ZARZĄDZENIE NR 80/2016

Dyrektora Centrum Onkologii – Instytutu im. Marii Skłodowskiej-Curie
z dnia 24 listopada 2016 r.

w sprawie wprowadzenia „Instrukcji ogólnej zarządzania systemami informatycznymi w Centrum Onkologii – Instytucie im. Marii Skłodowskiej-Curie w Warszawie".

Na podstawie § 6 Statutu Centrum Onkologii – Instytutu im. Marii Skłodowskiej-Curie, zarządza się, co następuje:

§ 1

1. Wprowadza się do stosowania w Centrum Onkologii – Instytucie im Marii Skłodowskiej-Curie w Warszawie „Instrukcję ogólną zarządzania systemami informatycznymi Centrum Onkologii – Instytutu im. Marii Skłodowskiej-Curie w Warszawie" stanowiący załącznik do niniejszego zarządzenia.
2. Nadzór nad wykonaniem niniejszego zarządzenia powierza się Administratorowi Bezpieczeństwa Informacji.

§ 2

Zarządzenie wchodzi w życie z dniem wydania.

D Y R E K T O R
Centrum Onkologii – Instytutu
im. Marii Skłodowskiej-Curie

Prof. dr hab. n. med. Jan Walewski

I N S T R U K C J A O G Ó L N A

ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI W CENTRUM ONKOLOGII − INSTYTUCIE IM. MARII SKŁODOWSKIEJ-CURIE

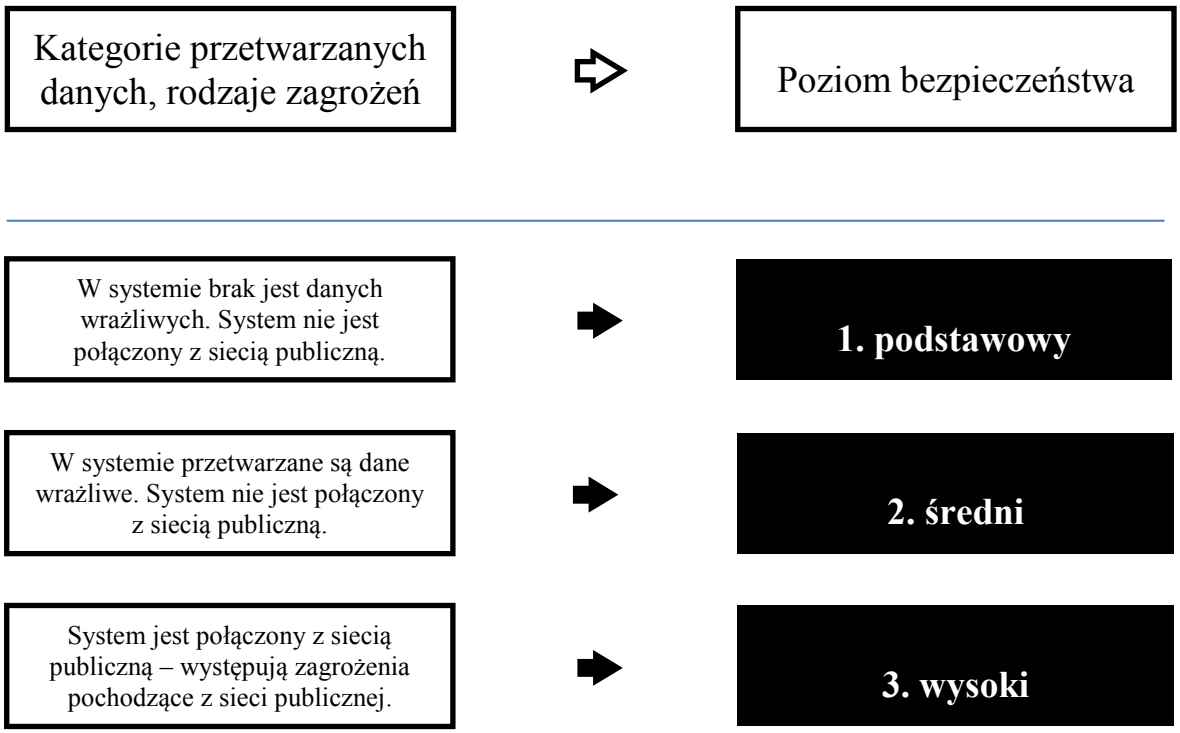
WARSZAWA 2016 r.

SPIS TREŚCI

ROZDZIAŁ I
WSTĘP

1. Instrukcja ogólna zarządzania systemami informatycznymi w Centrum Onkologii – Instytucie im. Marii Skłodowskiej-Curie, zwana dalej „Instrukcją ogólną" zatwierdzona przez Administratora Danych Osobowych tj. Dyrektora Centrum Onkologii – Instytutu im. Marii Skłodowskiej-Curie, zwanego dalej „Instytutem" przyjęta do stosowania stanowi dokument obowiązujący ogół pracowników i współpracowników. Zawarte w niej procedury i wytyczne dotyczą osób odpowiedzialnych w Instytucie za ich realizację stosownie do przydzielonych uprawnień, zakresu obowiązków i odpowiedzialności.
2. Mając na względzie obowiązek stosowania przez Administratora Danych Osobowych, odpowiednich zabezpieczeń systemów informatycznych określonych w art. 36–39a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 2016 poz. 922), **wprowadza się do stosowania środki bezpieczeństwa na poziomie wysokim** w rozumieniu rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004, nr 100 poz. 1024)

Zależności pomiędzy zakresem przetwarzanych danych, zagrożeniem na jakie są narażone przetwarzane dane, a wymaganym poziomem bezpieczeństwa obrazuje rys. nr 1.



ROZDZIAŁ II
DEFINICJE

W Instytucie funkcjonuje mieszany system podziału odpowiedzialności za obsługę elektronicznych danych medycznych (EDM). Administratora systemu/Administratora lokalnego, podzielono pomiędzy pracowników Instytutu i podmioty zewnętrzne, świadczące usługi informatycznego wsparcia. W ramach zawartych umów na informatyczne wsparcie funkcjonujących w Instytucie baz danych, w tym także na wsparcie systemu o strukturze rozproszonej terytorialnie (Krajowy Rejestr Nowotworów), wyznaczeni pracownicy Instytutu mają administracyjny dostęp do serwerów baz danych, zarządzają kontami i uprawnieniami użytkowników systemu, a także umożliwiają zdalny dostęp do serwera uprawnionemu podmiotowi na jego żądanie. Do obowiązków uprawnionych podmiotów należy instalacja, konfiguracja, aktualizacja oprogramowania, dbałość o bezpieczeństwo baz danych, nadzorowanie, wykrywanie, eliminowanie nieprawidłowości i zagrożeń.

W systemie Simple, ERP, Płatnik do obowiązków Administratorów lokalnych należy również instalacja, konfiguracja, aktualizacja oprogramowania, dbałość o bezpieczeństwo baz danych, nadzorowanie, wykrywanie, eliminowanie nieprawidłowości i zagrożeń.

1. **Administrator Danych Osobowych (ADO)** – organ, jednostka organizacyjna, podmiot lub osoba, decydująca o celach i środkach przetwarzania danych osobowych. Administrator Danych Osobowych jest powoływany na podstawie ustawy o ochronie danych osobowych, jest odpowiedzialny za przetwarzanie danych osobowych w systemie, wykonuje on czynności przewidziane w ww. ustawie.

