93-005 Łódź, ul. Czerwona 3
tel. 683-17-91, fax 683-13-78
*Prezydium*
*Okręgowej Rady Lekarskiej*
*w Łodzi*

**UCHWAŁA Nr 2951/P-V/2008**
**Prezydium**
**Okręgowej Rady Lekarskiej w Łodzi**
**z dnia 10 października 2008 roku**

## w sprawie ustalenia instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Łodzi

Na podstawie art. 24 ust. 2 ustawy z dnia 17 maja 1989 roku o izbach lekarskich (Dz. U. Nr 30 poz. 158 z późniejszymi zmianami), art. 7 pkt. 4 ustawy z dnia 29 sierpnia 1997 r o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 925; zmiana: Dz. U. z 2002 r. Nr 153, poz.1271; Dz. U. z 2004 r Nr 25, poz. 219 i Nr 33, poz. 285), oraz § 3 ust.3 rozporządzenia 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), Prezydium ORL w Łodzi postanawia:

§ 1.

Ustalić „Instrukcje zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w OIL w Łodzi", stanowiącą załącznik nr 1A i nr 1B do niniejszej Uchwały.

§ 2.

Zobowiązać wszystkich pracowników OIL w Łodzi przetwarzających dane osobowe, do osobistego zapoznania się do dnia 31.10.2008 r. z instrukcją, o której mowa w § 1 i do złożenia do Dyrektora Biura OIL w Łodzi, pisemnych oświadczeń osobistych, o zapoznaniu się z tą instrukcją.

§ 3.

Zobowiązać wszystkich pracowników OIL w Łodzi przetwarzających dane osobowe do przekazania w terminie do 31.10.2008 r. Dyrektorowi Biura OIL w Łodzi, podpisanych aneksów do ich zakresu obowiązków, uprawnień i odpowiedzialności.

§ 4.

Administrator Bezpieczeństwa Informacji w oparciu w wydane decyzje – upoważnienia do przetwarzania danych osobowych, w terminie do dnia 10.11.2008 r. wykona stosowne czynności związane z nadaniem pracownikowi uprawnień do korzystania z systemu informatycznego przetwarzającego dane osobowe.

§ 5.

Wzory oświadczeń, o których mowa w § 2 i w § 3 stanowią załączniki nr 2 i nr 3 do niniejszej Uchwały.

§ 6

Zobowiązać Dyrektora Biura OIL w Łodzi do włączenia aneksów do zakresu obowiązków, uprawnień i odpowiedzialności oraz złożonych oświadczeń, o których mowa w § 2 i w § 3, do akt osobowych pracowników dopuszczonych do przetwarzania danych osobowych.

§ 7.

Upoważnić Administratora Bezpieczeństwa Informacji do wyznaczania pozostałych informatyków zatrudnionych w OIL w Łodzi, do wykonywania niektórych zadań przypisanych Administratorowi Bezpieczeństwa Informacji w instrukcji, o której mowa w § 1.

§ 9.

Wykonanie uchwały powierzam Dyrektorowi Biura OIL w Łodzi.

§ 10.

Uchwała wchodzi w życie z dniem podjęcia.

**Sekretarz**
**Okręgowej Rady Lekarskiej w Łodzi**

**lek. Marek Nadolski**

**Przewodniczący**
**Okręgowej Rady Lekarskiej w Łodzi**

**dr n med. Grzegorz Krzyżanowski**

**Załącznik Nr 1A**
do Uchwały Nr 2951/P-V/2008
Prezydium ORL w Łodzi
z dnia 10.10. 2008 r.

## Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w OIL w Łodzi

Instrukcja obejmuje zagadnienia dotyczące zapewnienia bezpieczeństwa informacji, a w szczególności elementy wymienione w §5 rozporządzenia, na które składają się:

1) **procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności,**

### § 1

Zasady nadawania uprawnień.

**1.**Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych musi zapoznać się z:

- ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101 poz. 926 z późn. zm.),
- polityką bezpieczeństwa wdrożoną w OIL w Łodzi,
- poniższą instrukcją określającą zasady przetwarzania danych w systemie informatycznym, którego jest użytkownikiem.

**2.**Podstawą do rejestracji uprawnień w systemie jest wniosek o nadanie tych uprawnień.

### § 2

Procedura nadawania uprawnień do przetwarzania danych osobowych.

Uprawnienia do korzystania z systemu informatycznego przetwarzającego dane osobowe nadawane są przez Dyrektora Biura OIL w Łodzi na wniosek pracownika, zaopiniowany przez Administratora Bezpieczeństwa Informacji:
**1.** Wniosek składany jest za pośrednictwem Administratora Bezpieczeństwa Informacji.

