**INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM**

**W INDYWIDUALNEJ PRAKTYCE LEKARSKIEJ/PRAKTYCE STOMATOLOGICZNEJ/NZOZ**

***(wpisać właściwą nazwę)***



*(miejscowość, data)*

**§1**

**Postanowienia ogólne.**

1. 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.
2. Sieć informatyczną, w której przetwarzane są dane osobowe, stanowią wszystkie pracujące w …………………\*(wpisać pełną nazwę i adres podmiotu), obecne i przyszłe serwery, komputery stacjonarne i przenośne, a także urządzenia peryferyjne i sieciowe, a także inne urządzenia stanowiące elementy systemu informatycznego lub połączone z systemem informatycznym.
3. Sygnał internetowy dostarczany jest przez usługodawcę internetowego i jest odpowiednio zabezpieczony. System zabezpieczony jest oprogramowaniem antywirusowym zainstalowanym na każdym stanowisku oraz zasilaczami awaryjnymi utrzymującymi stałe zasilanie.
4. Dopuszcza się wykorzystywanie zewnętrznych miejsc przechowywania danych (usługi w tzw. chmurze) Praktyki o ile zapewniają one bezpieczeństwo i są zgodne z wytycznymi/ rekomendacjami w zakresie bezpieczeństwa wydanymi przez organy i instytucje organizujące system ochrony zdrowia.

**§2**

**Procedura nadawania uprawnień do przetwarzania danych oraz ich rejestrowanie w systemie informatycznym.**

1. Do obsługi systemu informatycznego służącego do przetwarzania danych osobowych, może być dopuszczona wyłącznie osoba posiadająca upoważnienie do przetwarzania danych osobowych, wydane przez Administratora danych osobowych. Wzór upoważnienia stanowi załącznik nr 3 do Polityki bezpieczeństwa danych osobowych.
2. Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora użytkownika i właściwego hasła.
3. Dla każdego użytkownika systemu informatycznego, który przetwarza dane osobowe, przydziela się niepowtarzalny identyfikator i hasło początkowe.
4. Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego nie powinien być przydzielany innej osobie.
5. W przypadku utraty przez daną osobę uprawnień do dostępu do danych osobowych w systemie informatycznym, należy niezwłocznie wyrejestrować ją z systemu informatycznego, unieważnić jej hasło oraz podjąć inne stosowne działania w celu zapobieżenia dalszemu dostępowi tej osoby do danych.

**§3**

**Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem.**

1. System informatyczny przetwarzający dane osobowe wykorzystuje mechanizm identyfikatora i hasła jako narzędzi umożliwiających bezpieczne uwierzytelnienie.
2. Użytkownik posiadający upoważnienie do przetwarzania danych osobowych powinien posiadać hasła do systemu operacyjnego oraz osobne do baz danych osobowych i aplikacji.
3. Hasło składa się z co najmniej ośmiu znaków, zawiera co najmniej jedną małą i wielką literę, jedną cyfrę lub jeden znak specjalny.
4. Hasło nie powinno zawierać żadnych informacji, które można skojarzyć z użytkownikiem komputera (imiona najbliższych, daty urodzenia, inicjały, itp.) i nie może być sekwencją kolejnych znaków klawiatury.
5. W przypadku, gdy istnieje podejrzenie, że hasło mogła poznać osoba nieupoważniona, użytkownik zobowiązany jest do zgłoszenia tego faktu ADO (Administratorowi Systemu Informatycznego\*, zwanym dalej ASI) i do natychmiastowej zmiany hasła.
6. Zmianę hasła należy dokonywać nie rzadziej niż co 30 dni.
7. Hasła najwyższego poziomu, którymi dysponuje ADO (ASI) gromadzone są w zamkniętej kopercie przez ADO.
8. Hasła użytkowników generuje ASI i przekazuje wraz z loginem w formie papierowej w zamkniętej kopercie.
9. Po zapoznaniu się z loginem i hasłem użytkownik zobowiązany jest do ich zniszczenia w odpowiednim urządzeniu niszczącym.
10. Hasło nie może być zapisywane i przechowywane.
11. Użytkownik nie może udostępniać identyfikatora oraz haseł osobom nieupoważnionym.

