**ZASADY ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM**

*Niniejsza instrukcja została opracowana w oparciu o art. 32 ust. 1 przepisów Rozporządzenia PE i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych.*

**ROZDZIAŁ 1**

**ZASADY WYKORZYSTYWANIA SPRZĘTU INFORMATYCZNEGO I OPROGRAMOWANIA W PODMIOCIE LECZNICZYM**

1. Sprzęt informatyczny w podmiocie leczniczym jest wykorzystywany jedynie do celów związanych z realizacją zadań podmiotu leczniczego.
2. W podmiocie leczniczym wykorzystuje się następujący sprzęt informatyczny:
3. Stacje robocze,
4. Serwery,
5. Komputery przenośne,
6. Dyski zewnętrzne,
7. Inne…….(jakie?)
8. Jeśli w podmiocie leczniczym wykorzystuje się stacje robocze są one wyposażone w urządzenia podtrzymujące napięcie tzw. UPS.
9. W celu realizacji zadań związanych z infrastrukturą informatyczną podmiotu leczniczego, Administrator może korzystać z pomocy Informatyka. Jeżeli Informatykiem jest podmiot zewnętrzny jego dane kontaktowe znajdują się w ogólnodostępnym miejscu dla pracowników podmiotu leczniczego.
10. Administrator lub Informatyk prowadzi ewidencję sprzętu komputerowego podmiotu leczniczego oraz wykaz niezbędnego oprogramowania. Prowadzenie wykazów i ewidencji może odbywać się za pomocą dedykowanych do tego narzędzi informatycznych.
11. W podmiocie leczniczym wykorzystuje się jedynie legalne oprogramowanie, które posiada licencje. Za przechowywanie licencji odpowiada Administrator. Administrator zobowiązuje się do aktualizowania oprogramowania zgodnie z zaleceniami jego producentów. Administrator może zlecić obowiązek zapewnienia aktualności oprogramowania Informatykowi.
12. W podmiocie leczniczym wprowadzono zasadę, że każdy użytkownik systemów komputerowych pracuje na własnym loginie i haśle. Wprowadzono zakaz udostępniania haseł innym użytkownikom oraz pracy na jednym loginie przez kilku użytkowników.
13. Użytkownicy przed dopuszczeniem do pracy w podmiocie leczniczym muszą odbyć szkolenie w zakresie zasad ochrony danych osobowych i użytkowania sprzętu komputerowego i oprogramowania służącego do przetwarzania danych osobowych.
14. Użytkownicy systemów informatycznych i sprzętu komputerowego otrzymują przed przystąpieniem do pracy w podmiocie leczniczym, po spełnieniu warunku, o którym mowa w punkcie 7 niniejszego rozdziału upoważnienia z zakresem dostępu do systemów informatycznych. Wzór upoważnienia stanowi Załącznik nr 1 C do niniejszej Instrukcji.
15. Dopuszcza się wykorzystywanie zewnętrznych miejsc przechowywania danych (usługi w tzw. chmurze) podmiotu leczniczego o ile zapewniają one bezpieczeństwo i są zgodne z wytycznymi/ rekomendacjami w zakresie bezpieczeństwa wydanymi przez organy i instytucje organizujące system ochrony zdrowia.
16. W podmiocie leczniczym wykonuje się regularne kopie bezpieczeństwa, za których wykonanie odpowiada Informatyk. Kopie bezpieczeństwa mogą być wykonywane z użyciem specjalistycznego, zautomatyzowanego oprogramowania. Zadaniem Informatyka jest regularna weryfikacji poprawności ich sporządzania i możliwości ich wykorzystania. Szczegółowo zasady sporządzania kopii bezpieczeństwa reguluje Rozdział 5 niniejszego załącznika.
17. W podmiocie leczniczym wprowadzono zasadę instalacji sprzętu komputerowego w taki sposób, aby wgląd w ekran miała jedynie osoba upoważniona do przetwarzania danych osobowych.
18. Na sprzęcie komputerowym zainstalowano wygaszacze ekranu, które po 3 minutach bez pracy ulegają automatycznemu uruchomieniu.
19. Odchodząc od stanowiska komputerowego, użytkownik winien zamknąć program służący do przetwarzania danych osobowych lub wprowadzić blokadę ekranu za pomocą klawiszy alt+ctrl+delete. Po powrocie do stanowiska pracy ponowne uruchomienie możliwości pracy powinno nastąpić po wpisaniu hasła użytkownika.
20. Zabrania się użytkownikom korzystania z internetowych sieci publicznych.
21. Zabrania się użytkownikom wykorzystywania zewnętrznych nośników danych niewiadomego pochodzenia.
22. Administrator ma obowiązek zabezpieczenia sprzętu komputerowego, systemów informatycznych, kopii bezpieczeństwa przed dostępem osób postronnych, a także przed zagrożeniami losowymi takimi jak pożar, zalanie itp.
23. Po zakończeniu pracy każdy użytkownik ma obowiązek zamknąć systemy służące do przetwarzania danych osobowych, używając opcji wylogowania się i zapisania danych przed zamknięciem systemu.
24. W przypadku korzystania z komputerów przenośnych do celów realizacji zadań służbowych w podmiocie leczniczym, użytkownik po zakończeniu pracy ma obowiązek zamknięcia sprzętu komputerowego w szafie zamykanej na klucz.

