADO prowadzi ewidencję osób uprawnionych do przetwarzania danych osobowych w poszczególnych systemach.
7. ADO organizuje szkolenia mające na celu zaznajomienie każdej osoby przetwarzającej dane osobowe z przepisami dotyczącymi ich ochrony.
8. ADO odpowiada za to, by zakres czynności osoby zatrudnionej przy przetwarzaniu danych osobowych określał odpowiedzialność tej osoby za:
    a. ochronę danych przed niepowołanym dostępem,
    b. nieuzasadnione modyfikacje lub zniszczenie danych,
    c. nielegalne ujawnienie danych,

    w stopniu odpowiednim do zadań realizowanych w procesie przetwarzania danych osobowych.
9. ADO nadzoruje przestrzeganie instrukcji określającej sposób zarządzania systemem informatycznym.

10. ADO nadzoruje właściwe zabezpieczanie sprzętu oraz pomieszczeń, w których przetwarzane są dane osobowe.
11. ADO nadzoruje wykorzystywane w Organizacji oprogramowanie oraz jego legalność.
12. ADO przeciwdziała dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe.
13. ADO podejmuje odpowiednie działania w celu właściwego zabezpieczenia danych.
14. ADO bada ewentualne naruszenia w systemie zabezpieczeń danych osobowych.
15. ADO podejmuje decyzje o instalowaniu nowych urządzeń oraz oprogramowania wykorzystywanego do przetwarzania danych osobowych.
16. ADO sprawuje nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych zawierających dane osobowe.
17. ADO sprawuje nadzór nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności.
18. ADO jest odpowiedzialny za wdrożenie szkoleń z zakresu przepisów dotyczących ochrony danych osobowych oraz środków technicznych i organizacyjnych przy przetwarzaniu danych w systemach informatycznych.
19. ADO sporządza plany kontroli zatwierdzane oraz przeprowadza zgodnie z nimi kontrole.
20. ADO sporządza raporty z naruszenia bezpieczeństwa systemu informatycznego.

§7
Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych

1. Określanie sposobów przetwarzania odbywa się przy wdrożeniu odpowiednich środków technicznych i organizacyjnych, takich jak m.in. pseudonimizacja, zaprojektowanych w celu skutecznej realizacji zasad ochrony danych określonych w RODO, w szczególności dotyczących zabezpieczeń oraz ochrony praw osób, których dane dotyczą.
2. Zasady określone w §7 ust. 1 niniejszej Polityki stosuje się również w czasie samego przetwarzania danych osobowych.
3. Wdrożenie zasad o których mowa w ustępach poprzedzających odbywa się przy uwzględnieniu stanu wiedzy technicznej, kosztu wdrażania oraz charakteru, zakresu, kontekstu i celów przetwarzania oraz ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikającego z przetwarzania.
4. ADO wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie dane

osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych.

5. Realizując zasady domyślnej ochrony danych osobowych w szczególności zapewnia się, aby wszelkie zgody osób fizycznych realizowane były w sposób dobrowolny, konkretny, świadomy oraz jednoznacznie okazujący wolę. Zakazane jest stosowanie domyślnie zaznaczonych pól zgody.
6. Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, ADO przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę.

§8
Postanowienia końcowe

1. Zgłoszenia wnoszone przez podmioty, których dane są przetwarzane przez Organizację realizowane są według postanowień Procedury realizacji praw osób, których dane dotyczą.
2. W przypadku stwierdzenia sytuacji naruszenia ochrony danych osobowych stosuje się Procedurę postępowania w przypadku naruszenia ochrony danych osobowych.

Załącznik nr 1 - Instrukcja zarządzania systemem informatycznym

Instrukcja zarządzania systemem informatycznym zwana dalej: „Instrukcją”, opisuje sposoby nadawania uprawnień Użytkownikom, określa sposób pracy w systemie informatycznym, procedury zarządzania oraz czynności mające wpływ na zapewnienie bezpieczeństwa systemu informatycznego.