**\**ASI, czyli Administrator Systemu Informatycznego odpowiada za bezpieczeństwo systemu komputerowego. Może go powołać Administrator Danych Osobowych, jeżeli posiada duży system, którego obsługa wymaga wiedzy w zakresie informatyki i programowania. W innym przypadku obowiązki ASI może wykonywać Administrator Danych. Jeżeli ASI nie zostanie powołany, proszę usunąć jego nazwę z tekstu.***

**§4**

**Procedury rozpoczęcia, zawieszenia i zakończenia pracy.**

1. Każdy pracownik korzystający z systemu informatycznego przystępując do pracy powinien podać swoje dane dostępu do komputera i systemu, tj. identyfikator i hasło.
2. Zawieszenie pracy polega na opuszczeniu stanowiska pracy bez wylogowania się i jest dopuszczalne tylko w przypadku pozostania w pomieszczeniu.
3. Zakończenie pracy w systemie następuje poprzez prawidłowe, wymagane przez daną aplikację oraz system operacyjny, wykonanie czynności kończących. Niedopuszczalne jest zakończenie pracy poprzez wyłączenie napięcia zasilającego bez pełnej procedury zamknięcia.
4. Ekrany monitorów stanowisk komputerowych, na których odbywa się przetwarzanie danych osobowych powinny być w miarę możliwości tak umieszczone, aby uniemożliwić wgląd w dane osobom postronnym przebywającym w pomieszczeniu oraz powinny automatycznie się wyłączać poprzez stosowanie wygaszaczy ekranowych uruchamiających blokadę pracy na komputerze.
5. Wydruki zawierające dane osobowe należy przechowywać w miejscu uniemożliwiającym do nich dostęp osobom postronnym. Wydruki niepotrzebne należy zniszczyć w niszczarce dokumentów.
6. Osoba przetwarzająca dane osobowe w przypadku konieczności opuszczenia pomieszczenia, obowiązana jest prawidłowo, zgodnie z instrukcją obsługi systemu, zakończyć pracę w systemie.
7. Czas rozpoczynania i kończenia pracy w systemach sieciowych, w tym systemach przetwarzających dane osobowe, zgodny jest z ustalonym czasem pracy.
8. Konieczność pracy w aplikacjach sieciowych poza ustalonym czasem pracy, powinna być uzgodniona z ADO.
9. ADO (ASI) monitoruje logowanie oraz wylogowanie się użytkowników oraz nadzoruje zakres przetwarzanych przez nich zbiorów danych.
10. W przypadku korzystania z komputerów przenośnych do celów realizacji zadań służbowych w podmiocie, użytkownik po zakończeniu pracy ma obowiązek zamknięcia sprzętu komputerowego w szafie zamykanej na klucz.

