INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

Starostwo Powiatowe w Żyrardowie

1. POSTANOWIENIA OGÓLNE

1.1. Podstawa prawna

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

1.2. Zakres stosowania

Instrukcja zarządzania systemami informatycznymi **w Starostwie Powiatowym w Żyrardowie,** zwana dalej instrukcją, opisuje sposoby nadawania uprawnień użytkownikom, określa sposób pracy w systemie informatycznym, procedury zarządzania oraz czynności mające wpływ na zapewnienie bezpieczeństwa systemu informatycznego ww. podmiotu. Instrukcja obowiązuje wszystkie komórki organizacyjne oraz wszystkich pracowników.

1.3. Definicje

PODMIOT – Starostwo Powiatowe w Żyrardowie,

ROZPORZĄDZENIE – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE,

SZBI – System Zarządzania Bezpieczeństwem Informacji – system organizacji bezpieczeństwa informacji oparty o wymogi normy PN-ISO/IEC 27001:2013,

ADO – Administrator Danych Osobowych,

ASI – Administrator Systemu Informatycznego (wymiennie informatyk),

IOD – Inspektor Ochrony Danych,

PBI – Polityka Bezpieczeństwa Informacji,

UŻYTKOWNIK SYSTEMU – osoba upoważniona do przetwarzania danych osobowych w systemie informatycznym podmiotu, pracownik lub pracownik innego podmiotu, który świadczy usługi związane z działalnością statutową **Starostwa Powiatowego w Żyrardowie,**

SIEĆ LOKALNA (LAN) – połączenie systemów informatycznych podmiotu wyłącznie dla własnych potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych.

2. PROCEDURA NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH I REJESTROWANIA TYCH UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM ORAZ WSKAZANIE OSOBY ODPOWIEDZIALNEJ ZA TE CZYNNOŚCI

2.1. Zasady nadawania uprawnień.

Przetwarzać dane, w tym dane osobowe w systemach informatycznych może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych. Nadanie przez Administratora danych (ADO) upoważnienia oraz rejestracja użytkownika systemu informatycznego przetwarzającego dane osobowe następuje na wniosek przełożonego użytkownika lub koordynatora zadania, na rzecz którego będą wykonywane czynności związane z przetwarzaniem danych osobowych. Składa on wniosek: **„Karta Uprawnień"** – załącznik nr 1 – wniosek o wydanie upoważnienia do przetwarzania danych osobowych.

Wniosek ten powinien zawierać:

a) imię i nazwisko osoby, której upoważnienie zostanie nadane,

b) zakres upoważnienia do przetwarzania danych osobowych,

c) datę, od kiedy upoważnienie ma obowiązywać.

Wniosek zostaje przekazany do ADO lub osoby uprawnionej przez ADO do wydawania upoważnień, w tym momencie następuje proces przyznawania uprawnień zgodnie z wytycznymi przełożonego osoby, której wniosek dotyczy (wnioskującej) wykonywany przez ADO *(lub, oraz)* ASI *(Administratora Systemów Informatycznych)*.

Oryginał upoważnienia zostaje przekazany osobie upoważnionej za potwierdzeniem odbioru, kopia zostaje dołączona do akt, a w przypadku pracowników podmiotu o nazwie: **Starostwo Powiatowe w Żyrardowie** do akt osobowych pracownika.

O okresie upoważnienia decyduje ADO.

Identyfikator i hasło do systemu informatycznego przetwarzającego dane osobowe są przydzielane użytkownikowi tylko w przypadku, gdy posiada on pisemne upoważnienie do przetwarzania danych osobowych wydane przez ADO lub osobę przez niego uprawnioną.

Za przydzielenie i wygenerowanie identyfikatora i hasła użytkownikowi, który pierwszy raz będzie korzystał z systemu informatycznego, odpowiada właściwy Administrator Systemu Informatycznego *(ASI)* (czynności te wykonuje na podstawie zatwierdzonej **„Karty Uprawnień"** – załącznik nr 1).

