Dokument	Polityka bezpieczeństwa danych osobowych				
Obszar zastosowania	Dokument ma zastosowanie do ochrony danych osobowych przetwarzanych w SP ZOZ MSWiA w Koszalinie				
Data ostatniej weryfikacji	14.12.2020	Zatwierdzony	20.05.2018	Liczba stron	**74**
Zatwierdził:	**Elżbieta Czeszewska**	Data	20.05.2018	Podpis	
Sporządził:	**Bernard Pacewicz**	Data	09.05.2018	Podpis	
Opracowano na podstawie	Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.				

Historia zmian

Nr wersji	Data	Autor	Opis zmian

Spis treści.

I. Postanowienia ogólne.

1.1. Polityka bezpieczeństwa przetwarzania danych osobowych w **SP ZOZ MSWiA w Koszalinie** zwaną dalej „Polityką" została ustanowiona z związku z art. 24 ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE -zwanym dalej RODO.

1.2. Celem Polityki jest zapewnienie ochrony danych osobowych przetwarzanych przez **SP ZOZ MSWiA w Koszalinie** zwanej dalej, jako **SPZOZ** przed wszelakiego rodzaju zagrożeniami, tak wewnętrznymi jak i zewnętrznymi, świadomymi lub nieświadomymi.

1.3. Polityka opisuje reguły dotyczące bezpieczeństwa danych osobowych przetwarzanych zarówno w formie tradycyjnej, np. w postaci teczek, akt czy wydruków oraz w systemach informatycznych służących do przetwarzania danych osobowych w **SPZOZ.**

1.4. Dokument ten ustanawia minimalne standardy ochrony danych osobowych oraz procedury postępowania i działania, które należy stosować, aby właściwie wykonać obowiązki Administratora Danych Osobowych w zakresie zabezpieczenia danych osobowych, o których mowa w RODO.

1.5. Zastosowane zabezpieczenia mają zapewnić:

a) poufność danych – rozumianą, jako właściwość polegająca na tym, że dane osobowe nie są udostępniana ani ujawniana nieautoryzowanym osobom, podmiotom lub procesom;
b) integralności danych – rozumianą, jako właściwość polegającą na tym, że dane osobowe nie zostały zmodyfikowane lub zniszczone w sposób nieuprawniony;
c) dostępność danych – rozumianą, jako właściwość polegającą na tym, że informacja jest możliwa do wykorzystania przez uprawniony podmiot na jego żądanie, w założonym czasie;

d) autentyczność danych – rozumianą, jako właściwość polegającą na tym, że pochodzenie lub zawartość danych opisujących obiekt są takie, jak deklarowane;
e) rozliczalność danych - rozumianą, jako właściwość pozwalająca przypisać określone działanie osoby w sposób jednoznaczny tej osobie oraz umiejscowić je w czasie;
f) niezaprzeczalność – rozumianą, jako brak możliwości zanegowania swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie;

1.6. Bezpieczeństwo danych osobowych przetwarzanych w **SPZOZ** jest **przedmiotem szczególnej troski kierownictwa** i wszelkie naruszenia ustanowionych zasad bezpieczeństwa będą spotykać się ze zdecydowaną reakcją przewidzianą w procedurach prawnych i dyscyplinarnych.

1.7. **SPZOZ** zobowiązuje się do podjęcia odpowiednich kroków, mających na celu zapewnienie prawidłowej ochrony danych osobowych, w szczególności do zapewnienia, że przez cały okres ich przetwarzania, dane będą:
1) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;
2) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;
3) adekwatne, stosownie oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;
4) prawidłowe i w razie potrzeby uaktualnianie;
5) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania;
6) zabezpieczone środkami technicznymi i organizacyjnymi, które zapewniają rozliczalność, integralność oraz poufność danych.

1.8. Zasady określone w niniejszej Polityce oraz w dokumentach powiązanych powinny być znane i stosowane przez wszystkie osoby, które biorą udział w procesie przetwarzania danych osobowych w **SPZOZ**, bez względu na zajmowane stanowisko, jak również charakter stosunku pracy.

1.9. Osoby mające dostęp do danych osobowych są zobligowane do stosowania niezbędnych środków zapobiegających ujawnieniu tych informacji osobom nieupoważnionym.

1.10. Zachowanie tajemnicy obowiązuje zarówno podczas trwania stosunku pracy jak i po jego ustaniu.

1.11. Żadne odstępstwa od zasad bezpieczeństwa przedstawionych w przedmiotowym dokumencie nie są dopuszczalne bez uzyskania zgody Administratora Danych Osobowych.

1.12. Wszelkie wątpliwości dotyczące sposobu interpretacji zapisów niniejszego dokumentu, powinny być rozstrzygane na korzyść zapewnienia możliwie najwyższego poziomu ochrony danych osobowych oraz zapewnienie praw i wolności osób fizycznych, których dane są przetwarzane.

II. Definicje.

2.1. Użyte w niniejszej Polityce pojęcia są wspólne dla wszystkich dokumentów powiązanych z niniejszą Polityką oraz dla wszystkich pozostałych dokumentów, które zostały przyjęte , w zakresie ochrony danych osobowych.

1) **Administrator Danych Osobowych (ADO)** - należy przez to rozumieć działalność SPZOZ Diecezji Koszalińsko-Kołobrzeskiej, która ustala cele i sposoby przetwarzania danych osobowych, i jest reprezentowana przez Dyrektor Elżbietę Czeszewską;
2) **Administrator Systemu Informatycznego (ASI)** - należy przez to rozumieć osobę wyznaczoną przez ADO, będącą odpowiedzialną za poprawne funkcjonowanie, zabezpieczenie oraz nadzór nad infrastrukturą i systemami informatycznymi służącymi do przetwarzania danych osobowych w SPZOZ. Dopuszcza się, aby funkcje ASI realizował podmiot zewnętrzny;
3) **aktywa -** zasoby niezbędne do realizacji czynności związanych z operacjami przetwarzania danych osobowych tj. procesy, informacje, personel, sprzęt, oprogramowanie, sieć, siedziba;
4) **analiza ryzyka** – systematyczne podejście mające na celu zidentyfikowanie w systemie źródeł ryzyka i przypisanie zidentyfikowanym ryzykom wartości;
5) **dane osobowe** - oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”);
6) **grupa aktywów** - zbiór aktywów rozpatrywanych wspólnie ze względu na podobny charakter i funkcjonalność**;**
7) **incydent** – zamierzone lub przypadkowe naruszenie środków technicznych i organizacyjnych zastosowanych w celu ochrony danych osobowych. Następuje w szczególności, gdy stan urządzenia, zawartości informacji, ujawnione metody pracy, sposób działania programu lub jakości komunikacji w sieci teleinformatycznej mogą wskazywać na naruszenie bezpieczeństwa danych osobowych;
8) **Inspektor Ochrony Danych (IOD)** – należy przez to rozumieć wyznaczoną osobę przez ADO, odpowiedzialną za nadzorowanie stosowanych środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszenia bezpieczeństwa danych osobowych przetwarzanych przez SPZOZ;

9) **ocena ryzyka** – proces porównywania wartości ryzyka z określonymi kryteriami w celu określenia znaczenia ryzyka;
10) **osoba upoważniona** – osoba przeszkolona z zakresu bezpieczeństwa danych osobowych przetwarzanych przez SPZOZ oraz posiadająca imienne upoważnienie wydane przez ADO;
11) **podatność**– słabość aktywów, która może być wykorzystana przez zagrożenie. Podatność charakteryzuje łatwość, z jaką dane zagrożenie może wyrządzić szkodę;
12) **podmiot przetwarzający** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
13) **polityka** – Polityka bezpieczeństwa danych osobowych – zestaw efektywnych, udokumentowanych zasad i procedur bezpieczeństwa wraz z ich planem wdrożenia i egzekwowania zatwierdzony przez ADO, będący zbiorem reguł dotyczących ochrony danych osobowych SPZOZ;
14) **postępowanie z ryzykiem** – proces wyboru i wdrażania środków sterowania ryzykiem mających na celu zmianę wartości poziomu ryzyka;
15) **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;
16) **ryzyko –** prawdopodobieństwo, że określone zagrożenie wykorzysta podatność aktywu lub grupy aktywów, aby spowodować straty lub szkody, co spowoduje niepożądane konsekwencje;
17) **ryzyko szczątkowe –** ryzyko, którego poziom nie przekracza akceptowanej wartości;
18) **skutek (ze strony zagrożenia**) - rezultat niepożądanego incydentu. Stopień strat powstałych w przypadku zaistnienia zagrożenia.
19) **SP ZOZ MSWiA w Koszalinie, ul. Szpitalna 2, 75- Koszalin** - ADO
20) **Uodo -** Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.2018.1000);
21) **właściciel aktywa** osoba lub podmiot, który ma zatwierdzoną kierowniczą odpowiedzialność w organizacji za nadzorowanie produkcji, rozwój, utrzymanie, korzystanie i bezpieczeństwo aktywów. Pojęcie to nie oznacza, że osoba ta rzeczywiście posiada jakiekolwiek prawa własności do aktywów;

22) **zagrożenie** – potencjalna przyczyna niepożądanego incydentu, która może wywołać naruszenie praw i wolności osób fizycznych lub bezpieczeństwa danych osobowych;
23) **zarządzanie ryzykiem** – jest to ciągły nadzór nad stanem bezpieczeństwa systemu. Zarządzanie ryzykiem jest to proces identyfikacji, kontrolowania, eliminacji lub ograniczania prawdopodobieństwa zaistnienia ewentualnych zdarzeń (zagrożeń), które mogą mieć wpływ na bezpieczeństwo danych osobowych;
24) **zbiór danych** – oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

III. Dokumenty powiązane.

3.1. Na dokumentację ochrony danych osobowych w SPZOZ składają się:

1) **Polityka bezpieczeństwa danych osobowych (Polityka)** – dokument określający prawa i obowiązki osób funkcyjnych biorących udział w procesie przetwarzania danych osobowych, odpowiedzialność oraz procedury postępowania w procesie przetwarzania w/w informacji.

2) **Metodyka zarządzaniem ryzykiem w ochronie danych osobowych (Metodyka)** - wypełniających wymogi art. 32 RODO.

3) **Sprawozdanie z analizy ryzyka -** wypełniających wymogi art. 32 RODO.

4) **Rejestr czynności przetwarzania danych osobowych;** - wypełniających wymogi art. 30 RODO.

5) **Ewidencja osób upoważnionych do przetwarzania danych osobowych, -** wypełniający wymogi art. 29 RODO.

6) **Rejestr incydentów bezpieczeństwa i działań korygujących –** wypełniający wymogi art. 33 ust 5 RODO.

7) **Dokumentacja techniczna wykorzystywanego oprogramowania do przetwarzania danych osobowych.**

8) **Oryginały i kopie dokumentów dotyczących ochrony danych osobowych.**

9) **Protokoły z przeprowadzonych kontroli wewnętrznych i zewnętrznych w zakresie ochrony danych osobowych.**

10) **Jeżeli dotyczy – Ocena skutków dla przetwarzania danych osobowych** – wypełniający wymogi art. 35 RODO.

11) **Protokoły z niszczenia dokumentów, nośników oraz sprzętu zawierające dane osobowe.**

3.2. Wymienione dokumenty stanowią komplet dokumentacji z zakresu bezpieczeństwa danych osobowych w SPZOZ.

IV. Obowiązki oraz odpowiedzialność osób funkcyjnych.

4.1. Administrator danych osobowych wdraża odpowiednie środki techniczne i organizacyjne mające na celu zapewnić przetwarzanie danych zgodnie z RODO, uwzględniając charakter, zakres, kontekst i cel przetwarzania oraz ryzyko naruszenia praw lub wolności osoby fizycznej a także utraty atrybutów danych.

4.2. Do kompetencji **administratora danych osobowych** należy w szczególności:

1) Wyznaczenie inspektora ochrony danych.
2) Wyznaczanie kierowników komórek organizacyjnych.
3) Wyznaczenie administratora systemu informatycznego.
4) Określenie celów i strategii ochrony danych osobowych.
5) Podział zadań i obowiązków związanych z organizacją ochrony danych osobowych.

