Załącznik nr 2 do Zarządzenia nr 18/2015

Dyrektora PCPR w Zgierzu z dnia 22 lipca 2015 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM W POWIATOWYM CENTRUM POMOCY RODZINIE W ZGIERZU

SPIS TREŚCI

I. WSTĘP

§1.

1. W Powiatowym Centrum Pomocy Rodzinie w Zgierzu zgodnie z rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. 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. Nr 100, poz. 1024), stosowany jest wysoki poziom bezpieczeństwa systemu informatycznego.
2. Zastosowanie wysokiego poziomu zabezpieczeń pozwala zagwarantować bezpieczeństwo i odpowiednią ochronę przetwarzanych danych osobowych w systemie informatycznym.

§2.

1. Infrastruktura teleinformatyczna w PCPR w Zgierzu oparta jest na sieci LAN w której połączone są wszystkie komputery oraz serwer, doprowadzony jest także sygnał Internetu do każdego z komputerów zabezpieczony w centralnym miejscu urządzeniem typ UTM, pełniącego funkcję ochronne i zabezpieczające przed niepowołanym dostępem z zewnątrz.
2. Na każdym stanowisku zainstalowane jest oprogramowanie antywirusowe, antyspamowe oraz firewall.

II. OGÓLNE ZASADY PRACY W SYSTEMIE

§3.

1. Administrator Bezpieczeństwa Informacji odpowiada za korygowanie niniejszej instrukcji w przypadku uzasadnionych zmian organizacyjno – funkcjonalnych w PCPR w Zgierzu
2. Przetwarzanie danych w systemie informatycznym może być realizowane wyłącznie poprzez dopuszczone przez „ABI" do eksploatacji licencjonowane oprogramowanie.
3. Administrator Bezpieczeństwa Informacji prowadzi ewidencję oprogramowania.
4. Do eksploatacji dopuszcza się systemy informatyczne wyposażone w:
   1) mechanizmy kontroli dostępu umożliwiające autoryzację użytkownika, z pominięciem narzędzi do edycji tekstu,
   2) mechanizmy umożliwiające wykonanie kopii bezpieczeństwa oraz archiwizacje danych, niezbędne do przywrócenia prawidłowego działania systemu po awarii,
   3) urządzenia niwelujące zakłócenia i podtrzymujące zasilanie.
5. Użytkownikom zabrania się:
   1) korzystania ze stanowisk komputerowych podłączonych do sieci informatycznej poza godzinami i dniami pracy bez pisemnej zgody Administratora Danych Osobowych,
   2) udostępniania stanowisk roboczych osobom nieuprawnionym,
   3) wykorzystania sieci komputerowej w celach innych niż wyznaczone przez ADO,
   4) samowolnego instalowania i używania programów komputerowych,
   5) korzystania z nielicencjonowanego oprogramowania oraz wykonywania jakichkolwiek działań niezgodnych z ustawą o ochronie praw autorskich,
   6) umożliwienia dostępu do zasobów wewnętrznej sieci teleinformatycznej oraz sieci internetowej osobom nieuprawnionym,
   7) używania komputera bez zainstalowanego oprogramowania antywirusowego.

III. PROCEDURA NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH I REJESTROWANIA ICH W SYSTEMIE INFORMATYCZNYM

§4.

1. Procedura nadawanie uprawnień

   1) Administrator Systemu Informatycznego w PCPR w Zgierzu przyznaje uprawnienia w zakresie dostępu do systemu informatycznego PCPR w Zgierzu na podstawie pisemnego wniosku pozytywnie opiniowanego przez Administratora Bezpieczeństwa Informacji oraz zatwierdzanego przez Administratora Danych – Dyrektora PCPR w Zgierzu, określającego zakres uprawnień pracownika do przetwarzania danych osobowych – wg procedury wew. opisanej w dokumencie „*POLITYKA BEZPIECZEŃSTWA INFORMACJI W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH W PCPR W ZGIERZU”.*
   2) uprawnienia do przetwarzania danych osobowych są nadawane tylko i wyłącznie w zakresie wykonywanych przez pracownika zadań. Nadanie uprawnień polega na utworzeniu unikatowego identyfikatora użytkownika w systemie informatycznym PCPR w Zgierzu.
   3) do przetwarzania danych osobowych zgromadzonych w systemie informatycznym jak również w rejestrach tradycyjnych wymagane jest upoważnienie.
   4) uprawnienia do pracy w systemie informatycznym odbierane są czasowo poprzez zablokowanie konta użytkownika w przypadku np. podczas zawieszenia w pełnieniu obowiązków służbowych.
   5) uprawnienia do przetwarzania danych osobowych w PCPR w Zgierzu odbierane są trwale w przypadku ustania stosunku pracy pracownika.
   6) jeżeli zachodzi konieczność modyfikacji nadanych uprawnień do przetwarzania danych osobowych w systemie informatycznym dokonuje niniejszego Administrator Systemów Informatycznych, zgodnie z całą procedurą nadawania uprawień do przetwarzania danych osobowych określoną w polityce bezpieczeństwa przetwarzania danych osobowych w PCPR w Zgierzu.