Wyrejestrowanie użytkownika z systemu informatycznego może nastąpić na wniosek Administratora danych, Inspektora Ochrony Danych, przełożonego użytkownika lub koordynatora zadania, na rzecz, którego były wykonywane czynności związane z przetwarzaniem danych osobowych. Zgłoszenie ustania potrzeby powierzania danych osobowych zgłasza poprzez **„Kartę Uprawnień"** – załącznik nr 1.

Pisemny wniosek o wyrejestrowanie użytkownika systemu należy złożyć do ADO. Wyrejestrowanie użytkownika oraz cofnięcie upoważnienia do przetwarzania danych osobowych następuje również w sytuacji rozwiązania stosunku pracy pomiędzy **Starostwem Powiatowym w Żyrardowie** a pracownikiem. Wyrejestrowanie użytkownika z systemu realizuje właściwy Administrator Systemu Informatycznego *(ASI)* na podstawie karty uprawnień.

ADO lub wyznaczona przez niego osoba jest zobowiązany do prowadzenia ewidencji osób upoważnionych do przetwarzania danych, w tym danych osobowych.

3. STOSOWANE METODY I ŚRODKI UWIERZYTELNIENIA ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZANIEM I UŻYTKOWANIEM

3.1. Identyfikator i hasło

Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła. Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi. Użytkownik odpowiedzialny jest za wszystkie czynności wykonane przy użyciu identyfikatora, którym się posługuje lub posługiwał.

Identyfikator składa się minimalnie z siedmiu znaków, znaki identyfikatora nie są rozdzielone spacjami ani znakami interpunkcyjnymi, identyfikator nie zawiera polskich liter.

Identyfikator wpisuje się do ewidencji, prowadzonej przez Administratora Systemów Informatycznych, wraz z imieniem i nazwiskiem użytkownika oraz nazwami systemów informatycznych, do których użytkownik uzyskał dostęp i wprowadzany jest przez Administratorów Systemów Informatycznych *(informatyków)* do właściwych systemów.

Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego nie może być przydzielany innej osobie.

3.2. System informatyczny przetwarzający dane osobowe jest konfigurowany w sposób wymagający bezpieczne zarządzanie hasłami użytkowników:

a) hasło przydzielone użytkownikowi musi być zmienione po pierwszym udanym zalogowaniu się do systemu informatycznego przetwarzającego dane osobowe,

b) hasła są zmieniane przez użytkownika,

c) system informatyczny wyposażony jest w mechanizmy wymuszające zmianę hasła po upływie 30 dni od dnia ostatniej zmiany hasła (w przypadku komputera w domenie lub systemu Windows w wersji profesjonalnej),

d) system informatyczny wyposażony jest w mechanizm pozwalający na wymuszenie jakości hasła (w przypadku stosowania systemu Windows w wersji profesjonalnej),

e) hasło powinno składać się z co najmniej 8 znaków. Hasło powinno zawierać małe i wielkie litery oraz cyfry lub znaki specjalne,

f) Użytkownik nie może nadać hasła, z którego korzystał wcześniej w danym systemie informatycznym.

3.3. Pracownicy **Starostwa Powiatowego w Żyrardowie**, uprawnieni do wykonywania prac administracyjnych w systemie informatycznym posiadają własne konta administracyjne, do których mają przydzielone hasło. Ze względu na konieczność utrzymania ciągłości działania kluczowych systemów informatycznych nazwy i hasła użytkowników posiadających uprawnienia administratorów powinny być przechowywane w bezpiecznej lokalizacji, do której dostęp jest w pełni kontrolowany, a dostęp do niej mają wyłącznie uprawnione osoby. Nazwy użytkowników posiadających uprawnienia administratorów oraz hasła powinny być przechowywane w opieczętowanej kopercie, opatrzonej podpisem ASI *(informatyka)*. W przypadku konieczności awaryjnego użycia nazw i haseł tych użytkowników konieczny jest wpis ilustrujący zaistniała sytuację w „Dzienniku haseł" (będącym wewnątrz regulaminowym dokumentem spoza polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym) znajdującym się w szafie wraz z kopertą, w której znajdują się hasła.