4.3. Do obowiązków **Administratora Danych Osobowych** należy:

1) uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, wdrażanie odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie z RODO. Administrator musi być w stanie wykazać adekwatność zastosowanych środków bezpieczeństwa. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane;
2) zapewnienie szkoleń dla pracowników w zakresie przepisów o ochronie danych osobowych oraz zagrożeń związanych z ich przetwarzaniem;
3) przyjmowanie i zatwierdzanie niezbędnych, wymaganych przez przepisy prawa dokumentów regulujących ochronę danych osobowych w SPZOZ;
4) nadawanie, zmienianie oraz cofanie uprawnień do przetwarzania danych osobowych na wniosek Kierowników komórek organizacyjnych dla pracowników oraz użytkowników zewnętrznych;
5) zapewnienie środków finansowych na ochronę fizyczną pomieszczeń, systemów informatycznych oraz zbiorów tradycyjnych, w których przetwarzane są dane osobowe;

6) zapewnienie środków finansowych na merytoryczne przygotowanie osób odpowiedzialnych za nadzór nad ochroną danych osobowych;
7) dbanie o wdrożenie IOD we wszystkie zagadnienia dotyczące ochrony danych osobowych przetwarzanych w SPZOZ;
8) uwzględnianie bezpieczeństwa danych osobowych na etapie projektowania sposobów przetwarzania, zakresu, podstawy prawnej oraz ochrony technicznej i organizacyjnej tych danych;
9) zapewnia wykonanie analizy ryzyka zgodnie z dokumentem „Metodyka analizy ryzyka danych osobowych";
10) wspieranie IOD w wypełnianiu przez niego zadań, o których mowa 4.6 i 4.7, zapewniając mu dostęp do informacji oraz operacji przetwarzania;

4.4. Administrator Danych Osobowych, wyznacza Inspektora Ochrony Danych.

4.5. W imieniu ADO nadzór nad przestrzeganiem zasad ochrony danych osobowych sprawuje IOD.

4.6. Do najważniejszych obowiązków **Inspektora Ochrony Danych** należy:

1) określenie i przedstawienie do zatwierdzenia dla ADO zasad ochrony danych osobowych;
2) stałe informowanie ADO oraz pracowników o obowiązkach i odpowiedzialności spoczywającej na nich na mocy przepisów prawa z szczególnym uwzględnieniem RODO i innych aktów prawa dotyczących ochrony danych osobowych;
3) monitorowanie przestrzegania przepisów prawa w zakresie bezpieczeństwa danych osobowych oraz polityki bezpieczeństwa ADO;
4) nadzorowanie i aktualizowanie dokumentacji w zakresie ochrony danych osobowych;
5) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami w tym zakresie;
6) udzielanie zaleceń, co do oceny skutków dla ochrony danych osobowych oraz monitorowanie ich wykonania;
7) wnioskowanie o ukaranie osób winnych naruszenia przepisów i zasad dotyczących ochrony danych osobowych;
8) nadzorowanie i kontrolowanie pracy Kierowników komórek organizacjach, wszystkich pracowników w zakresie ochrony danych osobowych oraz

podmiotów zewnętrznych realizujących zadania mające wpływ na ochronę i bezpieczeństwo danych osobowych;

9) dokonywanie systematycznych audytów i przeglądów stosowania przepisów w zakresie ochrony danych osobowych;
10) w ramach audytów i przeglądów, o których mowa w pkt. 4.6 ust. 10 IOD ma prawo:
    a) wstępu do pomieszczeń (również po godzinach pracy) w których przetwarzane są dane osobowe i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z RODO;
    b) żądać złożenia pisemnych lub ustnych wyjaśnień w zakresie niezbędnym do ustalenia stanu faktycznego;
    c) żądać okazania dokumentów i wszelkich danych mających bezpośredni związek z problematyką kontroli;
    d) żądać udostępnienia do kontroli urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych;
11) powołać za zgodą ADO do komisji kontrolującej przestrzeganie procedur ochrony danych osobowych pracowników SPZOZ w szczególności osoby pełniące funkcję ASI i Kierowników komórek organizacyjnych;
12) niezwłocznie informować ADO o przypadkach naruszenia przepisów RODO a także zapisów dokumentacji wewnętrznej regulującej ten zakres;
13) podejmowanie działań mających na celu doskonalenie procedur ochrony danych osobowych w SPZOZ;
14) przeprowadzanie szkoleń z zakresu ochrony danych osobowych;
15) reprezentowanie ADO w kontaktach z biurem UODO;
16) pełnienie funkcji punktu kontaktowego dla osoby, której dane dotyczą.

4.7. Inspektor ochrony danych w zakresie realizacji swoich obowiązków, ma prawo żądania od pozostałych osób, bez względu na rangę ich stanowiska udzielania natychmiastowej pomocy w razie stwierdzenia, ze doszło lub mogło dojść do naruszenia przepisów o ochronie danych osobowych.

4.8. Administrator danych osobowych wskazuje **administratora systemów informatycznych – obowiązki te mogą być realizowane poprzez firmę zewnętrzną bez wskazywania konkretnej osoby.**

4.9. Administrator systemu informatycznego w zakresie działań związanych z ochroną danych osobowych ściśle współpracuje z inspektorem ochrony danych.

4.10. Administrator systemu informatycznego realizuje zadania w zakresie bezpieczeństwa ochrony danych, a w szczególności poprzez:

1) zapewnienie ochrony i bezpieczeństwa danych osobowych zawartych w systemach informatycznych SPZOZ;
2) reagowanie bez zbędnej zwłoki, w przypadku naruszenia bądź powstania zagrożenia bezpieczeństwa danych osobowych w systemach informatycznych;
3) przeciwdziałanie próbom naruszeń bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych;
4) zapewnienie zgodności wszystkich wdrażanych systemów przetwarzania danych osobowych z RODO oraz z niniejszą Polityką:
5) administrowanie oprogramowaniem systemowym i sieciowym zabezpieczającym osobowe przed nieupoważnionym dostępem;
6) nadzór nad systemem komunikacji w sieci komputerowej oraz przesyłaniem danych za pośrednictwem urządzeń teletransmisyjnych;
7) nadzór i kontrolę systemów informatycznych służących do przetwarzania danych osobowych a także osoby przy nich zatrudnionych w zakresie bezpieczeństwa teleinformatycznego;
8) czynny udział w dokonywanej analizie bezpieczeństwa oraz analizie ryzyka danych osobowych realizowanej przez IOD;
9) zakładanie kont użytkowników ze ściśle określonym zakresem praw dostępu oraz blokowanie dostępu do kont w przypadku cofnięcia użytkownikowi upoważnienia dostępu do przetwarzania danych osobowych;
10) wykonywanie i zarządzanie kopiami bezpieczeństwa, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtworzenia danych w przypadku awarii systemu;
11) konfigurowanie komputerów użytkowników i instalację oprogramowania;
12) współpracę z zewnętrznymi specjalistami przy pracach instalacyjnych, konfiguracyjnych i naprawczych, oraz pełni nadzór nad pracami oraz osobami realizującym w/w zadania;
13) Nadzorowanie, wykrywanie i eliminację nieprawidłowości w systemach informatycznych;

14) sprawowanie nadzoru nad bieżącą aktualizacją „szczepionek" programu antywirusowego;
15) sprawowanie nadzoru nad naprawami, konserwacją oraz wymianą sprzętu, na którym zapisane są informacje w tym dane osobowe;
16) wnioskowanie do ADO o zastosowanie rozwiązań technicznych i organizacyjnych, które mają minimalizować zagrożenia utraty bezpieczeństwa informacji;

4.11. Administrator Danych Osobowych wyznacza Kierowników komórek organizacyjnych, którzy są odpowiedzialni za ochronę przypisanych i przetwarzanych danych osobowych w podległej komórce organizacyjnej.

4.12. Do obowiązków **Kierownika komórki organizacyjnej** należy:

1) Wskazanie podstaw prawnych, celu oraz zakresu przetwarzania danych osobowych od chwili rozpoczęcia ich zbierania do chwili usunięcia w podległej komórce organizacyjnej;
2) zapewnienie aktualności, adekwatności oraz merytorycznej poprawności danych osobowych przetwarzanych w określonym przez nich celu;
3) zapewnienie realizacji w imieniu ADO obowiązku informowania osób, których dane osobowe są pozyskiwane w danej komórce organizacyjnej zgodnie z rozdziałem XI;
4) zapewnienie na żądanie uprawnionych osób udostępniania informacji o przetwarzanych danych osobowych oraz podmiotach, którym zostały one udostępnione, zgodnie z rozdziałem XI;
5) wnioskowanie do Administratora Danych Osobowych o nadanie upoważnień dla pracowników podległej komórki organizacyjnej;
6) zapewnienie w podległej komórce organizacyjnej przetwarzania danych osobowych zgodnie z RODO a także z regulacjami zawartymi w niniejszej Polityce oraz dokumentami powiązanymi;
7) inicjowanie i podejmowanie w porozumieniu z IOD przedsięwzięć w zakresie doskonalenia ochrony danych osobowych w podległej komórce.
8) Informowanie IOD o wszelkich planach powierzenia danych osobowych, zmiany sposobu przetwarzania danych oraz innych zdarzeniach mających wpływ na bezpieczeństwo danych osobowych.

4.13. W celu osiągnięcia i utrzymania wysokiego poziomu bezpieczeństwa przetwarzania danych osobowych konieczne jest zaangażowanie ze strony każdego pracownika i osoby upoważnionej zewnętrznej.

4.14. **Pracownicy/ osoby upoważnione** są zobowiązane do:

1) znajomości zasad bezpieczeństwa zawartych w dokumentach: Polityka bezpieczeństwa oraz dokumentach powiązanych a także zasadach zawartych w przepisach prawa RODO w zakresie niezbędnym do zajmowanego stanowiska i zakresu upoważnienia;
2) bezwzględnego przestrzegania zapisów Polityki oraz pozostałych dokumentów regulujących zasady przetwarzania danych osobowych;
3) informowania o wszelkich podejrzeniach naruszenia oraz sytuacjach mających wpływ na bezpieczeństwo ochrony danych osobowych w SPZOZ zgodnie z zapisami zawartymi w dziale XVIII;
4) zachowania w tajemnicy wiedzy o przetwarzanych danych osobowych oraz o sposobach ich zabezpieczenia;
5) ochrony danych osobowych oraz aktywów wykorzystywanych do ich przetwarzania przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem;
6) zmiany hasła do systemów służących do przetwarzania danych osobowych nie rzadziej niż raz na trzy miesiące, chyba, że stosowane są dodatkowe zabezpieczenia w postaci dedykowanych kluczy certyfikujących.

V. Zarządzanie ochroną danych osobowych.

5.1. Przetwarzanie danych osobowych dopuszczalne jest jedynie w ramach zbiorów i czynności przetwarzania danych osobowych, które są zawarte w „Rejestrze czynności przetwarzania danych osobowych” (wzór stanowi załącznik nr. 3).

5.2. Rejestr, o którym mowa w pkt. 5.1 jest prowadzony przez IOD i podlega zatwierdzeniu przez ADO.

5.3. O utworzeniu nowego zbioru danych osobowych decyduje administrator danych osobowych na wniosek kierownika komórki organizacyjnej, u którego ma powstać zbiór lub inspektora ochrony danych.

5.4. W wniosku, o którym mowa w pkt. 5.3 podaje się w szczególności:
a) datę rozpoczęcia przetwarzania danych;
b) podstawę prawną;
c) cel przetwarzania danych;
d) kategorię osób, których dotyczą dane;
e) zakres danych;
f) źródło danych osobowych;
g) okresu przez jakie przewidziane jest przetwarzanie danych;
h) sposób przetwarzania danych osobowych;
i) informację o powierzeniu lub planowanym powierzeniu danych.

5.5. W przypadku wniosku wystosowanego przez kierownika komórki organizacyjnej przed akceptacją ADO wniosek ten jest weryfikowany przez IOD pod kontem elementów wymienionych w pkt. 5.4 oraz w zakresie zastosowania technicznych i organizacyjnych środków bezpieczeństwa.