7) osoby, które zostały upoważnione do przetwarzania danych są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia nawet w przypadku ustania stosunku pracy.
8) ewidencja osób upoważnionych do przetwarzania danych osobowych prowadzona jest przez Administratora Bezpieczeństwa Informacji.
9) wydane upoważnienia do przetwarzania danych osobowych w PCPR w Zgierzu załączane są do akt osobowych pracowników.
10) nadzór i kontrolę nad procesem rejestracji uprawnień do przetwarzania danych osobowych w systemie informatycznym sprawuje Administrator Systemów Informatycznych.
11) hasło Administratora Systemu Informatycznego do zarządzania uprawnieniami w wykorzystywanych w systemach, programach, aplikacjach wykorzystywanych w PCPR w Zgierzu przechowywane jest w sposób zabezpieczony przez Administratora Danych – Dyrektora PCPR w Zgierzu.

2. Osoby odpowiedzialne za nadawanie, modyfikacje, odbieranie uprawnień do przetwarzania danych i rejestrowanie tych uprawnień w systemach informatycznych:
   1) kontrola przestrzegania instrukcji przez pracowników PCPR w Zgierzu – Administrator Bezpieczeństwa Informacji w PCPR w Zgierzu
   2) aktualizacja instrukcji - Administrator Bezpieczeństwa Informacji wraz z Administratorem Systemów Informatycznych.
   3) nadawanie, rejestrowanie, modyfikacja, wyrejestrowanie uprawnień do przetwarzania danych w systemach informatycznych - Administrator Systemów Informatycznych PCPR w Zgierzu.

§5.

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

1. Przydział uprawnień i identyfikatorów użytkowników
   1) każdy użytkownik dopuszczony do przetwarzania danych osobowych posiada stosowane upoważnienie. Wzór upoważnienia do przetwarzania

danych stanowi **załącznik nr 3** do polityki bezpieczeństwa przetwarzania danych osobowych;

2) każdy użytkownik posiada indywidualny identyfikator umożliwiający logowanie do tych aplikacji z których musi korzystać w związku z realizacją obowiązków służbowych;
3) Administrator Systemu Informatycznego na wniosek Administratora Bezpieczeństwa Informacji definiuje poziom uprawnień użytkownika;
4) przyznanie uprawnień w zakresie dostępu do systemu informatycznego PCPR w Zgierzu polega na wprowadzeniu do systemu dla każdego użytkownika unikalnego identyfikatora oraz pierwszego hasła oraz określeniu zakresu dostępnych danych;
5) w przypadku zbieżności nadawanego identyfikatora z identyfikatorem wcześniej zarejestrowanego użytkownika „ASI" nadaje inny identyfikator odstępując od ogólnej zasady;
6) za gospodarkę loginami odpowiedzialny jest Administrator Systemu Informatycznego w porozumieniu z Administratorem Bezpieczeństwa Informacji;
7) pierwsze hasło użytkownika jest zawsze wprowadzane przez Administratora Systemów Informatycznych, użytkownik przy pierwszym logowaniu musi je zmienić na własne spełniające odpowiednie kryteria.

