OPRACOWAŁ:	SPRAWDZIŁ:	ZATWIERDZIŁ:
INSTRUKCJA OBOWIĄZUJE OD DNIA		

Podstawą prawną wdrożenia instrukcji jest Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie 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 r. Nr 100, poz. 1024).

1. CEL

Określenie zasad i sposobu zarządzania systemem informatycznym w zakresie ochrony danych osobowych.

2. Przedmiot i zakres stosowania

2.1 Instrukcja „Zarządzanie systemem informatycznym w zakresie ochrony danych osobowych" (dalej jako Instrukcja) w sposób szczególny uwzględnia wymogi bezpieczeństwa i ochrony danych osobowych w systemach informatycznych Wojewódzkiego Szpitala Zespolonego w Elblągu (dalej jako Szpital).

2.2 Instrukcja jest zbiorem czynności w zakresie przetwarzania danych osobowych wykonywanych przez pracowników Szpitala oraz inne osoby upoważnione przez Dyrektora Naczelnego.

3. DEFINICJE I TERMINY

Podstawowe definicje zostały przedstawione w „Polityce ochrony danych osobowych Wojewódzkiego Szpitala Zespolonego w Elblągu" (dalej jako Polityka).

4. ODPOWIEDZIALNOŚĆ I UPRAWNIENIA

4.1 Wszyscy pracownicy Szpitala są odpowiedzialni za przestrzeganie przepisów w zakresie ochrony danych osobowych, stosownie do powierzonych obowiązków, zgodnie z zapisami niniejszej Instrukcji oraz z ustaleniami zawartymi w Polityce.

4.2 Kierownicy komórek organizacyjnych są odpowiedzialni za przestrzeganie przepisów w zakresie ochrony danych osobowych w podległych komórkach organizacyjnych, za nadzór nad realizacją zapisów zawartych w Polityce

4.3 Kierownicy komórek organizacyjnych oraz Dyrektorzy Pionów, którzy definiują typy użytkowników w oparciu o zakres obowiązków podległych sobie pracowników, odpowiedzialni są za określanie ról użytkowników oraz przydział dostępu do odpowiednich systemów informatycznych.

4.4 Obowiązki i uprawnienia Inspektora Ochrony Danych (IOD) określa Regulamin Organizacyjny Pionu Administracyjnego WSZ w Elblągu.

4.5 Administrator Bezpieczeństwa Systemów Informatycznych (ABSI) wykonuje zadania w zakresie nadzoru, realizuje zadania związane z zarządzaniem systemem w zakresie bezpieczeństwa informatycznego w Szpitalu oraz współpracuje z IOD w zakresie nadzoru nad przestrzeganiem zasad bezpieczeństwa przetwarzania i ochrony danych osobowych Szpitala. Zadania ABSI określa Regulamin Organizacyjny Pionu Administracyjnego WSZ w Elblągu oraz zakres czynności wynikający z umowy.

5. OPIS POSTĘPOWANIA

5.1 *ZARZĄDZANIE SYSTEMEM INFORMATYCZNYM*

5.1.1 Nadawanie uprawnień do przetwarzania danych osobowych i rejestrowanie tych uprawnień

- Nadanie uprawnień do przetwarzania danych osobowych oraz identyfikatorów dających dostęp do systemów informatycznych i aplikacji następuje na pisemny wniosek kierownika danej komórki organizacyjnej Szpitala o nadanie uprawnień/modyfikację/ odebranie uprawnień Użytkownikowi do zasobów informatycznych. Wzór druku - Wniosek o nadanie/modyfikację/odebranie uprawnień Użytkownikowi do zasobów informatycznych stanowi Załącznik Nr 1 do niniejszej Instrukcji.