5.6. W przypadku planowanego nowego przetwarzania danych osobowych lub zmiany sposobu przetwarzania przeprowadza się analizę ryzyka zgodnie z „Metodyką zarządzania ryzykiem w ochronie danych osobowych”.

5.7. W przypadku, gdy podczas analizy ryzyka, o której mowa w pkt. 5.6 wskazuje się prawdopodobieństwo wystąpienia dużego ryzyka naruszenia praw lub wolności

osoby fizycznej, przed rozpoczęciem przetwarzania dokonuje się oceny skutków planowanego przetwarzania dla ochrony danych osobowych.

5.8. Ocenę skutków dla ochrony danych osobowych realizuje zespół powołany przez ADO pod przewodnictwem IOD.

5.9. Ocena skutków dla ochrony danych, o której mowa w pkt. 5.7, jest wymagana w szczególności w przypadku:

a) systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną;
b) przetwarzania na dużą skalę szczególnych kategorii danych osobowych lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa;
c) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.

5.10. Ocena o której mowa w pkt. 5.7 zawiera co najmniej:

a) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora;
b) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
c) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą, o którym mowa w pkt 5.6
d) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie niniejszego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.

5.11. Likwidację zbioru przeprowadza komisja powołana przez Administratora Danych Osobowych. W protokole potwierdzającym likwidację zbioru wskazuje się: skład osobowy komisji, datę likwidacji i sposób usunięcia zgromadzonych danych, zakres likwidowanych danych.

5.12. Likwidację dokumentów zawierających dane osobowe a powstałe w trybie normalnym pracy (w tym między innymi: błędnych i próbnych wydruków), niszczy użytkownik w sposób trwały uniemożlwiający odczytanie zniszczonych danych.

5.13. W przypadku danych, które straciły swoją aktualność lub danych, których dalsze przetwarzanie jest niemożliwe z powodu zrealizowania celu przez SPZOZ itp. likwiduje się je zgodnie z pkt 5.11.

5.14. Wszystkie osoby, o których mowa w pkt 5.11. - członkowie komisji muszą posiadać imienne upoważnienie nadane według warunków określonych w dziale VII – co najmniej na czas pracy w komisji likwidacyjnej.

5.15. Zestawienie środków organizacyjnych i technicznych zapewniających ochronę danych osobowych u ADO :

1) został wyznaczony IOD;
2) został wyznaczony ASI;
3) została opracowana i wdrożona „Polityka bezpieczeństwa danych osobowych”;
4) została opracowana i wdrożona „Metodyka zarządza ryzykiem danych osobowych”;
5) został opracowany i wdrożony „Rejestr czynności przetwarzania danych osobowych”;
6) zastosowane techniczne i organizacyjne środki bezpieczeństwa informacji oparte zostały na analizie ryzyka, posiadanej wiedzy oraz posiadanych środkach finansowych;
7) do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez administratora danych;
8) prowadzona jest ewidencja osób upoważnionych do przetwarzania danych;
9) osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego;
10) osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy oraz metod zastosowanych do ich zabezpieczeń;
11) przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy

przetwarzaniu w/w informacji oraz w warunkach zapewniających ich bezpieczeństwo;

12) wszystkie pomieszczenia, w których przetwarza się dane osobowe, są zamykane na klucz w przypadku opuszczenia pomieszczenia przez ostatniego pracownika upoważnionego do przetwarzania danych osobowych – także w godzinach pracy;
13) Dane osobowe przechowywane w wersji tradycyjnej (papierowej) lub elektronicznej (pendrive, płyta CD/DVD) po zakończeniu pracy są przechowywane w zamykanych na klucz meblach biurowych, a tam, gdzie jest to możliwe – w szafach metalowych lub pancernych;
14) nieaktualne lub błędne wydruki zawierające dane osobowe niszczone są w niszczarkach;
15) dostęp do systemu operacyjnego komputerów na których przetwarzane są dane osobowe został zabezpieczony hasłem;
16) dostęp do zbioru danych osobowych w systemie teleinformatycznym wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika i hasła;
17) zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe;
18) w pomieszczeniach gdzie obsługiwani są klienci SPZOZ monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane, w pozostałych pomieszczeniach dopuszcza się ustawienie monitora w inny sposób, jednak w przypadku przebywania w pomieszczeniu osoby nie upoważnionej do przetwarzania konkretnych danych osobowych – pracownik jest zobowiązany do uruchomienia wygaszacza, aby na monitorze nie było żadnych informacji zawierających dane osobowe;
19) cyklicznie wykonywane są kopie bezpieczeństwa, z których w przypadku awarii odtwarzane są dane;
20) Wszystkie urządzenia służące do przetwarzania danych osobowych połączone są kablem UTP kat.5 lub wyższej;
21) komunikacja z serwerem w sieci odbywa się przez sieć komputerową opartą na technologii FastEthernet 100 MB/s;
22) okablowanie strukturalne poprowadzone jest w korytach i nie ma do niego bezpośredniego dostępu;
23) programy zainstalowane na komputerach obsługujących przetwarzanie danych osobowych są użytkowane z zachowaniem praw autorskich i posiadają licencje;

24) drzwi wyposażone są, w co najmniej jeden zamek o skomplikowanym mechanizmie;
25) pomieszczenia zabezpieczone są pod względem pożarowym zgodnie z obowiązującymi przepisami w tej materii;
26) do zabezpieczenia stanowisk komputerowych przed oprogramowaniem złośliwym i wirusami stosowane jest oprogramowanie antywirusowe – Windows Defender oraz Kaspersky Antywirus - poprawki bezpieczeństwa instalowane są na bieżąco i automatycznie;
27) Firewall zabezpiecza sieć wewnętrzną przed niepowołanym dostępem z zewnątrz;
28) serwery oraz komputery realizujące funkcję serwerów w SPZOZ są zabezpieczone przed utratą danych spowodowaną awarią zasilania lub zakłóceń w sieci zasilającej poprzez zastosowanie odrębnych UPS-ów;
29) Dostęp do danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora i hasła zgodnie z działem XII;
30) Zastosowano mechanizm blokady dostępu po trzykrotnym błędnym wprowadzeniu hasła do systemu;
31) hasła użytkowników na serwerze przechowywane są w formie niejawnej;
32) wykorzystano dostępne w aplikacjach środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych;
33) zastosowano mechanizm umożliwiający automatyczną rejestrację identyfikatora użytkownika i datę pierwszego wprowadzenia danych osobowych;
34) zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych;
35) zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego;
36) użytkownicy są zobowiązani do realizowania obowiązku zmiany hasła nie rzadziej, niż co 30 dni, a tam gdzie jest to możliwe ustawiony jest mechanizm wymuszenia zmiany hasła, chyba, że używają dodatkowe klucze certyfikujące;

5.16. W SPZOZ informacje w tym dane osobowe przetwarza się w systemach informatycznych zgodnie z poniższym zestawieniem:

l.p	Nazwa zbioru	Nazwa oprogramowania
1	Dane osobowe pacjentów	System RUM
2	Dane osobowe klienci (kontrahenci	SYMFONIA, MS Office ,RUM-SPRZ
3	Kontrahenci	RUM-SPRZ, SYMFONIA, MS Office
4	Dane osobowe pracowników i zleceniobiorców	Płatnik
5	Przetargi	MS Office, poczta mail
6.	Rejestr skarg i zażaleń	MS Office, poczta mail
7.	Darczyńcy	MS Office, poczta mail

VI. Szkolenia użytkowników.

6.1. Każdy użytkownik przed przystąpieniem do przetwarzania danych osobowych musi zostać przeszkolony przez Inspektora Danych Osobowych z zakresu:

1) przepisów o ochronie danych osobowych, a także Polityki wprowadzonej przez ADO;
2) zasad przetwarzania danych osobowych;
3) procedur dotyczących bezpiecznego przetwarzania danych osobowych w systemach informatycznych;
4) zasady użytkowania urządzeń i systemów informatycznych służących do przetwarzania danych osobowych;
5) zagrożeń na jakie może być narażone przetwarzanie danych osobowych, a w szczególności zagrożeń informacji przetwarzanych w systemach informatycznych;
6) zasad dostępu do pomieszczeń, w których przetwarzane są dane osobowe;
7) sposobu postępowania w przypadku naruszenia ochrony danych osobowych.

6.2. Potwierdzenie odbytego szkolenia oraz zapoznanie się z dokumentami dotyczącymi przetwarzania danych osobowych w SPZOZ, pracownik potwierdza własnoręcznym podpisem na oświadczeniu, którego wzór stanowi załącznik nr 14. Dopuszcza się, aby potwierdzeniem odbycia szkolenia pracownika był podpis na liście obecności.

6.3. IOD zobowiązany jest do przeprowadzenia szkolenia w przypadku istotnych zmian w zakresie przetwarzania danych w SPZOZ, zmian przepisów RODO oraz istotnych zmian zapisów Polityki oraz w przypadku wystąpienia incydentu, – co najmniej w komórkach, w których on wystąpił.

VII. Upoważnienie do przetwarzania danych osobowych.

7.1. Do przetwarzania danych osobowych mogą być dopuszczone jedynie osoby posiadające upoważnienie wydane przez ADO.

7.2. Upoważnienie wydawane jest pracownikom zgodnie z zasadą „wiedzy uzasadnionej". Wnioskujący o wydanie upoważnienia w oparciu o analizę zakresu obowiązków, określa zakres i okres ważności upoważnienia.

7.3. Wzór upoważnienia stanowi załącznik **nr 1**.

7.4. Upoważnienie zatwierdza ADO.

7.5. Wzór odwołania upoważnienia stanowi **załącznik nr 4.**

7.6. W przypadku długotrwałej nieobecności pracownika (co najmniej raz na cztery miesiące) upoważnienie powinno być czasowo cofnięte.

7.7. W przypadku nadania ponownego upoważnienia w sytuacji opisanej w pkt 7.6 można odstąpić od ponownego szkolenia, o którym mówi się w pkt. 6.1 jeżeli od ostatniego szkolenia w którym brał udział pracownik nie minęło więcej niż 12 miesięcy.

7.8. Upoważnienie/odwołanie upoważnienia wystawiane jest w dwóch egzemplarzach, jeden otrzymuje pracownik, drugi egzemplarz przechowywany jest przez IOD.

7.9. ASI może nadać konto użytkownikowi w systemie elektronicznym dopiero po uzyskaniu informacji od IOD o odbytym szkoleniu przez pracownika oraz wydaniu mu upoważnienia.

VIII. Ewidencja osób upoważnionych.

8.1. Osoby upoważnione do przetwarzania danych osobowych, ewidencjonowane są w Ewidencja osób upoważnionych do przetwarzania danych osobowych zgodnie ze wzorem stanowiącym załącznik nr 2.

8.2. Ewidencjonowanie następuję bez zbędnej zwłoki po nadaniu lub cofnięciu upoważnienia.

8.3. W SPZOZ stosuje się jeden wykaz zawierający wszystkich użytkowników posiadających upoważnienie do przetwarzania danych osobowych.

8.4. Dopuszcza się stosowanie wykazu wymienionego w punkcie 8.1 w formie elektronicznej.

8.5. W przypadku prowadzenia rejestru w formie elektronicznej – dokonuje się wydruków rejestru, o którym mowa w pkt 8.1 celem dołączenia do dokumentacji w częstotliwości tożsamej z audytami bezpieczeństwa informacji.

8.6. W przypadku wydruku rejestru – rejestr poprzedni jest niszczony po upływie roku od wydruku nowej wersji.

IX. Powierzanie przetwarzania danych osobowych.

9.1. Kierownik komórki organizacyjnej, w której planuje się powierzyć dane osobowe lub zawrzeć inną umowę związaną z bezpieczeństwem informacji jest zobowiązany o tym fakcie poinformować IOD.

9.2. ADO może powierzyć dane do dalszego przetwarzania tylko takiemu podmiotowi przetwarzającemu, który zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.

9.3. Powierzenie przetwarzania danych osobowych może mieć miejsce tylko na podstawie pisemnej umowy określającej w szczególności przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora oraz podmiotu przetwarzającego a także zakres odpowiedzialności podmiotu przetwarzającego z tytułu niewykonania lub nienależytego wykonania umowy.