2. Wymagania i kryteria dotyczące hasła:
   1) uwierzytelnienie w systemie operacyjnym odbywa się za pomocą hasła, które musi zawierać minimum 8 znaków (małe i duże litery, cyfry oraz znaki specjalne),
   2) uwierzytelnienie w programach przetwarzających dane osobowe odbywa się za pomocą loginu i hasła, które musi zawierać minimum 8 znaków (małe i duże litery, cyfry oraz znaki specjalne),
   3) hasło nie może być takie samo jak identyfikator użytkownika systemu informatycznego,
   4) hasło podlega natychmiastowej zmianie w przypadku podejrzenia jego odkrycia przez nieupoważnioną osobę,
   5) każdy użytkownik zobowiązany jest do zachowania w tajemnicy własnych haseł, także po upływie ich ważności,

6) identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie,
7) hasła nie mogą być zapisywane w systemie w postaci jawnej,
8) przy ustalaniu haseł nie mogą być używane imiona, nazwiska, daty urodzenia, imiona dzieci, inicjały i inne kombinacje znaków mogących doprowadzić do łatwego rozszyfrowania haseł przez osoby nieupoważnione,
9) przy ustalaniu haseł nie mogą być w nich stosowane znaki następujące po sobie na klawiaturze bądź te same litery czy cyfry,
10) hasło musi być zmieniane nie rzadziej niż co 30 dni. Za systematyczną, terminową zmianę hasła odpowiada użytkownik systemu Informatycznego,
11) użytkownikowi nie wolno zapisywać hasła i pozostawianiu go w widocznym miejscu,
12) użytkownik jest zobowiązany do utrzymania hasła w tajemnicy, również po utracie jego ważności,
13) hasło przy wpisaniu nie może być wyświetlane na ekranie,
14) zabronione jest stosowanie rozwiązań programowych pozwalających na zapamiętywanie identyfikatorów i haseł,
15) hasło Administratora Systemu Informatycznego przechowywane jest w opieczętowanej kopercie w miejscu wyznaczonym przez Administratora Bezpieczeństwa Informacji. Hasło ASI musi być zmieniane nie rzadziej niż co 30 dni.

IV. PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY PRZEZNACZONE DLA UŻYTKOWNIKÓW SYSTEMU.

§6.

1. Procedura rozpoczęcia pracy
   1) przed rozpoczęciem pracy, w trakcie pracy oraz po jej zakończeniu należy zwrócić uwagę, czy nie występują przesłanki, mogące świadczyć o naruszeniu zasad ochrony danych osobowych;
   2) rozpoczęcie pracy użytkownika w systemie informatycznym PCPR w Zgierzu obejmuje uruchomienie komputera, wprowadzenie indywidualnego, niepowtarzalnego identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione;
   3) użytkownik systemu jest odpowiedzialny za zabezpieczenie danych wyświetlanych przez system przed osobami niemającymi uprawnień.
2. Procedura zawieszenia pracy
   1) opuszczając stanowisko pracy użytkownik systemu informatycznego, zobowiązany jest zablokować stacje roboczą naciskając kombinację przycisku (znaczek windows + L),
   2) w przypadku czasowego niekorzystania z komputera, po 5 minutach uruchomia się automatycznie wygaszacz ekranu zabezpieczający hasłem. Monitory komputerów usytuowane są w sposób uniemożliwiający odczytanie informacji z ekranu komputera osobom postronnym.
3. Procedura zakończenia pracy
   1) procedurę zakończenia pracy, należy rozpocząć od zamknięcia wszystkich używanych programów służących do przetwarzania danych osobowych oraz zapisać wszystkie otwarte dokumenty,
   2) użytkownik systemu nie powinien opuszczać stanowiska pracy do chwili całkowitego wyłączenia komputera.

V. PROCEDURA KORZYSTANIA Z POCZTY ELEKTRONICZNEJ I SIECI INTERNET W PCPR W ZGIERZU

§7.

1. Celem procedury jest udokumentowanie sposobu zapewnienia bezpieczeństwa dostępu i korzystania z zasobów sieci Internet oraz poczty elektronicznej, dla pracowników PCPR w Zgierzu.
2. Użytkownicy systemu Informatycznego, zobowiązani są do powiadamiania Administratora Systemu Informatycznego oraz Administratora Bezpieczeństwa Informacji o każdej nieprawidłowości użytkowania Internetu oraz poczty elektronicznej wykorzystywanej do celów służbowych przez pracownika.
3. Wszelkie informacje przechowywane na komputerach i w sieci są własnością PCPR w Zgierzu i nie uważa się ich za własność prywatną.