**2.** Dyrektor Biura bada poprawność dokumentu i w przypadku braku uwag przekazuje go ze swoją adnotacją ABI, w celu nadania uprawnień użytkownikowi, bądź podając przyczynę odmowy zatwierdzenia odsyła dokument w celu jej usunięcia.

**3.** ABI odpowiednio, zgodnie z przekazanym dokumentem:

- •rejestruje użytkownika w systemie i nadaje mu określone uprawnienia,
- •sporządza raport o zmianie uprawnień w systemie i przesyła go Dyrektorowi Biura,
- •ABI dokonuje aktualizacji ewidencji osób upoważnionych do przetwarzania danych osobowych w systemie,

**4.** Użytkownik systemu w obecności ABI uwierzytelnia się w systemie.

**5.** Użytkownik zmienia nadane mu przez ABI hasło i rozpoczyna pracę w aplikacji.

**6.** Procedurę nadania uprawnień do przetwarzania danych osobowych w systemie stosuje się odpowiednio w przypadku zmiany uprawnień w systemie albo odebrania uprawnień w systemie.

**7.** Administrator Bezpieczeństwa Informacji informuje o zakresie obowiązków i odpowiedzialności pracownika, któremu nadano uprawnienia do dostępu do systemu informatycznego przetwarzającego dane osobowe, za ochronę danych osobowych.

**8.** Zakres odpowiedzialności, o którym mowa w ust.1 w szczególności obejmuje:

- zabezpieczenie informacji poprzez nieujawnianie hasła do korzystania z systemu informatycznego oraz wprowadzanie hasła w sposób zabezpieczający je przed podejrzeniem przez inne osoby.
- blokowanie stacji roboczej, w czasie gdy pracownik przebywa poza swoim stanowiskiem pracy.
- wyłącznie aplikacji przetwarzającej dane osobowe, w czasie gdy w pomieszczeniu przebywają osoby nieuprawnione do dostępu do tych danych, a istnieje realne zagrożenie podejrzenia wyświetlanych na monitorze komputera danych.
- przestrzeganie zasad bezpieczeństwa związanych z korzystaniem z nośników przenośnych, na których zostały zapisane dane osobowe.
- przekazywanie danych osobowych wewnątrz systemu lub sieci informatycznej zgodnie z wymaganiami w zakresie ich zabezpieczenia.
- zabezpieczenie dostępu do obszaru, w którym odbywa się przetwarzanie danych osobowych poprzez zamykanie drzwi i okien oraz niedopuszczanie osób nieupoważnionych do przebywania w tym obszarze.
- zachowanie w tajemnicy danych osobowych również po ustaniu zatrudnienia.
- zachowanie w tajemnicy haseł, również po utracie ich ważności.
- zachowanie w tajemnicy informacji na temat procesów przetwarzania danych osobowych, również po ustaniu zatrudnienia.
- zachowanie w tajemnicy informacji na temat sposobów zabezpieczenia danych osobowych, również po ustaniu zatrudnienia.

9.Nadanie pracownikowi uprawnień do korzystania z systemu informatycznego przetwarzającego dane osobowe obejmuje:

- przeprowadzenie szkolenia w zakresie bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym oraz prawnych aspektów ochrony tych danych.
- poinformowanie o indywidualnym zakresie odpowiedzialności pracownika, któremu nadaje się uprawnienia do przetwarzania danych osobowych, za ochronę danych przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem oraz
- podpisanie przez pracownika aneksu do zakresu obowiązków, uprawnień odpowiedzialności i zobowiązanie się do jego przestrzegania – dokument ten sporządzany jest w 2 egzemplarzach z czego jeden egzemplarz przechowywany jest przez Dyrektora Biura OIL w Łodzi, drugi egzemplarz otrzymuje otrzymuje pracownik.
- wydanie przez Administratora Bezpieczeństwa Informacji, podpisanego przez Dyrektora Biura OIL w Łodzi, pisemnego upoważnienia pracownika do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych. Upoważnienie to określa zakres uprawnień nadawanych pracownikowi.
- przydzielenie użytkownikowi identyfikatora dostępu do aplikacji przetwarzającej dane osobowe – konto w systemie informatycznym jest wprowadzane przez Administratora Bezpieczeństwa Informacji. Identyfikator użytkownika winien mu być nadany tylko raz i nie powinien być później zmieniany.
- skonfigurowanie uprawnień użytkownika w ramach konta zgodnie z zakresem uprawnień zatwierdzonych przez Dyrektora Biura.
- wygenerowanie tymczasowego, losowego hasła dla użytkownika i przekazanie go użytkownikowi. Przy pierwszym logowaniu się do systemu użytkownik samodzielnie zmienia hasło. Za wygenerowanie hasła tymczasowego odpowiada Administrator Bezpieczeństwa Informacji, który wydaje pracownikowi hasło za pokwitowaniem zawierającym klauzulę zobowiązująca pracownika do zachowania w tajemnicy haseł do systemu informatycznego przetwarzającego dane osobowe, również po upływie okresu ich ważności.
- zaopatrzenie ekranu monitora komputerowego w wygaszacz z ustawioną opcją wymagania hasła, które po upływie maksymalnie 1 minuty nieaktywności użytkownika automatycznie wyłącza funkcje eksploatacji ekranu.
- administrator Bezpieczeństwa Informacji fakt wykonania czynności wymienionych w ust. 1 – 8 potwierdza dokonując stosownego zapisu w decyzji o udzieleniu upoważnienia do przetwarzania danych osobowych (wzór decyzji stanowi załącznik Nr 4 do Uchwały).