**ROZDZIAŁ 2**

**DOSTĘP DO PRZETWARZANIA DANYCH OSOBOWYCH NA SPRZĘCIE KOMPUTEROWYM I SYSTEMACH INFORMATYCZNYCH**

1. Dostęp do komputerów w podmiocie leczniczym mają jedynie upoważnieni użytkownicy i Informatyk, którzy posiadają indywidualne loginy i hasła dostępu.
2. Pierwsze hasło dostępowe zakłada Informatyk na polecenie Administratora, które jest wyrażone poprzez przekazanie Upoważnienia celem jego uzupełnienia, o którym mowa w punkcie 8 Rozdziału 1 niniejszego załącznika. Informatyk ma zakaz nadawania loginów użytkownikom, które już kiedyś wystąpiły w podmiocie leczniczym.
3. Użytkownik, po pierwszym logowaniu, winien niezwłocznie zmienić hasło, na takie, które odpowiada postanowieniom punktu 4 niniejszego Rozdziału.
4. Hasła składają się z co najmniej 8 znaków. W skład hasła powinny wchodzić duże i małe litery, cyfra i znak specjalny. Hasło nie może być ciągiem następujących po sobie klawiszy. Zakazana jest powtarzalność hasła w okresie 12 miesięcy.
5. Użytkowników obowiązuje bezwzględny zakaz zapisywania i pozostawiania haseł w miejscach ogólnodostępnych.
6. Hasła należy zmieniać co 30 dni. Za regularność zmiany hasła odpowiada użytkownik. Administrator może zlecić Informatykowi wykorzystanie narzędzi informatycznych do wymuszania regularnych zmian hasła.
7. Postanowienia niniejszego rozdziału dotyczą również haseł dostępowych do systemów informatycznych służących do przetwarzania danych osobowych. Stosowane systemy informatyczne winny zapewniać pełną rozliczalność procesów przetwarzania danych osobowych w podmiocie leczniczym.
8. Dopuszcza się ograniczenia w stosowaniu postanowień niniejszego rozdziału, z wyłączeniem sytuacji dotyczącej systemów informatycznych służących do przetwarzania danych osobowych, o ile na sprzęcie informatycznym nie ma zlokalizowanych żadnych plików zawierających dane osobowe, które znajdują się poza systemem informatycznym tj. dokumentów tekstowych zawierających dane osobowe, zdjęć, wyników badań itp.
9. W przypadku sytuacji, o której mowa w punkcie 8 Administrator ma obowiązek zasięgnąć pisemnej opinii w tym zakresie u Inspektora Ochrony Danych Osobowych, do której dołączona jest również opinia Informatyka o braku przeciwskazań ze względów bezpieczeństwa.
10. Administrator wprowadził zasadę blokady dostępu do sprzętu komputerowego po trzech nieudanych próbach autoryzacji przez użytkownika. Taka sama procedura jest zalecana w przypadku dostępu do systemu informatycznego służącego do przetwarzania danych osobowych.
11. W przypadku zablokowania dostępu, użytkownik ma obowiązek powiadomić o tym fakcie Informatyka, który przywraca mu dostęp na zasadach, o których mowa w punkcie 2-4 niniejszego rozdziału.
12. Hasło Informatyka, którego uprawnienia są szersze niż uprawnienia użytkowników, winno składać się z co najmniej 12 znaków, w tym dużych i małych liter, cyfr i znaków specjalnych. Hasło powinno być zmieniane co najmniej raz na 30 dni, a jego powtarzalność może nastąpić dopiero po 24 miesiącach. Zakazuje się tworzenia haseł administracyjnych z wykorzystaniem imion i nazwisk czy też ciągów klawiaturowych.

