Załącznik nr 3 do Zarządzenia nr 41/2015 Rektora
Warszawskiego Uniwersytetu Medycznego
z dnia 28 maja 2015 r.

INSTRUKCJA

zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Instrukcja została opracowana zgodnie z rozporządzeniem 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).

Rozdział I
Postanowienia ogólne.

§ 1.

1. Instrukcja, obejmuje swoim zakresem wszystkie osoby biorące udział w procesie przetwarzania danych osobowych w Warszawskim Uniwersytecie Medycznym (WUM), w szczególności zaś osoby pełniące funkcje:
   1) ABI;
   2) LADO;
   3) ASI;
   4) bezpośrednich przełożonych osób przetwarzających dane osobowe;
   5) inne osoby wskazane przez Administratora.
2. Instrukcja ma zastosowanie także, do podmiotów zewnętrznych i osób fizycznych, które współpracują z WUM i na podstawie przepisów współuczestniczą w procesie przetwarzania danych osobowych, a w szczególności:
   1) podmiotów, którym na podstawie przepisów prawa udostępniono dane osobowe;
   2) podmiotów, którym na podstawie umowy powierzono lub udostępniono dane osobowe do przetwarzania;
   3) przedsiębiorców świadczący usługi związane z konserwacją systemu informatycznego;
   4) innych osób, niebędących pracownikami Uczelni, wykonujących czynności na podstawie umów cywilnoprawnych.

Rozdział II
Procedury nadawania uprawnień do przetwarzania danych osobowych i rejestrowania tych uprawnień w systemach informatycznych.

§ 2

Do przetwarzania danych osobowych w systemach informatycznych mogą mieć dostęp wyłącznie osoby posiadające upoważnienie nadane przez Administratora.

§ 3

1. Użytkownika w systemie rejestruje ASI na wniosek przełożonego po nadaniu użytkownikowi przez Administratora upoważnienia do przetwarzania danych.
2. Uprawnienia użytkownika do pracy w systemie informatycznym, w którym przetwarzane są dane osobowe, mogą obejmować w swym zakresie dostęp do baz danych w swojej jednostce organizacyjnej oraz:
   1) odczyt danych;
   2) wprowadzanie nowych danych;
   3) modyfikację istniejących danych;
   4) wydruk danych;
   5) usuwanie danych ze zbiorów swojej jednostki organizacyjnej;
   6) przekazywanie danych wewnątrz jednostki organizacyjnej.
3. Uprawnienia użytkownika uprzywilejowanego do pracy w systemie informatycznym, zastosowanym do przetwarzania danych osobowych, mogą obejmować uprawnienia, o których mowa w ust. 2 oraz:
   1) dostęp do baz danych innych jednostek organizacyjnych;
   2) udostępnianie danych podmiotom i osobom, o których mowa w § 1 ust. 2;
   3) użytkowanie komputera przenośnego.

4. Administrator może cofnąć, ograniczyć lub nie wyrazić zgody na przyznanie określonych uprawnień użytkownikom, którzy powodują incydenty mające negatywny wpływ na bezpieczeństwo przetwarzania danych w systemach.
5. ABI jest zobowiązany zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.

§ 4

1. ASI wyrejestrowują lub ograniczają uprawnienia użytkownika w przypadkach, o których mowa w § 3 ust. 4 oraz na wniosek przełożonego użytkownika po zmianie lub utracie upoważnienia dostępu do danych, które może nastąpić w przypadku:
   1) ustania zatrudnienia użytkownika w WUM;
   2) zmiany zakresu obowiązków służbowych użytkownika;
   3) oddelegowania lub przeniesienia pracownika do innej jednostki organizacyjnej.
2. Informacje dotyczące zaistnienia okoliczności, o których mowa w ust. 1. kierownik jednostki przekazuje do Działu Personalnego.

Rozdział III
Metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem.