**2) stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem,**

1.Metody i środki uwierzytelniania:

- w systemie informatycznym stosuje się uwierzytelnianie dwustopniowe:
  - **a)** dostępu do aplikacji służącej do przetwarzania danych osobowych,
  - **b)** dostępu do systemu operacyjnego stacji roboczej i serwera danych.
- do uwierzytelniania użytkownika w systemie na obu poziomach stosuje się hasła,
- hasło dostępu do systemu operacyjnego składa się co najmniej z 6 znaków
- hasło dostępu do aplikacji składa się co najmniej:
  - **a)** z 6 znaków dla modułów, do których ma zastosowanie podstawa poziomu bezpieczeństwa,
  - **b)** z 8 znaków dla modułów, do których ma zastosowanie podwyższony poziom bezpieczeństwa,
- hasła dostępu do systemu operacyjnego i do aplikacji są różne
- hasła powinny zawierać litery, cyfry i znaki specjalne.
- hasła nie powinny być słowami ze słownika, imieniem, nazwiskiem, datą urodzenia, numerem telefonu itp.
- hasła są zmieniane przez użytkownika co najmniej raz na miesiąc oraz niezwłocznie w przypadku podejrzenia, że hasło mogło być ujawnione
- nowe hasła powinny być różne od 10 ostatnio używanych przez pracownika haseł

2. Użytkownik jest zobowiązany do:

- nieujawniania hasła innym osobom.
- zachowania hasła w tajemnicy również po wygaśnięciu jego ważności.
- niezapisywaniu hasła.
- przestrzegania zasad dotyczących jakości i częstotliwości zmian hasła.
- wprowadzania hasła do systemu informatycznego przetwarzającego dane osobowe w sposób minimalizujący ryzyko podejrzenia go.

3. W przypadku zapomnienia hasła użytkownik zwraca się do Administratora Bezpieczeństwa Informacji o wygenerowanie nowego hasła tymczasowego.

**3) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu,**

1. Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie:

- uruchomić komputer, podłączony fizycznie do sieci lokalnej i zalogować się, podając swój identyfikator i hasło dostępu,
- uruchomić aplikację do przetwarzania danych osobowych podając swój identyfikator i hasło dostępu,
- użytkownik podczas logowania do systemu nie może ujawnić hasła osobom trzecim,

- w trakcie pracy, przy każdorazowym opuszczeniu stanowiska komputerowego użytkownik musi dopilnować, aby na ekranie nie były wyświetlone dane osobowe,
- przy opuszczaniu pokoju na dłuższy czas użytkownik winien się skutecznie wylogować z systemu,
- aby skutecznie zakończyć pracę w systemie należy:
  - **a)** zamknąć aplikację,
  - **b)** zamknąć system,
  - **c)** wyłączyć monitor i drukarkę.

**4) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania,**

**1.** Dane osobowe przetwarzane w systemie informatycznym podlegają zabezpieczeniu poprzez tworzenie kopii zapasowych.

**2.** Za proces tworzenia kopii zapasowych odpowiada Administrator Bezpieczeństwa Informacji, a w szczególności określa:

- częstotliwość tworzenia kopii zapasowych wynikającą z częstotliwości wprowadzania zmian do zabezpieczanych danych,
- techniczny sposób tworzenia kopii zapasowych, w szczególności sprzęt, oprogramowanie i nośniki, których wykorzystanie uzasadnione jest wielkością danych osobowych, które podlegają zabezpieczeniu poprzez utworzenie kopii,
- rodzaj kopii zapasowych (pełne, przyrostowe, różnicowe).