Sposoby nadawania uprawnień i ich rejestrowania w systemach informatycznych

1. Każdy pracownik przed przystąpieniem do przetwarzania danych powinien zapoznać się z Polityką bezpieczeństwa przetwarzania danych osobowych, podpisać stosowne oświadczenie i uzyskać upoważnienie od ADO.
2. Przyznanie uprawnień w zakresie dostępu do systemu informatycznego polega na wprowadzeniu do systemu dla każdego Użytkownika unikalnego identyfikatora, hasła oraz zakresu dostępnych danych i operacji.
3. Wniosek o przyznanie uprawnień do systemu składa przełożony pracownika.
4. Użytkownik jest zobligowany podczas pierwszego logowania się w systemie do zmiany hasła ustanowionego podczas przyznawania uprawnień przez ASI na indywidualne.
5. Użytkownik ma prawo do wykonywania tylko tych czynności, do których został upoważniony.
6. Użytkownik ponosi pełną odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu.
7. Zabrania się Użytkownikom udostępniania identyfikatora, hasła i stacji roboczej osobom postronnym.
8. Przełożony pracownika jest zobligowany do niezwłocznego powiadomienia ASI o utraceniu uprawnień przez danego Użytkownika. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych należy niezwłocznie zablokować w systemie informatycznym oraz unieważnić hasło.
9. Identyfikator Użytkownika nie może być zmieniany bez wyraźnej przyczyny, a po wyrejestrowaniu Użytkownika z systemu informatycznego nie może zostać przydzielany innej osobie.

Zasady posługiwania się hasłami

1. Zabrania się zapisywania haseł w sposób umożliwiający wykorzystanie ich przez osoby postronne.
2. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie. W sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, pracownik zobowiązany jest do natychmiastowej zmiany hasła i poinformowania o zaistniałym fakcie ADO.
3. Przy wyborze hasła obowiązują następujące zasady:
    a. minimalna długość hasła - 8 znaków,
    b. zakazuje się stosować haseł, które Użytkownik:
        i. stosował uprzednio,
        ii. swojego identyfikatora w jakiejkolwiek formie,

iii. swojego imienia, drugiego imienia, nazwiska, przezwiska, pseudonimu w jakiejkolwiek formie,
iv. imion (w szczególności imion osób z najbliższej rodziny),
v. ogólnie dostępnych informacji o Użytkowniku (numer telefonu, numer rejestracyjny samochodu, numeru PESEL, itp.)
vi. przewidywalnych sekwencji znaków z klawiatury, takich jak np. „QWERTY”,”12345” itp.

c. należy stosować: hasła zwierające kombinacje liter i cyfr, hasła zawierające znaki specjalne: (.,();’@, #, & itp.) o ile system informatyczny i oprogramowanie na to pozwala.

4. Zmiany hasła nie wolno zlecać innym osobom.
5. W przypadku zagubienia/zapomnienia hasła Użytkownik musi skontaktować się z ASI w celu uzyskania nowego hasła.
6. Hasła w systemie informatycznym są przechowywane w postaci nie jawnej uniemożliwiającej odczytanie tej informacji przez osoby postronne.

Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie

1. Rozpoczęcie pracy w systemie komputerowym wymaga zalogowania się do stacji roboczej (dostęp kontrolowany przez usługę Active Directory), a następnie do systemu przy użyciu indywidualnego identyfikatora oraz hasła dostępu.
2. Przed opuszczeniem stanowiska pracy należy zablokować stację roboczą (poprzez wygaszacz ekranu) lub wylogować się z oprogramowania i systemu operacyjnego.
3. Przed wyłączeniem komputera należy bezwzględnie zakończyć prace uruchomionych programów, wylogować się z systemu operacyjnego i wykonać zamknięcie systemu.
4. Niedopuszczalne jest wyłączanie komputera przed zamknięciem oprogramowania i systemu operacyjnego.