   Administrator Danych Osobowych może powierzyć przetwarzanie danych innemu podmiotowi w drodze umowy zawartej na piśmie.

   Zgodnie z przepisem art. 7 pkt. 4 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2016 poz. 922) w zw. z art. 23 i 24 ustawy z dnia 30 kwietnia 2010 r. o instytutach badawczych (Dz. U. z 2016 r., poz. 371 z późn. zm.), Administratorem Danych Osobowych jest Dyrektor Instytutu.
2. **Administrator Bezpieczeństwa Informacji (ABI)** − osoba wyznaczona przez Administratora Danych Osobowych, odpowiedzialna za nadzór nad przestrzeganiem ustanowionych zasad ochrony danych osobowych. Administrator Bezpieczeństwa Informacji powoływany jest na podstawie ustawy o ochronie danych osobowych. Rolę Administratora Bezpieczeństwa Informacji może pełnić jedna osoba, wyznaczona przez Dyrektora Instytutu, działającą w jego imieniu, odpowiedzialna za nadzór nad bezpieczeństwem przetwarzanych danych osobowych.
3. **Administrator Systemów Informatycznych (ASI) (Kierownik Działu Informatyki)** – osoba odpowiedzialna za administrowanie systemem elektronicznych danych medycznych (EDM). W Instytucie, jest to osoba odpowiedzialna za nadzór nad prawidłowym przetwarzaniem elektronicznych danych medycznych, poprzez koordynację działań pracowników Działu/Sekcji Informatyki, przez wyznaczonych pracowników komórek i jednostek organizacyjnych, którym powierzono zadania Administratora lokalnego oraz podmiotów zewnętrznych świadczących usługi

informatycznego wsparcia baz danych. Zadaniem, jest nadzór nad bezpieczeństwem danych osobowych przetwarzanych w systemie informatycznym Instytutu oraz przeciwdziałanie naruszeniom bezpieczeństwa tych danych;

4. **Administrator systemu/Administrator lokalny** – osoba lub zespół odpowiedzialny za administrowanie/zarządzanie sprzętem (komputery robocze, urządzenia mobilne) i zainstalowanym oprogramowaniem (system operacyjny, oprogramowanie antywirusowe) będącymi w gestii Instytutu (w zależności od wybranego modelu).
5. **Bezpieczeństwo systemu informatycznego** − zapewnienie poufności, integralności i dostępności informacji na odpowiednim poziomie. Miarą bezpieczeństwa jest prawidłowe szacowanie ryzyka związanego z przetwarzaniem danych osobowych stanowiącym przedmiot Polityki Bezpieczeństwa Informacji;
6. **Dane osobowe** – zgodnie z art. 6 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 2016 poz. 922), są to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne
7. **Osoba upoważniona do przetwarzania danych osobowych**, − osoba zatrudniona na umowie o pracę lub osoba związana umową cywilno-prawną z Instytutem, zaznajomiona z Polityką Bezpieczeństwa Instytutu oraz Instrukcją ogólną, a także posiadająca upoważnienie imienne do przetwarzania danych osobowych.
8. W bazach danych o strukturze rozproszonej terytorialnie (np. KRN, SZOI, EWUŚ, ApKolce) **osobą upoważnioną** jest:
    1) osoba zapoznana z Polityką Bezpieczeństwa Instytutu oraz z Instrukcją ogólną, która podpisała oświadczenie (Załącznik nr 3 do „Polityki Bezpieczeństwa"), otrzymała od Dyrektora Instytutu upoważnienie (Załącznik nr 4 do „Polityki Bezpieczeństwa") przydzielono jej konto i określono zakres dostępu do systemu (pracownicy KRN i WRN, SZOI, EWUŚ, ApKolce);
    2) osoba, która stosować się będzie do Polityki Bezpieczeństwa oraz Instrukcji ogólnej u Kierownika placówki medycznej, w której jest zatrudniona, i której przydzielono konto i określono zakres dostępu do systemu (np. KRN);
    3) osoba, która wykonuje praktykę lekarską we własnym zakresie i stosuje się do zasad określonych w Ustawie o ochronie danych osobowych, i której przydzielono konto i określono zakres dostępu do systemu (np. KRN).
9. **Osoba trzecia** – każda osoba nieupoważniona i przez to nieuprawniona do dostępu do danych osobowych lub zbiorów tych danych. Osobą trzecią jest również osoba posiadająca upoważnienie wydane przez Dyrektora Instytutu, lecz podejmująca czynności przekraczające zakres udzielonego jej upoważnienia.
10. **Przetwarzanie danych** – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie,

udostępnianie i usuwanie, w zwłaszcza te, które wykonuje się w systemach informatycznych.

11. **Powierzanie danych** – przekazanie przez Instytut podmiotom zewnętrznym danych osobowych na podstawie zawartej umowy.
12. **Dalsze powierzanie danych** – przekazanie podwykonawcom przez podmioty zewnętrzne związane umową, danych osobowych powierzonych im przez Instytut.
13. **Stacja robocza** – każdy komputer przeznaczony do bezpośredniej pracy (w odróżnieniu od serwera, który tylko udostępnia zdalnie jakieś usługi).
14. **System informatyczny** – sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych; w systemie tym pracuje co najmniej jeden komputer centralny i system ten tworzy sieć teleinformatyczną Administratora Danych Osobowych.
15. **Szyfrowanie wiadomości** − proces służący zabezpieczeniu danych podczas przesyłania, chroniący wiadomości elektroniczne przed uzyskaniem do nich dostępu przez osoby trzecie, gdy są przesyłane między nadawcą a odbiorcą.
16. **Użytkownik systemu**:
    1) osoba upoważniona przez Administratora Danych Osobowych (lub działającego w jego imieniu Administratora Bezpieczeństwa Informacji) do przetwarzania danych osobowych, której nadano identyfikator i przyznano hasło;
    2) w systemach o strukturze terytorialnie rozproszonej (np. KRN, SZOI, EWUŚ, ApKolce) – osoba, której przydzielono konto i określono zakres dostępu do systemu/bazy danych.
17. **Teletransmisja** – przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej.
18. **Zabezpieczenie danych w systemie informatycznym** – wdrożenie stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.
19. **Zbiór danych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony, czy podzielony funkcjonalnie.