§ 5

1. System, w którym przetwarza się dane osobowe wyposażony jest w mechanizmy uwierzytelnienia użytkownika oraz kontroli dostępu osób. Jednym z elementów umożliwiających dostęp do systemu jest hasło, które pełni rolę weryfikatora tożsamości użytkownika.
2. Hasło dostępu składa się z ciągu znaków literowych, cyfrowych lub innych i nie może kojarzyć się bezpośrednio z użytkownikiem. Hasła dostępu nie mogą powtarzać się w danym roku.
3. Hasło dostępu wyświetlane jest na ekranie monitora w formie niejawnej i znane jest tylko użytkownikowi.
4. W przypadku gdy hasła dostępu używa się do uwierzytelnienia użytkowników w systemie, powinno ono składać się z:
   1) co najmniej 6 znaków - przy podstawowym poziomie bezpieczeństwa;
   2) co najmniej 8 znaków - przy podwyższonym i wysokim poziomie bezpieczeństwa.
5. W systemach informatycznych, w których hasła użytkowników nie są zmieniane cyklicznie przez ASI, użytkownik ma obowiązek zmieniać swoje hasło, co najmniej raz w miesiącu.
6. W wypadku podejrzenia lub stwierdzenia ujawnienia hasła użytkownik ma obowiązek niezwłocznie je zmienić.
7. Hasła dostępu do baz danych są różne od haseł uwierzytelniających użytkowników w systemie z wyjątkiem systemów informatycznych, gdzie stosowana jest tzw. autoryzacja domenowa użytkownika. W tym przypadku uwierzytelnienie użytkowników w systemie jest równoznaczne z dostępem do baz danych.

§ 6

1. Identyfikator przyznaje się użytkownikom w przypadku dostępu do systemu informatycznego więcej niż jednej osoby.
2. Identyfikator użytkownika składa się z ciągu znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujących w systemie osobę upoważnioną do przetwarzania danych osobowych.
3. Identyfikator użytkownikowi przyznaje ASI, o czym informuje ABI.
4. Podczas przetwarzania danych osobowych w systemie posługiwanie się identyfikatorem innej osoby jest zabronione.

§ 7

1. Użytkownik ponosi odpowiedzialność za czynności wykonywane w systemie przy użyciu jego identyfikatora i hasła.
2. Hasło nie może być przechowywane w taki sposób, aby mogły się z nim zapoznać osoby nieuprawnione w szczególności nie może ono zostać nigdzie zapisane w postaci jawnej.
3. Administrator dopuszcza możliwość stosowania do weryfikacji tożsamości użytkowników w systemie innych sposobów np.: karty mikroprocesorowe lub metody biometryczne.
4. Osobami odpowiedzialnymi za prawidłowe funkcjonowanie w systemie mechanizmów uwierzytelniających są ASI.

Rozdział IV
Procedury rozpoczęcia, zawieszenia i zakończenia pracy przez użytkowników systemów.

§ 8

1. Użytkownicy rozpoczynający pracę zobowiązani są do przestrzegania procedur mających na celu sprawdzenie działania systemu, a w szczególności:
   1) sprawdzenie ogólnego stanu sprzętu i miejsca przechowywania nośników zawierających dane osobowe;
   2) po włączeniu urządzeń - ocenienie jakości ich pracy.
2. Użytkownik przystępując do przetwarzania danych powinien zalogować się w systemie zgodnie z poleceniami wyświetlanymi na ekranie monitora, posługując się swoim identyfikatorem i hasłem - wiedząc, że:
   1) maksymalna liczba prób wprowadzenia hasła do systemu wynosi 3;
   2) po przekroczeniu liczby prób logowania zablokowany zostaje dostęp do systemu na poziomie użytkownika;
   3) użytkownik zobowiązany jest poinformować o zdarzeniu ASI, który podejmuje stosowne w tym zakresie działania.
3. Przetwarzając dane osobowe w systemie użytkownik zobowiązany jest do wykonywania czynności mających na celu zapewnienie im bezpieczeństwa poprzez:
   1) ustawienie monitorów w sposób uniemożliwiający osobom nieupoważnionym podgląd ekranów;
   2) stosowanie urządzeń zabezpieczających przed utratą danych, spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej;
   3) automatyczne zablokowanie komputera w przypadku, kiedy przerwa w pracy użytkownika w systemie trwa dłużej niż 15 minut, ponowne logowanie jest zabezpieczone hasłem, znanym tylko użytkownikowi;
   4) wylogowanie się z systemu, kiedy przerwa w pracy użytkownika w systemie trwa dłużej niż 30 minut,
4. Po zakończeniu pracy w systemie użytkownik zobowiązany jest:
   1) zapisać wszelkie zmiany w opracowywanych dokumentach;
   2) zamknąć wszystkie używane programy;
   3) zamknąć system przez polecenie „Zamknij system" i zaczekać na jego wyłączenie;
   4) sprawdzić, czy elektroniczne nośniki informacji zawierające dane osobowe nie zostały pozostawione bez nadzoru.