- Warunkiem uzyskania uprawnień do zasobów informatycznych, w tym uprawnień tymczasowych tj. na czas określony, jest złożenie oświadczenia o zachowaniu poufności oraz uprzednie uzyskanie upoważnienia do przetwarzania danych osobowych na wniosek kierownika komórki organizacyjnej. Wzory ww. dokumentów stanowią załączniki do Polityki.
- Wniosek zawierający opis zakresu uprawnień/ modyfikacji dotychczasowych uprawnień/odbieranych uprawnień Użytkownikowi do zasobów informatycznych podpisuje kierownik danej komórki organizacyjnej i po zaopiniowaniu przez Inspektora Ochrony Danych przedstawia do zatwierdzenia Dyrektorowi danego Pionu.
- Zatwierdzony przez Dyrektora Pionu wniosek kierowany jest do LAIT (Lokalnego Administratora Systemów Informatycznych), który podejmuje dalsze czynności związane z nadaniem uprawnienia użytkownikowi oraz nadaje hasła jednorazowego użytku.
- Nadanie uprawnienia użytkownikom LAIT odnotowuje w Rejestrze nadanych/modyfikowanych/ odebranych uprawnień użytkownikom systemu informatycznego. Rejestr stanowi Załącznik Nr 2 do niniejszej Instrukcji.
- Założenie konta użytkownika w systemie informatycznym oraz nadanie identyfikatora i hasła jednorazowego LAIT odnotowuje w prowadzonym przez siebie Rejestrze nadanych kont użytkownikom.
- Wszystkie zatwierdzone wnioski kierowane przez kierowników komórek organizacyjnych o nadanie uprawnień po naniesieniu numeru identyfikacyjnego z Rejestrze nadanych i odebranych uprawnień LAIT gromadzi w odrębnym zbiorze. Zbiory te są poddawane cyklicznemu sprawdzaniu przez ABSI.

5.1.2 Nadawanie uprawnień tymczasowych

- Nadanie uprawnień dla podmiotu zewnętrznego świadczącego usługi na rzecz Szpitala odbywa się na zasadach opisanych ~~wyżej w oparciu o~~ w umowie powierzenia przetwarzania danych osobowych stanowiącej załącznik do umowy na świadczenie usług.
- Wszystkie wydane wnioski o nadanie uprawnień tymczasowych LAIT przechowuje w swojej dokumentacji i stanowią one integralną część Rejestru nadanych/odebranych uprawnień tymczasowych użytkownikom systemu informatycznego.

5.1.3 Modyfikacja uprawnień użytkownika

- Zmiana uprawnień użytkownika następuje na pisemny wniosek kierownika komórki organizacyjnej, na tych samych zasadach, co nadanie uprawnień, przy czym IOD opiniuje wniosek po sprawdzeniu, czy wprowadzone zmiany są zgodne z wcześniej uzyskanymi upoważnieniami do przetwarzania danych osobowych.
- Zatwierdzony przez Dyrektora Pionu wniosek (modyfikację uprawnień) LAIT rejestruje w Rejestrze nadanych/modyfikowanych/odebranych uprawnień użytkownikom systemu informatycznego.
- W przypadku modyfikacji uprawnień wynikających ze zmiany obowiązków służbowych lub zmiany komórki organizacyjnej przez użytkownika, tok postępowania w sprawie nadania uprawnień jest taki sam jak dla pracowników nowo przyjętych.
- W celu uniknięcia omyłkowego nadania uprawnień, przy każdorazowej zmianie uprawnień, w pierwszej kolejności następuje odebranie wszystkich nadanych uprawnień do systemów informatycznych a następnie nadanie nowych.

5.1.4 Odbieranie uprawnień użytkownikom

- Całkowite odebranie uprawnień użytkownikom odbywa się w przypadkach rozwiązania bądź wygaśnięcia umowy.
- Na pisemny wniosek kierownika komórki organizacyjnej lub upoważnionego pracownika Działu Służb Pracowniczych uprawnienia do systemów informatycznych odbiera ADO. LAIT odnotowuje ten fakt w Rejestrze nadanych i odebranych uprawnień.
- Fizyczne odebranie uprawnień dostępu do zasobów systemu informatycznego wykonuje LAIT, który dokonuje stosownego zapisu w Rejestrze nadanych kont użytkownikom.
- Odebranie uprawnień może również nastąpić na wniosek IOD lub kierownika komórki organizacyjnej Szpitala skierowany do ADO lub upoważnionego Dyrektora Pionu, w wyniku przeprowadzonego postępowania stwierdzającego naruszenie zasad ochrony danych osobowych zawartych w Polityce.