ROZDZIAŁ III
OSOBY FUNKCYJNE W PRZETWARZANIU ELEKTRONICZNYCH DANYCH MEDYCZNYCH

1. ***Administrator Danych Osobowych*** stosuje wysoki poziom bezpieczeństwa systemów informatycznych, ponieważ w ramach istniejącej organizacji przetwarzania elektronicznych danych medycznych Instytutu, niektóre systemy pracują na styku z siecią publiczną (Internet).
2. ***Administrator Systemów Informatycznych (ASI) – Kierownik Działu Informatyki*** odpowiedzialny jest za administrowanie systemem elektronicznych danych medycznych (EDM) poprzez koordynację działania pracowników Działu Informatyki, przez

wyznaczonych pracowników komórek i jednostek organizacyjnych, którym powierzono zadania Administratora systemu/Administratora lokalnego oraz podmiotów zewnętrznych świadczących usługi informatycznego wsparcia systemu/baz danych a także, przeciwdziała naruszeniom bezpieczeństwa tych danych;

3. ***Administrator Systemów Informatycznych*** mając na względzie stan istniejącej infrastruktury oraz zasoby informatyczne Instytutu, realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad systemami informatycznymi Instytutu, określa metody i sposoby zabezpieczenia danych osobowych w tych systemach.
4. ***Administrator systemu/Administrator lokalny***, realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym, który mu powierzono zgodnie z § 13 Polityki Bezpieczeństwa.
5. Administratorzy systemu/Administratorzy lokalni zobowiązani są stworzyć i aktualizować Instrukcje zarządzania dla systemu, którym administrują.
6. Administratorzy systemu/Administratorzy lokalni, przedstawiają Administratorowi Bezpieczeństwa Informacji sprawozdanie dotyczące stanu ochrony danych osobowych w administrowanych przez nich systemach/bazach danych do końca każdego roku kalendarzowego.
7. Kontrola prawidłowości wykonania czynności związanych z ochroną danych osobowych należy do Administratora Bezpieczeństwa Informacji.
8. ***Administrator Bezpieczeństwa Informacji***, na podstawie sprawozdań sporządzonych przez Administratorów systemów/Administratorów lokalnych, przedstawia Administratorowi Danych Osobowych – Dyrektorowi Instytutu − sprawozdanie roczne, o którym mowa w art. 36a ust. 2 pkt.1 lit. a ustawy o ochronie danych osobowych.

ROZDZIAŁ IV
PROCEDURY NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH I REJESTROWANIA TYCH UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM ORAZ WSKAZANIE OSOBY ODPOWIEDZIALNEJ ZA TE CZYNNOŚCI

Zakres przedmiotowy stosowania:
Podmioty obowiązane do stosowania: ADO, ABI, ASI.
Do wiadomości: Osoby upoważnione

Niniejszy rozdział opisuje zasady przyznawania użytkownikowi systemu informatycznego loginu/identyfikatora, jak również zasady nadawania lub modyfikacji uprawnień dostępu użytkownika do tych zasobów.

4.1 Zasady ogólne

1. Przydzielanie uprawnień do jednego lub kilku systemów, realizowane jest w oparciu o następujące zasady:

1) **„Minimalnych przywilejów”** – każdy użytkownik posiada prawa dostępu do zasobów ograniczone wyłącznie do tych, które są niezbędne do wykonywania powierzonych mu obowiązków;
2) **„Wiedzy koniecznej”** – pracownicy posiadają wiedzę o zasobach ograniczoną wyłącznie do zagadnień, które są niezbędne do realizacji powierzonych im zadań;
3) **„Domniemanej odmowy”** – wszystkie działania, które nie są jawnie dozwolone są zabronione.

2. Dostęp do określonych zasobów informatycznych, mogą posiadać w zależności od wykonywanych czynności służbowych lub zadań wynikających z umowy:
   1) pracownicy Instytutu, w zakresie niezbędnym do właściwego wykonywania obowiązków służbowych;
   2) osoby, przy pomocy których Administrator Danych Osobowych, wykonuje swoje czynności, w szczególności:
      a) osoby zatrudnione na podstawie umowy cywilno-prawnej;
      b) pracownicy lub osoby działające w imieniu podmiotu zewnętrznego świadczącego usługi na rzecz Instytutu jeśli, wiąże się to z przetwarzaniem danych osobowych;
      c) stażyści, na podstawie umowy z Urzędem Pracy;
      d) praktykanci, na podstawie umowy ze szkołą wyższą;
      e) wolontariusze, na podstawie umowy o wolontariat.
      f) podmioty zewnętrzne, którym powierzono przetwarzanie danych osobowych w ramach podpisanej umowy powierzenia, a także umowy o zachowaniu poufności z uprawnionymi podmiotami zewnętrznymi, świadczących usługi informatycznego wsparcia systemu informatycznego Instytutu,
   g) użytkownicy systemów o strukturze terytorialnie rozproszonej (np. KRN, SZOI, EWUŚ, ApKolce), którzy otrzymali/otrzymają upoważnienia do przetwarzania danych osobowych od Administratora Danych Osobowych (lub działającego z jego upoważnienia Administratora Bezpieczeństwa Informacji).
3. Użytkownik systemu informatycznego jest jednoznacznie identyfikowany poprzez nadany mu indywidualny login/identyfikator użytkownika.

   Niedopuszczalne jest korzystanie z tego samego loginu/identyfikatora przez więcej niż jednego użytkownika. Przejściowo na część komputerów, podpiętych do starej domeny, użytkownicy logują się jednym kontem. Z tych komputerów do systemów logują się już za pomocą indywidualnych poświadczeń.
4. Raz użyty login/identyfikator nie może być przydzielony innemu użytkownikowi.
5. Uprawnienia dostępu są nadawane wyłącznie w zakresie wynikającym z zajmowanego stanowiska i potrzeby wykonywania obowiązków służbowych na danym stanowisku pracy. Bezzasadne nadawanie uprawnień będzie kwalifikowane jako incydent związany z naruszeniem bezpieczeństwa informacji.
6. Użytkownikowi zostaje nadany dostęp do zasobów informatycznych po:

1) zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych;
2) zapoznaniu się z Polityką Bezpieczeństwa Informacji Instytutu oraz Instrukcją ogólną;
3) podpisaniu oświadczenia o zachowaniu w tajemnicy informacji (w tym danych osobowych), do których użytkownik będzie miał dostęp podczas wykonywania obowiązków służbowych lub zobowiązań umownych oraz środków ich zabezpieczania (również po ustaniu łączącej strony umowy), w tym powstrzymanie się od wykorzystywania ich w celach pozasłużbowych;
4) otrzymaniu upoważnienia do przetwarzania danych osobowych;

7. Każdy Administrator lokalny w swoim systemie zawarty ma wykaz użytkowników systemu wraz z uprawnieniami do systemu informatycznego/bazy danych. Ewidencję wszystkich użytkowników wraz z uprawnieniami we wszystkich systemach informatycznych/bazach danych, prowadzi Administrator Bezpieczeństwa Informacji, którego wzór przedstawia Załącznik 13 do „Polityki Bezpieczeństwa".
8. Weryfikację Ewidencji Administrator Bezpieczeństwa Informacji prowadzi we współdziałaniu z osobami odpowiedzialnymi za wnioskowanie o nadanie, modyfikację lub odebranie uprawnień do określonego systemu/bazy danych oraz Działem Spraw Pracowniczych i Spraw Socjalnych.