**§5**

**Procedury tworzenia kopii awaryjnych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.**

1. Dane osobowe zabezpiecza się poprzez wykonywanie kopii awaryjnych.
2. Ochronie poprzez wykonanie kopii podlegają także programy i narzędzia programowe służące przetwarzaniu danych. Kopie programów i narzędzi wykonywane są zaraz po instalacji oraz po każdej aktualizacji na zewnętrznych, elektronicznych nośnikach informacji.
3. Zabezpieczeniu poprzez wykonywanie kopii awaryjnych podlegają także dane konfiguracyjne systemu informatycznego prze­twarzającego dane osobowe, w tym uprawnienia użytkowników systemu.
4. Za proces tworzenia kopii programów i narzędzi programowych oraz danych konfiguracyjnych systemu odpowiedzialny jest ADO (ASI). Kopie przechowywane są w zamkniętej szafie w zabezpieczonym pomieszczeniu.
5. Kopie awaryjne mogą być sporządzane automatycznie lub manualnie z wykorzystaniem specjalistycznych urządzeń do wykonywania kopii lub standardowych narzędzi oferowanych przez stacje robocze.
6. Kopie zbiorów danych osobowych zlokalizowanych na komputerach lokalnych wykonywane są przez poszczególnych użytkowników ostatniego dnia każdego miesiąca i zapisywane na dyskach lokalnych w ustalonej z ADO lokalizacji lub zapisywane na nośnikach zewnętrznych, autoryzowanych i dostarczonych przez ADO.
7. Pliki edytorów tekstu lub arkuszy kalkulacyjnych traktowane są jak kopie zbiorów, z których pochodzą przetwarzane w nich dane i nie są objęte procedurami wykonywania kopii awaryjnych.
8. Nośniki, na których są przechowywane kopie danych osobowych, powinny być wyraźnie oznaczone.
9. Za bezpieczeństwo kopii awaryjnych przetwarzanych lokalnie odpowiadają poszczególni użytkownicy systemu, którzy je wykonali. Kopie usuwa się niezwłocznie po ustaniu ich użyteczności w sposób uniemożliwiający odtworzenie danych.
10. ADO zobowiązany jest do okresowego wykonywania testów odtworzeniowych kopii awaryjnych.
11. Zewnętrzne nośniki kopii awaryjnych, które zostały wycofane z użycia, podlegają znisz­czeniu po usunięciu danych osobowych, w odpowiednim urządzeniu niszczącym.
12. Użytkownik tworzy wydruki związane z przetwarzaniem danych osobowych wyłącznie w zakresie i ilości niezbędnej dla celów służbowych w uzgodnieniu z przełożonym.
13. Wszystkie dokumenty, zestawienia i wydruki zawierające dane osobowe powinny być chronione przed dostępem osób nieupoważnionych. Użytkownik przechowuje je w zamkniętej szafie w pomieszczeniu zabezpieczonym przed nieuprawnionym dostępem.

**§6**

**Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych****.**

* 1. Okresowe kopie zapasowe wykonywane są na płytach CD/DVD lub innych elektronicznych nośnikach informacji. Kopie zapasowe przechowuje się w kasie pancernej w pomieszczeniu kierownika Praktyki, w sposób uniemożliwiający nieuprawnione przejęcie, modyfikacje, uszkodzenie lub zniszczenie.
	2. Okres przechowywania dokumentacji medycznej pacjenta oraz danych kadrowych określone są odrębnymi przepisami prawa. Po upływie wymaganych ustawowo okresów kopie zapasowe należy bezzwłocznie usuwać po ustaniu ich użyteczności.
	3. Usunięcie danych z systemu powinno zostać zrealizowane przy pomocy oprogramowania przeznaczonego do bezpiecznego usuwania danych z nośnika informacji.
	4. W przypadku kopii zapasowych sporządzanych indywidualnie przez użytkownika – odpowiedzialny za ich zniszczenie jest użytkownik.
	5. Przez zniszczenie nośników informacji rozumie się ich trwałe i nieodwracalne zniszczenie do stanu nie dającego możliwości ich rekonstrukcji i odzyskania danych.
	6. Serwery oraz komputery, na których odbywa się przetwarzanie danych osobowych, powinny być zabezpieczone przed utratą danych spowodowaną awarią zasilania poprzez stosowanie specjalnych urządzeń podtrzymujących zasilanie i eliminujących zakłócenia sieci zasilającej.
	7. Komputery przenośne oraz inne mobilne nośniki danych osobowych powinny być zabezpieczone ochroną kryptograficzną – powinny być zaszyfrowane.

**§7**

**Sposób zabezpieczenia systemu przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego. Zabezpieczenia techniczne.**

