Załącznik nr 2
do Zarządzenia nr 7
Dyrektora OLU SP ZOZ w Lublinie
z dnia 17 czerwca 2015r.

INSTRUKCJA ZARZADZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W OŚRODKU LECZENIA UZALEŻNIEN SP ZOZ W LUBLINIE

Podstawa prawna.

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. 2014r. poz. 1182) oraz rozporządzenie 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. Nr 100, poz. 1024 z późn. zm.)

§1

Przepisy ogólne.

1. Instrukcja zarządzania systemem informatycznym Ośrodka Leczenia Uzależnień SP ZOZ w Lublinie, zwana dalej instrukcją, opisuje sposoby nadawania uprawnień użytkownikom, określa sposób pracy w systemie informatycznym, procedury zarządzania oraz czynności mające wpływ na zapewnienie bezpieczeństwa systemu informatycznego.
2. Niniejsza instrukcja realizuje „Politykę bezpieczeństwa przetwarzania danych osobowych" obowiązującą w Ośrodku Leczenia Uzależnień SP ZOZ w Lublinie.

§2

Definicje.

Ilekroć w niniejszym dokumencie jest mowa o:

- OLU SP ZOZ – należy przez to rozumieć Ośrodek Leczenia Uzależnień w Lublinie.
- Administratorze Danych – należy przez to rozumieć Dyrektora OLU SP ZOZ,
- Pełnomocnik ds. Bezpieczeństwa Informacji – należy przez to rozumieć pracownika wyznaczonego do realizującego zadania w zakresie przestrzegania zasad ochrony danych osobowych ustanowionego zgodnie z Polityką bezpieczeństwa przetwarzania danych osobowych w OLU SP ZOZ,
- Administratorze Systemu Informatycznego – należy przez to rozumieć osobę odpowiedzialną za funkcjonowanie systemu informatycznego OLU
- użytkowniku systemu – należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym OLU.
- sieci lokalnej – należy przez to rozumieć fizyczne i logiczne połączenie systemów informatycznych OLU z wykorzystaniem urządzeń telekomunikacyjnych,
- sieci Internet – należy przez to rozumieć publiczną sieć telekomunikacyjną w rozumieniu ustawy Prawo telekomunikacyjne (Dz. U. z 2004 r., Nr 171, poz. 1800, z późn. zm.)

§3

1. .W Ośrodku Leczenia Uzależnień w Lublinie funkcję Pełnomocnika ds. bezpieczeństwa informacji pełni osoba wyznaczona spośród pracowników.
2. Pełnomocnik ds. ds. bezpieczeństwa informacji odpowiedzialny jest za zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:
   a) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych i sporządzanie raportów wraz z zaleceniami zmian w zabezpieczeniu danych przechowywanych i przetwarzanych w formie papierowej i w systemach informatycznych;
   b) opracowanie i aktualizację dokumentacji, tj.: Polityki bezpieczeństwa danych osobowych i Instrukcji zarządzania systemem informatycznym w którym przetwarzane są dane osobowe oraz przestrzegania zasad w nich określonych,
   c) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych;
   d) kontrolę stanu wydawanych upoważnień oraz ewidencję osób upoważnionych;
   e) nadzór nad działaniem Administratora systemów informatycznych w realizacji obowiązków związanych z zabezpieczeniem danych w systemach informatycznych,
   f) kontrolę poprawności stosowania procedur dotyczących ochrony danych osobowych przez wszystkie upoważnione osoby;
   g) wykrywanie i reagowanie na przypadki naruszania bezpieczeństwa danych osobowych przetwarzanych w dokumentacji papierowej i systemach informatycznych podejmowanie odpowiednich działań.
3. Administratorem systemu informatycznego jest osobą z firmy informatycznej utrzymującej w ruchu i wykonującej przeglądy sieci komputerowej Ośrodka
4. Administrator systemu informatycznego podejmuje następujące działania:
   a) identyfikuje i analizuje zagrożenia oraz ryzyko, na które mogą być narażone dane w systemach informatycznych;
   b) monitoruje działanie zabezpieczeń technicznych i organizacyjnych wdrożonych w celu ochrony danych osobowych w systemach informatycznych;
   c) wykrywa i reaguje na przypadki naruszenia bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych;
   d) instaluje i modyfikuje oprogramowanie systemowe i aplikacyjne, a także konfiguruje sprzęt;
   e) instaluje i aktualizuje oprogramowanie antywirusowe;
   f) tworzy kopie zapasowe baz danych, zawierających zbiory danych osobowych oraz zbiory dokumentacji medycznej.