**3.** W OIL w Łodzi wykonywane są kopie zapasowe następujących zbiorów:

- zawierające dane osobowe,
- zawierające inne dane wytwarzane przez pracowników OIL i przechowywane na serwerze/ serwerach

**4.** Kopie zapasowe zawierające dane osobowe tworzy się w następujący sposób:

- raz na tydzień wykonywana jest pełna kopia zapasowa wszystkich zbiorów zawierających dane osobowe. Kopie te wykonywane są na nośnikach optycznych przy pomocy programu Nero. Kopie tygodniowe przechowywane są przez okres nie krótszy niż 3 miesiące i nie dłuższy niż rok. O okresie przechowywania tych kopii decyduje Dyrektor Biura OIL.
- codziennie od poniedziałku do piątku wykonywana jest pełna kopia zapasowa wszystkich zbiorów zawierających dane osobowe na komputerze ABI. Po upływie tygodnia poprzednie dane są zamazywane nowymi danymi z bieżącego tygodnia.
- po przekroczeniu okresu przechowywania kopii zapasowych, o których mowa w pkt 1- 2 nośniki wykorzystane do ich sporządzenia są niszczone.

**5.** Dyrektor Biura OIL prowadzi ewidencję osób zatrudnionych przy przetwarzaniu danych osobowych. Wzór ewidencji określa załącznik nr 5

**6.** Załącznikami do ewidencji są:

- wniosek o nadanie, odebranie oraz zmianę uprawnień.
- decyzja – upoważnienie wydane przez Administratora Danych.
- inne dokumenty związane z procesem zarządzania uprawnieniami pracowników do dostępu do danych osobowych przetwarzanych

w systemie informatycznym.

7. Dyrektor Biura OIL jest zobowiązany do prowadzenia ewidencji na bieżąco i dołożenia wszelkich starań, aby była ona rzetelna i odzwierciedlała istniejący stan rzeczy.

**5) sposób, miejsce i okres przechowywania:**

**a) elektronicznych nośników informacji zawierających dane osobowe,**

**b) kopii zapasowych, o których mowa w pkt. 4,**

1. Nośniki danych osobowych zarówno w postaci elektronicznej, jak i papierowej winny być zabezpieczone przed dostępem osób nieupoważnionych, nieautoryzowaną modyfikacją i zniszczeniem.
2. Dane osobowe mogą być zapisywane na nośnikach przenośnych w przypadku tworzenia kopii zapasowych lub gdy istnieje konieczność przeniesienia tych danych w postaci elektronicznej, a wykorzystanie do tego celu sieci informatycznej jest nieuzasadnione, niemożliwe lub zbyt niebezpieczne.
3. Nośniki kopii zapasowych są przechowywane w pomieszczeniu innym niż to, w którym znajduje się sprzęt informatyczny przetwarzający dane osobowe.
4. Pomieszczenie, w którym przechowywane są kopie zapasowe, powinno być zabezpieczone ze względu na:
   - ochronę przed dostępem osób nieupoważnionych.
   - ochronę przed niewłaściwymi warunkami klimatycznymi (temperatura, wilgotność).
   - ochronę przed zalaniem (np. na skutek awarii sieci wodociągowej).
5. Nośniki kopii zapasowych powinny być przechowywane w zamykanej na klucz szafie.
6. Przy przenoszeniu nośników kopii zapasowych z miejsca ich tworzenia do miejsca przechowywania należy zabezpieczyć je przed kradzieżą, zagubieniem lub zniszczeniem.
7. Dane osobowe przechowywane na nośnikach przenośnych, jeżeli nie są dłużej potrzebne, podlegają procesowi bezpiecznego niszczenia.
8. Jeżeli charakter nośnika nie pozwala na usunięcie z niego danych, nośnik podlega trwałemu zniszczeniu.
9. Trwałe zniszczenie danych lub nośnika odbywa się na zlecenie osoby, na której wniosek nośnik zapisano, lub na zlecenie Administratora Bezpieczeństwa Informacji.
10. Zapisanie danych osobowych na nośniku przenośnym może nastąpić tylko w sytuacji, gdy operacja taka jest uzasadniona, w szczególności ze względu na:
    - tworzenie kopii zapasowych danych osobowych przetwarzanych w systemie informatycznym.
    - przenoszenie danych osobowych, jeżeli przesyłanie ich z wykorzystaniem sieci informatycznych jest zbyt niebezpieczne, niemożliwe lub zbyt skomplikowane ze względów technicznych lub organizacyjnych.
11. Nośnik przenośny może być wykorzystany do przenoszenia danych osobowych pod warunkiem zabezpieczenia go przed kradzieżą lub utratą.
12. Nośnik może być przekazywany tylko pomiędzy osobami upoważnionymi do

przetwarzania danych osobowych.