**ROZDZIAŁ 3**

**KORZYSTANIE Z INTERNETU W PODMIOCIE LECZNICZYM**

1. W podmiocie leczniczym wykorzystuje się sieć internetową do realizacji zadań podmiotu leczniczego.
2. Użytkownicy wykorzystują Internet jedynie do realizacji zadań na stanowiskach pracy i do celów służbowych.
3. Użytkownicy mają bezwzględny zakaz instalowania oprogramowania niewiadomego pochodzenia. O każdorazowej potrzebie instalacji dodatkowego oprogramowania powinni powiadomić Informatyka.
4. Użytkownicy mogą korzystać jedynie ze stron internetowych służących do realizacji zadań podmiotu leczniczego.
5. Wykorzystując do celów służbowych mechanizmy logowania się do zewnętrznych systemów za pomocą przeglądarek internetowych użytkownik ma bezwzględny zakaz stosowania narzędzi automatycznego zapamiętywania haseł.
6. Realizując zadania podmiotu leczniczego użytkownik zobowiązany jest do wykorzystywania jedynie sieci internetowej podmiotu leczniczego.
7. Zabrania się pobierania plików, zgrywania plików i innych czynności narażających sieć podmiotu leczniczego na nieprawidłowe działanie.

**ROZDZIAŁ 4**

**POCZTA ELEKTRONICZNA**

1. Pracownicy podmiotu leczniczego mają prawo wykorzystywać pocztę elektroniczną do zadań na stanowiskach pracy pod warunkiem, że korzystają z adresów pocztowych podmiotu leczniczego. Istnieje bezwzględny zakaz korzystania z prywatnych skrzynek do realizacji zadań pracowniczych.
2. Dopuszczalne jest wysyłanie plików zawierających dane osobowe drogą elektroniczną pod następującymi warunkami:
3. plik zawierający dane osobowe został zaszyfrowany i jest chroniony hasłem,
4. hasło do pliku winno spełniać kryteria, o którym mowa w punkcie 4 Rozdziału 2,
5. hasło do pliku winno być przekazane niezależnie od właściwej informacji: wiadomością sms, wiadomością telefoniczną lub w odrębnej wiadomości mailowej,
6. wiadomość mailowa powinna zawierać adnotację, że jest kierowana do konkretnego odbiorcy i powinna zawierać pouczenie, że jeśli została błędnie przesłana to jej przypadkowy odbiorca powinien ją usunąć,
7. należy zażądać potwierdzenia otrzymania wiadomości mailowej przez odbiorcę.
8. Sposoby szyfrowania plików w podmiocie leczniczym określa Administrator przy udziale Informatyka.
9. Użytkownik odbierający wiadomości mailowe kierowane do podmiotu leczniczego ma obowiązek zachować szczególną ostrożność w przypadkach, kiedy wiadomości zawierają załączniki, w których znajdują się pliki do rozpakowania lub tzw. hiperlinki. W każdej podejrzanej sytuacji użytkownik powinien skonsultować się z Informatykiem.
10. Użytkownik ma zakaz uczestniczenia w korespondencji „zbiorowej”, kiedy przesyłane są informacje z użyciem opcji „prześlij dalej” przez wielu użytkowników.
11. Wysyłając korespondencję mailową do kilku odbiorców, użytkownik ma obowiązek korzystania z opcji „UDW” tj. ukrycia odbiorców wiadomości.
12. Nie zaleca się użytkownikom przesyłania/ odbierania plików o dużych rozmiarach tj. o wielkości większej niż 5 MB.
13. Informatyk ma obowiązek okresowo weryfikować stan pojemności skrzynki pocztowej i w zależności od pojemności serwera i jego możliwości technicznych archiwizować zgromadzone wiadomości lub usuwać wiadomości niepotrzebne.