§ 4

Procedury nadawania i zmiany uprawnień do przetwarzania danych.

1. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych musi zapoznać się z:
   a) Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. 2014r. poz. 1182),
   b) Polityką bezpieczeństwa przetwarzania danych osobowych w Ośrodku Leczenia Uzależnień SP ZOZ w Lublinie oraz niniejszym dokumentem.

   Powinien posiadać upoważnienie do przetwarzania danych osobowych.
2. Zapoznanie się z powyższymi informacjami pracownik potwierdza własnoręcznym podpisem na oświadczeniu, którego wzór stanowi załącznik nr 1.
3. Administrator Systemu Informatycznego przyznaje uprawnienia w zakresie dostępu do systemu informatycznego na podstawie upoważnienia określającego zakres uprawnień pracownika załącznik nr 2 i wniosku którego wzór stanowi załącznik nr 3,

Oryginał upoważnienia określającego zakres uprawnień do dostępu do danych osobowych w OLU SP ZOZ w Lublinie zostaje przekazany pracownikowi za potwierdzeniem odbioru, kopia zostaje dołączona do akt osobowych pracownika.

4. Przyznanie uprawnień w zakresie dostępu do systemu informatycznego polega na wprowadzeniu do systemu dla każdego użytkownika unikalnego identyfikatora, hasła oraz zakresu dostępnych danych i operacji.
5. Hasło ustanowione podczas przyznawania uprawnień przez Administratora systemu informatycznego należy zmienić na indywidualne hasło podczas pierwszego logowania się w systemie.
6. Pracownik ma prawo do wykonywania tylko tych czynności, do których został upoważniony.
7. Pracownik ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu.
8. W systemie informatycznym stosuje się uwierzytelnianie dwustopniowe na poziomie dostępu do systemu operacyjnego i sieci lokalnej oraz dostępu do aplikacji.
9. Odebranie uprawnień pracownikowi następuje na pisemny wniosek Dyrektora OLU z podaniem daty oraz przyczyny odebrania uprawnień.
10. Dyrektor OLU informuje Pełnomocnika ds. bezpieczeństwa informacji o każdej zmianie dotyczącej pracowników mającej wpływ na zakres posiadanych uprawnień w systemie informatycznym.
11. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych należy niezwłocznie zablokować w systemie informatycznym oraz unieważnić hasło.
12. Administrator systemu informatycznego zobowiązany jest do prowadzenia i ochrony rejestru użytkowników i ich uprawnień w systemie informatycznym rejestr stanowi załącznik nr 4,

§ 5

Zasady posługiwania się hasłami.

1. Bezpośredni dostęp do systemu informatycznego może mieć miejsce wyłącznie po podaniu identyfikatora osoby i właściwego hasła.
2. Hasło użytkownika powinno być unikalne, znane tylko użytkownikowi i niezmienne.
3. Identyfikator użytkownika nie może być zmieniany bez wyraźnej przyczyny, a po wyrejestrowaniu użytkownika z systemu informatycznego nie może zostać przydzielany innej osobie.
4. Pracownicy są odpowiedzialni za zachowanie poufności swoich identyfikatorów i haseł.
5. Hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności.
6. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie. W sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, pracownik zobowiązany jest do natychmiastowej zmiany hasła i poinformowania o zaistniałym fakcie Pełnomocnika ds. bezpieczeństwa informacji.
7. Przy wyborze hasła obowiązują następujące zasady:
   a) minimalna długość hasła - 8 znaków;
   b) zakazuje się stosować: haseł, które użytkownik stosował uprzednio, swojego identyfikatora w jakiejkolwiek formie, swojego imienia, drugiego imienia, nazwiska, przezwiska, pseudonimu, ogólnie dostępnych informacji o użytkowniku (numer telefonu, numer rejestracyjny samochodu, numeru PESEL, itp.);
   c) należy stosować: hasła zawierające kombinacje liter i cyfr, hasła zawierające znaki specjalne: (.,();'@, #, & itp.) o ile system informatyczny i oprogramowanie na to pozwala;
   d) Zmiany hasła nie wolno zlecać innym osobom.