13. Nośnik podlega szyfrowaniu gdy jest używany do przenoszenia danych osobowych poza terenem OIL w Łodzi.
14. Administrator Bezpieczeństwa Informacji zapewni odpowiednie mechanizmy techniczne pozwalające na właściwe zabezpieczenie nośników przenośnych.
15. Nośnik przenośny może znajdować się poza terenem OIL w Łodzi w sytuacji gdy:
    - jest to kopia zapasowa, którą zgodnie z obowiązującymi przepisami przechowuje się poza terenem OIL w Łodzi.
    - został on przekazany innemu podmiotowi, któremu Administrator Danych, był obowiązany lub uprawniony przekazać dane osobowe.

**6) sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia,**

1. Sposoby zabezpieczenia w ramach oprogramowania systemu:

    - dane osobowe w systemie zabezpiecza się przez wykonywanie kopii zapasowych zarówno zbiorów danych osobowych, jak i programów służących do przetwarzania danych,
    - serwery, na których przechowywane są dane osobowe są zabezpieczone programami antywirusowymi,
    - wszystkie stacje robocze służące do przetwarzania danych osobowych chronione będą przed działaniem wirusów komputerowych aktualnym oprogramowaniem antywirusowym,
    - na stacjach roboczych przetwarzających dane osobowe wszystkie nowe pliki oraz poczta elektroniczna będą skanowane automatycznie. Ponadto raz w tygodniu automatycznie skanowane będą wszystkie dane zawarte na w/w komputerach,
    - w przypadku wykrycia jakiegokolwiek zagrożenia użytkownik niezwłocznie zawiadomi o tym fakcie ABI,
    - w przypadku wystąpienia infekcji i braku możliwości automatycznego usuwania wirusów przez system antywirusowy, Administrator Bezpieczeństwa Informacji winien podjąć działania zmierzające do usunięcia zagrożenia.

**7) sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4 rozporządzenia,**

1. System informatyczny przetwarzający dane osobowe musi posiadać mechanizmy pozwalające na odnotowanie faktu wykonania operacji na danych.

2. Zapis działań użytkowników uwzględnia:
    - identyfikator użytkownika.
    - datę i czas, w jakim zdarzenie miało miejsce.
    - identyfikator stacji roboczej, z której korzysta użytkownik.
    - rodzaj zdarzenia.
    - określenie informacji, których zdarzenie dotyczy – w zależności od możliwości technicznych określenie to może obejmować zbiór danych,

rekordy, które użytkownik przetwarzał lub poszczególne atrybuty w rekordach, które użytkownik przetwarzał.

3. Administrator Bezpieczeństwa Informacji jest odpowiedzialny za okresowe przeprowadzanie analizy zapisu operacji i zdarzeń w celu:
   - wykrycia potencjalnych naruszeń bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym.
   - weryfikacji zgodności sposobu wykorzystania przez użytkowników systemu informatycznego przetwarzającego dane osobowe z określonymi, w procesie nadawania uprawnień do korzystania z tego systemu, celami.
   - wykrycia potencjalnych niesprawności w funkcjonowaniu systemu informatycznego.
   - optymalizacji działania systemu informatycznego przetwarzającego dane osobowe.
   - wykrycia potencjalnych podatności na zagrożenia związane z przetwarzaniem danych osobowych oraz podjęcia działań w celu wzmocnienia mechanizmów zabezpieczających.

**8) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.**

1. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych:
   - przeglądów oraz konserwacji systemu dokonywać będzie ABI lub osoba prze niego upoważniona,
   - w przypadku, gdy zachodzi konieczność naprawy sprzętu poza siedzibą Firmy, ABI lub osoba przez niego upoważniona usuwa wszelkie dane osobowe z nośników informacji.
   - urządzenia, dyski lub inne nośniki zawierające dane osobowe przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych lub uszkadza w sposób uniemożliwiający ich odczytanie.
   - wydruki z danymi osobowymi przeznaczone do likwidacji należy likwidować przy pomocy niszczarki dokumentów w sposób uniemożliwiający ich odczytanie.
   - urządzenia i dyski, zawierające dane osobowe likwiduje się pod nadzorem osoby upoważnionej przez Administratora Bezpieczeństwa Informacji.
   - Trwałego zniszczenia zbędnych nośników i wydruków komputerowych dokonuje użytkownik upoważniony do przetwarzania danych osobowych na bieżąco w czasie pracy, nie później jednak niż przed opuszczeniem stanowiska pracy.
   - Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymania danych osobowych, pozbawia się wcześniej zapisu tych danych.