9.4. Podmiot przetwarzający przy przetwarzaniu danych osobowych zobowiązany jest stosować wszelkie środki wymagane art. 32 RODO. W celu wykonania obowiązku, o którym mowa w zdaniu poprzedzającym, podmiot przetwarzający zobowiązany jest prowadzić dokumentację opisującą sposób przetwarzania danych i realizację wymogu art. 32 RODO.

9.5. Podmiot przetwarzający nie jest uprawniony do przekazywania danych osobowych osobom trzecim, bez zgody SPZOZ, chyba, że strony postanowią inaczej w umowie.

9.6. Umowa może mieć charakter umowy oddzielnej lub być częścią umowy głównej dotyczącej świadczonej usługi.

9.7. Umowy dotyczące powierzenia danych osobowych są ewidencjonowanie w rejestrze umów powierzenia danych osobowych stanowiący załącznik nr 6.

X. Udostępnianie danych osobowych.

10.1. Udostępnienie danych osobowych podmiotowi zewnętrznemu (w tym organom publicznym) może nastąpić wyłącznie po pozytywnym zweryfikowaniu ustawowych przesłanek dopuszczalności takiego udostępnienia.

10.2. Przez weryfikację, o którym mowa w pkt 10.1 należy rozumieć przepis prawa nakazujący udostępnienie danych organom publicznym lub pisemny wniosek podmiotu uprawnionego z wskazaną podstawą prawną.

10.3. Udostępnianie danych osobowych podmiotom innym niż dla organów publicznych może nastąpić wyłącznie za zgodą Administratora Danych Osobowych lub inną uprawnioną przez niego osobę.

10.4. Za przygotowywanie danych osobowych do udostepnienia w zakresie wskazanym we wniosku odpowiedzialny jest kierownik komórki organizacyjnej.

10.5. Na wniosek pochodzący od osoby, której dane dotyczą, informacje o danych osobowych dotyczących tej osoby muszą być udzielone w terminie nie dłuższym niż 30 dni od daty złożenia wniosku.

10.6. Udostępnienie danych nie może się odbywać drogą telefoniczną, mailową lub inną gdzie nie ma możliwości weryfikacji podmiotu lub osoby, której dane się udostępnia.

XI. Prawa osób, których dane dotyczą.

11.1. Kierownik komórki organizacyjnej odpowiada za dokonanie obowiązku informacyjnego w stosunku do osoby, której dane dotyczą przy pierwszym pozyskiwaniu danych od niego.

11.2. Zakres informacji, jaki musi uzyskać osoba, której dane dotyczą został określony we wzorze dokonania obowiązku informacyjnego stanowiący załącznik nr 8.

11.3. Można odstąpić od informowania osoby, której dane dotyczą w zakresie wymienionym w pkt 11.2 w przypadku, gdy:

a) przepis prawa ogranicza zakres obowiązku informacyjnego;

b) osoba, której dane dotyczą, posiada informacje, o których mowa w pkt 11.2.

11.4. Wymóg określony w pkt 11.1 może być dokonywany na formularzach służących do zbierania danych.

11.5. W przypadku przetwarzania danych pozyskanych z innego źródła niż od osoby, której dane dotyczą obowiązek informacyjny należy zrealizować w najkrótszym rozsądnym terminie jednak nie dłuższym niż miesiąc od chwili pozyskania danych, a w przypadku, gdy dane mają służyć do komunikacji najpóźniej przy pierwszej komunikacji z tą osobą.

11.6. W przypadku przetwarzania danych pozyskanych z innego źródła niż od osoby, której dane dotyczą zakres informacji zawartych w obowiązku informacyjnym informacje należy rozszerzyć w stosunku do informacji wskazanych w pkt. 11.2 o kategorie odnośnie danych oraz źródle pochodzenia danych.

11.7. Jeżeli ADO ma zamiar przekazać dane do państwa trzeciego obowiązek informacyjny wskazany w pkt. 11.2 oraz 11.6 należy rozszerzyć o taką informację oraz o wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwości uzyskania kopii danych.

11.8. Każdy osoba, której dane dotyczą ma prawo uzyskania informacji o tym czy jego dane są przetwarzane.

11.9. Oprócz informacji wskazane w pkt 11.8 osoba, której dane dotyczą ma prawo dostępu do swoich danych oraz informacji wskazanych w art. 15 ust 1 i ust 2.

11.10. Za realizację prawa wskazanego w pkt 11.8 i 11.9 odpowiada kierownik komórki organizacyjne.

11.11. Osoba, której dane dotyczą ma prawo żądania sprostowania i uzupełnienia niekompletnych danych wykazując się dowodami na niekompletność lub nieprawidłowość danych.

11.12. Poprawienie lub uzupełnienie danych następuję bez zbędnej zwłoki i realizowane jest bezpośrednio przez pracownika upoważnionego do przetwarzania przedmiotowych danych.

11.13. W przypadku, gdy:

1) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
2) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie;
3) dane osobowe były przetwarzane niezgodnie z prawem;
4) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie, któremu podlega administrator;

osoba, której dane dotyczą ma prawo żądania usunięcia danych.

11.14. Punkt 11.13 nie ma zastosowania, gdy dane są przetwarzane:

1) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
2) do ustalenia, dochodzenia lub obrony roszczeń

11.15. Za realizację pkt. 11.13 odpowiada kierownik komórki organizacyjnej, w której są przetwarzane dane po wcześniejszym kontakcie z IOD z podaniem przyczyny przetwarzania danych mimo zaistnienia przesłanek wskazanych w pkt 11.13.

11.16. Osobie, której dane dotyczą przysługuje prawo żądania ograniczenia przetwarzania danych osobowych w następujących sytuacjach:

1) osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający administratorowi sprawdzić prawidłowość tych danych;

2) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
3) administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń.

11.17. W przypadku uznania zasadności żądania wskazanego w pkt. 11.16 dane osobowe mogą być tylko przechowywane, a dalsze przetwarzanie do czasu rozpatrzenia żądania może odbywać się tylko na podstawie zgody osoby, której dane dotyczą.

11.18. W przypadku skorzystania z prawa opisanego w pkt. 11.16 oraz przetwarzania danych osobowych w systemie informatycznym o fakcie ograniczenia przetwarzania danych osobowych IOD informuje ASI w celu ograniczenia dostępu do danych pracownikom SPZOZ do czasu rozpatrzenia żądania osoby, której dane dotyczą.

11.19. W przypadku uchylenia ograniczenia przetwarzania, o którym mowa w pkt. 11.16 IOD jest zobowiązany do poinformowania osoby, której dane dotyczą.

11.20. Realizacja pkt 11.8, 11.9, 11.11, 11.13, 11.16 może nastąpić tylko na wniosek osoby, której dane dotyczą a kierownik komórki organizacyjnej lub osoba przez niego wskazana przed realizacją żądania jest zobowiązana do zweryfikowania tożsamość osoby występującej z wnioskiem.

11.21. W przypadku realizacji żądań wskazanych w pkt 11.11, 11.13, 11.16 osoba realizująca te żądania za pośrednictwem IOD informuje każdego odbiorcę, któremu ujawniono dane (jeżeli występuje) o sprostowaniu lub usunięciu lub ograniczeniu przetwarzania danych osobowych.

11.22. Ograniczenie praw osoby, której dane dotyczą wskazanych w pkt. 11.8, 11.11, 11.13, 11.16 musi być określone w przepisach prawa.

11.23. ADO nie profiluje oraz nie podejmuje decyzji dotyczących osób, których dotyczą dane w sposób zautomatyzowany.

11.24. W przypadku jakichkolwiek żądań osoby, której dane dotyczą (również innych niż opisane w dziale XI) lub wątpliwości, co do zasadności żądania kierownik komórki organizacyjnej każdorazowo kontaktuje się z IOD.

XII. Nadawanie i zmiany uprawnień do przetwarzania osobowych oraz środki uwierzytelnienia.

12.1. Do sytemu informatycznego służącego do przetwarzania danych osobowych mogą być dopuszczeni jedynie pracownicy posiadający upoważnienie do przetwarzania konkretnych danych osobowych wydanego zgodnie z działem VIII Polityki.

12.2. Przyznanie uprawnień w zakresie dostępu do systemu informatycznego polega na wprowadzeniu do systemu dla każdego użytkownika indywidualnego identyfikatora, hasła oraz zakresu dostępnych danych i operacji zgodnie z upoważnieniem do przetwarzania danych osobowych. Fakt dodania nowego użytkownika do systemu zapisuje się w „Dzienniku dla systemów informatycznych" stanowiącego załącznik nr 9 oraz należy dokonać odpowiedniego wpisu w „Ewidencja osób upoważnionych do przetwarzania danych osobowych" stanowiący załącznik nr 2.

12.3. Hasło ustanowione podczas przyznawania uprawnień przez Administratora Systemu Informatycznego użytkownik musi zmienić na indywidualne podczas pierwszego logowania się w systemie.

12.4. Użytkownik ma prawo do wykonywania tylko tych czynności w systemie informatycznym, do których został upoważniony.

12.5. Użytkownik ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu.

12.6. W systemie informatycznym stosuje się uwierzytelnianie dwustopniowe: na poziomie dostępu do systemu operacyjnego oraz dostępu do aplikacji.

12.7. Odebranie uprawnień użytkownikowi następuje zgodnie z zasadami określonymi w dziale VIII Polityki.

12.8. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych należy niezwłocznie zablokować w systemie informatycznym, w którym są one przetwarzane oraz unieważnić jej hasło.

12.9. Identyfikator użytkownika nie powinien być zmieniany bez wyraźnej przyczyny, a po wyrejestrowaniu użytkownika z systemu informatycznego nie może być przydzielany innej osobie.

12.10. Hasło użytkownika musi być zmieniane, co najmniej raz na miesiąc. Należy zapewnić możliwość zmiany przez wymuszenie przez system, w przypadku braku takiej możliwości za systematyczną zmianę hasła odpowiada użytkownik.

12.11. Pracownicy są odpowiedzialni za zachowanie poufności swoich haseł.

12.12. Hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności.

12.13. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie.

12.14. W sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, pracownik zobowiązany jest do natychmiastowej zmiany hasła.

12.15. Przy wyborze hasła obowiązują następujące zasady:

a) minimalna długość hasła - 8 znaków;
b) zakazuje się stosować: haseł, które użytkownik stosował uprzednio w okresie minionego roku, swojej nazwy użytkownika w jakiejkolwiek formie (pisanej dużymi literami, w odwrotnym porządku, dublując każdą literę, itp.), swojego imienia, drugiego imienia, nazwiska, przezwiska, pseudonimu w jakiejkolwiek formie, imion (w szczególności imion osób z najbliższej rodziny), ogólnie dostępnych informacji o użytkowniku takich jak: numer telefonu, numer rejestracyjny samochodu, jego marka, numer dowodu osobistego, nazwa ulicy na której mieszka lub pracuje, itp. wyrazów słownikowych, przewidywalnych sekwencji znaków z klawiatury np.: QWERTY”,”12345678”,itp.;
c) należy stosować:
   - hasła zwierające kombinacje małych i wielkich liter oraz cyfr lub znaków specjalnych (znaki interpunkcyjne, nawiasy, symbole @, #, & itp.);
   - hasła, które można zapamiętać bez zapisywania;
   - hasła łatwe i szybkie do wprowadzenia, po to by trudniej było podejrzeć je osobom trzecim.

12.17. Zmiany hasła nie wolno zlecać innym osobom.

12.18. W systemach, które umożliwiają opcję zapamiętania hasła nie wolno korzystać z tego ułatwienia.

12.19. Hasła użytkowników są zapisywane w systemie operacyjnym w postaci zaszyfrowanej.

12.20. W przypadku konieczności zmiany awaryjnej hasła (np. zapomnienie hasła przez użytkownika) operację tą realizuje administrator systemu służącego do przetwarzania danych osobowych analogicznie jak w przypadku zakładania nowego konta opisanego w pkt. 12.3 (bez zmiany identyfikatora).