Wpis powinien zawierać następujące informacje:

a) imię i nazwisko oraz stanowisko osoby upoważnionej udostępniającej dostęp do szafy, w której znajdują się hasła,

b) imię i nazwisko oraz stanowisko osoby, która pobiera nazwy użytkowników i hasła,

c) krótki opis sytuacji, która zmusiła do awaryjnego wykorzystania haseł.

O konieczności i okolicznościach awaryjnego użycia nazw i haseł musi niezwłocznie zostać powiadomiony Administrator danych oraz Inspektor Ochrony Danych.

4. PROCEDURA ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY PRZEZNACZONA DLA UŻYTKOWNIKÓW SYSTEMU

4.1. Przed rozpoczęciem pracy, w trakcie rozpoczynania pracy z systemem informatycznym oraz w trakcie pracy każda osoba obowiązana jest do zwrócenia bacznej uwagi, czy nie wystąpiły

symptomy mogące świadczyć o naruszeniu ochrony danych osobowych. Szczegółowy opis takich symptomów oraz sposób postępowania w przypadku ich wykrycia został opisany w dokumencie: „Procedura Alarmowa".

4.2. Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione oraz ogólne stwierdzenie poprawności działania systemu.

4.3. Maksymalna ilość prób wprowadzenia hasła przy logowaniu się do systemu wynosi trzy (o ile nie zostanie to zmienione przez ASI *(Administrator Systemów Informatycznych).*

4.4. Po przekroczeniu określonej dla wybranego systemu liczby prób logowania, określonej w pkt 4.3, system blokuje dostęp do zbioru danych na poziomie danego użytkownika. Odblokowanie konta dokonuje się samoczynnie po upływie 20 minut (zgodnie z pkt 4.3 – o ile nie zostanie to zmienione przez ASI *(informatyk)*).

4.5. W przypadku bezczynności użytkownika na stacji roboczej przez okres dłuższy niż 15 minut automatycznie włączany jest wygaszasz ekranu. Wznowienie pracy po wygaszeniu ekranu wymagać musi ponownego podania hasła użytkownika.

4.6. Zmianę użytkownika stacji roboczej każdorazowo musi poprzedzać wylogowanie się poprzedniego użytkownika. Niedopuszczalne jest aby dwóch lub większa ilość użytkowników wykorzystywała wspólnie jedno konto użytkownika.

4.7. Zakończenie pracy w systemie informatycznym dokonuje się poprzez wylogowanie użytkownika ze wszystkich aplikacji oraz systemu operacyjnego komputera.