**Załącznik Nr 1 B**
do Uchwały
Nr 2951/P-V/2008
Prezydium Okręgowej
Rady Lekarskiej w Łodzi
z 10.10.2008 roku.

**Instrukcja określająca sposób zarządzania systemem informatycznym Kadry i Płace firmy Wonlok Sp. z o.o. w Łodzi.**

Niniejszą instrukcję wprowadza się w oparciu o wymogi bezpieczeństwa informacji określone w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004 roku 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).

§ 1

System, na którym pracują użytkownicy jest systemem operacyjnym NOVELL.

§ 2

Zasady przyznawania użytkownikowi identyfikatora w systemie informatycznym.

1. Użytkownikowi przyznany zostanie identyfikator wraz z poufnym hasłem.
2. O przyznaniu identyfikatora decydować będzie administrator danych.
3. Identyfikator wraz z prawidłowym hasłem umożliwiać będzie użytkownikowi dostęp do systemu.
4. Każdy z użytkowników przed dopuszczeniem do systemu podpisze umowę o zachowanie poufności, zapozna się z niniejszą instrukcją oraz zostanie pouczony o wdrożonych procedurach bezpieczeństwa.
5. Administratorowi przysługuje prawo do zablokowania konta użytkownika w każdym czasie.
6. Po zakończeniu operacji w systemie użytkownik obowiązany jest wylogować się z systemu.
7. W przypadku awarii, zagubienia hasła lub innych nieprzewidzianych sytuacji zagrażających bezpieczeństwu danych każdy z użytkowników obowiązany jest niezwłocznie powiadomić administratora danych lub administratora bezpieczeństwa informacji.

§ 3

Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem

1. Każdy z użytkowników odbędzie szkolenie dotyczące zasad bezpieczeństwa oraz postępowania w sytuacjach awaryjnych.
2. Użytkownik określi indywidualne hasło dostępu do systemu.

3. Użytkownik obowiązany będzie zapamiętać hasło, o którym mowa powyżej.
4. Hasło składać się będzie z ciągu, co najmniej 6 znaków.
5. Hasła użytkownika będą przechowywane w systemie w postaci zaszyfrowanej.
6. Hasła będą zmieniane nie rzadziej, niż co 30 dni.

§ 4

Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu.

1. W celu uruchomienia systemu informatycznego użytkownik powinien:
- uruchomić komputer,
- wybrać odpowiednią opcję umożliwiającą logowanie do systemu,
- zalogować się do systemu przez wskazanie loginu i aktualnego hasła.

2. Użytkownik podczas logowania do systemu nie może ujawnić hasła osobom trzecim, w tym innym administratorom oraz pozostawiać zapisanego hasła w pobliżu systemu i innych pracowników.

3. Użytkownik zobligowany jest do skutecznego wylogowania się z systemu za każdym razem, gdy zamierza opuścić stanowisko pracy, niezależnie od tego, na jak długo ma zamiar odejść od komputera.

4. Wylogowanie następuje przez wybranie w systemie opcji wyloguj lub zablokowanie ekranu w sposób, który uniemożliwia odblokowanie bez znajomości hasła.

5. W przypadku stwierdzenia fizycznej ingerencji w systemie lub innych podejrzeń dotyczących możliwości naruszenia bezpieczeństwa systemu użytkownik niezwłocznie zawiadomi o tym fakcie administratora bezpieczeństwa informacji.

§ 5

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

1. System chroniony będzie przed działaniem wirusów komputerowych aktualnym oprogramowaniem antywirusowym.
2. W celu przeciwdziałania wirusom i atakom zainfekowanych plików system będzie skanowany przez administratora bezpieczeństwa informacji co 48 godzin.
3. W przypadku wykrycia jakiegokolwiek zagrożenia użytkownik niezwłocznie zawiadomi administratora danych lub administratora bezpieczeństwa informacji.
4. Dane osobowe w systemie zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych.
5. Kopie zapasowe:

a) przechowuje się w miejscu zabezpieczającym je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem,
b) usuwa się niezwłocznie po ustaniu ich użyteczności.

§ 6

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

1. Przeglądów oraz konserwacji systemu dokonywać będzie administrator bezpieczeństwa informacji.
2. W przypadku przekazania elementów systemu celem naprawy innym podmiotom wszelkie dane osobowe zostaną usunięte przez administratora danych.

§ 7

1. Administratorem danych będzie Pan Grzegorz Krzyżanowski
2. Administratorem bezpieczeństwa będzie Pan Bartłomiej Nowak.

§ 8

Tekst instrukcji zostanie udostępniony użytkownikom w taki sposób, aby mogli się z nimi zapoznać i wdrożyć w życie jej postanowienia.