§8.

Użytkownicy korzystający z poczty elektronicznej zobowiązani s a do przestrzegania zawartych poniżej zasad:

1) Informacje przesyłane za pośrednictwem poczty elektronicznej, musza być zgodne z prawem i nie mogą naruszać ogólnie przyjętych zasad dotyczących korespondencji wychodzącej i przychodzącej przyjętych w PCPR w Zgierzu.
2) Przesyłanie informacji za pośrednictwem poczty elektronicznej winno odbywać się zgodnie z uprawnieniami adresatów do korzystania z określonego typu danych. W przypadku wątpliwości nadawca powinien sprawdzić, czy dana osoba ma uprawnienia do korzystania z dokumentów danego typu lub o określonej klauzuli poprzez skonsultowanie się z Administratorem Bezpieczeństwa Informacji.
3) Zaleca się stosowanie klauzuli informującej, iż „przesyłana korespondencja jest poufna i może podlegać ochronie prawnej i jeżeli odbiorca nie jest zamierzonym adresatem nie może jej ujawniać, kopiować ani w żaden inny sposób udostępniać i wykorzystywać”;

4) Zabrania się używania adresu mailowego, reprezentującego podmiot lub jego pracownika do celów prywatnych;
5) Zabrania się konfigurowania prywatnych adresów mailowych na służbowych komputerach;
6) Przesyłanie informacji poza obręb PCPR w Zgierzu może odbywać się tylko przez osoby do tego upoważnione.
7) Użytkownicy powinni zwrócić szczególną uwagę na poprawność adresu odbiorcy treści maila, załączonego dokumentu zawierającego dane osobowe.
8) Jeżeli istotne jest potwierdzenie otrzymania przez adresata wiadomości, użytkownik winien skorzystać, o ile jest to technicznie możliwe, z opcji systemu poczty elektronicznej informującej o dostarczeniu i otwarciu dokumentu. Dodatkowo zaleca się, aby użytkownik zawarł w treści dokumentu prośbę o potwierdzenie otrzymania i zapoznania się z informacją. Adresat zobowiązany jest w takiej sytuacji przesłać nadawcy potwierdzenie.
9) Użytkownicy nie powinni otwierać przesyłek od nieznanych adresatów, których tytuł nie sugeruje związku z wypełnianymi przez nich obowiązkami służbowymi. W przypadku otrzymania takiej przesyłki, użytkownik powinien ją zniszczyć lub skontaktować się z Administratorem Bezpieczeństwa Informacji.
10) Nakazuje się zachowania szczególnej ostrożności podczas odbierania poczty elektronicznej, a w szczególności nie klikanie linków w niej zawartych, ani otwierania załączników jeżeli nie mamy pewności co do autentyczności adresata wiadomości.
11) Użytkownicy nie powinni uruchamiać wykonywalnych załączników dołączonych do wiadomości przesyłanych pocztą elektroniczną. W takim przypadku użytkownik powinien poinformować o zdarzeniu Administratora Bezpieczeństwa Informacji, który winien sprawdzić, czy załącznik stanowi zagrożenie dla przetwarzanych w systemie informatycznym informacji.
12) Użytkownik poczty elektronicznej zobowiązany jest archiwizować istotną dla siebie korespondencję elektroniczną;
13) Użytkownicy nie powinni rozsyłać, wiadomości zawierających załączniki o dużym rozmiarze dla większej liczby adresatów - określenie krytycznych

rozmiarów przesyłek i krytycznej liczby adresatów jest uzależnione od wydajności systemu poczty elektronicznej

14) Użytkownicy powinni okresowo kasować niepotrzebne wiadomości pocztowe.
15) Administrator Danych Osobowych zastrzega sobie prawo do wglądu w służbową pocztę elektroniczną pracowników PCPR w Zgierzu, jeżeli są ku temu podstawy tzn. dla celów bezpieczeństwa, kiedy jest to wymagane przez prawo lub jako element śledztwa. Każdorazowy wgląd w pocztę elektroniczną pracownika musi zostać wcześniej zapowiedziany w sposób jasny i zrozumiały dla użytkownika systemu Informatycznego.
16) Niewłaściwe użycie poczty elektronicznej w PCPR w Zgierzu może doprowadzić do wszczęcia postępowania dyscyplinarnego, a czynności zakazane prawem są przestępstwem i mogą doprowadzić do postępowania karnego.