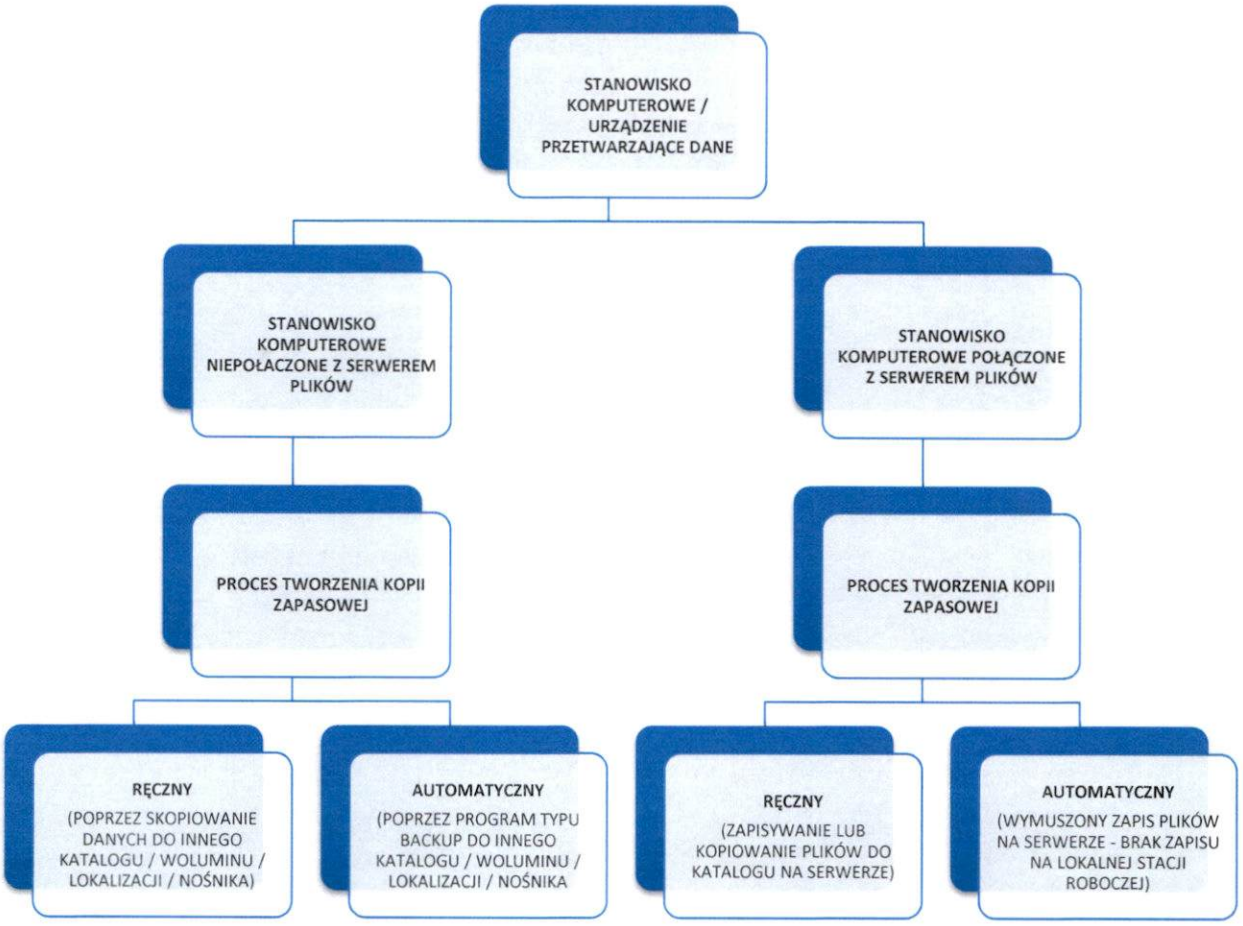
4.8. W pomieszczeniach, w których przetwarzane są dane i w których jednocześnie mogą przebywać osoby postronne, monitory stanowisk dostępu do danych powinny być ustawione w taki sposób, żeby uniemożliwić tym osobom wgląd w dane.

4.9. W przypadku, gdy użytkownik opuszcza czasowo stanowisko pracy obowiązany jest zablokować stację roboczą lub wylogować się z aplikacji i systemu stacji roboczej, na której pracuje oraz sprawdzić czy nie zostały pozostawione bez nadzoru nośniki informacji zawierające dane osobowe. Wznowienie pracy w systemach operacyjnych oraz systemach przetwarzających dane, w tym dane osobowe może nastąpić jedynie po podaniu hasła użytkownika.

5. TWORZENIE KOPII ZAPASOWYCH ZBIORÓW DANYCH ORAZ PROGRAMÓW I NARZĘDZI PROGRAMOWYCH SŁUŻĄCYCH DO ICH PRZETWARZANIA

5.1. Dane, w tym dane osobowe przetwarzane w systemach informatycznych podlegają zabezpieczeniu poprzez tworzenie kopii zapasowych. Za proces tworzenia kopii zapasowych odpowiada Administrator Systemu Informatycznego *(informatyk)* lub osoba specjalnie do tego celu wyznaczona.

5.2. W przypadku lokalnego przetwarzania danych osobowych na stacjach roboczych użytkownicy systemu informatycznego zobowiązani są do zapisywania danych:



5.3. Kopie zapasowe informacji przechowywanych w systemie informatycznym przetwarzającym dane osobowe tworzone są w następujący sposób opisany w dokumencie „**Schemat tworzenia kopii baz danych**" – załącznik nr 2, którego wzór stanowi załącznik do niniejszej instrukcji.