§ 6

Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie.

1. Przed rozpoczęciem pracy, w trakcie rozpoczynania pracy z systemem informatycznym oraz w trakcie pracy każdy pracownik obowiązany jest do zwrócenia bacznej uwagi, czy nie wystąpiły symptomy mogące świadczyć o naruszeniu ochrony danych osobowych. Szczegółowy opis takich symptomów oraz sposób postępowania w przypadku ich wykrycia został opisany w dokumencie „Polityka bezpieczeństwa" punkt 5A.d.
2. Rozpoczęcie pracy w systemie komputerowym wymaga zalogowania się do systemu przy użyciu indywidualnego identyfikatora oraz hasła dostępu.
3. Przed opuszczeniu stanowiska pracy należy zablokować stację roboczą lub wylogować się z oprogramowania i systemu operacyjnego.
4. Przed wyłączeniem komputera należy bezwzględnie zakończyć prace uruchomionych programów, wylogować się z systemu operacyjnego i wykonać zamkniecie systemu
5. Niedopuszczalne jest wyłączanie komputera przed zamknięciem oprogramowania i systemu operacyjnego.

§ 7

Procedury tworzenia kopii zapasowych.

1. Za systematyczne przygotowanie kopii bezpieczeństwa odpowiada Administrator systemu informatycznego.
2. Kopie bezpieczeństwa mogą być wykonywane codzienne na dysku wewnętrznym, innym niż systemowy. Poprawność kopii pod względem zapisu i braku zainfekowania wirusem sprawdza raz w tygodniu Administrator systemu informatycznego.
3. Kopie bezpieczeństwa zapisywane są raz w miesiącu na płytach CD lub innych zewnętrznych nośnikach i przechowywane w zabezpieczonych szafach metalowych
4. Zachowuje się kopie bezpieczeństwa z sześciu poprzednich miesięcy.
5. Dodatkowe zabezpieczenie wszystkich programów i danych wykonywane jest raz w miesiącu w postaci zapisu na płytach CD-R.
6. W przypadku wykonywania zabezpieczeń długoterminowych na płytach CD/DVD, nośniki te należy co kwartał sprawdzać pod katem ich dalszej przydatności.

§ 8

Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz wydruków.

1. Elektroniczne nośniki informacji.
   a) Dane osobowe w postaci elektronicznej - za wyjątkiem kopii bezpieczeństwa – zapisane na płytach CD, dyskach przenośnych czy dyskach twardych nie mogą opuścić obszaru przetwarzania danych osobowych.
   b) Elektroniczne nośniki informacji są przechowywane w pokojach stanowiących obszar przetwarzania danych osobowych, określony w Polityce bezpieczeństwa przetwarzania danych osobowych, w zamkniętych szafach lub metalowych kasetach.
   c) Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a następnie uszkadza się w sposób mechaniczny.
   d) Elektroniczne nośniki informacji, zawierające dane osobowe, nie mogą zostać przekazane innemu podmiotowi nieuprawnionemu do dostępu do tych danych , nawet po uprzednim usunięciu danych z nośnika.
   e) Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej.

2. Kopie zapasowe.
   a) Kopie bezpieczeństwa są przechowywane w szafie w pokoju nr 106 budynku Ośrodka lub w Serwerowni OLU SP ZOZ w Lublinie.
   b) Dostęp do danych opisanych w punkcie 1 ma Administrator systemu informatycznego oraz upoważnieni pracownicy.
3. Wydruki.
   a) W przypadku konieczności przechowywania wydruków zawierających dane osobowe należy je przechowywać w miejscu uniemożliwiającym bezpośredni dostęp osobom niepowołanym.
   b) Pomieszczenie, w którym przechowywane są wydruki robocze musi być należycie zabezpieczone po godzinach pracy.
   c) Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