- Czasowe odebranie (zawieszenie) uprawnień następuje obligatoryjnie stosunku do osób, co do których istnieje podejrzenie rażącego naruszenia zasad polityki bezpieczeństwa lub popełnienia przestępstwa przeciwko informacji (w myśl rozdziału XXI Kodeksu karnego).
- Odebrania dostępu do zasobów systemu informatycznego dokonuje LAIT.
- Przywrócenie uprawnień następuje po zakończeniu postępowania wyjaśniającego i oczyszczeniu z zarzutów, popartych pisemnym wnioskiem skierowanym do ADO.

5.1.5 **Przegląd uprawnień użytkowników w systemie informatycznym**

- W celu zachowania ciągłości nadzoru nad nadawaniem uprawnień użytkownikom w systemie informatycznym przeprowadza się okresowo analizę nadanych uprawnień:
  - po każdorazowym uaktualnieniu aplikacji, systemu informatycznego zawierającego dane osobowe, jednak nie rzadziej niż raz na kwartał z uwzględnieniem nadanych uprawnień dla podmiotów zewnętrznych i ich pracowników.
- Za okresowy przegląd nadawanych uprawnień wymienionych w pkt. 5.1.2 odpowiedzialny jest Administrator Bezpieczeństwa Systemów Informatycznych (ABSI). Fakt dokonania analizy, kontroli nadanych, odebranych bądź modyfikowanych uprawnień odnotowuje odpowiednio w comiesięcznych raportach z działalności ABSI.
- Po każdorazowym uaktualnieniu aplikacji, nie rzadziej niż raz na kwartał, ABSI przy współpracy z IOD kierownikami komórek organizacyjnych dokonuje przeglądu zmian w nadawanych uprawnieniach w stosunku do przydzielonych ról dla poszczególnych grup użytkowników. Z przeprowadzonej analizy sporządza protokół zmian.

5.2 *STOSOWANE METODY I ŚRODKI UWIERZYTELNIANIA*

5.2.1 **Przydzielanie haseł wraz ze wskazaniem osoby odpowiedzialnej za przydział haseł**

- Osobą odpowiedzialną za przydzielanie pierwszego hasła dostępu jest LAIT.
- Użytkownik otrzymuje hasło w formie pisemnej wraz z identyfikatorem użytkownika i podpisuje zobowiązanie do zachowania hasła w tajemnicy. Po otrzymaniu identyfikatora i hasła użytkownik zobowiązany jest do zmiany hasła po pierwszym, poprawnym zalogowaniu się do systemu informatycznego.

5.2.2 **Wymogi dotyczące powtarzalności haseł oraz zestawu tworzących je znaków**

- Zabrania się udostępniania swojego identyfikatora i hasła innym pracownikom, jak również osobom nieupoważnionym do dostępu do systemu informatycznego.
- Hasła dostępu użytkownika do systemu tworzone są zgodnie z instrukcjami operacyjnymi specyficznymi dla poszczególnych systemów oraz aplikacji i stanowią tajemnicę służbową, znaną wyłącznie temu użytkownikowi.
- Hasła nie mogą być powiązane z danym użytkownikiem (np. imię, nazwisko, data urodzenia itp.).
- Hasła wszystkich użytkowników przechowywane są na serwerze w formie zaszyfrowanej z ostatnich 24 miesięcy.
- Hasło użytkownika:
  - ✓ musi się składać, z co najmniej 8 znaków, w tym wielkich i małych liter oraz cyfry lub znaku specjalnego,
  - ✓ należy zmieniać nie rzadziej, niż co 30 dni, wymóg zmiany hasła wymusza dany system informatyczny
  - ✓ nowe hasło musi różnić się od poprzedniego.