4.2. Nadanie uprawnień

1. Bezpośredni przełożony użytkownika, zobowiązany jest złożyć wniosek o nadanie uprawnień do określonej zasobu informatycznego, którego wzór przedstawia Załącznik 2 do „Polityki Bezpieczeństwa".
2. Bezpośredni przełożony określając zakres uprawnień, o który wnioskuje dla użytkownika obowiązany jest do stosowania zasad minimalnych uprawnień oraz wiedzy koniecznej.
3. Po dopełnieniu powyższych wymagań wniosek powinien zostać przekazany do Administratora Bezpieczeństwa Informacji.
4. Administrator Bezpieczeństwa Informacji realizuje otrzymany wniosek i wydaje upoważnienie, którego wzór określa Załącznik 4 do „Polityki Bezpieczeństwa", lub odmawia nadania uprawnień w przypadku uchybienia wymogom określonym w pkt. 2 lub zgłoszenia przez Administratora lokalnego, podejrzeń co do przekroczenia uprawnień wymaganych na danym stanowisku.
5. W przypadku nadania uprawnień wymagających logowania, Administrator lokalny, przekazuje użytkownikowi informację zawierającą wymienione z nazwy systemy/bazy danych, do których użytkownik otrzymał dostęp oraz login i hasło na potrzeby pierwszego logowania.

4.3. Modyfikacja uprawnień

1. Bezpośredni przełożony, jest zobowiązany do złożenia wniosku o zmianę uprawnień danego zasobu informatycznego – Załącznik 2.

2. Wniosek modyfikujący uprawnienia pracownika powinien zostać złożony do Administratora Bezpieczeństwa Informacji w możliwie najkrótszym czasie po wystąpieniu zapotrzebowania na dostęp do danego zasobu informatycznego.
3. Wniosek powinien zawierać uzasadnienie wnoszonych zmian oraz informację o przedmiocie modyfikacji:
   1) zmiana/dodanie/usunięcie uprawnień w profilu uprawnień;
   2) zestawienie łącza VPN;
   3) nadanie indywidualnych uprawnień do systemów poza zdefiniowanym profilem.
4. Administrator Bezpieczeństwa Informacji poddaje analizie otrzymany wniosek i wydaje nowe Upoważnienie - Załącznik 4 do ,,Polityki Bezpieczeństwa. W przypadku nabrania podejrzeń co do przekroczenia uprawnień na danym stanowisku, odmawia nadania uprawnień. Gdy uzna wniosek za zasadny, kieruje wniosek do Administratora systemu/ Administratora lokalnego celem realizacji.
5. W przypadku nadania uprawnień wymagających logowania, Administrator systemu/Administrator lokalny przekazuje użytkownikowi informację zawierającą wymienione z nazwy zasoby informatyczne/bazy danych, do których użytkownik otrzymał dostęp oraz login i hasło na potrzeby pierwszego logowania.

4.4. Odebranie uprawnień

1. Bezpośredni przełożony jest zobowiązany do złożenia Wniosku o odebranie uprawnień do określonego zasobu informatycznego.
2. Terminami obowiązującymi przy składaniu wniosku są w szczególności:
   1) w przypadku ustania stosunku pracy – wniosek odbierający wszystkie uprawnienia – natychmiast, najpóźniej ostatniego dnia pracy zatrudnionego;
   2) długotrwała nieobecność wywołana niezdolnością do pracy – wniosek odbierający wszystkie uprawnienia – natychmiast po upływie 30 (trzydziestu) dni kalendarzowych trwania zwolnienia lekarskiego;
   3) zmiana stanowiska pracy – wniosek odbierający część uprawnień lub nadanie szerszych uprawnień – natychmiast, najpóźniej ostatniego dnia pracy przed zmianą stanowiska na stanowisko wymagające zmniejszenia/poszerzenia uprawnień.
3. Po spełnieniu powyższych wymagań wniosek należy przekazać do Administratora Bezpieczeństwa Informacji, który dokonuje weryfikacji poprawności wniosku.
4. Administrator Bezpieczeństwa Informacji weryfikuje informację o okolicznościach powodujących odebranie/poszerzenie uprawnień w Dziale Spraw Pracowniczych i Spraw Socjalnych.
5. Zmiany zgodne z ust. 1, powodują wyrejestrowanie użytkownika z dniem odejścia z Ewidencji, zablokowanie kont w systemach informatycznych oraz służbowych kont email (jeśli takie posiadał).

6. Wydaje nowe upoważnienie oraz wprowadza dane do Ewidencji w przypadku zmiany stanowiska na stanowisko wymagające zmniejszenia/poszerzenia uprawnień.
7. Wniosek przekazuje następnie do Administratora systemu/Administratora lokalnego, który zgodnie ze wskazanymi terminami realizuje otrzymany wniosek.

ROZDZIAŁ V
ZARZĄDZANIE PRZYWILEJAMI

5.1. Nadawanie przywilejów

1. Nadawane przywileje (większe uprawnienia niż wynika to z realizowanych rutynowych zadań użytkownika) podlegają ścisłej ewidencji prowadzonej przez Administratora Bezpieczeństwa Informacji.
2. Przywileje w systemie nadaje Administrator Systemu Informatycznego.
3. Uprzywilejowane konto nie może służyć do realizacji przez użytkownika rutynowych zadań.
4. Przywileje podlegają cofnięciu niezwłocznie po ustaniu potrzeby uzasadniającej ich nadanie.
5. Nadawane przywileje podlegają regularnym przeglądom i kontroli.

5.2. Zasady postępowania z hasłami użytkowników uprzywilejowanych

1. W stosunku do haseł użytkowników uprzywilejowanych stosuje się zaostrzone standardy bezpieczeństwa.
2. Standardy, o których mowa powyżej stosuje się również do haseł:
    1) elementów aktywnych sieci teleinformatycznych;
    2) konfiguracji komputerów.
3. Hasła, o których mowa w ust. 1 i 2 przechowuje się w postaci zaszyfrowanej.

ROZDZIAŁ VI
STOSOWANE METODY I ŚRODKI UWIERZYTELNIENIA ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZANIEM I UŻYTKOWANIEM

Zakres przedmiotowy stosowania:
Podmioty obowiązane do stosowania: ADO, ABI, ASI, osoby upoważnione

6.1. Zasady ogólne

1. Każdy użytkownik systemu informatycznego musi posiadać unikalny identyfikator i wprowadzone przez siebie hasło autoryzujące jego osobę w systemie informatycznym.
2. Hasła użytkowników lub inne dane uwierzytelniające podlegają szczególnej ochronie.
3. Użytkownik ponosi pełną odpowiedzialność za utworzenie hasła (prócz pierwszego hasła do systemu nadawanego przez administratora systemu informatycznego) i jego przechowywanie.

4. Osoba pełniąca funkcję Administratora systemu/Administratora lokalnego powinna posiadać dodatkowo odrębne konto służące tylko i wyłącznie do administracji danym systemem informatycznym o ile dany system udostępnia taką funkcjonalność.