§9.

Użytkownicy korzystający z dostępu do sieci Internet zobowiązani są do przestrzegania zawartych poniżej zasad:

1) Dostęp do sieci Internetu powinien odbywać się wyłącznie w celach niezbędnych do wykonywania zadań służbowych;
2) Nie zaleca się otwierania stron zawierających treści nie związane bezpośrednio z merytoryka pracy PCPR w Zgierzu, ze względu na możliwość przypadkowego pobrania niebezpiecznego, złośliwego oprogramowania infekującego system komputerowy, a w wybranych przypadkach nawet całą sieć;
3) Zabrania się klikania/uruchamiania linków na „nieznanych” stronach internetowych;
4) Niewłaściwe korzystanie z Internetu może doprowadzić do wszczęcia postępowania dyscyplinarnego lub nawet zwolnienia z pracy. Ponadto, korzystanie z Internetu dla celów niezgodnych z prawem może pociągnąć użytkowników do odpowiedzialności karnej.

5) Zabrania się oglądania/słuchania materiałów multimedialnych zawartych w Internecie, co może w znacznym stopniu wysycić łącze internetowe i uniemożliwić pracę innym użytkownikom;
6) Zabrania się przekazywania na zewnątrz poufnych informacji oraz łamania prawa.
7) Zabrania się używania różnych form transferu danych za pomocą Internetu bez wcześniejszej wiedzy i pozwolenia od ASI oraz ABI;
8) Zabrania się pobierania aplikacji z sieci Internet bez wcześniejszej zgody i powiadomienia ASI.
9) Zabrania się przeglądania, zgrywania lub ujawniania informacji dostępnych przez Internet, które PCPR w Zgierzu uznaje w jakikolwiek sposób za obraźliwe lub niebezpieczne dla wewnętrznych systemów informatycznych.
10) Zabrania się czerpania korzyści osobistych lub prowadzenia działalności gospodarczej wykorzystując dostęp do Internetu w PCPR w Zgierzu.

VI. PROCEDURY TWORZENIA KOPII ZAPASOWYCH ZBIORÓW DANYCH ORAZ PROGRAMÓW I NARZĘDZI SŁUŻĄCYCH DO ICH PRZETWARZANIA.

§10.

1. Dane osobowe zabezpiecza się poprzez wykonywanie kopii awaryjnych.
2. Ochronie poprzez wykonywanie kopii podlegają także programy i narzędzia programowe służące przetwarzaniu danych. Kopie programów i narzędzi wykonywane są zaraz po instalacji oraz po każdej aktualizacji na zewnętrznych, elektronicznych nośnikach informacji.
3. Kopie zapasowe baz danych stosowanych w PCPR w Zgierzu systemów, programów, aplikacji sporządza systematycznie Administrator Systemów Informatycznych.
4. Kopie zapasowe powinny być przechowywane w pomieszczeniu odrębnym od pomieszczeń, w których przechowywane są zbiory danych osobowych eksploatowane na bieżąco.
5. W przypadku lokalnego przetwarzania danych osobowych na stacjach roboczych, użytkownicy systemu Informatycznego zobowiązani są do wykonywania samodzielnego kopii bezpieczeństwa zbiorów i zapisywania kopii zapasowych na odrębnych zewnętrznych nośnikach danych.
6. Kopie awaryjne mogą być wykonywane tylko na nośnikach informatycznych zaakceptowanych przez ABI.
7. Kopie awaryjne (zapasowe) baz danych gromadzonych na serwerach przechowuje Administrator Danych w zabezpieczonym miejscu, a przypadku przetwarzania danych na stacjach roboczych poszczególni użytkownicy. Kopie usuwa się niezwłocznie po ustaniu ich użyteczności.
8. ASI sprawuje nadzór nad wykonywaniem kopii zapasowych oraz weryfikuje ich poprawność.
9. Wszelkie wydruki zawierające dane osobowe powinny być przechowywane w miejscu uniemożliwiającym ich odczyt przez osoby nieupoważnione, zaś po upływie czasu ich przydatności – niszczone w niszczarkach dokumentów.
10. Kopie zapasowe, które uległy uszkodzeniu lub ustała ich użyteczność podlegają natychmiastowemu zniszczeniu.