Rozdział V
Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.

§ 9

1. W celu zapewnienia bezpieczeństwa przetwarzania danych osobowych istnieje obowiązek tworzenia kopii zapasowych.
2. Kopie zapasowe tworzy się według potrzeb, na odpowiedniej jakości nośnikach informacji:
   1) w kopii dziennej – metodę przyrostową;
   2) w kopii tygodniowej – metodę całościową;
   3) w kopii miesięcznej – metodę całościową.
3. Kopie zapasowe tworzy się wykorzystując narzędzia programowe i urządzenia systemu do tego przystosowane. Kopie zapasowe wykonują ASI.

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

§ 10

1. Elektroniczne nośniki informacji zawierające dane oraz wydruki przechowuje się wewnątrz obszaru przetwarzania danych, w meblach posiadających sprawne zamknięcia. Nośniki i wydruki nie powinny być wynoszone poza obszar przetwarzania danych bez zgody przełożonego.
2. Kopie zapasowe przechowuje się w szafach metalowych w pomieszczeniach, które zapewniają właściwą ochronę przed nieuprawnionym dostępem, modyfikacją, uszkodzeniem lub zniszczeniem.
3. Czas przechowywania kopii zapasowych zależy od aktualności zapisanych danych oraz potrzeby tworzenia kolejnych kopii.

§ 11

1. Kopie zapasowe i elektroniczne nośniki informacji, które zostały uszkodzone lub przeznaczone do likwidacji należy niszczyć mechanicznie pod nadzorem ASI, w sposób uniemożliwiający ich ponowne użycie.
2. Niepotrzebne wydruki z systemu, które zawierają dane osobowe należy niszczyć w niszczarkach w sposób uniemożliwiający ich odtworzenie.

§ 12

1. Przekazanie i niszczenie elektronicznych nośników informacji zawierających dane osobowe, odbywa się na podstawie protokółu sporządzanego i podpisanego przez ASI oraz wskazanych użytkowników.
2. Kopię protokołu zatwierdzonego przez przełożonego użytkownika należy przesłać do ABI.

§ 13

1. Na czas trwania transportu nośniki, kopie i wydruki, o których mowa w § 10 ust. 1 i 2, umieszcza się w trwałych opakowaniach i chroni przed utratą, zniszczeniem lub uszkodzeniem. Przenosić lub przewozić mogą je tylko osoby do tego upoważnione.
2. Urządzenia, elektroniczne nośniki informacji i wydruki z systemu zawierające dane wrażliwe, przekazywane poza obszar ich przetwarzania zabezpiecza się w sposób zapewniający poufność, integralność i rozliczalność tych danych.
3. Osoby użytkujące komputery przenośne, które są wykorzystywane do przetwarzania danych osobowych, zobowiązane są do stosowania właściwych zabezpieczeń technicznych i ochrony

kryptograficznej oraz zachowania szczególnej ostrożności podczas ich transportu i przechowywania.

Rozdział VII
Sposób zabezpieczenia systemu informatycznego przed działalnością wirusów komputerowych, nieuprawnionym dostępem oraz awarią zasilania.

§ 14

1. System, w którym przetwarzane są dane osobowe jest wyposażony w mechanizmy ochrony antywirusowej.
2. Obszarami systemu narażonymi na ingerencję wirusów oraz innego szkodliwego oprogramowania są dyski twarde urządzeń i pamięć RAM oraz elektroniczne nośniki informacji.
3. Drogą przedostania się wirusów lub szkodliwego oprogramowania może być sieć publiczna, wewnętrzna sieć teleinformatyczna lub elektroniczne nośniki informacji.
4. Kontrola antywirusowa obejmuje urządzenia oraz wszelkiego rodzaju nośniki służące do przetwarzania danych.
5. Obowiązkiem ASI jest zarządzanie bazą antywirusową, w tym określanie warunków działania oprogramowania przy zachowaniu maksymalnej efektywności i minimalizacji jej negatywnego wpływu na korzystanie przez użytkowników z systemu, a w szczególności:
   1) instalowanie i konfigurowanie modułów bazy antywirusowej;
   2) uaktualnianie sygnatur w bazie antywirusowej;
   3) dostosowywanie czasu pracy urządzeń systemu do określonego przez Administratora czasu pracy użytkowników.