Załączniki:

Ewidencja osób upoważnionych do przetwarzania danych osobowych.

**Administrator bezpieczeństwa danych** **Administrator danych**

**podpis** **podpis**

**Załącznik Nr 2**
do Uchwały Nr 2951/P-V/2008
Prezydium ORL w Łodzi
z dnia 10.10. 2008 r.

Łódź .....

.....
imię i nazwisko pracownika

.....
komórka organizacyjna

.....
stanowisko

# OŚWIADCZENIE

Niniejszym oświadczam, że zapoznałem się z treścią Uchwały Prezydium ORL w Łodzi z dnia ..... roku w sprawie ustalenia instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w OIL w Łodzi.

.....
podpis pracownika

**Załącznik Nr 3**
do Uchwały Nr 2951/P-V/2008
Prezydium ORL w Łodzi
z dnia 10.10. 2008 r.

# ANEKS DO ZAKRESU OBOWIĄZKÓW, UPRAWNIEŃ I ODPOWIEDZIALNOŚCI PRACOWNIKA .....
## OIL w Łodzi

**Nazwa stanowiska** - .....

**Obsada stanowiska** - .....

**Tytuł służbowy** - .....

W związku z dopuszczeniem Pana/Pani do przetwarzania danych osobowych w OIL w Łodzi, działając na podstawie art. 37 i art. 39 ustawy z dnia 29 sierpnia 1997 r o ochronie danych osobowych (Dz. U. z 2002 r. Nr 153, poz.1271; zmiana: Dz. U. z 2004 r Nr 25, poz. 219 i Nr 33, poz. 285), uzupełniam Pana/ Pani zakres obowiązków, uprawnień i odpowiedzialności w sposób następujący:

## I. ZAKRES OBOWIĄZKÓW

Do zakresu obowiązków związanych z przetwarzaniem danych osobowych należy w szczególności:

1. Przestrzeganie przepisów ustawy z dnia 29 sierpnia 1997 r o ochronie danych osobowych i wydanych na jej podstawie przepisów wykonawczych.
2. Przestrzeganie zasad określonych w uchwałach Prezydium ORL w Łodzi a dotyczących ochrony danych osobowych, polityki bezpieczeństwa, przetwarzania danych osobowych w systemach informatycznych oraz zasad korzystania z oprogramowania komputerowego w OIL w Łodzi.
3. Zapoznawanie się na bieżąco z przepisami dotyczącymi ochrony danych osobowych, a w szczególności z przesyłanymi pisemnymi poleceniami Administratora Bezpieczeństwa Informacji OIL w Łodzi oraz„Materiałami Informacyjnymi" i „Odpowiedziami na pytania" sporządzanymi przez Biuro Generalnego Inspektora Ochrony Danych Osobowych zamieszczanymi na stronie internetowej www.giodo.gov.pl
4. Udzielanie na piśmie informacji osobom, od których zbierane są dane osobowe, stosownie do postanowień art. 24 ustawy z dnia 29 sierpnia 1997 r o ochronie danych osobowych.
5. W przypadku zbierania danych osobowych nie od osoby, której one dotyczą, udzielanie tej osobie informacji na piśmie, stosownie do postanowień art. 25 ustawy z dnia 29 sierpnia 1997 r o ochronie danych osobowych.
6. Prawidłowe zabezpieczanie danych osobowych w przypadku opuszczania stanowiska pracy w czasie godzin pracy oraz po zakończeniu pracy.

7. Prawidłowe zabezpieczanie przydzielonych haseł i identyfikatorów przed dostępem innych pracowników lub osób i podmiotów do tego nieuprawnionych.
8. Udostępnianie danych osobowych wyłącznie osobom i podmiotom do tego uprawnionym.
9. Sygnalizowanie na bieżąco Administratorowi Bezpieczeństwa Informacji występujących nieprawidłowości przy przetwarzaniu danych osobowych oraz ich prawidłowym zabezpieczeniu.
10. Natychmiastowe informowanie Administratora Bezpieczeństwa Informacji lub innej osoby wskazanej przez niego, w przypadku zauważenia zdarzenia mogącego być przyczyną naruszenia ochrony danych osobowych lub mogącego spowodować naruszenie danych osobowych.