11. Zniszczenie kopii zapasowych, na nośnikach magnetycznych i optycznych dokonuje Administrator Systemu Informatycznego w obecności Administratora Bezpieczeństwa Informacji lub osoby przez niego wyznaczonej.
12. Z nośników magnetycznych i optycznych wielokrotnego użytku, np. CDRW dane należy usunąć w sposób uniemożliwiający ich odczytanie, a w przypadku, gdy usunięcie danych nie jest możliwe, nośniki podlegają zniszczeniu w stopniu uniemożliwiającym odzyskanie danych.
13. Dane zawarte na nośnikach optycznych jednokrotnego użytku, np. CD-R należy usuwać poprzez całkowite zniszczenie nośnika.

VII. PRZETWARZANIE DANYCH OSOBLIWYCH

§11.

1. Dane osobowe przetwarzane są w kartotekach oraz w komputerach do tego przeznaczonych (serwerach, stacjach roboczych) zlokalizowanych w obszarach przetwarzania danych osobowych.
2. W przypadku przekazywania urządzeń lub nośników zawierających dane osobowe, zwłaszcza tzw. „dane wrażliwe” o których mowa w art. 27 ust. 1 ustawy o ochronie danych osobowych, poza obszar przetwarzania danych osobowych, zabezpiecza się je w sposób zapewniający poufność i integralność tych danych, przez co rozumie się:
   1) ograniczenie dostępu do danych osobowych hasłem zabezpieczającym dane przed osobami nieupoważnionymi, lub
   2) stosowanie metod kryptograficznych, lub
   3) stosowanie odpowiednich zabezpieczeń fizycznych lub
   4) w zależności od stopnia zagrożenia zalecane jest stosowanie kombinacji wyżej wymienionych zabezpieczeń.
3. Dane osobowe zapisywane na nośnikach zewnętrznych tworzące kopie zapasowe kolejnych okresów powinny być przechowywane w wyznaczonych, odpowiednio zabezpieczonych pomieszczeniach.
4. Kartoteki powinny być przechowywane w szafach znajdujących się w wyznaczonych, odpowiednio zabezpieczonych pomieszczeniach.
5. Wydruku robocze, błędne lub zdezaktualizowane powinny być niezwłocznie niszczone przy użyciu niszczarki do papieru lub w inny sposób zapewniający skuteczne ich usunięcie lub zanonimizowane.

VIII. SPOSÓB ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO PRZED DZIAŁALNOŚCIĄ OPROGRAMOWANIA, KTÓREGO CELEM JEST UZYSKANIE NIEUPRAWNIONEGO DOSTĘPU DO SYSTEMU INFORMATYCZNEGO.

§12.

1. Komputery służące do przetwarzania danych osobowych w PCPR w Zgierzu posiadają dostęp do sieci publicznej, wówczas system informatyczny narażony jest na oprogramowanie którego celem jest uzyskanie nieuprawnionego dostępu do tego systemu – zatem wprowadza się w systemie informatycznym **wysoki poziom bezpieczeństwa** przetwarzania danych osobowych.
2. Można wyróżnić następujące rodzaje występujących zagrożeń:
   1) nieuprawniony dostęp bezpośrednio do baz danych;
   2) uszkodzeniu kodu aplikacji umożliwiającej dostęp do bazy danych w taki sposób, że przetwarzane dane osobowe ulegną zafałszowaniu lub zniszczeniu;
   3) przechwycenie danych z aplikacji umożliwiającej dostęp do bazy danych na stacji roboczej wykorzystywanej do przetwarzania danych osobowych przez wyspecjalizowany program szpiegowski i nielegalne przesyłanie tych danych poza miejsce przetwarzania danych;
   4) uszkodzenie lub zafałszowanie danych osobowych przez wirus komputerowy zakłócający pracę aplikacji umożliwiającej dostęp do bazy danych na stacji roboczej wykorzystywanej do przetwarzania danych osobowych.
3. W celu przeciwdziałania zagrożeniom system informatyczny powinien posiadać następujące zabezpieczenia:
   1) logowanie użytkowników przy zachowaniu odpowiedniego poziomu komplikacji haseł dostępu;
   2) użytkownicy systemu pracują wyłącznie na zbiorach danych osobowych do których posiadają upoważnienie wydane przez Administratora Danych Osobowych.