12.21. Wszelkie operacje przeprowadzane na koncie użytkownika przez administratora aplikacji (zakładanie, likwidacja identyfikatora, oraz awaryjna zmiana hasła) winne być odnotowane w dzienniku dla systemu informatycznego stanowiącego załącznik nr 12.

12.22. Procedura zarządzania hasłem systemowym stanowi załącznik nr 12 i jest przeznaczona jedynie dla ADO, ASI i osób wskazanych przez ADO.

XIII. Rozpoczęcie, zawieszenie i kończenie pracy w systemie.

13.1. Przed wejściem do pomieszczenia, w którym przetwarzanie są informacje w tym dane osobowe użytkownik powinien sprawdzić stan zamknięcia, stan zamków drzwi wejściowych oraz ogólny stan pomieszczenia. W przypadku stwierdzenia śladów nieuprawnionego wejścia do pomieszczenia, należy postępować zgodnie z działem XIV Polityki - Postępowanie w sytuacji naruszenia bezpieczeństwa danych osobowych.

13.2. Zasady rozpoczęcia pracy w systemie informatycznym:

a) należy się upewnić, że na stanowisku, na którym przetwarzane są dane osobowe ekran monitora jest tak ustawiony, aby osoby nieupoważnione nie miały dostępu do informacji na nich wyświetlanych;
b) użytkownik jest zobowiązany do powiadomienia ADO o próbach logowania się do systemu osoby nieupoważnionej, jeśli system to sygnalizuje;
c) w przypadku, gdy użytkownik podczas próby zalogowania się zablokuje system, zobowiązany jest powiadomić o tym ASI, który odpowiada za odblokowanie systemu użytkownikowi;
d) uwierzytelnienie się w systemie informatycznym przy pomocy nazwy użytkownika i hasła;
e) po pozytywnym przejściu systemu uwierzytelnienia uzyskanie praw dostępu do systemu.

13.3. Użytkowni jest zobowiązany do uniemożliwienia osobom nieuprawnionym (np. klientom, pracownikom innych działów) wglądu do danych wyświetlanych na monitorach komputerowych oraz stosować politykę tzw. czystego monitora.

13.4. Zasady zawieszenia i wznowienia rozpoczęcia pracy w systemie informatycznym:

a) w razie przerwania pracy należy stosować wygaszacz ekranu blokowany hasłem;
b) przy wznowieniu pracy należy wprowadzić odpowiednie hasło;
c) w przypadku opuszczenia stanowiska pracy na odległość uniemożliwiającą jego obserwację należy wykonać opcję zablokowania dostępu, lub jeżeli taka możliwość nie istnieje wyjść z programu;
d) w przypadku wyjścia z pomieszczenia, pomieszczenie należy zamknąć na klucz;
e) niedopuszczalne jest pozostawienie w pomieszczeniu, w którym zlokalizowany jest system informatyczny przeznaczony do przetwarzania danych osobowych nieupoważnionej osoby bez nadzoru osoby upoważnionej.

13.5. Zasady zakończenia pracy w systemie informatycznym:

a) użytkownik ma obowiązek zamykania sesji aplikacji i systemu po zakończeniu pracy;
b) przed wyłączeniem komputera należy bezwzględnie zakończyć pracę uruchomionych programów, wykonać zamknięcie systemu i jeżeli jest to konieczne wylogować się z sieci komputerowej;
c) niedopuszczalne jest wyłączanie komputera przed zamknięciem oprogramowania oraz zakończeniem pracy w sieci;
d) przed opuszczeniem pomieszczenia dokumenty i nośniki informacji należy umieścić w zamykanej szafie;
e) sprawdzić, czy wszystkie urządzenia elektryczne zostały wyłączone, czy wszystkie szafy zostały pozamykane na klucz oraz czy zamknięto okna;
f) zamknąć drzwi na klucz a następnie go zdeponować zgodnie z przyjętymi zasadami .

13.6. Czas pracy przy urządzeniach informatycznych, w których przetwarza się dane osobowe jest tożsamy z godzinami pracy SPZOZ, wynikającymi z regulaminu pracy SPZOZ. Na pracę przy w/w urządzeniach poza godzinami pracy konieczna jest zgoda Administratora Danych Osobowych lub osób przez niego wyznaczonych, oraz poinformowanie o tym fakcie ASI - by nie kolidowało to z zaplanowanymi przez niego pracami konserwacyjno-modernizacyjnymi.

XIV. Tworzenie kopi zapasowych i zarządzanie nośnikami elektronicznymi.

14.1. Zasady tworzenia kopii zapasowych umożliwiające otworzenie funkcjonalności systemu informatycznego określa załącznik nr 13 i jest przeznaczony jedynie dla ADO, ASI i osób wskazanych przez ADO.

14.2. W przypadku braku możliwości wykonywania kopii bezpieczeństwa wykonywanych na komputerach użytkowników dotyczących plików pomocniczych, za kopie odpowiada użytkownik komputera.

14.3. Przechowywanie elektronicznych nośników odbywa się zgodnie z technicznymi warunkami składowania nośników magnetycznych, określonych przez producenta nośników.

14.4. Po zakończeniu pracy przez użytkowników systemu, wymienne elektroniczne nośniki informacji są przechowywane w zamykanych szafach biurowych lub sejfie, za wyjątkiem dysków komputerowych, które są zamontowane na stałe w komputerach.

14.5. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie.

14.6. Podlegające likwidacji uszkodzone lub przestarzałe nośniki, a w szczególności twarde dyski z danymi osobowymi są komisyjnie niszczone w sposób fizyczny.

14.7. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, nie mogą podlegać przekazaniu innemu podmiotowi, nieuprawnionemu do otrzymywania w/w informacji.

14.8. W sytuacji przekazania nośników z danym poza obszar organizacji należy stosować następujące zasady bezpieczeństwa:

1) nadawca musi znać podstawę prawną przekazania danych poza organizację;
2) adresat winien być poinformowany o przesyłce;
3) nadawca wykonuje kopie wysyłanych danych;
4) dane przed wysłaniem winne być zaszyfrowane i zabezpieczone hasłem;
5) hasło podaje się adresatowi innym kanałem komunikacyjnym niż przesłany plik z danymi;
6) adresat jest zobowiązany do potwierdzenia otrzymania danych.

14.9. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej.

14.10. Czas przechowywania nośników elektronicznych, na których są przechowywane dane osobowe nie może być dłuższy niż wynikający z celu przetwarzania danych.

14.11. W przypadku konieczności przechowywania wydruków zawierających dane osobowe należy je przechowywać w miejscu uniemożliwiającym bezpośredni dostęp osobom niepowołanym.

14.12. Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, użytkownik zniszczy w sposób uniemożliwiający ich odczytanie.

14.13. Wydruki przechowywane w pomieszczeniach przeznaczonych do przetwarzania danych osobowych po godzinach pracy muszą być zamykane w szafach zabezpieczonych zamkami.

14.14. Zewnętrzne nośniki elektroniczne są ewidencjonowane przez ASI.

XV. Środki ochrony systemu przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu.

15.1. Użytkownik zobowiązany jest do korzystania z Internetu wyłącznie w celach służbowych.

15.2. W przypadku przesyłania informacji w szczególności zawierających dane osobowe pocztą e-mail wewnątrz lub na zewnątrz SPZOZ należy wykorzystywać mechanizmy kryptograficzne (szyfrowanie danych lub pakowanie i zabezpieczenie hasłem wysyłanych informacji).

15.3. Nie należy otwierać załączników (plików) w korespondencji elektronicznej nadesłanej od nieznanego nadawcy lub podejrzanych załączników nadanych od znanego nadawcy.

15.4. Na każdym stanowisku komputerowym jest zainstalowane oprogramowanie antywirusowe.

15.5. Wszelkie oprogramowanie instalowane na komputerach może być tylko instalowane przez ASI, lub inną wskazaną osobę.

15.6. Niedopuszczalne jest zmienianie ustawień oprogramowania antywirusowego oraz instalowanie oprogramowania niebędącego własnością SPZOZ na komputerach przez użytkowników.

15.7. Każdy e-mail wpływający do SPZOZ jest sprawdzany pod kątem występowania wirusów.

15.8. Zabrania się zgrywania na dysk twardy komputera oraz uruchamiania jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła.

15.9. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hakerskim, pornograficznym, lub innym zakazanym przez prawo.

15.10. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.

15.11. Definicje wzorców wirusów aktualizowane są na bieżąco – on-line.

15.12. Zabrania się używania nośników niewiadomego pochodzenia oraz podłączania do komputerów jakichkolwiek urządzeń prywatnych (np. telefonów, pendrive itp.).

15.13. Zabrania się wynoszenia nośników będących własnością SPZOZ poza obszar SPZOZ.

15.14. Nośnik zewnętrzny każdorazowo jest sprawdzany programem antywirusowym.

15.15. Zabrania się pobierania z Internetu plików niewiadomego pochodzenia.

15.16. W razie wykrycia wirusa przez program, użytkownik winien niezwłocznie zgłosić to zdarzenie do ASI.

15.17. W przypadku podjęcia podejrzeń, iż oprogramowanie mogło powodować ryzyko naruszenia bezpieczeństwa danych osobowych należy postępować zgodnie z działem XVII Polityki - Postępowanie w sytuacji naruszenia bezpieczeństwa danych osobowych.

15.18. Kontrola antywirusowa przeprowadzana jest również na wybranym komputerze w przypadku zgłoszenia nieprawidłowości w funkcjonowaniu sprzętu komputerowego lub oprogramowania.

15.19. W przypadku wykrycia wirusów komputerowych komputer, na którym wykryto wirusy odłączany jest od sieci.

15.20. Kontrole, antywirusowe wykonuje się bez zbędnej zwłoki na wszystkich komputerach i nośnikach w przypadku wykrycia oprogramowania złośliwego na jednym komputerze lub nośniku będącym własnością SPZOZ.

15.21. Za zaplanowanie, konfigurowanie, aktywowanie specjalistycznego oprogramowania monitorującego wymianę danych na styku sieci lokalnej i sieci rozległej odpowiada ASI.

XVI. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych a także ich napraw i niszczenia.

16.1. Przeglądy i konserwacja urządzeń wchodzących w skład systemu informatycznego powinny być wykonywane w terminach określonych przez producenta sprzętu.

16.2. Nieprawidłowości ujawnione w trakcie tych działań powinny być niezwłocznie usunięte, a ich przyczyny przeanalizowane. Zaistniały fakt ASI odnotowuje w dzienniku dla systemu informatycznego (stanowiącego załącznik nr 12).

16.3. Konserwacja baz danych przeprowadzana jest zgodnie z zaleceniami twórców poszczególnych programów.

16.4. Bezwzględnie należy przestrzegać zasady, że gdy naprawa/serwis/przegląd /konserwacja sprzętu, na którym są przetwarzane informacje w tym dane osobowe ma odbywać się w siedzibie SPZOZ – to tylko w obecności upoważnionego pracownika.

16.5. Ze sprzętu uszkodzonego przeznaczonego do naprawy poza jednostką, lub zniszczenia muszą zostać usunięte wszystkie nośniki informacji, a fakt wymontowania musi być odnotowany w dzienniku dla systemu informatycznego.

16.6. Każde działanie serwisu musi zostać poprzedzone wcześniejszą informacją dla ASI lub osoby przez niego wyznaczonej o zakresie planowanych prac, terminie oraz czasie prac.

16.7. Po zakończeniu działań serwisu zewnętrznego na sprzęcie i aplikacjach służących do przetwarzania danych osobowych należy sprawdzić stan systemu, poprawność praw dostępu i uprawnień użytkowników systemu.

16.8. Awarie, naprawy, przeglądy oraz konserwacje należy odnotować w dzienniku dla systemu informatycznego urządzenia- stanowiący zał. nr 9.

16.9. W przypadku podjęcia podejrzeń, iż awaria sprzętu mogła powodować ryzyko naruszenia bezpieczeństwa danych osobowych należy postępować zgodnie z działem XIV Polityki – Postępowanie w sytuacji naruszenia bezpieczeństwa danych osobowych.

16.10. 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.

16.11. Dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie. Fakt ten musi być odnotowany w dzienniku dla systemu informatycznego.