Zabezpieczenia

1. Monitory komputerów, na których odbywa się przetwarzanie danych osobowych muszą być zlokalizowane w sposób uniemożliwiający osobom trzecim podgląd wyświetlanych danych. Konfiguracja wyświetlania obrazu na monitorach komputerów musi zawierać włączenie wygaszacza ekranu po zadanym czasie (5 minut), powrót do pracy po okresie bezczynności wymaga podania hasła dostępu (np. hasło wygaszacza ekranu).
2. W celu ochrony antywirusowej stosuje się oprogramowanie antywirusowe z codzienną aktualizacją baz wirusów. ASI przeprowadza cykliczne kontrole antywirusowe na wszystkich komputerach - minimum co trzy miesiące.
3. Zabrania się stosowania nośników niewiadomego pochodzenia bez wcześniejszego sprawdzenia ich programem antywirusowym. Za skanowanie odpowiedzialny jest użytkownik stacji roboczej.
4. Poczta elektroniczna jest automatycznie sprawdzana przez skaner antywirusowy.
5. Wykrycie wirusa Użytkownik stacji roboczej ma obowiązek zgłosić natychmiast ASI.
6. W celu zabezpieczenia danych systemu informatycznego wykonuje się kopie zapasowe zgodnie z polityką zarządzania kopiami zapasowymi stanowiącą **Załącznik nr 2** do Polityki ochrony danych osobowych.

7. W przypadku konieczności przechowywania wydruków zawierających dane osobowe należy je przechowywać w miejscu uniemożliwiającym dostęp osobom nieuprawnionym.
8. W przypadku stwierdzenia uszkodzenia urządzenia, dyski i inne informatyczne nośniki danych zawierające dane osobowe przed ich przekazaniem w celu naprawy innemu podmiotowi pozbawiane są zawartości.
9. W przypadku likwidacji urządzenia, dyski i inne informatyczne nośniki danych zawierające dane osobowe są uszkadzane w sposób uniemożliwiający odczytanie danych.
10. Naprawa wymienionych urządzeń zawierających dane osobowe, jeżeli nie można danych usunąć, wykonywana jest pod nadzorem ASI.

Załącznik nr 2 – Polityka zarządzania kopiami zapasowymi

§1

1. Osobą odpowiedzialną za wykonywanie działań określonych w niniejszej polityce jest Administrator Systemu Informatycznego (ASI).
2. ASI wyznacza osobę upoważnioną do wykonywania działań określonych w niniejszej polityce w jego imieniu (dalej: „Osoba Wyznaczona")
3. ASI zapewnia, aby urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, zasilane energią elektryczną, były zabezpieczone przed utratą tych danych wskutek awarii zasilania lub zakłóceń w sieci zasilającej. Zabezpieczenie powinno być tak skonstruowane, aby umożliwiało zapisanie danych we wszystkich uruchomionych aplikacjach i wykonanie kopii zapasowych.