**ROZDZIAŁ 5**

**WYKONYWANIE KOPII BEZPIECZEŃSTWA W PODMIOCIE LECZNICZYM**

1. W celu zapewnienia ciągłości pracy oraz rozliczalności systemu ochrony danych osobowych w podmiocie leczniczym wykonywane są kopie bezpieczeństwa baz danych.
2. Za wykonanie kopii bezpieczeństwa odpowiada Informatyk.
3. Informatyk w porozumieniu z Administratorem oraz Inspektorem Ochrony Danych Osobowych określa krytyczne obszary, z których niezbędne jest sporządzanie kopii bezpieczeństwa.
4. Kopie bezpieczeństwa sporządzane są w odstępach czasowych umożliwiających zachowanie ciągłości pracy podmiotu leczniczego. Częstotliwość sporządzania kopii zapasowych określa Administrator w porozumieniu z Inspektorem Ochrony Danych Osobowych.
5. Informatyk odpowiada za poprawność sporządzenia kopii zapasowej oraz możliwości jej wykorzystania.
6. Kopie zapasowe są nadpisywane na poprzednie jej wersje.
7. Kopia zapasowa nie może być przechowywana w pomieszczeniach, w których znajduje się podstawowa baza danych.
8. Kopie bezpieczeństwa wykonywane są w następujący sposób:
9. Wykonuje je osobiście Informatyk sporządzając kopię na zewnętrzny nośnik pamięci, który jest chroniony hasłem. Następnie nośnik z kopią bezpieczeństwa zostaje umieszczony w odrębnym pomieszczeniu, w szafie zamykanej na klucz\*,
10. Kopia wykonywana jest w sposób zautomatyzowany za pomocą narzędzi…………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………\* *(opisać sposób sporządzania kopii)*

*\*niepotrzebne skreślić*

**ROZDZIAŁ 6**

**ZABEZPIECZENIA TECHNICZNE I OCHRONA ANTYWIRUSOWA**

1. Podmiot leczniczy stosuje zabezpieczenia techniczne i ochronę antywirusową związane z systemami informatycznymi i sprzętem komputerowym.
2. W przypadku dostępu do danych osobowych za pomocą sieci zewnętrznej podmiot leczniczy stosuje szyfrowanie połączeń za pomocą narzędzi typu SSL, VPN lub innych, które są powszechnie uznane za spełniające kryteria bezpieczeństwa. Zgodę na wykorzystanie takich narzędzi wydaje Informatyk, po zasięgnięciu opinii Inspektora Ochrony Danych Osobowych.
3. W podmiocie leczniczym zastosowano następujące zabezpieczenia:
4. Analityczny system do wykrywania zagrożeń (SIEM),
5. Redundancja krytycznych zasobów,
6. Sondy IDS/IPS,
7. Skanery podatności,
8. System firewall, NG firewall, UTM,
9. Hardening,
10. Wirtualizacja,
11. Stosowanie techniki rozpraszania danych CDN,
12. Autoryzacja dostępu do serwera DHCP,
13. Blokowanie możliwości instalacji oprogramowania przez użytkownika,
14. Blokowanie portów USB w stacjach roboczych,
15. Blokowanie ruchu sieciowego z określonych adresów IP,
16. Budowanie topologii sieci z uwzględnieniem obszarów bezpiecznych i zdemilitaryzowanych (DMZ),
17. Monitorowanie ruchu sieci,
18. Stosowanie serwerów PROXY,
19. Okresowe przeglądanie logów stacji roboczej przez administratorów,
20. Nadzór nad ruchem wychodzącym,
21. Wykrywanie i blokowanie spamu,
22. Translacja adresów sieciowych
23. System do inwentaryzacji sprzętu, zarządzania licencjami,
24. …………………………….(inne)