§ 9

Sposób zabezpieczenia systemu informatycznego przed wirusami i szkodliwym oprogramowaniem

a) Na każdym stanowisku komputerowym musi być zainstalowane oprogramowanie antywirusowe z włączoną ochroną antywirusową i antyspyware oraz ochroną poczty elektronicznej i zaporą sieciową.
b) Każdy e-mail wpływający na konta pocztowe OLU musi być sprawdzony pod kątem występowania wirusów przez oprogramowanie antywirusowe.
   Definicje wzorców wirusów aktualizowane są nie rzadziej niż 1 raz w tygodniu.
c) Bezwzględnie zabrania się używania nośników niewiadomego pochodzenia
d) Bezwzględnie zabrania się pobierania z sieci Internet plików niewiadomego pochodzenia.
e) Administrator Systemu Informatycznego przeprowadza cykliczne kontrole antywirusowe na wszystkich komputerach - minimum co trzy miesiące.
f) Kontrola antywirusowa przeprowadzana jest również na wybranym komputerze w przypadku zgłoszenia nieprawidłowości w funkcjonowaniu sprzętu komputerowego lub oprogramowania.
g) W przypadku wykrycia wirusów komputerowych sprawdzane jest stanowisko komputerowe na którym wirusa wykryto oraz wszystkie posiadane przez użytkownika nośniki.

§ 10

Zasady i sposób odnotowywania w systemie informacji o udostępnieniu danych osobowych.

1. Dane osobowe z eksploatowanych systemów mogą być udostępniane wyłącznie osobom uprawnionym.
2. Udostępnienie danych osobowych nie może być realizowane drogą telefoniczną.
3. Aplikacje wykorzystywane do obsługi baz danych osobowych powinny zapewniać odnotowanie informacji o udzielonych odbiorcom danych. Zakres informacji powinien obejmować co najmniej: dane odbiorcy, datę wydania, zakres udostępnionych danych.

§ 11

Procedury wykonywania przeglądów i konserwacji systemu.

1. Przeglądy i konserwacja urządzeń.

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

□Nieprawidłowości ujawnione w trakcie tych działań powinny być niezwłocznie usunięte, a ich przyczyny przeanalizowane. O fakcie ujawnienia nieprawidłowości należy zawiadomić Pełnomocnika bezpieczeństwa informacji.

2. Przegląd programów i narzędzi programowych.

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

□Administrator Systemu Informatycznego zobowiązany jest uaktywnić mechanizm zliczania nieudanych prób dostępu do systemu oraz ustawić blokadę konta użytkownika po wykryciu trzech nieudanych prób, we wszystkich systemach posiadających taką funkcję.

3. Rejestracja działań konserwacyjnych, awarii oraz napraw.

□ Pełnomocnik ds. Bezpieczeństwa Informacji prowadzi „Dziennik systemu informatycznego OLU".
Wzór i zakres informacji rejestrowanych w dzienniku określony jest w załączniku nr 5.

□Wpisów do dziennika może dokonywać Administrator Danych, Pełnomocnik ds. Bezpieczeństwa Informacji lub osoby przez nich wyznaczone.

§ 12

Połączenie do sieci Internet.

Połączenie do sieci Internet jest realizowane poprzez sieć Orange Polska S.A. z zastosowaniem zaawansowanych metod ochrony.

DYREKTOR
Ośrodka Leczenia Uzależnień
[illegible]

Inspektor
ds Pracowniczych
mgr [illegible]

Kancelaria Radcy Prawnego
Beata Kowalska
20-023 Lublin, ul. Chopina 26/7

OŚWIADCZENIE

Oświadczam, że zapoznałem się z przepisami dotyczącymi ochrony danych osobowych i zobowiązuję się do przestrzegania:

1. Ustawy z dni 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 2014 poz. 1182 – tekst jednolity).
2. Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. nr 100, poz. 1024).
3. Polityki bezpieczeństwa przetwarzania danych osobowych w Ośrodku Leczenia Uzależnień SP ZOZ w Lublinie.
4. Instrukcji zarządzania systemem informatycznym Ośrodku Leczenia Uzależnień SP ZOZ w Lublinie.