5.2.3 **Nadzór nad uwierzytelnianiem**

- Nadzór nad logowaniem się do systemu informatycznego sprawuje LAIT.
- Uprawniony użytkownik powinien logować się do systemu tylko i wyłącznie w godzinach pracy ustalonych w grafiku pracy.
- Zabrania się logowania, dostępu do systemu informatycznego osobom uprawnionym do tego, gdy wynikający z grafiku ich pracy harmonogram nie uwzględnia obecności danego pracownika.

5.2.4 **Działania w przypadkach zapomnienia i/lub ujawnienia hasła**

- Wszelkie przypadki zapomnienia oraz ujawnienia haseł należy niezwłocznie zgłosić LAIT.

- LAIT w przypadku:
  - ✓ zapomnienia hasła – nadaje użytkownikowi nowe hasło, po pisemnym wniosku osoby, której hasło dotyczy,
  - ✓ ujawnienia hasła – podejmuje czynności związane z naruszeniem zasad polityki bezpieczeństwa, w szczególności informuje ABSI i IOD o zaistniałym incydencie. IOD/ABSI sporządzają raport oraz dokonują stosownego wpisu w Rejestrze naruszeń ochrony danych osobowych.

  Hasło w stosunku, do których zaistniało podejrzenie o jego ujawnieniu podlega bezzwłocznej zmianie;

5.2.5 **Hasła użytkowników uprzywilejowanych**

- W celu zabezpieczenia awaryjnego dostępu do systemu przetwarzającego dane osobowe, aktualne hasło administratora systemu i aplikacji jest deponowane w sejfie Kasy Szpitala, w zalakowanej kopercie.
- Hasła użytkowników uprzywilejowanych zachowane są przez nich w ścisłej tajemnicy.
- Hasło użytkownika root na serwerach znane jest jedynie LAIT.

5.2.6 **Rejestrowanie i usuwanie użytkowników z rejestru osób dopuszczonych do przetwarzania danych osobowych w systemie informatycznym:**

- LAIT prowadzi w imieniu Administratora Danych Rejestr osób dopuszczonych do przetwarzania danych osobowych w oparciu o gromadzone wnioski o nadanie /modyfikację /odebranie uprawnień.
- LAIT, po otrzymaniu wniosku o usunięcie, niezwłocznie blokuje konto użytkownika. Fakt ten odnotowuje w Rejestrze.
- Konto użytkownika usuwa (blokuje) administrator systemu zgodnie ze szczegółowymi instrukcjami operacyjnymi specyficznymi dla danej aplikacji lub systemu informatycznego.

5.2.7 **Czynności towarzyszące rozpoczęciu pracy**

- Użytkownik przed przystąpieniem do pracy jest zobowiązany do sprawdzenia stanu urządzeń tj. stacji roboczej (komputera/ terminala), na których będzie pracował.
- W przypadku stwierdzenia problemów związanych z logowaniem się do systemów informatycznych lub domeną, awarią sprzętu komputera oraz w przypadku stwierdzenia ingerencji w przetwarzane dane należy niezwłocznie powiadomić ABSI i IOD. Natomiast w przypadku stwierdzenia fizycznej ingerencji w sprzęt, stwierdzenia naruszenia fizycznych zabezpieczeń pomieszczeń należy niezwłocznie powiadomić również Pełnomocnika ds. Ochrony Informacji Niejawnych. W przypadkach zgłoszeń opisanych wyżej, IOD w porozumieniu z ABSI przygotowują notatkę służbową.
- W przypadku zdarzeń opisanych powyżej, pracownik zobowiązany jest podać imię i nazwisko, identyfikator, miejsce wystąpienia (nr stacji roboczej), oraz określić problem, jaki wystąpił, sporządzić odpowiednią notatkę, którą niezwłocznie przekazuje IOD i ABSI.