16.12. Likwidację nośników informacji przeprowadza komisja powołana przez Administratora Danych Osobowych. W protokole potwierdzającym likwidację danych wskazuje się: skład osobowy komisji, datę likwidacji i sposób usunięcia nośnika danych, nazwa zbioru, do którego był on wykorzystywany.

XVII. Użytkowanie urządzeń przenośnych.

17.1. W przypadku przechowywania na komputerze przenośnym danych osobowych, pracownik zobowiązany jest do ich przechowywania ich na dysku szyfrowanym, zabezpieczonym, co najmniej ośmioznakowym hasłem (duże, małe litery, znaki specjalne lub cyfry).

17.2. Wszystkie urządzenia przenośne (smartfony służbowe, tablety, komputery przenośne) muszą być zabezpieczone mechanizmem identyfikującym uprawnionego użytkownika.

17.3. Przenośne urządzenia służbowe nie mogą być wykorzystywane przez inne osoby (w tym rodzina) niż pracownik, który otrzymał w/w sprzęt do pracy służbowej.

17.4. Przenośne urządzenia służbowe mogą być tylko wykorzystywane do zadań służbowych wynikających z zakresu obowiązków lub poleceń bezpośredniego przełożonego.

17.5. Na komputerach przenośnych przeznaczonych do zewnętrznych prezentacji multimedialnych nie powinny, o ile jest to możliwe, znajdować się dane osobowe lub stanowiące tajemnicę SPZOZ.

17.6. W przypadku kradzieży lub zgubienia urządzenia przenośnego pracownik powinien natychmiast poinformować o tym fakcie kierownika komórki organizacyjnej (bezpośredniego przełożonego), zaznaczając jednocześnie, jakiego rodzaju dane były na tym urządzeniu przechowywane. kierownik komórki organizacyjnej (przełożony)o tym fakcie ma obowiązek poinformować ADO.

17.7. Pracownik zobowiązany jest do zabezpieczenia laptopa w czasie transportu, a w szczególności:

- zaleca się przenoszenie go w specjalnym futerale;
- urządzenia przenośne nie powinny być użytkowane w miejscach publicznych, gdzie nie ma możliwości zabezpieczenia informacji znajdujących się na tych urządzeniach;
- podczas jazdy samochodem zaleca się przechowywanie komputera przenośnego w miejscu niedostępnym dla osób trzecich.

17.8. W przypadku pozostawiania komputerów przenośnych w biurze zaleca się umieszczanie ich po zakończeniu pracy w zamykanych szafkach lub sejfie.

17.9. Użytkownik laptopa jest zobowiązany do regularnego tworzenia kopii bezpieczeństwa danych na serwerze lub zapasowych nośnikach elektronicznych (pendrive, CD, DVD). Nośniki z takimi kopiami powinny być przechowywane w bezpiecznym miejscu, z uwzględnieniem ochrony przed dostępem osób niepowołanych.

17.10. ASI zobowiązany jest do podejmowania działań mających na celu zabezpieczenie komputerów przenośnych. W szczególności powinien on:

1) dokonać konfiguracji oprogramowania na komputerach przenośnych w sposób wymuszający korzystanie z haseł, wykorzystywanie haseł odpowiedniej, jakości oraz wymuszającym okresową zmianę haseł zgodnie z wymaganiami dla systemu informatycznego przetwarzającego dane osobowe;
2) zabezpieczyć dyski komputerów przenośnych poprzez zastosowanie oprogramowania szyfrującego;
3) dokonać na komputerze przenośnym instalacji i konfiguracji oprogramowania antywirusowego;
4) oznaczyć komputer przenośny programowo lub fizycznie w sposób identyfikujący właściciela tego urządzenia z wskazaniem jednostki organizacyjnej i jej adresu, jako właściciela komputera.

XVIII. Postępowanie w sytuacji naruszenia bezpieczeństwa danych osobowych.

18.1. Przez naruszenie bezpieczeństwa danych osobowych należy rozumieć wszelkie mogące mieć miejsce zdarzenia lub działania, które stanowią lub mogą stanowić przyczynę utraty zasobów, zmian poufności, integralności, dostępności informacji lub niezawodności systemów, a także odstępstwa od obowiązujących procedur postępowania, nawet, jeżeli nie prowadzą do wyżej wymienionych skutków. W szczególności są to wszelkie sytuacje, w których nastąpiła utrata (np. kradzież lub zniszczenie) lub nieuzasadniona modyfikacja danych lub części danych (nawet, jeśli możliwe jest całkowite odtworzenie utraconych danych) a także możliwość dostępu do danych dla osób nieposiadających upoważnienia do ich przetwarzania.

18.2. Na możliwość wystąpienia naruszenia bezpieczeństwa danych osobowych mogą wskazywać między innymi:

1) nietypowy stan pomieszczeń przetwarzania (naruszone zabezpieczenia, otwarte pomieszczenia, okna, drzwi od szaf, biurek, włączone urządzenia);
2) zaginięcie sprzętu lub nośników informacji (dyskietek, dokumentów papierowych, itp.);
3) nieuzasadnione modyfikacje lub usunięcie danych, niezgodności w danych;
4) nieprawidłowe lub nietypowe działanie systemu informatycznego (lub nietypowe komunikaty wyświetlane na monitorze).
5) przesłania danych osobowych do niewłaściwego miejsca lub adresata.
6) znalezienia poza pomieszczeniami przetwarzania wszelkich dokumentów, wydruków, dyskietek i innych nośników informacji;

18.3. Przykłady typowych zagrożeń zostały wymienione w załączniku nr 15 „Metodyki zarządzania ryzykiem w ochronie danych osobowych”.

18.4. Administratorzy systemów informatycznych powinni zwracać uwagę między innymi na:

1) przypadki niskiej wydajności systemu;
2) nietypowy przepływ danych;
3) nietypowe czasy wykorzystywania systemu;

4) dużą liczbę nieudanych prób logowania.

18.5. Po stwierdzeniu lub podejrzeniu wystąpienia incydentu naruszenia bezpieczeństwa informacji użytkownik powinien:

1) bez zbędnej zwłoki poinformować ASI w przypadku, gdy incydent miał miejsce w systemie informatycznym;
2) poinformować bezpośredniego przełożonego o zaistniałym fakcie;
3) Kierownik komórki organizacyjnej lub ASI bez zbędnej zwłoki informuje ADO;
4) powstrzymać się od wszelkich czynności w pomieszczeniu przetwarzania mogących zatrzeć ślady naruszenia bezpieczeństwa informacji;
5) powstrzymać się od wszelkich działań w systemie informatycznym, zwłaszcza od usuwania podejrzanego oprogramowania;

18.6. W przypadku otrzymania od użytkownika systemu informatycznego, zgłoszenia o wystąpieniu lub podejrzeniu wystąpienia incydentu, ASI powinien:

1) ustalić, czy incydent rzeczywiście miał miejsce;
2) ustalić, czy istnieje zagrożenie dla dalszego prawidłowego funkcjonowania systemu;
3) ustalić, czy system powinien zostać odizolowany od sieci, jeśli tak, to poinformować o tym ADO, IOD oraz osobę kierującą komórką informatyczną;
4) zabezpieczyć dowody zdarzenia;
5) zalecić użytkownikowi sposób dalszego postępowania lub, jeśli podejrzenie naruszenia bezpieczeństwa nie zostało potwierdzone, poinformować go o możliwości kontynuowania pracy.

18.7. ASI sporządza notatkę dla IOD zawierającą: datę, godzinę wystąpienia incydentu, opis incydentu, opis okoliczności incydentu oraz podjęte działania.

18.8. Po otrzymaniu zgłoszenia o wystąpieniu zagrożenia lub incydentu, IOD:

1) zbiera od zgłaszającego zagrożenie lub incydent oraz w razie potrzeby od ASI, szczegóły dotyczące zagrożenia lub incydentu m.in. czas wystąpienia, opis i okoliczności zdarzenia;
2) ustala zakres i przyczyny zagrożenia lub incydentu oraz ewentualne skutki zagrożenia;
3) zabezpiecza ewentualne dowody;
4) ustala czy zagrożenie spowodowało realny incydent;

5) ustala wpływ incydentu na zagrożenie praw lub wolności osób, których dane dotyczą;
6) w porozumieniu z ASI rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń i incydentów w przyszłości;
7) ustala osoby odpowiedzialne za naruszenie;
8) inicjuje działania dyscyplinarne;
9) zaleca użytkownikowi oraz w razie potrzeby także ASI, sposób dalszego postępowania;
10) wyznacza użytkownikowi oraz, jeśli to konieczne, ASI, termin sporządzenia notatki służbowej o incydencie.

18.9. Z każdego incydentu naruszenia bezpieczeństwa informacji IOD sporządza dla ADO raport, zgodnie z wzorem określonym w załączniku 10.

18.10. Do sporządzenia raportu ADO ma prawo żądać wyjaśnień i współpracy od pracowników.

18.11. W przypadku incydentu, który może powodować wysokie ryzyko naruszenia prawa lub wolność osoby fizycznej IOD opracowuje zgłoszenie naruszenia ochrony danych osobowych do organu nadzorczego, który po podpisaniu przez ADO jest przesyłamy do PUODO w terminie nie późniejszym niż 72 h od stwierdzenia naruszenia.

18.12. Pkt. 18.11 dotyczy sytuacji, kiedy naruszenie wystąpiło na danych, których SPZOZ jest ADO

18.13. Treść zgłoszenia musi wypełniać wymogi art. 33 ust 3 RODO.

18.14. W przypadku sytuacji opisanych w pkt. 18.11 oraz 18.12 IOD przygotowuje zawiadomienie do osoby, której dane dotyczą, w którym jasnym i prostym językiem opisuje charakter naruszenia oraz zawiera informacje zawarte w art. 33 ust 3 RODO.

18.15. W przypadku, gdy naruszenie bezpieczeństwa informacji dotyczy danych osobowych powierzonych dla SPZOZ, IOD jest zobowiązany do poinformowania ADO, od którego dane otrzymano o naruszeniu bezpieczeństwa i udzielenia pełnej informacji o zaistniałym incydencie. IOD jest zobowiązany udzielić w/w informacji w ciągu 24 h od chwili ujawnienia incydentu.

18.16. Wszystkie incydenty i zagrożenia są ewidencjonowane w Rejestrze incydentów i zagrożeń bezpieczeństwa oraz działań korygujących i zabezpieczających stanowiący załącznik nr 11.

XIX. Audyty i sprawdzenia zgodności przetwarzania informacji w tym danych osobowych.

19.1. Audyty realizowane są w trybie audytów planowych.

19.2. IOD sporządza plan audytu, który przedstawia dla ADO, na co najmniej dwa tygodnie przed planowanym audytem.

19.3. Plan audytu jest przygotowywany przez IOD na okres nie krótszy niż kwartał i nie dłuższy niż rok.

19.4. Zbiory danych oraz systemy informatyczne służące do przetwarzania lub zabezpieczania informacji w tym danych osobowych winny być objęte audytem nie rzadziej niż raz na trzy lata.

19.5. Poza audytem wymienionym w pkt 19.1 IOD dokonuje sprawdzeń doraźnych, mających ustalić bieżące respektowanie zapisów polityki bezpieczeństwa.

19.6. W przypadku sprawdzenia doraźnego IOD zawiadamia ADO o rozpoczęciu sprawdzenia przed podjęciem pierwszej czynności w toku sprawdzenia.

19.7. Podczas audytu i sprawdzenia wszyscy pracownicy są zobowiązani do aktywnej współpracy z IOD.

19.8. Po zakończeniu audytu IOD przygotowuje raport z audytu w terminie nie dłuższym niż 30 dni.

19.9. Raport z audytu zawiera co najmniej:

1) Datę sporządzenia raportu
2) Pełna nazwa ADO
3) Imiona i nazwiska osób biorących udział w audycie
4) Termin przeprowadzenia audytu
5) Okres objęty audytem
6) Cel audytu
7) Zakres przedmiotowy audytu
8) Podjęte działania i zastosowane techniki audytu
9) Ustalenia stanu faktycznego
10) Określenie oraz analiza przyczyn i skutków ewentualnych uchybień
11) Rekomendacje

19.10. Po zakończeniu sprawdzenia IOD przygotowuje sprawozdanie ze sprawdzenia niezwłocznie po jego zakończeniu, jednak w terminie nie dłuższym niż 14 dni.

XX. Postanowienia końcowe.

20.1. Polityka oraz wszystkie pozostałe dokumenty dotyczące ochrony danych osobowych w SPZOZ są dokumentami wewnętrznymi i nie mogą być udostępniane osobom postronnym w żadnej formie.

20.2. W celu zwiększenia bezpieczeństwa część załączników Polityki może być wyłączona z publikacji wewnętrznej SPZOZ a dostęp do nich mogą mieć tylko osoby, które niezbędnie muszą się z nimi zapoznać.

20.3. Niezależnie od odpowiedzialności określonej w przepisach prawa powszechnie obowiązującego, naruszenie zasad określonych w niniejszej Polityce będzie traktowane, jako ciężkie naruszenie obowiązków pracowniczych.

20.4. W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie przepisy RODO i UODO.

20.5. Pracownicy Administratora Danych zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce, w wypadku odrębnych od zawartych w niniejszej Polityce uregulowań występujących w innych procedurach obowiązujących w SPZOZ, użytkownicy mają obowiązek stosowania zapisów dalej idących, których stosowanie zapewni wyższy poziom ochrony danych osobowych.

20.6. Niniejsza Polityka oraz dokumenty z nią powiązane powinny być aktualizowane wraz ze zmieniającymi się przepisami prawnymi o ochronie danych osobowych, oraz zmianami faktycznymi w ramach Administratora Danych Osobowych, które mogą powodować, że zasady ochrony ochrony danych osobowych określone w obowiązujących dokumentach będą nieaktualne lub nieadekwatne.

20.7. Zmiany niniejszej Polityki wymagają przeglądu innych dokumentów dotyczących ochrony danych osobowych obowiązujących u Administratora Danych Osobowych.

20.8. Niniejszą Politykę wprowadza się w życie w formie zarządzenia właściciela SPZOZ.

20.9. Wszelkie zmiany w niniejszej Polityce wprowadza się w życie w formie zarządzenia właściciela SPZOZ.

Załącznik nr 1 - Wzór upoważnienia

Upoważnienie do przetwarzania danych nr …./……..

na podstawie art. 29 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/ oraz oraz Ustawy o Ochronie Danych Osobowych Dz.Ust. 2018.1000 z 24.05.2018r..

Osoba, której nadawane jest upoważnienie do przetwarzania danych osobowych:

……..……

Imię i nazwisko, stanowisko

Zakres nadanego upoważnienia do przetwarzania danych osobowych:

Lp.	**Dane osobowe objęte zbiorem o nazwie:**		
1.			
2.			
3.			
4.			
Przetwarzane na nośnikach papierowych:	☐ tak ☐ nie	**Przetwarzane w formie elektronicznej:**	☐ tak ☐ nie

z wykorzystaniem systemów informatycznych[1]:

Nazwa systemu[2]	**Zakres uprawnień systemowych[3]**

Okres na jaki nadano upoważnienie: ……..

W imieniu Administratora Danych (podpis): ……..

[1] Wypełnić w razie przetwarzania danych w formie elektronicznej.

[2] Należy uzupełnić wiersze poniżej, podając nazwę systemu w przypadku, gdy dane osobowe przetwarzane są w systemie informatycznym.

[3] Należy wskazać zakres uprawnień poprzez wskazanie funkcji systemowych: (P) pełne / (WG)wgląd do danych / (W)wprowadzanie danych / (M) modyfikacja danych / (U) usuwanie danych.

Załącznik nr 2 - Wzór oświadczenia o przeszkoleniu

…….. ……

(imię i nazwisko) *(miejscowość, data)*

OŚWIADCZENIE

Oświadczam, iż zostałam/zostałem przeszkolona/przeszkolony z zakresu przepisów dotyczących ochrony danych osobowych, w szczególności Rozporządzenia Parlamentu Europejskiego i Rady (UE 2016/679) z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE oraz Ustawy o Ochronie Danych Osobowych Dz.Ust. 2018.1000 z 24.05.2018r. a także wydanych na jej podstawie aktów wykonawczych oraz wprowadzonych i wdrożonych do stosowania przez Administratora Danych „Polityki Bezpieczeństwa danych osobowych".

Zobowiązuję się do:

- respektowanie w/w wymienionych aktów prawnych i dokumentów;
- zachowania w tajemnicy danych osobowych uzyskanych w związku z zatrudnieniem oraz sposobów ich zabezpieczania, również po ustaniu stosunku pracy;
- korzystania ze sprzętu teleinformatycznego będącego własnością pracodawcy wyłącznie w związku z wykonywaniem obowiązków pracowniczych;
- wykorzystywania jedynie legalnego oprogramowania będącego własnością pracodawcy;
- należytej dbałości o sprzęt i oprogramowanie

……

podpis pracownika

Załącznik nr 2 - Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

L.p.	Nazwa zbioru danych	Nazwisko i imię osoby upoważnionej	Identyfikator	Numer upoważnienia	Data nadania upoważnienia	Zakres upoważnienia	Data wygaśnięcia / cofnięcia upoważnienia	Uwagi (przyczyny cofnięcia uprawnień)

Załącznik nr 3 – Wzór rejestru czynności przetwarzania danych osobowych

Wykaz zbiorów danych osobowych

Nr wpisu: …….

Opis kategorii osób (zbioru) w formie rejestru czynności przetwarzania	Aktywa	Proces przetwarzania / opis funkcjonalny
1. Opis kategorii osób (nazwa zbioru) **……** **1a. Opis kategorii danych osobowych** …… **2. Cele przetwarzania** …… **3. Kategorie odbiorców** …… **4. kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych (i ich nazwy) – …… **5. planowane terminy usunięcia poszczególnych kategorii danych** …… **6. opis technicznych i organizacyjnych środków bezpieczeństwa** Patrz: Regulamin Ochrony Danych Osobowych **7. Podstawa prawna przetwarzania** ……	**1. Informacje (dokumentacja papierowa)** **……..** **2. Programy i systemy operacyjne** **……..** **3. Infrastruktura IT** **……..** **4. Infrastruktura** **……..** **5. Pracownicy i współpracownicy** **……..** **6. Outsourcing** **…….**	**……..**

Załącznik nr 4 - Wzór odwołania upoważnienia

ODWOŁANIE UPOWAŻNIENIA
Nr … / …

Na podstawie art. 29 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.

z dniem ……odwołuję upoważnienie/a nr……..…….

Dla Pani/Pana ……

(imię i nazwisko upoważnionego)

W związku z ……..

:……

(podpis ADO)

Załącznik nr 5 – Wzór umowy powierzenia danych

Umowa powierzenia przetwarzania danych osobowych

zawarta dnia _____ pomiędzy:

(zwana dalej „Umową")

…… z siedzibą w ……., przy……
NIP……..REGON…….

Reprezentowana przez:

……

Zwana w dalszej części umowy „**Podmiotem przetwarzającym**"

oraz

SP ZOZ MSWiA w Koszalinie

Zwana dalej „**Administratorem danych osobowych**"

Zwanymi łącznie „Stronami"

§ 1

Powierzenie przetwarzania danych osobowych

1. Administrator danych powierza Podmiotowi przetwarzającemu, w trybie art. 28 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 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 w dalszej części „RODO", dane osobowe do przetwarzania, na zasadach i w celu określonym w niniejszej Umowie.

2. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą Umową, RODO oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
3. Podmiot przetwarzający oświadcza, iż stosuje środki bezpieczeństwa spełniające wymogi RODO.

§2

Zakres i cel przetwarzania danych

1. Podmiot przetwarzający będzie przetwarzał, powierzone na podstawie Umowy następujące kategorie danych i w zakresie:
   a) Dane Osobowe Pracowników w zakresie:

   b) Dane Kontrahentów (dostawcy) w zakresie:
      - Dane identyfikacyjne,
      - dane adresowe

   c) Dane klientów (odbiorcy):
      - Dane identyfikacyjne,
      - dane adresowe

   itp.

2. Powierzone przez Administratora danych dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu realizacji umowy z dnia …….. *nr* …… zwanej dalej Umową Główną.

§3

Obowiązki podmiotu przetwarzającego

1. Podmiot przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, o których mowa w art. 32 Rozporządzenia.
2. Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
3. Podmiot przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy, (o której mowa w art. 28 ust 3 pkt b RODO) przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej

umowy, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu.

4. Podmiot przetwarzający zobowiązany jest do przeszkolenia swoich pracowników lub współpracowników w zakresie sposobów zabezpieczenia przetwarzanych danych.
5. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej umowy.
6. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem usuwa/ zwraca* Administratorowi wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.
7. W miarę możliwości Podmiot przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 Rozporządzenia.
8. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki, nie później niż w ciągu 24 h, zgłasza je administratorowi.
9. W przypadku zgłoszenia o którym mowa w pkt. 8 podmiot przetwarzający musi zawrzeć wszystkie informacje wymagane art. 33 ust 3 RODO.
10. W przypadku nie dotrzymania terminu wskazanym w pkt. 8 podmiot przetwarzający jest zobowiązany podać przyczyny opóźnienia.

§4

Prawo kontroli

1. Administrator danych zgodnie z art. 28 ust. 3 pkt h) RODO ma prawo kontroli, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia umowy.
2. Administrator danych realizować będzie prawo kontroli w godzinach pracy Podmiotu przetwarzającego i z minimum 32 h jego uprzedzeniem.
3. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora danych nie dłuższym niż 7 dni.
4. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 i 32 RODO w zakresie powierzonych danych.

§5

Dalsze powierzenie danych do przetwarzania

1. Podmiot przetwarzający może powierzyć dane osobowe objęte niniejszą umową do dalszego przetwarzania podwykonawcom jedynie w celu wykonania umowy po uzyskaniu uprzedniej pisemnej zgody Administratora danych.
2. Podwykonawca, o którym mowa w §5 ust. 1 Umowy winien spełniać te same gwarancje i obowiązki jakie zostały nałożone na Podmiot przetwarzający w niniejszej Umowie.
3. Podmiot przetwarzający może dokonać dalszego podpowierzenia danych dopiero w chwili uzyskania potwierdzenia, iż podwykonawca spełnia wymogi określone art. 28 i 32 RODO.
4. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za nie wywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.

§ 6

Odpowiedzialność Podmiotu przetwarzającego

1. Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią umowy, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.
2. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora danych o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający danych osobowych określonych w umowie, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Podmiotu przetwarzającego, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania w Podmiocie przetwarzającym tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez Prezesa Urzędu Ochrony Danych Osobowych. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora danych.

§7

Czas obowiązywania umowy

1. Niniejsza umowa obowiązuje prze okres trwania Umowy Głównej.
2. Każda ze stron może wypowiedzieć niniejszą umowę z dniem, z którym przestają być związane postanowienia Umowy Głównej

§8

Rozwiązanie umowy

1. Administrator danych może rozwiązać niniejszą umowę ze skutkiem natychmiastowym gdy Podmiot przetwarzający:
   a) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;
   b) przetwarza dane osobowe w sposób niezgodny z umową;
   c) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora danych;

§9

Zasady zachowania poufności

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora danych i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej.
2. Podmiot przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora danych w innym celu niż wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy.

§10

Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach dla każdej ze stron.
2. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego oraz RODO.
3. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej umowy będzie sąd właściwy Administratora danych.