*\* niepotrzebne skreślić*

1. W podmiocie leczniczym, na sprzęcie komputerowym zainstalowano oprogramowanie antywirusowe, które jest na bieżąco aktualizowane.
2. Za aktualizację oprogramowania antywirusowego odpowiada Informatyk. Zaleca się, aby oprogramowanie antywirusowe aktualizowało się automatycznie.
3. Program antywirusowy zabezpiecza co najmniej pliki systemowe oraz pocztę elektroniczną, a także ma włączoną opcję przeciwwłamaniową.
4. Użytkownik jest odpowiedzialny za skanowanie stacji roboczej/ komputera przenośnego, co najmniej raz na 3 dni.
5. Użytkownik ma bezwzględny zakaz wyłączania funkcji programu antywirusowego.
6. W przypadku podejrzenia pojawienia się szkodliwego pliku lub wirusa, użytkownik ma bezwzględny obowiązek powiadomienia o tym fakcie Administratora.

**ROZDZIAŁ 7**

**ZASADY KORZYSTANIA Z KOMPUTERÓW PRZENOŚNYCH**

1. W podmiocie leczniczym dopuszcza się możliwość korzystania z komputerów przenośnych do realizacji zadań podmiotu leczniczego.
2. W przypadku korzystania z komputerów przenośnych użytkownicy muszą zachować szczególne środki ostrożności, które uniemożliwią kradzież sprzętu, pozostawienie go bez nadzoru.
3. W trakcie transportu komputerów przenośnych użytkownik jest zobowiązany do zabezpieczenia go w taki sposób, aby dostęp do niego był utrudniony tzn. nie należy przewozić takich komputerów na siedzeniach w samochodzie lub pozostawiać go w widocznym miejscu podczas parkowania.
4. Komputer przenośny, na którym przechowuje się dane osobowe musi być bezwzględnie zabezpieczony hasłem, zarówno do systemu operacyjnego, jak i do systemu informatycznego, w którym przetwarzane są dane osobowe. Hasła te nie mogą być identyczne. Zasady tworzenia haseł dostępowych są analogiczne jak w punkcie 4 Rozdziału 2 niniejszego załącznika.
5. Na komputerach przenośnych zalecane jest instalowanie dodatkowych narzędzi szyfrujących tj. specjalnych dysków i macierzy.
6. Jeśli korzystamy stacjonarnie z komputera przenośnego w podmiocie leczniczym użytkownik ma obowiązek dbałości o jego naładowanie, które umożliwia pracę bez zasilania elektrycznego przez co najmniej 2 godziny.
7. Po zakończeniu pracy użytkownik jest zobowiązany do przeprowadzenia czynności, o których mowa w punkcie 19 Rozdziału 1 niniejszego załącznika.
8. Użytkownik ma zakaz wykorzystywania na komputerach przenośnych niezweryfikowanych sieci bezprzewodowych tj. publicznych, hotelowych i innych, które mogą umożliwić przeglądanie operacji przez osoby postronne.
9. Korzystając z komputera przenośnego poza podmiotem leczniczym, użytkownik powinien ograniczyć użytkowanie programów zawierających dane osobowe, a jeśli tego dokonuje powinien zadbać, aby osoby postronne nie miały wglądu w ekran komputera.
10. Użytkownik jest zobowiązany do sporządzania kopii bezpieczeństwa z komputerów przenośnych w sposób uzgodniony z Informatykiem i zaakceptowany przez Administratora.