3) dostęp do miejsca przechowywania serwera ma wyłącznie Administrator Systemów Informatycznych i osoby upoważnione przez Administratora Danych, zawsze w obecności „ASI”,
4) stosowanie szyfrowanej transmisji danych przy zastosowaniu odpowiedniej długości klucza szyfrującego,
5) zabronione jest pobieranie oraz instalowanie bez nadzoru „ASI” jakichkolwiek programów na wszystkich komputerach służących do przetwarzania danych osobowych;
6) komunikacja w sieci lokalnej musi umożliwiać identyfikację pracujących użytkowników;
7) stosowanie odpowiedniej ochrony antywirusowej na stacjach roboczych wykorzystywanych dla przetwarzania danych osobowych.

4. Potencjalnymi źródłami przedostania się programów szpiegowskich oraz wirusów komputerowych na stacje robocze są:
   1) załączniki do poczty elektronicznej,
   2) przeglądane strony internetowe,
   3) pliki i aplikacje pochodzące z nośników wymiennych uruchamiane i odczytywane na stacji roboczej.
5. W celu zapewnienia ochrony antywirusowej Administrator Systemów Informatycznych jest odpowiedzialny za zarządzanie systemem wykrywającym i usuwającym wirusy.
6. Do ochrony antywirusowej należy stosować program antywirusowy zainstalowany na wszystkich komputerach połączony z siecią lokalną na których odbierana jest poczta elektroniczna i sprawdzane są wszystkie zewnętrzne nośniki informacji przed ich uruchomieniem w sieci.
7. Każdą przesyłkę otrzymaną za pomocą transmisji danych należy sprawdzić obowiązkowo programem antywirusowy. W celu zapewnienia maksymalnej ochrony program antywirusowy oraz jego baza jest aktualizowana kilkukrotnie w ciągu dnia.
8. Na stacjach roboczych oprogramowanie antywirusowe powinno być aktywne cały czas i powinno dokonywać sprawdzenia każdego otwieranego lub uruchamianego pliku.

9. Użytkownicy są zobowiązani do dokonywania kontroli antywirusowej wszystkich nośników danych przychodzących z zewnątrz oraz okresowo własnych nośników danych.
10. Program antywirusowy zainstalowany na stacjach roboczych jest skonfigurowany w następujący sposób:
    1) zablokowana możliwość ingerencji użytkownika w ustalenia oprogramowania antywirusowego,
    2) możliwość centralnego, automatyczne uaktualniania wzorców wirusów.
11. Każdy pracownik przetwarzający dane osobowe przy użyciu komputera w wypadku jakichkolwiek podejrzeń dotyczących obniżenia bezpieczeństwa danych osobowych, powinien poinformować o tym fakcie Administratora Systemów Informatycznych oraz Administratora Bezpieczeństwa Informacji.

IX. SPOSÓB, MIEJSCE I OKRES PRZECHOWYWANIA ELEKTRONICZNYCH NOŚNIKÓW.

§13.

1. Nośniki danych oraz programów służących do przetwarzania danych osobowych, a także danych konfiguracyjnych systemu Informatycznego, przechowuje się w odpowiednio zabezpieczonym pomieszczeniu.
2. Za zgodą „ADO" dane osobowe można przetwarzać na dyskach twardych komputerów stacjonarnych lub zarejestrowanych nośnikach informacji dostarczonych przez „AB"I lub „ASI".
3. Przenośne nośniki danych powinny być zabezpieczone ochroną kryptograficzną.
4. Przenośne nośniki danych nie mogą być wykorzystywane do wynoszenia danych poza dozwolony obszar ich przetwarzania wskazany w załączniku nr 5 do *POLITYKA BEZPIECZEŃSTWA INFORMACJI W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH W PCPR W ZGIERZU*.
5. Przenośne nośniki danych należy tak przechowywać aby osoby nieupoważnione nie miały do nich dostępu.
6. Dane przenoszone na przenośnych nośnikach danych powinny zostać z nich usunięte niezwłocznie po ich wykorzystaniu.
7. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
   1) **LIKWIDACJI** – pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie.
   2) **PRZEKAZANIE PODMIOTOWI NIEUPRAWNIONEMU DO PRZETWARZANIA DANYCH** – pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie.
   3) **NAPRAWY** – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie.
8. Kopie bezpieczeństwa zawierające dane osobowe przechowywane są na serwerze oraz archiwizowane na dyskach zewnętrznych i przechowywane w metalowej szafie zamykanej na klucz do której dostęp mają wyłącznie ADO, ABI i ASI.

