**Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych**

**w ………………………………………**

**§ 1**

1. Celem Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych (dalej *„Instrukcja”*) jest ustalenie zasad zabezpieczania i bezpiecznego przetwarzania informacji zbieranych w formie elektronicznej w podmiocie leczniczym pod firmą: ………………………………………………, zwanym dalej również *„PL”*.
2. Instrukcja obowiązuje wszystkie osoby realizujące jakiekolwiek zadania w PL, niezależnie od podstawy wykonywania tych zadań w PL, zwane dalej łącznie dla celów niniejszej Instrukcji *„pracownikami”.*
3. Zakresem instrukcji objęte są działania związane z zabezpieczeniami sprzętu i oprogramowania komputerowego oraz postępowaniem personelu mającym na celu zapewnienie poufności gromadzonych danych.
4. Administrator danych odpowiada za zapewnienie stosowania odpowiednich zabezpieczeń bazy informacji zbieranych w formie elektronicznej.
5. IOD odpowiada za organizację sieci, kontrolę przestrzegania zasad opisanych w instrukcji, instalację oprogramowania, nadzorowanie sieci.
6. Obszarem przetwarzania danych osobowych są pomieszczenia PL wskazane w załączniku nr 2 do Polityki.

**§ 2**

Dane elektroniczne są zabezpieczane za pomocą pełnych kopii zapasowych. Metoda ta opiera się na kopiowaniu danych przynajmniej jeden raz w miesiącu lub przed aktualizacją programu, na pamięć przenośną. Nośnik zewnętrzny danych, zawierający kopie zapasowe, jest przechowywany poza obszarem przetwarzania, wskazanym w § 1 ust. 6.

**§ 3**

1. Wszyscy użytkownicy systemów informatycznych zarejestrowani są w „Karcie użytkowników”, stanowiącej załącznik do niniejszej Instrukcji.
2. W „Karcie użytkowników” zawarte są informacje o pracowniku, dacie uzyskania dostępu do systemów informatycznych oraz dacie pozbawienia tego dostępu. Pracownik zostaje pozbawiony dostępu do systemów informatycznych w wypadku zakończenia pracy w PL lub nieobecności w pracy przekraczającej 21 dni. Zmiany w „Karcie użytkowników” wprowadza IOD.

**§ 4**

1. Każdy pracownik zarejestrowany w „Karcie użytkowników”, aby uzyskać dostęp do systemu, posługuje się hasłem. Hasło musi składać się z 8 znaków, w tym minimum z 2 cyfr i 2 znaków specjalnych[[1]](#footnote-1).
2. Hasła zmienia każdy pracownik nie rzadziej niż co 90 dni[[2]](#footnote-2). Nowe hasło musi się różnić od poprzedniego minimum 3 znakami. Zabrania się pracownikom udostępniania haseł osobom trzecim. Zabrania się korzystania przez pracowników z haseł innych osób zatrudnionych w PL.
3. Z poziomu IOD istnieje możliwość kontroli haseł użytkowników. Hasło IOD jest każdorazowo przekazywane Administratorowi danych.
4. W zakresie bezpieczeństwa użytkowania programów komputerowych ………………… oraz …………….. obowiązują następujące zasady:
5. Dostęp do aplikacji ……………………….. mają wyłącznie użytkownicy posiadający założone konto z przypisanym hasłem – system pozwala na wymuszenie zmiany hasła po upływie określonego czasu,
6. Wszystkie działania użytkownika (dodawanie i zmiana danych pacjentów/badań) zapisywane są w historii,
7. Każdy z użytkowników ma dostęp do wybranych funkcji aplikacji, które określa poziom przyznanych mu uprawnień,
8. Do głównego serwera wystawiony jest dostęp dla serwisu, realizowany przy pomocy szyfrowanego protokołu połączenia (zabezpieczonego hasłem).

**§ 5**

1. Kopie zapasowe tworzone są[[3]](#footnote-3):
2. codziennie – na serwerze,
3. raz na tydzień/miesiąc – na nośniku zewnętrznym.
4. Przy wykonywaniu kopii na nośniku zewnętrznym, obowiązuje rotacja trzech nośników. Kopie zapasowe przekazywane są zarządowi PL, który przechowuje kopie poza PL.

**§ 6**

1. Wszystkie komputery zabezpieczone są w licencjonowane oprogramowanie antywirusowe ……………………., podlegające aktualizacji drogą Internetu. Programy antywirusowe zainstalowane są na serwerze i stacjach roboczych. Po każdej naprawie i konserwacji komputera sprzęt jest sprawdzany pod kątem występowania wirusów i konieczności ponownego zainstalowania programu antywirusowego. Elektroniczne nośniki informacji pochodzenia zewnętrznego podlegają automatycznemu sprawdzeniu programem antywirusowym przed rozpoczęciem korzystania z nich.
2. Dane uzyskiwane drogą teletransmisji podlegają sprawdzeniu przed udostępnieniem użytkownikom.