5.2.8 **Czynności towarzyszące logowaniu się do systemu informatycznego oraz praca w tym systemie**

- Bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym następuje wyłącznie po podaniu identyfikatora i hasła danego użytkownika.
- W celu zalogowania się do systemu informatycznego jak i domeny Szpitala użytkownik powinien wpisać własny identyfikator i hasło w sposób uniemożliwiający podpatrzenie hasła przez osoby nieuprawnione, postronne.
- Podczas procesu logowania się oraz pracy w systemie użytkownik zobowiązany jest korzystać tylko i wyłącznie z własnego unikalnego identyfikatora i hasła.
- Zabronione jest udostępnianie identyfikatora i hasła innym pracownikom.
- Podczas pracy zabrania się przebywania osobom nieuprawnionym w miejscu, gdzie dane osobowe są przetwarzane.
- Osoba nieupoważniona może przebywać w miejscu, gdzie dane są przetwarzane tylko i wyłącznie w obecności osoby upoważnionej do przetwarzania tych danych.

- W przypadku gdy osoby niepowołane mają wgląd na wyświetloną na ekranie monitora zawartość, pracownik zobowiązany jest niezwłocznie przerwać pracę i zablokować stację roboczą, po czym udać się do innej stacji celem kontynuowania pracy.

5.2.9 **Czynności związane z zawieszeniem pracy**

- W przypadku zawieszenia, przerwania pracy pracownik zobowiązany jest do zablokowania stacji roboczej przed dostępem osób nieuprawnionych.
- W celu uniemożliwienia dostępu osobom nieuprawnionym do systemu należy:
  - ✓ wylogować się z systemu,
  - ✓ aktywować wygaszasz ekranu posiadający zabezpieczenie hasłem,
  - ✓ zabezpieczyć miejsce, gdzie dane są przetwarzane (zamknąć drzwi na klucz, zabezpieczyć przed wejściem osób nieuprawnionych).

5.2.10 **Czynności związane z zakończeniem pracy**

- W przypadku gdy pracownik kończy pracę w systemie, zobowiązany jest do wyjścia (wylogowania) z systemu informatycznego i wyłączenia stacji roboczej, na której odbywał pracę.
- Każdy pracownik jest zobowiązany do przestrzegania zasady „czystego biurka".
- Każdy pracownik jest zobowiązany do przestrzegania podstawowych zasad bezpieczeństwa informatycznego, które stanowią Załącznik nr 3 do niniejszej Instrukcji.

5.3 *ZABEZPIECZENIE SYSTEMU INFORMATYCZNEGO PRZED SZKODLIWYM OPROGRAMOWANIEM*

5.3.1 **Zarządzanie dostępem użytkowników do sieci zewnętrznej**

- Użytkownicy systemu informatycznego posiadają dostęp do sieci INTERNET.
- Dostęp do sieci INTERNET jest monitorowany.
- Zablokowane są witryny, umożliwiające wymianę plików, niepożądane strony internetowe, polityka restrykcji jest na bieżąco monitorowana i aktualizowana przez ABSI.
- Wszelkie stacje robocze, które posiadają dostęp do sieci zewnętrznej INTERNET są monitorowane pod kątem odwiedzonych witryn internetowych oraz plików, które zostały ściągnięte na twardy dysk komputera.
- Zablokowane jest instalowanie jakiegokolwiek oprogramowania przez użytkowników.

5.3.2 **Stosowane systemy antywirusowe**

- Ochrona antywirusowa jest realizowana przez oprogramowanie antywirusowe instalowane na serwerach, maszynach wirtualnych i stacjach roboczych użytkowników.
- Użytkownicy nie mają możliwości dezaktywowania oprogramowania antywirusowego. Oprogramowanie antywirusowe jest systematycznie uaktualniane, sygnatury wirusów są aktualizowane na bieżąco.
- W razie stwierdzenia obecności wirusa lub niepożądanego, szkodliwego oprogramowania przez program antywirusowy należy przerwać pracę na stacji roboczej i poinformować o zaistniałym fakcie LAIT oraz ABSI.