§ 15

1. System posiada zabezpieczenia przed działaniem oprogramowania mającego na celu uzyskanie nieuprawnionego dostępu do danych.
2. ASI mają obowiązek realizacji przedsięwzięć mających na celu wdrażanie technicznych i logicznych zabezpieczeń chroniących system przed nieuprawnionym dostępem do danych.
3. Nadzór nad czynnościami, o których mowa w ust. 2, sprawuje Kierownik Działu Informatyki.

§ 16

1. System, w którym przetwarzane są dane osobowe posiada mechanizmy pozwalające zabezpieczyć je przed utratą lub nieautoryzowaną zmianą spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.
2. Dane osobowe przetwarzane w systemie chroni się stosując filtry zabezpieczające przed skutkami spadku napięcia oraz urządzenia podtrzymujące zasilanie do momentu poprawnego zapisania danych i wylogowania się użytkownika z systemu.
3. Dane osobowe przetwarzane w bazach umieszczonych na serwerach zabezpiecza się przed zanikiem napięcia wykorzystując centralne UPS.

§ 17

1. Administrator lub ABI na wniosek kierownika Działu Informatyki lub ASI może wprowadzić alternatywne metody ochrony przed szkodliwym działaniem programów mających na celu uzyskanie nieuprawnionego dostępu do danych.
2. Do alternatywnych metod ochrony zalicza się:
   1) odłączenie systemu od sieci publicznej oraz urządzeń umożliwiających odczyt danych z elektronicznych nośników informacji na określonych stanowiskach komputerowych;
   2) tworzenie indywidualnych stanowisk komputerowych, które spełniają wymogi bezpieczeństwa przetwarzania danych osobowych na poziomie wysokim;
   3) zastosowanie w urządzeniach kart PCI (RecoveryCard), itp.

Rozdział VIII
Sposoby realizacji wymogów dotyczących przetwarzania danych w systemie.

§ 18

1. Osobom, których dane są przetwarzane w systemie, ASI udostępnia informacje dotyczące:
   1) daty pierwszego wprowadzenia danych do systemów;
   2) identyfikatora użytkownika wprowadzającego dane osobowe do systemu chyba, że dostęp do systemu posiada tylko jedna osoba;
   3) źródła danych, w przypadku zbierania danych nie od osoby, której one dotyczą;
   4) informacji o odbiorcach, którym dane osobowe zostały udostępnione (data i zakres udostępnienia) chyba, że system używany jest do przetwarzania danych w zbiorach jawnych.
2. Odnotowywanie w systemie informacji, o których mowa w ust. 1 pkt. 1-2 następuje automatycznie, po zatwierdzeniu przez użytkownika operacji wprowadzania danych.
3. System zapewnia każdej osobie, której dane są przetwarzane, wydrukowanie raportu zawierającego w zrozumiałej formie informacje, o których mowa w ust. 1.
4. Dane osobowe przetwarzane w systemie przechowywane są nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania tych danych. W każdym przypadku, gdy cel przetwarzania danych osobowych został osiągnięty dane te podlegają niezwłocznemu usunięciu.

Rozdział IX
Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych

§ 19

Wykonywanie przeglądów i konserwacja systemu ma na celu:
1) sprawdzenie działania technicznych zabezpieczeń;
2) sprawdzenie funkcjonalności i jakości pracy;
3) sprawdzenie i określenie przydatności elektronicznych nośników informacji;
4) zakwalifikowanie urządzeń do naprawy.

Rozdział X
Postanowienia końcowe.

§ 20

W sprawach nieuregulowanych niniejszą Instrukcją zastosowanie znajdują:
1) Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2014 r.,poz.1182 z późn. zm.);
2) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 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).