6.2. Polityka haseł

1. Każdy użytkownik posiadający dostęp do systemów/baz danych i innych zasobów informatycznych Instytutu, jest obowiązany do:
   1) zachowania w poufności wszystkich swoich haseł lub innych danych uwierzytelniających wykorzystanych do pracy w systemie informatycznym;
   2) niezwłocznej zmiany haseł w przypadkach zaistnienia podejrzenia lub rzeczywistego ujawnienia;
   3) niezwłocznej zmiany hasła tymczasowego, przekazanego przez Administratora lokalnego;
   4) poinformowania Administratora lokalnego oraz Administratora Bezpieczeństwa Informacji o podejrzeniu lub rzeczywistym ujawnieniu hasła;
   5) stosowania haseł o minimalnej długości 8 znaków, zawierających kombinację małych i dużych liter oraz cyfr lub znaków specjalnych;
   6) stosowania haseł nie posiadających w swojej strukturze części loginu;
   7) stosowania haseł nie będących zbliżonymi do poprzednich (np. Tadeusz$2013 - Tadeusz$2014);
   8) zmiany wykorzystywanych haseł nie rzadziej niż raz na 30 dni.
2. Hasła zachowują swoją poufność również po ustaniu ich użyteczności.
3. Zabronione jest:
   1) zapisywanie haseł w sposób jawny i umieszczania ich w miejscach dostępnych dla innych osób;
   2) stosowanie haseł opartych na skojarzeniach, łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących danej osoby, np. imiona, numery telefonów, daty urodzenia itp.;
   3) używanie tych samych haseł w różnych bazach danych i aplikacjach;
   4) udostępnianie haseł innym użytkownikom;
   5) przeprowadzanie prób łamania haseł;
   6) wpisywanie haseł „na stałe” (np. w skryptach logowania) oraz wykorzystywania opcji auto-zapamiętywania haseł (np. w przeglądarkach internetowych).
4. Administrator lokalny, obowiązany jest do skonfigurowania systemu tak, aby próby dostępu do tego systemu były limitowane, zarówno w ujęciu ilościowym, jak i czasowym, jeżeli system umożliwia wymienioną konfigurację.
5. W przypadku, gdy system umożliwia limitowanie wprowadzenia błędnego hasła, należy przyjąć próg ilości wprowadzonych błędnych haseł na 3, po czym ustanowić blokadę konta.

6. Należy ograniczyć możliwość wielokrotnego logowania, gdzie użytkownik loguje się na kilku komputerach równocześnie wykorzystując ten sam identyfikator. W systemie CliniNet oraz Simple ERP ta funkcjonalność jest włączona.
7. Administrator lokalny, odblokowuje/resetuje hasło do danego zasobu informatycznego, w przypadku przekroczenia przez użytkownika ustalonej ilości prób logowania.
8. Po dokonaniu tej czynności, Administrator lokalny przekazuje użytkownikowi konta stosowną informację.

6.3. Zasady postępowania z kluczami kryptograficznymi

1. W systemach obsługujących transmisję danych osobowych wrażliwych lub informacji poufnych w Instytucie, powinny być wykorzystywane klucze kryptograficzne służące do zabezpieczenia danych.
2. Klucze generowane są przez zewnętrzne podmioty spełniające wymagania ustawy o usługach zaufania oraz identyfikacji elektronicznej z dnia 5 września 2016 r. (Dz. U. 2016 r., poz. 1579) na wniosek kierownika danego działu
3. Przekazywanie kluczy użytkownikom powinno odbywać się w sposób protokolarny, o ile nie następuje w drodze teletransmisji.
4. Obowiązkiem użytkownika jest zabezpieczenie kluczy (prywatnych) przed dostępem osób nieupoważnionych.
5. W przypadku stwierdzenia ujawnienia klucza osobie nieupoważnionej lub podejrzenia jego ujawnienia, należy bezzwłocznie powiadomić Kierownika Działu Informatyki oraz Administratora Bezpieczeństwa Informacji.
6. Każdy użytkownik korzystający z kluczy kryptograficznych jest zobowiązany do ich użytkowania i przechowywania w sposób uniemożliwiający utratę lub dostęp osób niepowołanych.

ROZDZIAŁ VII
PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY

Niniejszy rozdział opisuje kolejne czynności, jakie należy wykonać w celu uruchomienia systemu informatycznego, a w szczególności zasady postępowania użytkowników podczas przeprowadzania procesu uwierzytelniania (logowania się do systemu). Przestrzeganie określonych w instrukcji zasad ma na celu zachowanie poufności haseł oraz uniemożliwienie nieuprawnionego przetwarzania danych.

Zakres przedmiotowy stosowania:
Podmioty obowiązane do stosowania: ADO, ABI, ASI, osoby upoważnione

1. Rozpoczęcie pracy w każdym systemie lub dostęp do innych zasobów systemu informatycznego Instytutu następuje po wprowadzeniu unikalnego identyfikatora i hasła.

2. Zawieszenie pracy, tj. brak wykonywania jakichkolwiek czynności przez dłuższy okres (np. CliniNet), powoduje automatycznie uruchomienie systemowego wygaszacza ekranu blokowanego hasłem.
3. Przed zakończeniem pracy należy upewnić się czy dane zostały zapisane, aby uniknąć utraty danych.
4. Przed opuszczeniem miejsca pracy, użytkownik obowiązany jest wylogować się, zabezpieczyć nośniki informacji (elektroniczne i papierowe) oraz wyłączyć komputer (wyłączenie nie dotyczy stanowisk pracujących w systemie ciągłym).
5. W sytuacji gdy wgląd w wyświetlane na monitorze dane może mieć nieuprawniona osoba należy tymczasowo zmienić widok wyświetlany na monitorze lub obrócić monitor (przymknąć ekran laptopa) w sposób uniemożliwiający wgląd w wyświetlaną treść.
6. Użytkownik systemu przetwarzającego dane osobowe, niezwłocznie powiadamia Administratora lokalnego w przypadku, gdy:
    1) sposób działania, zakres danych lub sposób ich przedstawienia, odbiega od standardowego stanu uznawanego za typowy dla danego zasobu informatycznego;
    2) niektóre opcje, dostępne użytkownikowi w normalnej sytuacji, przestały być dostępne lub też opcje niedostępne użytkownikowi w normalnej sytuacji, stały się dostępne.

ROZDZIAŁ VIII
ZASADY KORZYSTANIA ZE SŁUŻBOWEJ POCZTY ELEKTRONICZNEJ

1. Użytkownikowi zostaje nadany dedykowany adres skrzynki poczty elektronicznej działający w domenie Instytutu.
2. Informacja o służbowym adresie skrzynki pocztowej jest jawna i dostępna powszechnie.
3. Nadany użytkownikowi adres skrzynki poczty elektronicznej służy wyłącznie do realizacji celów służbowych lub umownych. Korespondencja, realizowana drogą elektroniczną z wykorzystaniem systemów informatycznych Instytutu, podlega rejestrowaniu i może być monitorowana. Informacje przesyłane za pośrednictwem sieci Instytutu (w tym do i z Internetu), nie stanowią własności prywatnej użytkownika.
4. Korzystanie z systemu poczty elektronicznej dla celów prywatnych nie może wpływać na wydajność systemu poczty elektronicznej.
5. Zabronione jest:
    1) wykorzystywanie systemu poczty elektronicznej do działań mogących zaszkodzić wizerunkowi Instytutu,
    2) odbieranie przesyłek z nieznanych źródeł;
    3) otwieranie załączników z plikami samorozpakowującymi się bądź wykonalnymi typu exe, com, itp.;
    4) przesyłanie pocztą elektroniczną plików wykonywalnych typu: bat, com, exe, plików multimedialnych;

5) ukrywanie lub dokonywanie zmian tożsamości nadawcy;
6) czytanie, usuwanie, kopiowanie lub zmiana zawartości skrzynek pocztowych innego użytkownika;
7) odpowiadanie na niezamówione wiadomości reklamowe lub wysyłane łańcuszki oraz na inne formy wymiany danych określanych spamem - w przypadku otrzymania takiej wiadomości należy przesłać ją Administratorowi Systemu Informatycznego;
8) posługiwanie się adresem służbowym e-mail w celu rejestrowania się na stronach handlowych, informacyjnych, czatach lub forach dyskusyjnych, które nie dotyczą zakresu wykonywanej pracy lub obowiązków umownych;
9) wykorzystywanie poczty elektronicznej do reklamy prywatnych towarów lub usług, działalności handlowo-usługowej innej niż wynikającej z potrzeby Instytutu lub do poszukiwania dodatkowego zatrudnienia.