## II. ZAKRES ODPOWIEDZIALNOŚCI

W związku z przetwarzaniem danych osobowych pracownik ponosi w szczególności odpowiedzialność za:

1. Zabezpieczenie dostępu do informacji poprzez nieujawnianie hasła do korzystania z systemu informatycznego oraz wprowadzanie hasła w sposób zabezpieczający je przed podejrzeniem przez inne osoby.
2. Blokowanie stacji roboczej, w czasie gdy pracownik przebywa poza swoim stanowiskiem pracy.
3. Wyłącznie aplikacji przetwarzającej dane osobowe, w czasie gdy w pomieszczeniu przebywają osoby nieuprawnione do dostępu do tych danych, a istnieje realne zagrożenie podejrzenia wyświetlanych na monitorze komputera danych.
4. Przestrzeganie zasad bezpieczeństwa związanych z korzystaniem z nośników przenośnych, na których zostały zapisane dane osobowe.
5. Przekazywanie danych osobowych wewnątrz systemu lub sieci informatycznej zgodnie z wymaganiami w zakresie ich zabezpieczenia.
6. Zabezpieczenie dostępu do obszaru, w którym odbywa się przetwarzanie danych osobowych poprzez zamykanie drzwi i okien oraz niedopuszczanie osób nieupoważnionych do przebywania w tym obszarze.
7. Zachowanie w tajemnicy danych osobowych również po ustaniu zatrudnienia.
8. Zachowanie w tajemnicy haseł, również po utracie ich ważności.
9. Zachowanie w tajemnicy informacji na temat procesów przetwarzania danych osobowych, również po ustaniu zatrudnienia.
10. Zachowanie w tajemnicy informacji na temat sposobów zabezpieczenia danych osobowych, również po ustaniu zatrudnienia.

.....
podpis Administratora Bezpieczeństwa Informacji

.....
podpis pracownika

.....
podpis bezpośredniego przełożonego

Łódź, dnia.....

**Załącznik Nr 4**
do Uchwały Nr 2951/P-V/2008
Prezydium ORL w Łodzi
z dnia 10.10. 2008 r.

# Wniosek o nadanie (modyfikację, odebranie) uprawnień jednostkowych w systemie informatycznym FINN

| ☐ Nowy użytkownik | ☐ Modyfikacja uprawnień | ☐ Odebranie uprawnień |
|---|---|---|

| Imię i nazwisko użytkownika | Komórka organizacyjna / pokój |
|---|---|
| | |
| Opis zakresu uprawnień użytkownika w systemie informatycznym | |
| | |

| Data wystawienia | Podpis ABI i data | Podpis Dyrektora OIL i data |
|---|---|---|
| | | |

**Załącznik Nr 5**
do Uchwały Nr 2951/P-V/2008
Prezydium ORL w Łodzi
z dnia 10.10. 2008 r.

**DECYZJA – UPOWAŻNIENIE Nr ..... / .....**
**DO PRZETWARZANIA DANYCH OSOBOWYCH**

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r o ochronie danych osobowych (Dz. U. z 2002 r Nr 101, poz. 926 z póź. zm.), po zapoznaniu się z opinią Administratora Bezpieczeństwa Informacji z dnia .....,

**Upoważniam**

**Pana / Panią .....**

**zatrudnionego / zatrudnioną na stanowisku .....**

**w .....**

do przetwarzania danych osobowych i obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład służących do przetwarzania danych osobowych.
Upoważnienie niniejsze obejmuje następujący zakres:
.....
.....
.....
.....
.....
.....
.....
.....
.....

Niniejsze upoważnienie wydaje się na czas nieoznaczony.

.....
pieczątka i podpis Dyrektora OIL w Łodzi

## CZĘŚĆ II

## ZAPISY ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI DOTYCZĄCE WYKONANIA OKREŚLONYCH CZYNNOŚCI

W dniu ..... wykonałem czynności przewidziane w § 8 ust. 1 – 8 Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w OIL w Łodzi

Łódź .....

podpis Administratora Bezpieczeństwa Informacji

## CZĘŚĆ III

## ZAPISY ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI DOTYCZĄCE REALIZACJI UDZIELONEGO UPOWAŻNIENIA

( np. zmiana zakresu upoważnienia , naruszenie ochrony danych osobowych, cofnięcie uprawnień, dodatkowe przeszkolenie, z podaniem odpowiednich dat i terminów itp).

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

Łódź, dnia .....

podpis Administratora Bezpieczeństwa Informacji

**Załącznik Nr 6**
do Uchwały Nr 2951/P-V/2008
Prezydium ORL w Łodzi
z dnia 10.10. 2008 r.

# EWIDENCJA OSÓB ZATRUDNIONYCH PRZY PRZETWARZANIU DANYCH OSOBOWYCH
## W SYSTEMACH INFORMATYCZNYCH

| Lp. | Nazwa bazy danych (1) | Nazwisko i imię użytkownika | Nazwa identyfikatora | Rodzaj uprawnień (2) | Data zarejestrowania | Data wyrejestrowania | Lokalizacja | Uwagi |
|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |