Załącznik nr 1 do zarządzenia nr 1/01/2017
Dyrektora Młodzieżowego Ośrodka Socjoterapii w Lublinie
z dnia 2.01.2017 r.

Młodzieżowy Ośrodek Socjoterapii w Lublinie

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwaną dalej „Instrukcją Zarządzania" wprowadza się w oparciu o wymogi bezpieczeństwa informacji określone w rozporządzeniu 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).

System, na którym pracują użytkownicy, jest zbiorem samodzielnych lub połączonych zależnościami podsystemów informatycznych w których ma miejsce przetwarzanie danych osobowych.

Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności

§ 1

1. Użytkownikowi zostaje przyznany unikalny w konkretnym podsystemie identyfikator wraz z poufnym hasłem, który proponuje Administrator Informacji występując z wnioskiem o przyznanie użytkownikowi uprawnień do przetwarzania danych w podsystemie (Załącznik 1 do Regulaminu Ochrony Danych Osobowych). Hasło wymaga uzgodnienia z Administratorem Bezpieczeństwa Informacji.
2. O przyznaniu identyfikatora decyduje Administrator Danych, co jest tożsame z przyznaniem użytkownikowi prawa do przetwarzania danych osobowych w systemie informatycznym.
3. Identyfikator wraz z prawidłowym hasłem umożliwia użytkownikowi dostęp do podsystemu przetwarzania danych osobowych.
4. Każdy z użytkowników przed dopuszczeniem do podsystemu podpisuje umowę o zachowaniu poufności (Załącznik 5 do Regulaminu Ochrony Danych Osobowych), zapoznaje się z Instrukcją Zarządzania i Regulaminem Ochrony Danych Osobowych oraz zostaje pouczony o wdrożonych procedurach bezpieczeństwa.
5. Administratorowi Bezpieczeństwa Informacji przysługuje prawo do zablokowania konta użytkownika w każdym czasie.
6. Po zakończeniu operacji w systemie informatycznym, użytkownik zobowiązany jest wylogować się z podsystemu.

7. W przypadku awarii, zagubienia hasła lub innych nieprzewidzianych sytuacji zagrażających bezpieczeństwu danych – każdy użytkownik zobowiązany jest do niezwłocznego powiadomienia Administratora Danych lub Administratora Bezpieczeństwa Informacji.
8. Użytkownikom przyznaje się równe uprawnienia w dostępie do podsystemu (poziom podstawowy) chyba, że specyfika systemu wymaga innego podejścia.
9. Administratorowi Bezpieczeństwa Informacji przysługuje prawo dostępu do podsystemu na poziomie wyższym (Administratora Systemu).

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

§ 2

1. Użytkownicy którym przyznano dostęp do podsystemu przetwarzania danych osobowych (w tym identyfikator dostępu do systemu) ustalają hasło dostępu z Administratorem Bezpieczeństwa Informacji.
2. Hasło jest informacją o poufnym charakterze i należy zachować je w tajemnicy.
3. Obowiązuje ścisły zakaz ujawniania hasła osobom trzecim, w tym innym użytkownikom.
4. Hasła do wszystkich podsystemów użytkowanych w Zakładzie/Dziale należy przechowywać w zamykanym pomieszczeniu, w miejscu niedostępnym dla osób trzecich, w szafce zamykanej na klucz lub zabezpieczonej szyfrem.
5. Osobą odpowiedzialną za bezpieczne przechowywanie listy identyfikatorów wraz z hasłami wymienionymi w pkt. 4 jest Administrator Informacji.
6. Dostęp do listy identyfikatorów i haseł użytkowników wszystkich podsystemów użytkowanych w Placówce posiada Administrator Informacji. Użytkownik, który utracił hasło, zobowiązany jest zgłosić ten fakt bezzwłocznie Administratorowi Informacji lub bezpośrednio Administratorowi Bezpieczeństwa Informacji, który ustali nowe hasło.

§ 3

1. Hasło składa się z ciągu co najmniej 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.
2. Hasła są różne dla każdego z użytkowników.
3. Hasła są przechowywane w podsystemie w postaci zaszyfrowanej.
4. Para „identyfikator i hasło” przyznane jednemu użytkownikowi nie może zostać powtórnie wykorzystane.
5. Hasła są zmieniane nie rzadziej niż co 30 dni.
6. Użytkownik zobowiązany jest zapamiętać hasło, o którym mowa wyżej.
7. Jeżeli system informatyczny środkami technicznymi nie wymusza podjęcia czynności określonych w pkt 1-6, użytkownik zobowiązany jest do przestrzegania powyższych zasad, a tym samym do okresowej zmiany hasła i ustanowieniu nowego, spełniającego wymogi określone w niniejszym paragrafie.

§ 4

Osobą odpowiedzialną za ustalanie poprawności haseł jest Administrator Bezpieczeństwa Informacji. Jeśli użytkownik podsystemu odpowiedzialny za zmianę hasła nie jest pewien jego poprawności, zobowiązany jest do konsultacji z osobą odpowiedzialną za ustalanie poprawności bezpiecznych haseł.

Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu

§ 5

1. W celu uruchomienia podsystemu informatycznego użytkownik powinien:
   1) uruchomić komputer,
   2) wybrać odpowiednią opcję umożliwiającą logowanie do podsystemu,
   3) zalogować się do podsystemu poprzez wskazanie loginu oraz poufnego i aktualnego hasła.
2. Użytkownik podczas logowania do podsystemu nie może ujawniać hasła osobom trzecim, w tym innym administratorom oraz pozostawiać zapisanego hasła w pobliżu stanowiska pracy i innych pracowników.
3. Użytkownik zobligowany jest do skutecznego wylogowania się z podsystemu za każdym razem, gdy zamierza opuścić stanowisko pracy, niezależnie od tego na jak długo ma zamiar odejść od komputera.
4. Wylogowanie następuje poprzez wybranie w systemie opcji „wyloguj” lub zablokowanie ekranu w sposób, który uniemożliwia odblokowanie bez znajomości hasła, dzięki zastosowaniu funkcji wygaszacza ekranu.
5. Ekrany komputerów, na których przetwarzane są dane osobowe, należy chronić wygaszaczami zabezpieczonymi hasłem. Monitory należy ustawić tak, aby ograniczyć dostęp do danych osobom nieupoważnionym do przetwarzania danych.
6. W przypadku stwierdzenia fizycznej ingerencji w systemie lub innych podejrzeń dotyczących możliwości naruszenia bezpieczeństwa systemu, użytkownik niezwłocznie zawiadamia o zaistniałym fakcie Administratora Informacji lub bezpośrednio Administratora Bezpieczeństwa Informacji.

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

§ 6

1. Kopie zapasowe zbiorów danych osobowych tworzone są codziennie po zakończonym dniu pracy ze zbiorem, chyba że danego dnia nie dokonano żadnych zmian w zbiorze.
2. Za tworzenie kopii zapasowych odpowiedzialny jest Opiekun Zbioru.
3. Opiekun Zbioru dokonuje zapisu kopii zbiorów danych osobowych na nośnikach CD, DVD, Pendrive lub innych nośnikach informacji przynajmniej co 14 dni lub częściej jeśli zmian na zbiorze jest dostatecznie wiele lub gdy uważa to za stosowne.

4. Opiekun Zbioru oznacza i przechowuje kopie zbiorów danych w zamykanym pomieszczeniu, w miejscu niedostępnym dla osób trzecich, w szafce zamykanej na klucz lub zabezpieczonej szyfrem.
5. Poprawność procesu tworzenia i przechowywania kopii zapasowych – nadzoruje Administrator Informacji.

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

§ 7

1. Elektroniczne nośniki informacji zawierające dane osobowe są przechowywane w zamkniętych szafkach z zabezpieczeniem dostępu osób trzecich.
2. Kopie bezpieczeństwa są niezwłocznie zniszczone po ustaniu użyteczności danych osobowych tam zawartych.
3. Zniszczenia kopii dokonuje się w sposób uniemożliwiający późniejsze odtworzenie danych, poprzez fizyczne zniszczenie nośników danych lub jeśli to niemożliwe, poprzez trwałe usunięcie danych przy pomocy specjalistycznego oprogramowania służącego do tego celu. W przypadku wątpliwości, należy zwrócić się do Administratora Bezpieczeństwa Informacji.
4. Fakt zniszczenia kopii zapasowych wymaga sporządzenia na tę okoliczność protokółu opatrzonego podpisem Administratora Bezpieczeństwa Informacji i osoby sporządzającej ten dokument.
5. Kopie zapasowe przechowuje się przez okres 2 lat o ile przepisy nie stanowią inaczej, lub gdy użyteczność danych osobowych ustała przed upływem 2 lat licząc od dnia utworzenia kopii zapasowej, na której te dane są utrwalone.

Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do 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)

§ 8

1. System informatyczny Instytutu jest zabezpieczony przed atakami z zewnątrz sieci za pomocą oprogramowania typu firewall. Dodatkowo na serwerze pocztowym program antywirusowy chroni system przed przedostaniem się do wewnątrz sieci złośliwego oprogramowania.
2. Komponenty serwerowe chronione są przed zakłóceniami w sieci zasilającej przy pomocy urządzeń typu UPS, podtrzymujących zasilanie.
3. Każdy podsystem w którym ma miejsce przetwarzanie danych osobowych, podlega ochronie przed działaniem wirusów komputerowych aktualnym oprogramowaniem antywirusowym aktualizowanym na bieżąco.

4. W celu przeciwdziałania atakom zainfekowanych plików, podsystem musi być skanowany przynajmniej raz dziennie pod kątem obecności w systemie wirusów i innych zagrożeń. Za proces ten odpowiedzialny jest Opiekun Zbioru.
5. W przypadku wykrycia jakiegokolwiek zagrożenia użytkownik niezwłocznie zawiadamia Administratora Bezpieczeństwa Informacji.
6. Wszystkie komputery, na których uruchomione są podsystemy przetwarzające dane osobowe muszą być zaopatrzone w urządzenia typu UPS, podtrzymujące zasilanie, a tym samym zabezpieczające podsystem przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.
7. W przypadku stwierdzenia braku zasilania należy dokonać natychmiastowego zapisu danych osobowych oraz przeprowadzić procedurę opuszczenia podsystemu.

Sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 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)

§ 9

1. Podsystemy informatyczne niesłużące do przetwarzania danych osobowych, a ograniczone wyłącznie do edycji tekstu w celu udostępnienia go na piśmie, zapewniają odnotowanie:
    1) informacji o odbiorcach, którym dane osobowe zostały udostępnione,
    2) dacie i zakresie tego udostępnienia.
2. Odnotowanie następuje przez automatyczny zapisek okoliczności w podsystemie.

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

§ 10

1. Przeglądów oraz konserwacji systemu dokonuje Administrator Bezpieczeństwa Informacji.
2. W przypadku przekazania innym podmiotom elementów systemu w celu naprawy, wszelkie dane osobowe muszą zostać z nich usunięte. Proces ten nadzoruje Administrator Bezpieczeństwa Informacji.
3. Dane osobowe muszą być zabezpieczone przed dostępem osób trzecich zanim nośnik lub element systemu zostanie przekazany podmiotowi innemu niż Administrator Informacji lub Administrator Bezpieczeństwa Informacji.

Zasady bezpiecznego korzystania z urządzeń mobilnych

§ 11

1. Nie należy pobierać aplikacji z nieoficjalnych źródeł - dzięki sklepom z aplikacjami – Apple App Store i Google Play Store – użytkownicy mogą pobierać aplikacje z centralnego, stale monitorowanego źródła.
2. Należy sprawdzać poziom uprawnień, jakiego żądają aplikacje - należy zawsze uważnie przeglądać uprawnienia, o które prosi aplikacja. Użytkownik musi zdecydować, czy zakres wymaganych uprawnień odpowiada teoretycznemu działaniu aplikacji.
3. Należy zwrócić uwagę, w jakie linki się klika - trzeba też pamiętać, że w przypadku niewielkich ekranów smartfonów dokładne sprawdzanie adresu URL może być problematyczne z uwagi na ograniczoną ilość miejsca na pasku adresu. Najpewniejszym sposobem na uniknięcie zainfekowania telefonu w ten sposób jest po prostu powstrzymanie się od korzystania z odsyłaczy pochodzących z nieznanego lub niezaufanego źródła. Co istotne, warto sprawdzać adres odwiedzanej strony nawet wtedy, gdy odsyłacz pochodzi z zaufanego źródła.
4. Należy uważać na niezabezpieczone i publiczne sieci bezprzewodowe - najlepszym sposobem na uniknięcie ataku tego rodzaju jest odwiedzanie w ważnych celach wyłącznie serwisów i usług szyfrujących ruch z wykorzystaniem protokołu HTTPS. Protokół ten powoduje szyfrowanie wszystkich danych przesyłanych między smartfonem a miejscem docelowym, w związku z czym osoba podglądająca sieć nie zdoła ich odczytać.
5. Blokuj niechciane reklamy - najprostszym rozwiązaniem tego problemu jest zainstalowanie oprogramowania blokującego wyświetlanie reklam. Oprogramowanie to blokuje cały ruch związany z reklamami, chroniąc w ten sposób wrażliwe dane użytkownika
6. Pamiętaj o wylogowaniu się z serwisów WWW - dobrze jest zawsze wylogować się z serwisu WWW po zakończeniu korzystania z niego. Spowoduje to usunięcie danych logowania (przechowywanych np. w postaci plików cookie), zmniejszając podatność użytkownika na ataki tego rodzaju.
7. Zainstaluj antywirusa - Niektórzy producenci oprogramowania antywirusowego oferują bezpłatne programy antywirusowe na telefony z systemem Android. Są to zautomatyzowane rozwiązania, które będą dość skutecznie chronić urządzenie przed wirusami.
8. Miej świadomość ataków przeprowadzanych przez porty USB - forma ataku, polegająca na przesłaniu szkodliwego oprogramowania z zainfekowanego komputera PC po podłączeniu do niego telefonu za pomocą kabla USB.
9. Aktualizuj system operacyjny - Dobrze jest regularnie aktualizować system operacyjny. Poza usprawnieniem działania i uzyskaniem dostępu do nowych funkcji użytkownik zwiększa w ten sposób również poziom bezpieczeństwa swojego smartfona lub laptopa.
10. Blokuj ekran - brak blokady ekranu może sprawić, że każdy, kto uzyska fizyczny dostęp do niezablokowanego telefonu, ma praktycznie taki sam dostęp do wszystkich przechowywanych na nim informacji, co sam użytkownik.

Użytkowanie komputerów przenośnych

§ 12

Komputery takie powinny być zabezpieczone przed uszkodzeniem w czasie transportu. Ze względu na ochronę dostępności informacji przechowywanych na laptopie, jak również podwyższone ryzyko jego uszkodzenia, użytkownicy laptopa zobowiązani są do systematycznego tworzenia kopii zapasowych. Nośniki z takimi kopiami powinny być przechowywane w bezpiecznym miejscu, z uwzględnieniem ochrony przed dostępem osób niepowołanych. W celu zabezpieczenia komputera przenośnego przed kradzieżą należy zastosować się do następujących zasad:

1. Komputer przenośny powinien być transportowany pod kontrolą użytkownika lub innej upoważnionej osoby.
2. Komputer przenośny nie powinien być pozostawiany w sposób narażający go na kradzież.
3. W przypadku pozostawiania komputerów przenośnych w biurze zaleca się umieszczanie ich po zakończeniu pracy w zamykanych szafkach. ·
4. Zaleca się, aby komputer przenośny pozostawiony w miejscu dostępnym dla osób innych niż użytkownik był przypinany do stołu przy pomocy odpowiedniego kabla zabezpieczającego - w szczególności dotyczy to zabezpieczenia komputera podczas konferencji, prezentacji, szkoleń, targów itp. Na komputerach przenośnych przeznaczonych do prezentacji podczas opisanych powyżej imprez nie mogą znajdować się informacje wrażliwe, chyba, że jest to związane z celem prezentacji i uzyskało akceptację administratora bezpieczeństwa informacji. Ponadto zaleca się szyfrowanie dysków w komputerach przenośnych zgodnie z zasadami opisanymi w części „Dostęp do systemu informatycznego".
5. Nie zezwala się na pracę nad informacjami wrażliwymi w miejscach publicznych.
6. Użytkownik otrzymujący komputer przenośny podpisuje oświadczenie o zobowiązaniu się do przestrzegania zaleceń związanych z ochroną laptopa.

Postępowanie z kluczami kryptograficznymi

§ 13

Wybór mechanizmów kryptograficznych uwzględnia miedzy innymi następujące kryteria:

1. Realizacja wymaganych usług kryptograficznych (szyfrowanie symetryczne, asymetryczne, podpis cyfrowy, znakowanie czasem itp.).
2. Odpowiednia moc mechanizmów kryptograficznych (zastosowane algorytmy, długości kluczy).
3. Wymagany sposób zarządzania kluczami kryptograficznymi.
4. Wymagana wydajność mechanizmu kryptograficznego.
5. Kompatybilność z istniejącą infrastrukturą informatyczną jednostki.
6. Rodzaj zabezpieczanych danych (dane przechowywane na nośniku, przesyłane przez sieci lokalne, transmitowane w sieciach rozległych lub publicznych).
7. Wymagania dotyczące certyfikacji produktu (o ile występują).
8. Wymagania dotyczące zgodności z normami branżowymi i wykorzystanie standardowych protokołów dla mechanizmów kryptograficznych (o ile występują).
9. Łatwość wdrożenia mechanizmu i integracji z systemem informatycznym.
10. Odporność na próby kompromitacji mechanizmu.
11. Wymagany stopień interakcji z użytkownikiem.