ROZDZIAŁ IX
ZASADY KORZYSTANIA Z SIECI PUBLICZNEJ (INTERNET)

1. Sieć, w której pracują urządzenia komputerowe Instytutu, jest odseparowana od sieci publicznej zaporą ogniową (firewall), oraz systemem wykrywania włamań (IPS).
2. Zdalne korzystanie z systemów informatycznych Instytutu poprzez sieć publiczną może mieć miejsce po zastosowaniu systemu uwierzytelniania użytkownika i szyfrowanego kanału transmisji.
3. Zdalny dostęp do serwerów w celach administracyjnych dopuszczalny jest po zastosowaniu systemu uwierzytelniania użytkownika i szyfrowanego kanału transmisji.
4. Dostęp użytkowników do sieci publicznej (Internet) powinien być ograniczony do niezbędnego minimum na danym stanowisku pracy.
5. Wprowadza się całkowite ograniczenia w dostępie do treści uznanych za pornograficzne, rasistowskie, traktujące o przemocy, przestępstwach, jak również do protokołów umożliwiających wymianę plików w sieciach z naruszeniem przepisów prawa.

ROZDZIAŁ X
PROCEDURY TWORZENIA KOPII ZAPASOWYCH ZBIORÓW DANYCH ORAZ PROGRAMÓW I NARZĘDZI PROGRAMOWYCH SŁUŻĄCYCH DO ICH PRZETWARZANIA

Zakres przedmiotowy stosowania:
Podmioty obowiązane do stosowania: ADO, ABI, ASI, osoby upoważnione
Do wiadomości: osoby upoważnione

Niniejszy rozdział opisuje metody i częstotliwość tworzenia kopii zapasowych danych oraz kopii zapasowych systemu informatycznego używanego do ich przetwarzania.

10.1. Zasady ogólne

1. Kopie zapasowe, aplikacji baz danych i dokumentów użytkowanych przez Instytut, służą do zapewnienia możliwości odtworzenia w przypadku utraty aktualnie użytkowanych danych i/lub konfiguracji baz danych i aplikacji.
2. Tworzenie kopii zapasowych odbywa się automatycznie, ale na serwerze plików „Zamówień Publicznych", serwerze plików „Kadry, Płace" oraz „Płatnik" kopie wykonuje się manualnie. Administratorzy lokalni odpowiedzialni są za nadzór nad tym procesem.
3. Miejsce przechowywania kopii jest zabezpieczone przed nieuprawnionym dostępem.
4. Należy dążyć do tego, aby kopie przechowywane były w bezpiecznej odległości (w innej lokalizacji) od miejsca, w którym jest prowadzona eksploatacja systemów.
5. W przypadku, gdy okres trwałości zapisu na nośniku elektronicznym lub magnetycznym jest krótszy od wymaganego okresu przechowywania wynikającego z uwarunkowań prawnych dane z nośników są przenoszone na inny nośnik.
6. Nośnik, z którego przeniesiono zapis jest niszczony zgodnie z zasadami obowiązującymi w Instytutu.

10.2. Zasady tworzenia kopii bezpieczeństwa i kopii archiwalnych

1. Zbiory danych, oprogramowanie oraz konfiguracja systemów operacyjnych serwerów Instytutu są zabezpieczone poprzez wykonywanie kopii w taki sposób, że umożliwiają odtworzenie systemu w przypadku awarii. W aktualnej sytuacji, ze względu na ograniczoną pojemność macierzy dyskowych, nie jest możliwe wykonywanie kopii archiwalnych zgodnie z zaleceniami w tym zakresie.

   Docelowo dążyć się będzie w kierunku spełnienia wymagań w tym zakresie.

   Po osiągnięciu pożądanego stanu pamięci w zasobach informatycznych powinny zostać spełnione poniższe wymagania w odniesieniu do kopii archiwalnych.
2. Kopie bezpieczeństwa należy wykonywać:
   1) przed dokonaniem zmian w konfiguracji systemów operacyjnych lub oprogramowania;
   2) przed dokonaniem zmian w programach (np. zmiana wersji);
   3) przed i/lub po każdej istotnej zmianie danych w bazie danych;
3. Oprócz kopii, o których mowa w ust. 2., należy wykonywać kopie archiwalne:
   1) miesięczne – na koniec danego miesiąca;
   2) roczne – na koniec danego roku;
4. Kopie bezpieczeństwa należy:
   1) wykonać w co najmniej dwóch egzemplarzach każdą, przy czym przynajmniej jedną na nośniku wymiennym;

2) przechowywać w dwóch różnych miejscach innych niż te, w którym eksploatowane zbiory przechowywane są na bieżąco.

7. Kopie archiwalne należy:
   1) wykonać w co najmniej dwóch egzemplarzach, każdą na osobnych nośnikach wymiennych;
   2) przechowywać w dwóch różnych miejscach innych niż te, w których przechowywane są zbiory eksploatowane na bieżąco.
   3) w trakcie transportu zabezpieczyć przed osobami nieupoważnionymi i niekorzystnymi zjawiskami fizycznymi mogącymi doprowadzić do ich zniszczenia bądź uszkodzenia;
8. Kopie bezpieczeństwa należy przechowywać do momentu wykonania następnej kopii bezpieczeństwa.

ROZDZIAŁ XI
UŻYTKOWANIE SPRZĘTU KOMPUTEROWEGO, OPROGRAMOWANIA, NOŚNIKÓW DANYCH

Zakres przedmiotowy stosowania:
Podmioty obowiązane do stosowania: ADO, ABI, ASI, osoby upoważnione
Do wiadomości: osoby upoważnione

1. Do sprzętu komputerowego zalicza się między innymi:
   1) komputery stacjonarne,
   2) komputery przenośne,
   3) tablety,
   4) smartfony,
   5) drukarki,
   6) modemy,
   7) monitory,
   8) routery,
   9) osprzęt dostarczony razem z wyżej wymienionym sprzętem lub zakupiony oddzielnie, a w szczególności zasilacze, torby, klawiatury, myszki komputerowe.
2. Kierownik Działu Informatyki odpowiada za poprawne działanie sprzętu komputerowego.
3. Przekazanie sprzętu jest to czynność polegająca na dostarczeniu sprzętu komputowego wraz z odpowiednim oprogramowaniem użytkownikowi.
4. Kierownik Działu Informatyki odpowiedzialny jest za przygotowanie sprzętu komputerowego do prawidłowej i zgodnej z przeznaczeniem pracy.