1. ADO zapewnia ochronę antywirusową oraz zarządza systemem wykrywającym i usuwającym wirusy i inne niebezpieczne kody.
2. System antywirusowy jest skonfigurowany w sposób zapewniający na bieżąco skanowanie wszystkich informacji przetwarzanych w systemie, a zwłaszcza poczty elektronicznej i stron internetowych.
3. System antywirusowy musi mieć aktywną funkcję automatycznej aktualizacji wzorców wirusów.
4. W przypadkach wystąpienia infekcji użytkownik powinien niezwłocznie powiadomić o tym fakcie ADO.
5. W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy, ADO podejmuje działania zmierzające do usunięcia zagrożenia.
6. Użytkownicy systemu mają również obowiązek skanowania każdego zewnętrznego elektronicznego nośnika informacji, który chcą wykorzystać.
7. 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.
8. W podmiocie leczniczym zastosowano następujące zabezpieczenia\*:
9. Analityczny system do wykrywania zagrożeń (SIEM),
10. Redundancja krytycznych zasobów,
11. Sondy IDS/IPS,
12. Skanery podatności,
13. System firewall, NG firewall, UTM,
14. Hardening,
15. Wirtualizacja,
16. Stosowanie techniki rozpraszania danych CDN,
17. Autoryzacja dostępu do serwera DHCP,
18. Blokowanie możliwości instalacji oprogramowania przez użytkownika,
19. Blokowanie portów USB w stacjach roboczych,
20. Blokowanie ruchu sieciowego z określonych adresów IP,
21. Budowanie topologii sieci z uwzględnieniem obszarów bezpiecznych i zdemilitaryzowanych (DMZ),
22. Monitorowanie ruchu sieci,
23. Stosowanie serwerów PROXY,
24. Okresowe przeglądanie logów stacji roboczej przez administratorów,
25. Nadzór nad ruchem wychodzącym,
26. Wykrywanie i blokowanie spamu,
27. Translacja adresów sieciowych
28. System do inwentaryzacji sprzętu, zarządzania licencjami,
29. …………………………….(inne)

*\* niepotrzebne usunąć*

**§8**

**Udostępnianie danych osobowych i sposób odnotowania informacji o udostępnionych danych**

Udostępnienie danych instytucjom może odbywać się wyłącznie zgodnie z przepisami prawa, w sposób opisany w Polityce bezpieczeństwa danych osobowych.

**§9**

 **Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.**

1. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
2. likwidacji — pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,
3. przekazania podmiotowi nieuprawnionemu do przetwarzania danych — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie,
4. naprawy — o ile to możliwe pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie.
5. Instalacji, konserwacji oraz napraw sprzętu komputerowego dokonuje ASI lub pracownicy firm przez wskazanych przez ADO.
6. Przeglądy i konserwacje systemu oraz nośników informacji służących do przetwarzania danych mogą być wykonywane jedynie przez osoby posiadające upoważnienie wydane przez ADO lub z którymi zawarto umowy powierzenia przetwarzania danych w zakresie konserwacji i napraw.
7. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe muszą uwzględniać zachowanie wymaganego poziomu zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych.
8. ADO wykonuje okresowy przegląd nośników danych osobowych eliminując te, które nie zapewniają odpowiedniego poziomu bezpieczeństwa oraz niezawodności.

**§10**

**Poczta elektroniczna.**

1. Pracownicy podmiotu 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 §3,
5. hasło do pliku winno być przekazane niezależnie od właściwej informacji: wiadomością sms, wiadomością telefoniczną lub drogą pocztową, skierowane imiennie do adresata wiadomości elektronicznej,
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 ASI.
9. Użytkownik odbierający wiadomości mailowe kierowane do podmiotu 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 ASI.
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. ASI 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.

**§11**

**Urządzenia wspomagające działalność Praktyki/NZOZ**

1. Podmiot 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.

**§12**

**Postanowienia końcowe.**

1. Użytkownikom zabrania się:
2. korzystania ze stanowisk komputerowych podłączonych do sieci informatycznej poza godzinami pracy bez pisemnej zgody ADO,
3. udostępniania stanowisk roboczych osobom nieuprawnionym,
4. wykorzystywania sieci komputerowej w celach innych niż wyznaczone przez ADO,
5. samowolnego instalowania i używania programów komputerowych,
6. korzystania z nielicencjonowanego oprogramowania oraz wykonywania jakichkolwiek działań niezgodnych z ustawą o ochronie praw autorskich,
7. umożliwiania dostępu do zasobów wewnętrznej sieci informatycznej oraz sieci Internetowej osobom nieuprawnionym,
8. używania komputera bez zainstalowanego oprogramowania antywirusowego.
9. Zabrania się użytkownikom korzystania z internetowych sieci publicznych.
10. Zabrania się użytkownikom wykorzystywania zewnętrznych nośników danych niewiadomego pochodzenia.
11. Użytkownicy mogą korzystać jedynie ze stron internetowych służących do realizacji zadań Praktyki.