5.3.3 **Systemy wykrywania włamań oraz zabezpieczenia przed nimi**

- Nadzór nad włamaniami, nieuprawnionym dostępem z zewnątrz do zasobów sieci wewnętrznej Szpitala sprawuje odpowiednio skonfigurowany firewall w zależności od potrzeb i aktualnego stanu systemu.
- Nadzór nad aktualizacją, zarządzaniem oraz wprowadzaniem odpowiednich reguł bezpieczeństwa firewall'a sprawuje LAIT.
- W razie wykrycia włamania LAIT podejmuje czynności związane z ustaleniem przyczyny naruszenia integralności systemu wg procedur opisanych w instrukcji zarządzania systemem informatycznym oraz prowadzi ewidencję tych włamań.
- O każdym przypadku włamania LAIT powiadamia ABSI oraz IOD.
- W celu wykrywania włamań stosuje się odpowiednie oprogramowanie IDS oraz IPS.

5.3.4 **Analiza logów systemowych**

- Co najmniej raz w miesiącu logi podlegają analizie. Za analizę logów systemowych odpowiedzialność ponosi LAIT.
- LAIT w cyklu comiesięcznym zdaje sprawozdanie z analizy logów ABSI.

- Szczegółowej analizie podlegają logi z połączeń z siecią zewnętrzną. W tym przypadku IOD/ABSI podejmuje czynności związane z naruszeniem bezpieczeństwa określonych w Instrukcji „Postępowanie w przypadku naruszenia ochrony danych osobowych".
- W przypadku stwierdzenia naruszeń bezpieczeństwa Szpitala LAIT powiadamia niezwłocznie IOD oraz ABSI o zaistniałym fakcie.

5.3.5 **Aktualizacja systemów operacyjnych, aplikacji i programów antywirusowych i systemów wykrywania włamań**

- Odpowiedzialność za wszelkie aktualizacje systemów informatycznych Szpitala ponosi kierownik Sekcji Informatyki i Telekomunikacji oraz odpowiednio według zakresu czynności LAIT.
- Sprawdzanie nowych aktualizacji powinny odbywać się w przypadku:
  - ✓ systemów operacyjnych oraz aplikacji – co najmniej raz w miesiącu,
  - ✓ programów antywirusowych oraz systemów wykrywania włamań – co najmniej raz w tygodniu.

5.3.6 **Przekazywanie danych**

- W obrębie Szpitala dane osobowe mogą być wymieniane pomiędzy użytkownikami jedynie za pomocą sytemu informatycznego.
- Wszelkie przekazywanie dokumentacji elektronicznej obywa się poprzez sieć wewnętrzną lub odpowiednie aplikacje systemu informatycznego.
- W przypadku gdy przeniesienie wymaga zastosowania nośnika, każdy nośnik jest odpowiednio oznakowany, opisany i zabezpieczony poprzez kodowanie lub kryptografię.
- Wszystkie nośniki są zaewidencjonowane w spisie nośników, osobno dla każdej komórki organizacyjnej.

5.3.7 **Wykonywanie przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych**

- Celem wykonywania przeglądów i konserwacji jest utrzymanie systemu informatycznego w ciągłej sprawności oraz unikanie awarii tego systemu.
- LAIT jest odpowiedzialny za dokonywanie konserwacji systemów informatycznych i elektronicznych nośników informacji.
- Prace dotyczące przeglądów, konserwacji i napraw, wymagające zaangażowania autoryzowanych firm zewnętrznych, są wykonywane przez uprawnionych przedstawicieli tych firm (serwisantów) pod nadzorem LAIT na terenie Szpitala.
- W przypadku konieczności dostępu do danych osobowych przez serwisantów i wdrożeniowców stosuje się każdorazowo zasady określone w umowie powierzenia przetwarzania danych osobowych, stanowiącej załącznik do umowy serwisowej, a której wzór znajduje się w Polityce.
- Niezależnie od wyżej wskazanych zasad, zawsze gdy jest to możliwe dyski twarde lub inne elektroniczne nośniki informacji przeznaczone do naprawy pozbawia się zawartości zapisanych informacji w sposób uniemożliwiający ich odczyt. W przypadku gdy serwisowany sprzęt wymaga naprawy poza terenem Szpitala, pozbawia się go przed wysłaniem dysków twardych. Uprzednio przed każdą czynnością serwisową „na nośnikach danych" wykonuje się kopię tych nośników w charakterze 1:1.
- W umowach zawieranych z firmami zewnętrznymi odnośnie konserwacji, naprawy bądź wdrażania systemów informatycznych znajduje się zapis zobowiązujący te firmy do przestrzegania przepisów wewnętrznych obowiązujących w Szpitalu w zakresie ochrony danych osobowych.
- LAIT prowadzi dokumentację w zakresie wykonywanych czynności naprawczo - konserwacyjnych i modernizacyjnych systemów informatycznych.