§2

1. Kopie zapasowe należy odpowiednio zabezpieczyć przed nieuprawnionym dostępem lub uszkodzeniem.
2. Kopie zapasowe należy wykonywać codziennie w dni robocze.
3. Tworzenie kopii zapasowych odbywa się poprzez *automatyczne zgranie danych.*
4. Kopie zapasowe należy opisywać w sposób pozwalający na określenie ich zawartości.
5. Kopie zapasowe należy przechowywać w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych eksploatowane na bieżąco.
6. Kopie zapasowe należy przechowywać w sejfie lub w przypadku braku takiej możliwości w odpowiednich, przeznaczonych do tego zamkniętych szafach, znajdujących się w pomieszczeniach, które są zamykane na klucz.
7. Kopie zapasowe należy okresowo sprawdzać pod kątem ich dalszej przydatności do odtworzenia danych w przypadku awarii systemu oraz bezzwłocznie usuwać po ustaniu ich użyteczności.
8. Kopie zapasowe, które uległy uszkodzeniu lub stały się niepotrzebne należy pozbawić zapisu danych w sposób uniemożliwiający ich odtworzenie.
9. Jeżeli pozbawienie zapisu nie jest możliwe, kopie zapasowe należy zniszczyć w sposób uniemożliwiający odczytanie bądź odtworzenie danych zawartych na nośniku kopii.
10. Okres przechowywania kopii zapasowych zawierających dane osobowe powinien być ustalony przez osobę kierującą komórką organizacyjną Administratora, w której te dane są przetwarzane i przekazany do Osoby Wyznaczonej.
11. Kopie zapasowe zawierające dane osobowe, dla których cel przetwarzania ustał, powinny być pozbawiane zapisu tych danych a w przypadku gdy nie jest to możliwe, należy je zniszczyć w sposób uniemożliwiający odczytanie/odzyskanie danych osobowych.

§3

1. Wydruki komputerowe z systemu zawierające dane osobowe, należy sporządzać jedynie dla celów operacyjnych.
2. Wydruk komputerowy z systemu, zawierający dane osobowe, podlega zasadom ochrony danych osobowych przetwarzanych metodami tradycyjnymi.
3. Wydruki ze zbiorów danych osobowych tworzone i używane do celów roboczych, (operacyjnych) należy przechowywać w odpowiednich, przeznaczonych do tego zamykanych szafach.
4. Likwidację wydruków z systemu, zawierających dane osobowe należy przeprowadzić się za pomocą niszczarki do dokumentów lub w inny sposób, trwale uniemożliwiający odczytanie danych.
5. Z urządzeń, dysków lub innych nośników informatycznych, które zostały przeznaczone do przekazania innemu podmiotowi, należy usunąć zapisane na nich dane osobowe.

§4

1. Ochronę antywirusową należy realizować poprzez zainstalowanie odpowiedniego oprogramowania antywirusowego na komputerach.
2. W przypadku wykrycia wirusa komputerowego, użytkownik systemu zobowiązany jest do natychmiastowego poinformowania o tym fakcie Osobę Wyznaczoną lub ASI.
3. System informatyczny podlega regularnej (co najmniej raz w tygodniu) kontroli pod kątem obecności wirusów komputerowych.
4. Wykryte zagrożenia należy usunąć niezwłocznie z systemu informatycznego.
5. Przed przystąpieniem do unieszkodliwienia wirusa, należy zabezpieczyć dane zawarte w systemie przed ich utratą.

§5

1. Okres przechowywania nośników elektronicznych zawierających dane osobowe powinien być ustalony przez osobę kierującą komórką organizacyjną Administratora, w której te dane są przetwarzane.
2. Na każdym nośniku powinna być odnotowywana data maksymalnego okresu przechowywania np. data ustania celu przetwarzania danych osobowych.
3. Nośniki elektroniczne zawierające dane osobowe, dla których cel przetwarzania ustał powinny być pozbawiane zapisu tych danych, a w przypadku gdy nie jest to możliwe, należy je zniszczyć w sposób uniemożliwiający odczytanie/odzyskanie danych osobowych.
4. W przypadku przekazywania urządzeń lub nośników zawierających dane osobowe, w tym dane szczególnej kategorii, poza obszar przetwarzania danych osobowych,

zabezpiecza się je w sposób zapewniający poufność, integralność i rozliczalność tych danych, przez co rozumie się:

a) ograniczenie dostępu do danych osobowych hasłem zabezpieczającym dane przed osobami nieupoważnionymi;
b) stosowanie metod kryptograficznych;
c) stosowanie odpowiednich zabezpieczeń organizacyjnych;
d) stosowanie odpowiednich zabezpieczeń fizycznych;
e) stosowanie kombinacji wyżej wymienionych zabezpieczeń.