**ROZDZIAŁ 8**

**KONSERWACJA I NAPRAWY SPRZETU INFORMATYCZNEGO I OPROGRAMOWANIA W PODMIOCIE LECZNICZYM**

1. Administrator przy udziale Informatyka odpowiada za niezawodność pracy systemów informatycznych i sprzętu informatycznego, z uwzględnieniem wytycznych dostawców sprzętu i oprogramowania.
2. Konserwacja sprzętu i oprogramowania winna odbywać się w miarę potrzeb, nie rzadziej jednak niż raz do roku.
3. Administrator określił sposoby realizacji napraw w Załączniku nr 6 do niniejszej Instrukcji.
4. Administrator odpowiada za zabezpieczenie komputerów przed nieuprawnionym dostępem w trakcie napraw poza siedzibą podmiotu poprzez uprzednie, trwałe usunięcie wszystkich informacji zawierających dane osobowe. Po powrocie z naprawy, Administrator przy udziale Informatyka, konfiguruje sprzęt w sposób umożliwiający jego powtórne wykorzystanie w działalności podmiotu leczniczego.
5. Naprawy i konserwacje w siedzibie podmiotu leczniczego odbywać się muszą w czasie obecności lub pod nadzorem administratora lub upoważnionej przez niego osoby.
6. Administrator dopuszcza możliwość dokonywania serwisowania i napraw za pomocą narzędzi zdalnych, z zastrzeżeniem postanowień, o których mowa w punkcie 2 Rozdziału 6 niniejszego załącznika.
7. W przypadku serwisowania urządzeń towarzyszących, o których mowa w Rozdziale 9 niniejszego załącznika, wykorzystywanych do działalności podmiotu leczniczego, niezbędnych do realizacji świadczeń zdrowotnych, takich jak np. urządzenia ultrasonograficzne, urządzenia rtg i inne, Administrator jest zobowiązany do przeprowadzania napraw i ich konserwacji na zasadach, o których mowa w niniejszym Rozdziale.
8. Jeśli Administrator nie ma możliwości zastosowania metod, o których mowa w niniejszym rozdziale musi zasięgnąć opinii Inspektora Ochrony Danych Osobowych o sposobach realizacji napraw i konserwacji.

**ROZDZIAŁ 9**

**URZĄDZANIA WSPOMAGAJĄCE DZIAŁALNOŚĆ PODMIOTU LECZNICZEGO**

1. Podmiot leczniczy może wykorzystywać urządzenia i systemy informatyczne inne niż komputery, które są niezbędne w procesach diagnostycznych i udzielania świadczeń zdrowotnych.
2. Administrator w takich przypadkach ma obowiązek korzystać z urządzeń posiadających stosowne legalizacje i licencjonowane oprogramowanie.
3. Do urządzeń, o których mowa w punkcie 1 niniejszego rozdziału zaliczyć należy przede wszystkim:
4. Ultrasonografy,
5. Aparaty rtg,
6. Echokardiografy,
7. Tomografy,
8. Inne.
9. Wykaz urządzeń wspomagających prowadzi Administrator.
10. O ile jest to możliwe do zabezpieczeń urządzeń wspomagających zastosowanie mają przepisy dotyczące sprzętu komputerowego.
11. Jeśli nie ma możliwości zastosowania standardowych zabezpieczeń urządzeń towarzyszących na których mogą znajdować się dane osobowe, Administrator jest zobowiązany do zastosowania metod anonimizacji tych danych. Jeśli urządzenia te nie dają takich możliwości, Administrator określa środki zabezpieczające przy udziale Inspektora Ochrony Danych Osobowych oraz dostawcy tych urządzeń.

**ROZDZIAŁ 10**

**ODPOWIEDZIALNOŚĆ UŻYTKOWNIKÓW**

1. Administrator jest zobowiązany do nadzoru w zakresie uprawnień użytkowników w taki sposób, aby zrealizowana została zasada minimalizacji tj. aby każdy użytkownik dopuszczony do pracy w systemach informatycznych posiadał jedynie uprawnienia niezbędne do realizacji zadań na stanowisku pracy.
2. Użytkownik odpowiada za wszystkie czynności, które zostały wykonane z użyciem jego loginu i hasła.
3. Użytkownik odpowiada również za wszystkie czynności, które doprowadziły do awarii systemów i sprzętu komputerowego w podmiocie leczniczym.

……………………………….

 *(podpis Administratora)*