5. Administratorzy lokalni są zobowiązany do prowadzenia spisu posiadanego pod opieką sprzętu komputerowego oraz oprogramowania wraz z dostarczoną dokumentacją (program eAudytor).
6. Gwarancja na sprzęt i oprogramowanie wynika z umowy i faktur zakupu. Przechowywana jest w Dziale Zaopatrzenia oraz częściowo u osób odpowiedzialnych za sprzęt w klinikach i zakładach.
7. Kierownik Działu Informatyki ma prawo instalować wyłącznie licencjonowane oprogramowanie lub oprogramowanie, które nie wymaga opłaty licencyjnej, zgodnie z warunkami licencji.
8. Użytkownik jest zobowiązany do dbałości o sprzęt oraz oprogramowanie, a także odpowiedzialny za zabezpieczenie go przed używaniem przez osoby nieuprawnione oraz do ochrony przed kradzieżą lub zagubieniem.
9. Zabronione jest samodzielne zmienianie konfiguracji przekazanego sprzętu komputerowego oraz instalowanie lub usuwanie oprogramowania przez użytkownika - w tym nie może używać na przekazanym sprzęcie prywatnego oprogramowania.

ROZDZIAŁ XII
ZABEZPIECZENIE SYSTEMU INFORMATYCZNEGO PRZED UTRATĄ DANYCH SPOWODOWANĄ AWARIĄ ZASILANIA LUB ZAKŁÓCENIAMI W SIECI ZASILAJĄCEJ

1. Serwery systemów CliniNet, Simple, Patarch, KRN funkcjonują w układzie „Farmy serwerów”, w wyniku czego, pojęcie serwera systemu jest pojęciem wirtualnym. Dzięki temu, zapewniona jest większa niezawodność całej sieci. „Farma” zabezpieczona jest przed krótkotrwałymi zanikami napięcia, przepięciami itp., przy pomocy zasilaczy awaryjnych (UPS). Zapewnia to bezpieczne zamknięcie w przypadku przedłużającego się zaniku napięcia. Na chwilę obecną „Farma” nie jest podłączona do awaryjnego źródła zasilania, ale docelowo zostanie podłączona do generatorów, gdyż posiadają one funkcje automatycznego uruchomienia na wypadek zaniku napięcia, co zapewni ciągłość jej funkcjonowania.
2. Stacje robocze użytkowników tylko w 5% posiadają UPS-y.

ROZDZIAŁ XIII
SPOSÓB ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO PRZED DZIAŁALNOŚCIĄ OPROGRAMOWANIA, KTÓREGO CELEM JEST UZYSKANIE NIEUPRAWNIONEGO DOSTĘPU DO SYSTEMU INFORMATYCZNEGO

Zakres przedmiotowy stosowania:
Podmioty obowiązane do stosowania: ADO, ABI, ASI
Do wiadomości: osoby upoważnione

Niniejszy rozdział opisuje sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do zasobów informatycznych. Zawarte w niniejszym rozdziale procedury obejmują również:

1) zdefiniowane źródła przedostania się szkodliwego oprogramowania do systemu oraz działania jakie należy podejmować, aby minimalizować możliwość jego zainstalowania się;
2) zastosowane narzędzia programowe, których zadaniem jest przeciwdziałanie skutkom szkodliwego oprogramowania;
3) metody i częstotliwość aktualizacji definicji wirusów oraz osoby odpowiedzialne za zarządzanie oprogramowaniem antywirusowym;
4) sposób postępowania użytkowników na okoliczność zidentyfikowania zagrożeń.

13.1. Ochrona przed szkodliwym oprogramowaniem

1. Zidentyfikowanymi obszarami systemu informatycznego Instytutu, narażonymi na ingerencję wirusów oraz innego szkodliwego oprogramowania są dyski twarde lub karty pamięci urządzeń, pamięć RAM oraz elektroniczne nośniki informacji.
2. Drogą przedostania się wirusów lub szkodliwego oprogramowania może być sieć publiczna, lub elektroniczne nośniki informacji.
3. Stacje robocze, komputery przenośne oraz serwery objęte są ochroną w czasie rzeczywistym za pomocą oprogramowania antywirusowego.
4. Serwery systemów (Farma serwerów) odseparowane są od sieci publicznej przy pomocy wielofunkcyjne zapory sieciowej, zapewniających integralność zasobów przechowywanych i przetwarzanych w systemie informatycznym Instytutu.
5. Oprogramowanie antywirusowe na stacjach roboczych uruchamiane jest przy starcie komputera a użytkownik w żadnym wypadku nie powinien dążyć do jego wyłączenia .
6. Konfiguracja programu antywirusowego zapewnia ciągłe monitorowanie otrzymywanych i wysyłanych, a także uruchamianych plików pod kątem występowania oprogramowania złośliwego.
7. Użytkownicy systemu mają obowiązek skanowania każdego zewnętrznego elektronicznego nośnika informacji, który chcą wykorzystać.
8. W przypadku stwierdzenia pojawienia się wirusa i braku możliwości usunięcia go przez program antywirusowy, użytkownik powinien skontaktować się z Administratorem systemu/Administratorem lokalnym odpowiedzialnym za poprawne funkcjonowanie systemu/bazy danych.
9. W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy, Administrator systemu/Administrator lokalny, podejmuje działania zmierzające do usunięcia zagrożenia. W szczególności działania te mogą obejmować:
    1) usunięcie zainfekowanych plików, o ile jest to akceptowalne ze względu na prawidłowe funkcjonowanie zasobu informatycznego;

2) odtworzenie plików z kopii zapasowych, po uprzednim sprawdzeniu, czy dane zapisane na kopiach zapasowych nie są zainfekowane;
3) samodzielną ingerencję w zawartość pliku – w zależności od posiadanych kwalifikacji lub skonsultowanie się z odpowiednim serwisem.

13.2. Konfiguracja sieci bezprzewodowej

1. Wszystkie sieci bezprzewodowe znajdujące się na terenie Instytutu, muszą być zabezpieczone przed nieautoryzowanymi użytkownikami i urządzeniami za pomocą odpowiedniej konfiguracji routera. Za prawidłowe skonfigurowanie routera odpowiedzialni są pracownicy Działu Informatyki.
2. Minimalne dopuszczalne zabezpieczenie sieci bezprzewodowej zakłada stosowanie protokołu szyfrującego WPA2.
3. Podczas konfiguracji routera powinno się natychmiast zmienić hasło do panelu administracyjnego, aby zabezpieczyć się przed nieautoryzowanym dostępem w celu konfiguracji routera.
4. W trakcie konfigurowania routera sieci bezprzewodowej, należy w ustawieniach routera aktywować szyfrowanie.
5. Należy wprowadzić hasło dla sieci bezprzewodowej unikalne i złożone tak, by osoby spoza sieci nie mogły go w prosty sposób złamać. Hasło powinno składać się z 8 znaków oraz zawierać kombinację liter dużych, małych i cyfr i znaków specjalnych.
6. Należy zmienić hasła dla domyślnych SSID.
7. Należy usunąć wszystkie identyfikatory SSID, z których się nie korzysta;

13.3. Zapora sieciowa (Firewall)

1. Program lub urządzenie ma za zadanie zabezpieczać sieć LAN przed dostępem i działaniami osób niepowołanych z zewnątrz. Firewall najczęściej lokowany jest na styku sieci lokalnej i Internetu i uniemożliwia bezpośrednią komunikację komputerów z zewnątrz (Internet) z komputerami w sieci LAN. Bardzo ważną funkcją zapory sieciowej jest monitorowanie ruchu sieciowego i zapisywanie najważniejszych zdarzeń do dziennika (logu). Umożliwia to administratorowi wczesne dokonywanie zmian konfiguracji. Poprawnie skonfigurowany firewall powinien odeprzeć wszelkie znane typy ataków. Osobą odpowiedzialną za prawidłowe działanie zapory sieciowej jest Kierownik Działu Informatyki.
2. Sugerowane techniki obrony:
   1) filtrowanie pakietów, czyli sprawdzanie pochodzenia pakietów i akceptowanie pożądanych;
   2) stosowanie algorytmów identyfikacji użytkownika (hasła, cyfrowe certyfikaty);
   3) zabezpieczanie programów obsługujących niektóre protokoły (np. FTP).
3. Dopuszczone do użytku typy zapór sieciowych:
   1) zapory filtrujące – monitorują przepływające przez nie pakiety sieciowe i przepuszczają tylko zgodne z regułami ustawionymi na danej zaporze (zapora pracująca dodatkowo jako router);

2) translacja adresów sieciowych (NAT) – polega na dokonywaniu zamiany adresu IP hosta wewnętrznego w celu ukrycia go przed zewnętrznym monitorowaniem. Mechanizm ten jest również nazywany maskowaniem adresu IP;
3) zapory pośredniczące (*proxy*) - wykonujące połączenie z serwerem w imieniu użytkownika.

ROZDZIAŁ XIV
PROCEDURY WYKONYWANIA NAPRAW SPRZĘTU KOMPUTEROWEGO ORAZ NOŚNIKÓW INFORMACJI SŁUŻĄCYCH DO PRZETWARZANIA DANYCH

1. Naprawa sprzętu komputerowego, systemów informatycznych oraz nośników informacji Administratora ma na celu zapewnienie nieprzerwanej i bezpiecznej pracy tych systemów, zapobieganie utracie, uszkodzenia lub naruszenia bezpieczeństwa.
2. Naprawy urządzeń komputerowych przeprowadzane są częściowo przez pracowników Działu Informatyki. Jednakże ze względu na bardzo dużą ilość sprzętu, część urządzeń przekazywana jest do podmiotów zewnętrznych. Dotyczy to sprzętu w okresie gwarancji, ale także będącego poza tym okresem. Aktualizacje i zmiany w systemach informatycznych Instytutu, przeprowadzane są w głównej mierze zdalnie przez podmioty zewnętrzne za pomocą szyfrowanego połączenia .
3. Naprawy sprzętu poza siedzibą Instytutu, odbywają się po uprzednim usunięciu elementów zawierających dane osobowe.
4. Wszelkie prace, o których mowa powyżej, wykonywane przez podmiot zewnętrzny, odbywają się na zasadach określonych w szczegółowej umowie pomiędzy Instytutem a tymże podmiotem.
5. W przypadku zdalnej obsługi serwisowej systemów informatycznych Instytutu, porty komunikacyjne powinny być włączane jedynie na wyraźne żądanie dostawcy takich usług, za zgodą Administratora lokalnego i muszą być ponownie odłączone tuż po zakończeniu prac serwisowych.
6. Jeśli nośnik danych (dysk, płyta lub inne) zostanie uszkodzony i nie można go odczytać ani usunąć z niego danych, należy go zniszczyć mechanicznie lub w istniejącej niszczarce.

ROZDZIAŁ XV
POSTEPOWANIE NA WYPADEK AWARII/KATASTROF I UTRATY DANYCH. ZAPEWNIENIE CIĄGŁOŚCI DZIAŁANIA

1. W Instytucie przygotowany jest plan postępowania na wypadek wystąpienia poważnych awarii systemu, uszkodzeń lub utraty danych w wyniku pożaru, zalania lub innych nie dających się przewidzieć zdarzeń. W przypadku zdarzenia, które uniemożliwia zachowanie ciągłości działania podstawowych zasobów informatycznych, uruchamiana jest procedura przywracania kluczowych funkcji systemu. Służy temu procedura tworzenia kopii zapasowych systemów właściwa dla danego systemu a także docelowo jeśli zasoby pamięci na to pozwolą, procedura tworzenia kopii archiwalnych.

2. W przypadku awarii podstawowego systemu do obsługi pacjentów (CliniNet), do czasu przywrócenia kluczowych funkcji systemu, wypełnia się dokumentację w formie papierowej, a po przywróceniu systemu wprowadza się do niego dane z dokumentacji w formie papierowej.
3. Systemy autonomiczne, aplikacje (Aria, IntraRis, Spectra Pacs, Oncentra, Mosaiq, iView, XVI1, XVI2, XVI3, Oncentra Brachy, Oncentra Prostate), przywracane są do działania w trybie właściwym dla tych systemów i aplikacji, zgodnie z procedurami opracowanymi przez Administratorów tych Systemów lub przez firmy zewnętrzne (dostawcy usług), zobowiązane na podstawie podpisanych przez Instytut umów.
4. Systemy, dla których Instytut jest Gestorem (Baza Danych ZSI-CRN), przywraca się do działania zgodnie z procedurą opracowaną przez Administratora Systemu.
5. Procedury odtwarzania systemów, zawierają szczegółowe kroki związane z odtworzeniem systemu, wskazują na lokalizację wszystkich zasobów niezbędnych do odtworzenia systemu oraz wskazują osoby odpowiedzialne za jego wykonanie.
6. W Instytucie ustalony jest Zespół Zarządzania Kryzysowego, który w sytuacji kryzysowej - podejmuje odpowiednie działania. W skład Zespołu wchodzą:
   1) Zastępca Dyrektora ds. Zarządzania i Finansów
   2) Administrator Systemów (ASI) – Kierownik Działu Informatyki
   3) Administratorzy Systemu/Administratorzy Lokalni
   4) Przedstawiciele uprawnionych podmiotów zewnętrznych świadczących usługi informatycznego wsparcia systemu (wg potrzeb).

ROZDZIAŁ XVI
POSTANOWIENIA KOŃCOWE

1. Dokumentacja przetwarzania danych osobowych stanowi wewnętrzną regulację Dyrektora Instytutu i obowiązuje wszystkich pracowników i współpracowników.
2. Instrukcja ogólna podlega przeglądowi i aktualizacji co pół roku.
3. Instrukcje Zarządzania Systemami Informatycznymi właściwe dla poszczególnych systemów i baz danych aktualizowane są raz na pół roku lub częściej, jeśli wymagają tego okoliczności.
4. Dokumentacja przetwarzania danych osobowych obowiązuje od dnia jej wprowadzenia w życie.
5. Każdy, kto przetwarza dane posiadane przez Instytut, zobowiązany jest do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Dokumentacji przetwarzania danych osobowych
6. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub niewykonanie zobowiązania w przypadku stosunku prawnego innego niż stosunek pracy.
7. W sprawach nieuregulowanych w niniejszej instrukcji mają zastosowanie przepisy powszechnie obowiązującego prawa, w tym w szczególności przepisy ustawy.