9. Nośniki kopii awaryjnych, które zostały wycofane z użycia podlegają zniszczeniu po usunięciu danych osobowych w odpowiednim urządzeniu niszczącym przez „ABI”.

X. PROCEDURY WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMÓW ORAZ NOŚNIKÓW INFORMACJI SŁUŻĄCYCH DO PRZETWARZANIA DANYCH.

§14.

1. Przeglądy i konserwacje systemu Informatycznego oraz nośników informacji służących do przetwarzania danych mogą być wykonywane jedynie przez osoby posiadające upoważnienie wydane przez Administratora Danych Osobowych.
2. Wszelkie prace związane z naprawami i konserwacją systemu Informatycznego przetwarzającego dane osobowe muszą uwzględniać zachowanie wymaganego poziomu zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych, w szczególności poprzez bezpośredni nadzór prowadzony przez „ABI".
3. W przypadku uszkodzenia zestawu komputerowego, nośniki danych, na których są przechowywane dane osobowe powinny zostać zabezpieczone przez „ABI".
4. W przypadku konieczności przeprowadzenia prac serwisowych poza PCPR w Zgierzu, dane osobowe znajdujące się w naprawianym urządzeniu muszą zostać w sposób trwały usunięte.
5. Jeżeli nie ma możliwości usunięcia danych z nośnika na czas naprawy komputera, należy zapewnić stały nadzór nad tym nośnikiem przez osobę upoważnioną do przetwarzania danych osobowych na nim zgromadzonych.
6. Zabronione jest dokonanie napraw sprzętu komputerowego samodzielnie przez pracowników oraz użytkowników systemu informatycznego w PCPR w Zgierzu. O wszelkich nieprawidłowościach lub awariach użytkownik systemu powinien niezwłocznie powiadomić Administratora Systemów Informatycznych oraz Administratora Bezpieczeństwa Informacji.

XI. PRZESYŁANIE DANYCH POZA OBSZAR PRZETWARZANIA

§15.

1. Urządzenia i nośniki zawierające dane osobowe przekazywane poza obszar przetwarzania zabezpiecza się w sposób zapewniający poufność i integralność tych danych, w szczególności poprzez zastosowanie ochrony kryptograficznej.
2. W wypadku przesyłania danych osobowych poza sieć przystosowaną do transferu danych osobowych należy zastosować szczególne środki bezpieczeństwa, które obejmują:
   1) zatwierdzeniu przez „ADO" i sprawdzeniu przez „ABI" zakresu danych osobowych przeznaczonych do wysłania,
   2) zastosowanie mechanizmów szyfrowania danych osobowych,
   3) zastosowanie mechanizmów podpisu elektronicznego zabezpieczającego transmisje danych osobowych oraz rejestrację transmisji wysyłania danych osobowych.
3. Umożliwienie wysyłania danych osobowych tylko z wykorzystaniem określonej aplikacji i tylko przez określonych użytkowników.

XII. POSTANOWIENIA KOŃCOWE

§16.

1. Wobec osoby, pracownika PCPR w Zgierzu który w przypadku naruszenia ochrony danych osobowych lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zadaniami, a także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie dyscyplinarne.
2. Administrator Bezpieczeństwa Informacji zobowiązany jest prowadzić ewidencję osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych.
3. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być traktowane jako ciężkie naruszenie obowiązków pracowniczych, w szczególności przez osobę, która wobec naruszenia ochrony danych osobowych lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym Administratora Bezpieczeństwa Informacji.
4. Orzeczona kara dyscyplinarna wobec osoby uchylającej się od powiadomienia Administratora Bezpieczeństwa Informacji nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2014r. poz. 1182 ze zm.) oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
5. W sprawach nie uregulowanych niniejszym dokumentem mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2014r. poz. 1182) rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. 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).