Za określenie wymagań związanych z ochroną informacji odpowiada administrator bezpieczeństwa informacji. Za określenie wymagań związanych z kompatybilnością mechanizmu kryptograficznego z funkcjonującą w jednostce infrastrukturą odpowiada administrator systemu informatycznego, a wymagania te z uwzględnieniem problematyki ochrony informacji, zatwierdzane są przez administratora bezpieczeństwa informacji. Osobą odpowiedzialną za administrację komponentami kryptograficznymi jest administrator systemu. Krytyczne operacje związane z zarządzaniem tymi komponentami winny być przeprowadzane komisyjnie przez dwie osoby. Za określenie operacji krytycznych dla mechanizmów kryptograficznych jest odpowiedzialny administrator bezpieczeństwa informacji. Wszystkie operacje krytyczne powinny być odpowiednio dokumentowane. Dokumentacja powinna być chroniona przed zniszczeniem, zafałszowaniem i dostępem osób nieupoważnionych. Korzystać z niej może administrator bezpieczeństwa informacji, osoby przez niego upoważnione. Użytkownicy systemu kryptograficznego są zobowiązani do zabezpieczenia wykorzystywanych przez siebie prywatnych lub tajnych kluczy kryptograficznych przed dostępem osób nieupoważnionych. W przypadku podejrzenia kompromitacji prywatnego lub tajnego klucza użytkownik jest zobowiązany do natychmiastowego poinformowania o zaistniałym incydencie administratora bezpieczeństwa informacji. Wszystkie klucze kryptograficzne (w tym klucze publiczne) muszą być chronione przed nieautoryzowaną modyfikacją lub nieautoryzowanym zniszczeniem. Sprzęt kryptograficzny, służący do przechowywania i wykorzystywania krytycznego materiału kryptograficznego (na przykład podpisywania certyfikatów zawierających klucze publiczne), musi znajdować się w wydzielonej strefie, chronionej przed dostępem osób nieupoważnionych. Do strefy tej mają dostęp wyłącznie administrator bezpieczeństwa informacji, osoby przez niego upoważnione. Klucze kryptograficzne (również prywatne i tajne, służące do zabezpieczania dokumentów o długim okresie życia - inne niż sesyjne) podlegają archiwizacji. Ich archiwum znajduje się, podobnie jak urządzenia z krytycznym materiałem kryptograficznym, w szczególnie chronionej, wydzielonej strefie. Dostęp do archiwum ma administrator bezpieczeństwa informacji oraz osoby przez niego wskazane. Odtworzenie klucza kryptograficznego może być przeprowadzone komisyjnie (przez co najmniej dwie osoby uprawnione do administrowania systemu kryptograficznego), wyłącznie w szczególnie uzasadnionych przypadkach, za zgodą administratora bezpieczeństwa informacji. Operację odtworzenia zarchiwizowanych kluczy uznaje się za operację krytyczną. Okres archiwizacji uzależniony jest od rodzaju dokumentów zabezpieczanych przez klucze i ustalany jest przez administratora bezpieczeństwa informacji. Administrator bezpieczeństwa informacji jest odpowiedzialny za proces unieważniania kluczy, co do których istnieje podejrzenie, iż zostały skompromitowane, których okres życia zakończył się, oraz które winny utracić ważność z innych powodów - w szczególności wykorzystywanych przez zwolnionych pracowników lub współpracowników, którzy zakończyli świadczenie usług dla jednostki.

Uwagi końcowe

§ 14

1. Dopuszcza się możliwość wprowadzania w Instrukcji Zarządzania procedur uzupełniających, jeśli wymagać będzie tego specyfika komórki organizacyjnej.
2. Stworzone procedury w szczególności powinny uściślać postanowienia określone w § 2, § 3, § 5, § 6, § 9.

Zmiany i udostępnienie tekstu Instrukcji Zarządzania

§ 15

1. Dopuszcza się możliwość dokonywania zmian w Instrukcji Zarządzania.
2. Tekst Instrukcji Zarządzania jest udostępniany użytkownikom w taki sposób, aby mogli się z nim zapoznać i wdrożyć w życie jej postanowienia.