5.4. Każdorazowo po wykonaniu kopii bezpieczeństwa baz danych Administrator Systemu Informatycznego *(informatyk)* weryfikuje poprawność jej wykonania w sposób wymienny tj.:

a) w przypadku serwera / programu archiwizacyjnego: oprogramowanie archiwizujące wykonuje automatyczną analizę poprawności wykonania i odczytu kopii po wykonaniu kopii,

b) w przypadku samodzielnych stacji roboczych poprzez „ręczne" sprawdzenie poprawności wykonania kopii,

c) poprawność wykonania kopii potwierdzana jest w dokumencie „**Lista kontrolna kopii zapasowych**" – załącznik nr 3, której wzór stanowi załącznik do niniejszej instrukcji.

5.5. Nośniki kopii zapasowych, które zostały wycofane z użycia pozbawiane są zapisanych danych za pomocą specjalnego oprogramowania do bezpiecznego usuwania zapisanych danych lub przez zewnętrzną firmę która wyda stosowny certyfikat trwałego usunięcia danych. W przeciwnym wypadku podlegają fizycznemu zniszczeniu z wykorzystaniem metod adekwatnych do typu nośnika, w sposób uniemożliwiający odczytanie zapisanych na nich danych, protokolarnie potwierdzonym przez Administratora Systemów Informatycznych.

5.6. Ponadto:

a) Dane osobowe przechowywane są na serwerze obsługującym system informatyczny. Wszelkie dane przetwarzane w pamięci poszczególnych stacji roboczych oraz komputerów przenośnych są niezwłocznie umieszczane w odpowiednich, przydzielonych dla danego użytkownika przez Administratora Systemów Informatycznych *(informatyk)* miejscach na serwerze lub innych wskazanych i określonych lokalizacjach.

b) Zakazuje się zapisywania danych chronionych, w tym danych osobowych na zewnętrznych nośnikach magnetycznych, optycznych i innych bez zaszyfrowania. Przesyłanie korespondencji wewnątrz **Starostwa Powiatowego w Żyrardowie** może odbywać się bez zabezpieczeń. Przesyłanie danych chronionych na zewnątrz może odbywać się jedynie po zabezpieczeniu informacji poprzez hasło dostępu, spełniające wymogi opisane w pkt. 3.2.e.

c) W przypadku posługiwania się nośnikami danych pochodzącymi od podmiotu zewnętrznego, użytkownik jest zobowiązany do sprawdzenia go programem antywirusowym.

d) Nośniki magnetyczne raz użyte do przetwarzania danych osobowych mogą być wykorzystywane do innych celów, tylko po nadpisaniu danych w trybie kasowania formatującego przy zastosowaniu specjalistycznego oprogramowania lub demagnetyzacji. Nośniki na których nie można powtórnie zapisać informacji powinny być niszczone poprzez pocięcie, zgniecenie lub spopielenie.

e) Przenośne nośniki danych z zaszyfrowanymi, jednostkowymi danymi osobowymi są – na czas ich użyteczności, przechowywane w zamkniętych na klucz szafach, a po wykorzystaniu dane na nich zawarte są trwale usuwane lub nośniki są niszczone poprzez pocięcie, zgniecenie lub spopielenie.

f) Kopie zapasowe programów i aktualizowane kopie systemu informatycznego przechowywane są w szafie metalowej zamykanej na klucz, stojącej w innym pomieszczeniu niż serwery.

g) Po wygaśnięciu okresu przydatności tychże kopii (zastąpieniu ich przez aktualne wersje lub zakończeniu okresu trwałości), są one trwale kasowane lub nośniki je przechowujące niszczone są mechanicznie.

6. SPOSÓB, MIEJSCE I OKRES PRZECHOWYWANIA ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE ORAZ KOPII ZAPASOWYCH

6.1. Nośniki danych zarówno w postaci elektronicznej, jak i papierowej powinny być zabezpieczone przed dostępem osób nieuprawnionych, nieautoryzowaną modyfikacją i zniszczeniem. 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.