_____ _____

Administrator danych Podmiot przetwarzający

Załącznik nr 6 - Wzór ewidencji umów powierzenia danych

L.p.	Nr umowy	Data zawarcia	Okres obowiązywania umowy	Podmiot przetwarzający	Zakres powierzonych danych	Cel powierzenia	uwagi

Załącznik nr 7 - Wzór ewidencji udostępnionych danych

EWIDENCJA UDOSTĘPNIANIA DANYCH

L.p.	Data udostępnienia danych	Podstawa prawna udostepnienia	Podmiot, któremu dane udostępniono (nazwa, adres)	Zakres udostępnionych danych	Podpis pracownika

Załącznik nr 8 - Wzór dokonania obowiązku informacyjnego

Zgodnie z art. 13 ust. 1 i ust. 2 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. informuję, iż:

1. administratorem Pani/Pana danych osobowych jest SP ZOZ MSWiA w Koszalinie z siedzibą w Koszalinie przy ulicy Szpitalna 2 (zwaną dalej SPZOZ);
2. Dane kontaktowe inspektora ochrony danych w SPZOZ - e-mail
3. Pani/Pana dane osobowe przetwarzane będą w celu … (*należy podać cel przetwarzania) na podstawie … (*należy podać podstawę prawną przetwarzania np. art. 6 ust 1 pkt a/b/c/d/e/f, art. 9 ust 2 a)-j));
4. odbiorcą Pani/Pana danych osobowych będą … (*należy podać również podmioty przetwarzające);
5. Pani/Pana dane osobowe będą przechowywane przez okres … (* okres można ustalić na podstawie JRWA, jeżeli nie ma możliwości wskazania okresu przechowywania należy podać kryterium ustalania tego okresu np. do czasu wyłonienia zwycięscy konkursu, do czasu zakończenia rekrutacji itd.);
6. posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania (*jeżeli przetwarzanie odbywa się na podstawie zgody), którego dokonano na podstawie zgody przed jej cofnięciem;
7. ma Pan/Pani prawo wniesienia skargi do UODO gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.;
8. podanie przez Pana/Panią danych osobowych jest … (*wybrać odpowiednio: wymogiem ustawowym/warunkiem umownym/warunkiem zawarcia umowy). Jest Pan/Pani zobowiązana do ich podania a konsekwencją niepodania danych osobowych będzie … (* jeżeli osoba, której dane dotyczą, jest zobowiązana do ich podania należy wskazać ewentualne konsekwencje niepodania danych);

jeżeli występuje:

9. Pani/Pana dane będą przetwarzane w sposób zautomatyzowany w tym również w formie profilowania. Zautomatyzowane podejmowanie decyzji będzie odbywało się na zasadach … , konsekwencją takiego przetwarzania będzie … (*należy wskazać istotne informacje o zasadach zautomatyzowanego podejmowania decyzji

oraz informacje o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.)

Załącznik nr 9 – Wzór dziennika dla systemów informatycznych

DZIENNIK DLA SYSTEMÓW INFORMATYCZNYCH

Lp.	Data i godzina zdarzenia	Opis zdarzenia	Podjęte działania/wnioski	Podpis

Raport z incydentu

Załącznik nr 10 – Wzór raportu z incydentu naruszenia bezpieczeństwa informacji

……., data ……

Administrator

Danych Osobowych

Raport z incydentu naruszenia bezpieczeństwa informacji **Nr ...../rok…..**

Data incydentu			
Godzina incydentu			
Miejsce incydentu (nr pomieszczenia)			
System/aplikacja			
Dane osoby zgłaszającej			
Imię i nazwisko			
Stanowisko			
Komórka organizacyjna			
Charakter zdarzenia (*)			
	Nieuprawniony dostęp do systemu		Kradzież danych
	Nieuprawniony dostęp do danych		Utrata danych
	Nieuprawniony przekaz danych		Mechaniczne uszkodzenie urządzeń do przetwarzania danych
	Wykrycie wirusa (podać rodzaj wirusa):		
	Inne (podać jakie):		
Informacje o danych, których dotyczy incydent.(**)			
Wpływ zdarzenia na prawa i wolność osoby której dane dotyczą			
Świadkowie zdarzenia			
Imię i nazwisko			
Stanowisko			
Komórka organizacyjna			

Opis incydentu i wnioski:(***)

.....

Załączniki:

Inspektor Ochrony Danych

/data, podpis/

/verte/

(*) Należy zaznaczyć właściwe pola.

(**) Należy podać:

- Kategorię osób
- Liczbę osób których incydent dotyczy
- Kategorie danych
- Liczbę wpisów które dotyczy naruszenia

(***) Należy podać:

- Opis przebiegu zdarzenia,
- Opis zabezpieczonych dowodów,
- Wpływ incydentu na infrastrukturę systemu informatycznego,
- Wpływ incydentu na stan zbiorów danych osobowych,
- Opis podjętych decyzji i przeprowadzonych czynności wraz z uzasadnieniem,
- Wnioski i propozycje w celu podniesienia poziomu bezpieczeństwa informacji.

Do raportu należy dołączyć notatkę użytkownika oraz ASI.

Załącznik nr 11 – Wzór rejestru incydentów i zagrożeń oraz działań korygujących i zabezpieczających

Rejestr incydentów– i zagrożeń bezpieczeństwa oraz działań korygujących i zabezpieczających										
Nr raportu	Data stwierdzenia incydentu	Osoba		Podjęte działania		Czy wystąpiło prawdopodobieństwa naruszenia wolności i prawa osoby, której dotyczą dane	Zawiadomienie PUODO w ramach art. 33 RODO (data i potwierdzenie)	Zawiadomienie osoby, której dotyczą dane w ramach art. 34 RODO (data i potwierdzenie)	Data zamknięcia incydentu/ zagrożenia	Uwagi
		zgłaszająca	Powodująca naruszenia	Zapobiegawcze i korygujące	Skuteczność					

Załącznik nr 12 – Procedura zarządzania hasłem systemowym

Procedura zarządzania hasłem systemowym

1 Każdy Administrator systemu zobowiązany jest do bieżącej pracy na koncie roboczym. Użycie tzw. konta typu „root", lub „Administrator" dopuszczalne jest jedynie w sytuacjach awaryjnych lub podczas poważnych zmian wprowadzanych w administrowanym systemie.

2 Hasło administratora do systemów i programów, w których przetwarza się dane osobowe powinno być zmieniane nie rzadziej, niż co 30 dni.

3 ASI jest odpowiedzialny za zachowanie poufności haseł systemowych.

4 Hasła systemowe utrzymuje się w tajemnicy również po upływie ich ważności.

5 Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie.

6 W sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, ASI zobowiązany jest do natychmiastowej zmiany hasła.

7 Przy wyborze hasła obowiązują następujące zasady:

d) minimalna długość hasła - 8 znaków;

e) zakazuje się stosować: haseł, które użytkownik stosował uprzednio w okresie minionego roku, swojej nazwy użytkownika w jakiejkolwiek formie (pisanej dużymi literami, w odwrotnym porządku, dublując każdą literę, itp.), swojego imienia, drugiego imienia, nazwiska, przezwiska, pseudonimu w jakiejkolwiek formie, imion (w szczególności imion osób z najbliższej rodziny), ogólnie dostępnych informacji o użytkowniku takich jak: numer telefonu, numer rejestracyjny samochodu, jego marka, numer dowodu osobistego, nazwa ulicy na której mieszka lub pracuje, itp. wyrazów słownikowych, przewidywalnych sekwencji znaków z klawiatury np.: QWERTY","12345678",itp.;

f) należy stosować:

- hasła zwierające kombinacje małych i wielkich liter oraz cyfr lub znaków specjalnych (znaki interpunkcyjne, nawiasy, symbole @, #, & itp.);
- hasła, które można zapamiętać bez zapisywania;
- hasła łatwe i szybkie do wprowadzenia, po to by trudniej było podejrzeć je osobom trzecim,

8 Zmiany hasła nie wolno zlecać innym osobom.
9 W systemach, które umożliwiają opcję zapamiętania nazw użytkownika lub jego hasła nie należy korzystać z tego ułatwienia.
10 Po każdorazowej zmianie hasła ASI listę haseł przekazuje dla osoby wskazanej przez ADO.
11 Lista haseł powinna zawierać: login, treść hasła, datę jego wprowadzenia do systemu, datę modyfikacji hasła.
12 Punkt 10 dotyczy wszystkich systemów wykorzystywanych
13 Dostęp do haseł systemowych ma jednie ASI oraz ścisłe kierownictwo .
14 Otwarcie kopert z hasłami może się odbyć tylko komisyjnie przez ADO, ASI lub inne osoby upoważnione przez ADO.
15 Za zgodność zdeponowanych haseł ze stanem rzeczywistym odpowiada ASI.
16 W przypadku utraty uprawnień przez osobę administrującą systemem należy niezwłocznie zmienić hasła, do których miała dostęp.
17 W przypadku skompromitowania przynajmniej jednego hasła systemu informatycznego należy zmienić wszystkie hasła.
18 Wszelkie operacje związane z hasłem systemowym muszą być odnotowane w dzienniku dla systemu informatycznego.

Załącznik nr 13 – Procedura tworzenia kopi bezpieczeństwa

Procedura tworzenia kopii bezpieczeństwa

W celu zapewnienia bezpieczeństwa pracy systemu i możliwości odtworzenia danych po wystąpieniu awarii w SPZOZ wykonuje się kopie bezpieczeństwa zgodnie z poniższym trybem:

- Kopie wykonywane są codziennie za pomocą skryptu na serwerze na partycji dysku
- Od poniedziałku do piątku kopia jest kopiowana, pakowana i zapisywana na serwerze zewnętrznym.

1. ASI posiada wersje instalacyjne systemów operacyjnych oraz oprogramowania służącego do przetwarzania danych osobowych na nośnikach zewnętrznych.
2. Ponadto kopie baz i oprogramowania wykonuje się zawsze przed zainstalowaniem nowych składników oprogramowania lub zmianie konfiguracji.
3. Kopie danych powinny być okresowo sprawdzane pod kontem ich przydatności, prawidłowości wykonania oraz możliwości odtworzenia.
4. W przypadku wykonania kopii bezpieczeństwa wykonywanymi poza przypadkami opisanymi w pkt 1, na nośniku zewnętrznym (płyta DVD, dysk zewnętrzny), osoba wykonująca kopie odnotowuje w dzienniku dla systemu informatycznego stanowiącego załącznik nr 12 Polityki, gdzie należy wpisać datę wykonania kopi, osobę wykonującą kopie, numer nośnika, oraz oznaczenie zbioru. Dopuszcza się odnotowywanie tego faktu w logach systemu.
5. W przypadku automatycznej realizacji kopii bezpieczeństwa można odstąpić od pkt. 4
6. Nośniki kopii bezpieczeństwa, które zostały wycofane z użytkowania, podlegają zniszczeniu.
7. Zabrania się wykorzystywania nośników, na których wykonywane są kopie bezpieczeństwa do innych celów.
8. Zabrania się przenoszenia kopii bezpieczeństwa poza strefę przetwarzania danych osobowych opisaną w „Rejestrze czynności przetwarzania danych osobowych”.
9. Kopie bezpieczeństwa przechowywane są:
   - Na dyskach komputerów realizujących funkcję serwerów
   - Płyty DVD przechowywane w pomieszczeniu kasy w szafie pancernej
   - Na serwerach zewnętrznych.

Załącznik nr 14 – Wzór oświadczenie pracownika

……... ……

(imię i nazwisko) *(miejscowość, data)*

OŚWIADCZENIE

Oświadczam, iż **zostałam/zostałem przeszkolona/przeszkolony** z zakresu przepisów dotyczących ochrony danych osobowych, w szczególności Rozporządzenia Parlamentu Europejskiego i Rady (UE 2016/679) z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE Ustawy o Ochronie Danych Osobowych Dz.Ust. 2018.1000 z 24.05.2018r., a także wydanych na jej podstawie aktów wykonawczych oraz wprowadzonych i wdrożonych do stosowania przez Administratora Danych „Polityki Bezpieczeństwa danych osobowych", Regulaminu Ochrony Danych Osobowych.

Zobowiązuję się do:

- respektowanie w/w wymienionych aktów prawnych i dokumentów;
- zachowania w tajemnicy danych osobowych uzyskanych w związku z zatrudnieniem oraz sposobów ich zabezpieczania, również po ustaniu stosunku pracy;
- korzystania ze sprzętu teleinformatycznego będącego własnością pracodawcy wyłącznie i w związku z wykonywaniem obowiązków pracowniczych;
- wykorzystywania jedynie legalnego oprogramowania będącego własnością pracodawcy;
- należytej dbałości o sprzęt i oprogramowanie

…….

podpis pracownika