Jednocześnie w czasie wykonywania swoich obowiązków służbowych zobowiązuję się do:

1. Zapewnienia ochrony danym osobowym przetwarzanym w zbiorach Ośrodku Leczenia Uzależnień SP ZOZ w Lublinie., zabezpieczenia przed udostępnianiem osobom trzecim i nieuprawnionym, zabraniem, uszkodzeniem oraz nieuzasadnioną modyfikacją lub zniszczeniem,
2. Zachowaniem w tajemnicy, także po ustaniu stosunku pracy, wszelkich informacji dotyczących funkcjonowania systemów lub urządzeń służących do przetwarzania danych osobowych oraz haseł dostępu do tych zbiorów.

Lublin, dn. . . . . .

. . . . . .
(podpis pracownika)

....
Nr ewidencyjny miejscowość i data

Upoważnienie
do przetwarzania danych osobowych

1. Upoważniam Pana(ią)

.....

zatrudnionego(ą) na stanowisku .....

do dostępu do następujących danych osobowych:

- .....
- .....

.....

2. Identyfikator.....
w przypadku gdy dane przetwarzane są w systemie informatycznym

3. Okres trwania upoważnienia od .....do.....

Wystawił: .....
pracodawca – administrator danych (imię i nazwisko) (podpis i pieczęć)

4. Osoba upoważniona do przetwarzania danych objętych zakresem, o którym mowa w punkcie 1, jest zobowiązana do zachowania ich w tajemnicy również po ustaniu zatrudnienia oraz zachowania w tajemnicy informacji o ich zabezpieczeniu.

.....
data i podpis osoby upoważnionej

WNIOSEK O NADANIE UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM

Rodzaj zmiany w systemie informatycznym:

Nowy użytkownik ☐ Modyfikacja uprawnień ☐ Odebranie uprawnień ☐

Imię i nazwisko użytkownika:	
Opis zakresu uprawnień użytkownika w systemie informatycznym:	

Data wystawienia: .....

..... (Podpis Dyrektora OLU SP ZOZ.)

..... (Akceptacja ABI)

Załącznik nr 4
do Instrukcji Zarządzania Systemem Informatycznym
Ośrodka Leczenia Uzależnień SP ZOZ w Lublinie

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRACY W SYSTEMIE INFORMATYCZNYM ORAZ UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

L.p.	Nazwisko i Imię (identyfikator)	Data nadania upoważnienia	Data ustania uprawnień	System/aplikacja/ zbiór danych osobowych	Identyfikator w systemie informatycznym
1					
2					

DZIENNIK SYSTEMU INFORMATYCZNEGO OŚRODKA LECZENIA UZALEŻNIEŃ SP ZOZ W LUBLINIE

Dziennik zawiera opisy wszelkich zdarzeń istotnych dla działania systemu Informatycznego, a w szczególności:

- w przypadku awarii - opis awarii, przyczyna awarii, szkody wynikłe na skutek awarii, sposób usunięcia awarii, opis systemu po awarii, wnioski;
- w przypadku konserwacji systemu – opis podjętych działań, wnioski.

L.p.	Data i godzina zdarzenia	Opis zdarzenia	Podjęte działania	Podpis
1				
2				

Wykaz osób, które zostały zapoznane z „Polityką bezpieczeństwa" i „Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Ośrodku Leczenia Uzależnień SP ZOZ w Lublinie", przeznaczonych dla osób zatrudnionych przy przetwarzaniu tych danych.

Lp.	Nazwisko i imię	Stanowisko	Data	Podpis
1.				
2.				

DZIENNIK SYSTEMU INFORMATYCZNEGO OŚRODKA LECZENIA UZALEŻNIEŃ SP ZOZ W LUBLINIE

Dziennik zawiera opisy wszelkich zdarzeń istotnych dla działania systemu Informatycznego, a w szczególności:

- w przypadku awarii - opis awarii, przyczyna awarii, szkody wynikłe na skutek awarii, sposób usunięcia awarii, opis systemu po awarii, wnioski;
- w przypadku konserwacji systemu – opis podjętych działań, wnioski.

L.p.	Data i godzina zdarzenia	Opis zdarzenia	Podjęte działania	Podpis
1				
2				

Wykaz osób, które zostały zapoznane z „Polityką bezpieczeństwa" i „Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Ośrodku Leczenia Uzależnień SP ZOZ w Lublinie", przeznaczonych dla osób zatrudnionych przy przetwarzaniu tych danych.

Lp.	Nazwisko i imię	Stanowisko	Data	Podpis
1.				
2.				