6.2. Nośniki elektroniczne, zawierające bazy danych, w tym danych osobowych powinny być przechowywane wewnątrz obszaru przeznaczonego do przetwarzania danych osobowych i nie powinny być bez uzasadnionej przyczyny wynoszone poza ten obszar. Przekazywanie nośników danych, o których mowa powyżej, poza budynek/ki podmiotu powinno odbywać się za wiedzą Administratora Systemów Informatycznych.

6.3. W przypadku, gdy nośnik danych, w tym danych osobowych nie jest dłużej potrzebny, należy przeprowadzić zniszczenie nośnika lub usunięcie danych z nośnika. Jeżeli wydruk danych, w tym

danych osobowych nie jest dłużej potrzebny, należy przeprowadzić zniszczenie wydruku przy użyciu niszczarki, zapewniającej odpowiednie zniszczenie dokumentu.

6.4. W przypadku, gdy kopia zapasowa nie jest dłużej potrzebna, należy przeprowadzić jej zniszczenie lub usunięcie danych z nośnika, na którym się ona znajduje.

6.5. W przypadku dokonania brakowania dokumentów tradycyjnych lub przekazania ich do Archiwum Państwowego, należy odpowiadające im zapisy w bazach danych usunąć lub zabezpieczyć przed ich odczytaniem. Dokonanie brakowania dokumentów tradycyjnych, potwierdzone protokołem brakowania musi być skorelowane z protokołem brakowania (usunięcia) zapisów z baz danych na serwerach, stacjach roboczych a także z bieżących i archiwalnych kopii bezpieczeństwa.

6.6. Jeżeli brakowanie danych, znajdujących się w kopiach baz danych jest niemożliwe lub nieuzasadnione ze względów ekonomicznych, kopia, w której znajdują się dane objęte brakowaniem musi zostać odpowiednio oznaczona. Nadzór nad tym, żeby część danych objętych brakowaniem nie została ponownie użyta spoczywa na Administratorze Systemów Informatycznych.

7. ZABEZPIECZENIE PRZED DZIAŁALNOŚCIĄ OPROGRAMOWANIA, KTÓREGO CELEM JEST UZYSKANIE NIEUPRAWNIONEGO DOSTĘPU DO SYSTEMU INFORMATYCZNEGO

7.1. W związku z tym, że system informatyczny narażony jest na działanie oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do tego systemu konieczne jest podjęcie odpowiednich środków ochronnych.

Można wyróżnić następujące rodzaje występujących tu zagrożeń:

a) nieuprawniony dostęp bezpośrednio do bazy danych,

b) uszkodzenie kodu aplikacji umożliwiającej dostęp do bazy danych w taki sposób, że przetwarzane dane osobowe ulegną zafałszowaniu lub zniszczeniu,

c) przechwycenie danych podczas transmisji w przypadku rozproszonego przetwarzania danych z wykorzystaniem ogólnodostępnej sieci Internet,

d) przechwycenie danych z aplikacji umożliwiającej dostęp do bazy danych na stacji roboczej wykorzystywanej do przetwarzania danych osobowych przez wyspecjalizowany program szpiegowski i nielegalne przesłanie tych danych poza miejsce przetwarzania danych,

e) uszkodzenie lub zafałszowanie danych osobowych przez wirus komputerowy zakłócający pracę aplikacji umożliwiającej dostęp do bazy danych na stacji roboczej wykorzystywanej do przetwarzania danych osobowych.

7.2. W celu przeciwdziałania wymienionym zagrożeniom system informatyczny musi posiadać następujące zabezpieczenia:

a) logiczne odseparowanie serwera bazy danych od sieci zewnętrznej,

b) autoryzacja użytkowników przy zachowaniu odpowiedniego poziomu komplikacji haseł dostępu,

c) stosowanie rygorystycznego systemu autoryzacji dostępu do wszystkich serwerów, na których znajdują się elementy aplikacji umożliwiających przetwarzanie danych osobowych,

d) stosowaniu aplikacji w postaci skompilowanej i nie umieszczenie kodu źródłowego aplikacji na powszechnie dostępnych serwerach,

e) stosowanie szyfrowanej transmisji danych przy zastosowaniu odpowiedniej długości klucza szyfrującego,

f) stosowanie odpowiedniej ochrony antywirusowej na stacjach roboczych wykorzystywanych do przetwarzania danych osobowych.