5.3.8 **Tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania - o**dpowiedzialność za wykonywanie kopii zapasowych ponosi Kierownik Sekcji Informatyki i Telekomunikacji oraz odpowiedni LAIT.

5.3.9 **Sposób, miejsce i okres przechowywania elektronicznych nośników informacji oraz kopii zapasowych**

- **Przechowywanie elektronicznych nośników informacji zawierających dane osobowe**

- ✓ Każda komórka organizacyjna, która dokonuje zapisu plików zawierających dane osobowe na elektronicznych nośnikach informacji zobowiązana jest do zabezpieczenia tych nośników przed dostępem osób niepowołanych.
- ✓ Nośniki te muszą być przechowywane w zamkniętych szafach, do których dostęp mają tylko i wyłącznie osoby uprawnione do korzystania z tych danych.
- ✓ Zabrania się wynoszenia wszelkich elektronicznych nośników informacji poza teren Szpitala.
- ✓ Przechowywanie elektronicznych nośników informacji powinno być ograniczone do minimum i niezwłocznie po wykorzystaniu danych powinny one być usunięte z tych nośników.
- ✓ Zaleca się przechowywanie wszelkich elektronicznych dokumentów zawierających dane osobowe do przechowywania na dysku twardym w zabezpieczonym katalogu.
- ✓ Zabrania się przechowywania wszelkich dokumentów zawierających dane osobowe w katalogach udostępnionych systemu informatycznego; powyższa procedura poddana jest cyklicznej comiesięcznej kontroli przez ABSI, sporządzany jest raport kontroli.

➢ **Przechowywanie kopii zapasowych**
- ✓ Za sporządzenie kopii zapasowych odpowiedzialny jest LAIT lub osoba przez niego upoważniona.

6. ZAPISY (druki, formularze)

- ➢ Wniosek o nadanie/modyfikację/odebranie uprawnień użytkownikowi do zasobów informatycznych
- ➢ Rejestr nadanych kont i uprawnień użytkownikom systemu informatycznego
- ➢ Rejestr nadanych uprawnień tymczasowych użytkownikom systemu informatycznego

Wzory zapisów/druków są dostępne do wglądu w Sekcji Organizacyjno-Prawnej.

7. ZAŁĄCZNIKI

- ➢ Załącznik Nr 1 -Wniosek o nadanie/modyfikację/odebranie uprawnień Użytkownikowi do zasobów informatycznych
- ➢ Załącznik Nr 2 - Rejestr nadanych/modyfikowanych/ odebranych uprawnień użytkownikom systemu informatycznego
- ➢ Załącznik nr 3 - Podstawowe zasady bezpieczeństwa w zakresie przetwarzania danych osobowych w Wojewódzkim Szpitalu Zespolonym w Elblągu.

ODPOWIEDZIALNOŚĆ ZA TREŚĆ I AKTUALIZACJĘ INSTRUKCJI PONOSI AUTOR DOKUMENTU ORAZ OSOBA SPRAWDZAJĄCA:

Osoba opracowująca/aktualizująca niniejszy dokument jest zobowiązana do zapoznania się z aktualnie obowiązującymi wymaganiami prawnymi i regulacyjnymi, standardami akredytacyjnymi, ogólnymi standardami postępowania i wymaganiami dobrej praktyki medycznej oraz do przeanalizowania nieudokumentowanych sposobów postępowania w danym zakresie. W celu wypracowania jak najlepszych rozwiązań uwzględnia także informacje zebrane od przyszłych użytkowników oraz konsultuje treść dokumentu z osobą kompetentną w danym obszarze (tj. Radca Prawny, Dyrektor Pionu).