**§ 7**

Wydruki z systemu komputerowego podlegają zasadom zabezpieczania stosowanym do dokumentacji w formie papierowej.

**§ 8**

W zakresie korzystania z sieci komputerowej obowiązują następujące zasady:

1. pracownicy nie są uprawnieni do instalacji jakiegokolwiek prywatnego oprogramowania bez odpowiedniej zgody IOD. W przypadku zainstalowania takiego oprogramowania bez odpowiedniej akceptacji pracownik ponosi odpowiedzialność porządkową i prawną,
2. oprogramowanie na komputerach może być zainstalowane wyłącznie przez IOD lub innego upoważnionego pracownika PL,
3. pracownicy mogą używać połączenia z Internetem jedynie w celach służbowych, jedynie z przeznaczonych do tego celu komputerów,
4. pracownicy nie mają prawa przekazywać za pośrednictwem sieci komputerowej do stron trzecich jakichkolwiek danych stanowiących własność PL,
5. pracownicy nie mogą ściągać za pośrednictwem sieci komputerowej żadnego nielegalnego lub pirackiego oprogramowania,
6. pracownicy nie mogą podłączać się do sieci zewnętrznej za pośrednictwem modemów lub sieci wi-fi.

**§ 9**

W trakcie pracy z wykorzystaniem systemu komputerowego obowiązuje przestrzeganie następujących zasad:

1. należy w miarę możliwości, ustawiać monitor komputerowy w taki sposób, aby informacje na ekranie nie były widoczne dla osób postronnych,
2. zawsze należy stosować hasła dostępu,
3. przy opuszczaniu stanowiska pracy należy wylogować się z systemu,
4. wszelkie usterki należy zgłaszać IOD.

**§ 10**

W przypadku, gdy w ramach współpracy z innymi podmiotami, zachodzi konieczność eksportu lub importu lub udostępnienia danych osobowych przetwarzanych w systemie informatycznym PL obowiązują, udostępnienie tych danych następuje z zachowaniem następujących zasad:

1. w ramach współpracy z ……………………………… :
2. …………………………………………………………………………….
3. …………………………………………………………………………….
4. …………………………………………………………………………….
5. W zakresie zdalnego udostępnienia danych osobowych pacjentów, zgromadzonych w związku z wykonanymi badaniami, lekarzom POZ lub lekarzom specjalistom, kierującym na te badania, jak również pacjentom wykonującym badanie (zdalne udostępnienie wyników badań i opisu):
6. Dostęp do tych danych uzyskują wyłącznie lekarze, z którymi PL w tym zakresie nawiązał stosowną współpracę,
7. Dostęp do tych danych uzyskują wyłącznie pacjenci, którzy na powyższe wyrazili odrębną zgodę na taki sposób udostępnienia oraz na korzystanie w tym celu ze strony internetowej PL lub poczty elektronicznej,
8. W przypadku korzystania w tym celu ze strony internetowej PL dostęp do tych danych następuje wyłącznie w oparciu o nadany upoważnionej osobie login i hasło,
9. W zakresie zdalnego udostępnienia danych osobowych pacjentów celem dalszej konsultacji obowiązują następujące zasady postępowania: ……………………………………
10. w pozostałych przypadkach w ramach współpracy z innymi podmiotami zabezpieczenie w zakresie dostępu do określonych zasobów oraz w zakresie wzajemnej wymiany danych określają strony w postanowieniach umów lub w drodze dwustronnych uzgodnień,
11. W każdym wypadku współpracy z innymi podmiotami, zarówno w zakresie importu danych do programów ……………………………………………., jak i udostępniania danych zawartych w tych programach, obowiązuje najwyższy poziom zabezpieczenia tego dostępu.

***Załącznik do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w …………………………………………………………………………***

**Karta Użytkowników**

**systemu informatycznego służącego do przetwarzania danych osobowych w ……………………………………………………………………………..**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **L.P.** | **Data wpisu** | **Pracownik** **(imię i nazwisko)** | **Data uzyskania dostępu do systemów informatycznych**  | **Data pozbawienia dostępu do systemów informatycznych** |
| **1** |  |  |  |  |
| **2** |  |  |  |  |
| **3** |  |  |  |  |
| **4** |  |  |  |  |
| **5** |  |  |  |  |
| **6** |  |  |  |  |
| **7** |  |  |  |  |
| **8** |  |  |  |  |
| **9** |  |  |  |  |
| **10** |  |  |  |  |



1. *Można oczywiście określić inne wymogi co do hasła.* [↑](#footnote-ref-1)
2. *Można określić inną częstotliwość zmiany hasła.* [↑](#footnote-ref-2)
3. *Można ustalić inne zasady i częstotliwość wykonywania kopii zapasowych.* [↑](#footnote-ref-3)