7.3. Potencjalnymi źródłami przedostawania się programów szpiegowskich oraz wirusów komputerowych na stacje robocze są:

a) załączniki do poczty elektronicznej,

b) przeglądane strony internetowe,

c) pliki i aplikacje pochodzące z nośników wymiennych uruchamiane i odczytywane na stacji roboczej.

7.4. W celu zapewnienia ochrony antywirusowej Administrator Systemu Informatycznego *(informatyk)* przetwarzającego dane osobowe lub osoba specjalnie do tego celu wyznaczona, jest odpowiedzialna za zarządzanie systemem wykrywającym i usuwającym wirusy. System antywirusowy powinien być skonfigurowany w następujący sposób:

a) rezydentny monitor antywirusowy (uruchomiony w pamięci operacyjnej stacji roboczej) powinien być stale włączony,

b) antywirusowy skaner ruchu internetowego powinien być stale włączony,

c) monitor zapewniający ochronę przed wirusami makr w dokumentach typu Office powinien być stale włączony,

d) skaner poczty elektronicznej powinien być stale włączony.

7.5. Systemy antywirusowe zainstalowane na stacjach roboczych powinny być skonfigurowane w sposób następujący:

a) zablokowanie możliwości ingerencji użytkownika w ustawienia oprogramowania antywirusowego, o ile pozwalają na to możliwości techniczne,

b) skanowanie informacji przesyłanych do systemu informatycznego pod kątem pojawienia się niebezpiecznych kodów - na bieżąco,

c) skanowania zawartości dysków stacji roboczej pracującej w systemie informatycznym pod względem potencjalnie niebezpiecznych kodów – na bieżąco.

System antywirusowy powinien być aktualizowany na podstawie materiałów publikowanych przez producenta oprogramowania.

7.6. Użytkownicy systemu informatycznego zobowiązani są do:

a) skanowania zawartości nośników wymiennych odczytywanych na stacji roboczej pracującej w systemie informatycznym pod względem potencjalnie niebezpiecznych kodów - przy każdym odczycie,

b) nie ingerowania w ustawienia konfiguracyjne systemu antywirusowego

c) natychmiastowego powiadomienia Administratora Systemu Informatycznego (informatyk) o zauważonych przypadkach wykrycia zagrożeń przez oprogramowanie antywirusowe.

7.7. W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy Administrator Systemu Informatycznego lub inny wyznaczony pracownik powinien podjąć działania zmierzające do usunięcia zagrożenia. w szczególności działania te mogą obejmować:

a) usunięcie zainfekowanych plików, o ile jest to akceptowalne ze względu na prawidłowe funkcjonowanie systemu informatycznego,

b) odtworzenie plików z kopii zapasowych po uprzednim sprawdzeniu, czy dane zapisane na kopiach nie są zainfekowane,

c) samodzielną ingerencję w zawartość pliku - w zależności od posiadanych kwalifikacji lub skonsultowanie się z zewnętrznymi ekspertami.

7.8. System informatyczny przetwarzający dane osobowe powinien posiadać mechanizmy pozwalające na zabezpieczenie ich przed utratą lub wystąpieniem zafałszowania w wyniku awarii zasilania lub zakłóceń w sieci zasilającej. W związku z tym system informatyczny powinien być wyposażony w co najmniej:

a) filtry zabezpieczające stacje robocze przed skutkami przepięcia,

b) zasilacze awaryjne serwerów baz danych, serwerów aplikacji oraz urządzeń pamięci masowej pozwalające na bezpieczne zamkniecie aplikacji przetwarzających dane osobowe w sposób umożliwiający poprawne zapisanie przetwarzanych danych.

8. REALIZACJA WYMOGU UWIERZYTELNIENIA UŻYTKOWNIKA i REJESTRACJI ZDARZEŃ

8.1. System informatyczny przetwarzający dane, w tym dane osobowe musi posiadać mechanizm uwierzytelniający użytkownika, wykorzystujący identyfikator i hasło. Powinien także posiadać mechanizmy pozwalające na określenie uprawnień użytkownika do korzystania z przetwarzanych informacji (np. prawo do odczytu danych, modyfikacji istniejących danych, tworzenia nowych danych, usuwania danych).

8.2. System informatyczny przetwarzający dane osobowe musi posiadać mechanizmy pozwalające na odnotowanie faktu wykonania operacji na danych. w szczególności zapis ten powinien obejmować:

a) rozpoczęcie i zakończenie pracy przez użytkownika systemu,

b) operacje wykonywane na przetwarzanych danych, a w szczególności ich dodanie, modyfikację oraz usunięcie,

c) przesyłanie za pośrednictwem systemu danych osobowych przetwarzanych w systemie informatycznym innym podmiotom nie będącym właścicielem ani współwłaścicielem systemu,

d) nieudane próby dostępu do systemu informatycznego przetwarzającego dane osobowe oraz nieudane próby wykonania operacji na danych osobowych,

e) błędy w działaniu systemu informatycznego podczas pracy danego użytkownika.

Zapis działań użytkownika uwzględnia:

a) identyfikator użytkownika,

b) datę i czas, w którym zdarzenie miało miejsce,

c) rodzaj zdarzenia,

d) określenie informacji, których zdarzenie dotyczy (identyfikatory rekordów).

8.3. W ramach możliwości technicznych system informatyczny powinien posiadać mechanizmy pozwalające na automatyczne powiadomienie Administratora Systemów Informatycznych lub osoby przez niego uprawnionej o zaistnieniu zdarzenia krytycznego (mogącego mieć krytyczne znaczenie dla bezpieczeństwa przetwarzanych danych osobowych).

8.4. Ponadto system informatyczny powinien zapewnić zapis faktu przekazania danych, w tym danych osobowych z uwzględnieniem:

a) identyfikatora osoby, której dane dotyczą

b) osoby przesyłającej dane,

c) odbiorcy danych,

d) zakresu przekazanych danych osobowych,

e) daty operacji,

f) sposobu przekazania danych.

9. PRZEGLĄD I KONSERWACJA SYSTEMÓW ORAZ NOŚNIKÓW INFORMACJI SŁUŻĄCYCH DO PRZETWARZANIA DANYCH

9.1. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe muszą uwzględniać wymagany poziom zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych.

9.2. Prace serwisowe na terenie podmiotu prowadzone w tym zakresie mogą być wykonywane wyłącznie przez pracowników własnych lub przez upoważnionych przedstawicieli wykonawców zewnętrznych będących pod nadzorem pracowników podmiotu.

9.3. Przed rozpoczęciem prac serwisowych na rzecz **Starostwa Powiatowego w Żyrardowie**, przez osoby nie będące pracownikami ww. podmiotu, konieczne jest potwierdzenie tożsamości serwisantów.

9.4. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane, w tym dane osobowe, przeznaczone do:

a) likwidacji — pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;

b) przekazania podmiotowi nieuprawnionemu do przetwarzania danych — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;

c) naprawy — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez Administratora

danych, chyba, że podmiot świadczący usługi serwisowe został upoważniony do przetwarzania danych chronionych.

9.5. Wszelkie prace serwisowe prowadzone na sprzęcie **Starostwa Powiatowego w Żyrardowie** w jego siedzibie lub w siedzibie serwisu, muszą być potwierdzone protokołem opisującym czas, datę rozpoczęcia i zakończenia prac, zakres prac oraz osoby prowadzące prace.

9.6. Prowadzenie prac w trybie zdalnym odbywać się może jedynie za zgodą ADO, lub ASI Pracownik, który chce udostępnić połączenie dla firm serwisujących oprogramowanie, może to zrobić jedynie po otrzymaniu pisemnej zgody (np. e-mail). Dla każdego połączenia musi być sporządzona notatka lub wpis do dziennika systemu informatycznego, zawierający informacje o:

a) czasie trwania prac,

b) ich zakresie,

c) osobie prowadzącej serwis,

d) osobie udostępniającej zdalny dostęp.

Udostępnianie połączenia w trybie zdalnym może odbywać się jedynie w godzinach pracy podmiotu.

10. DOKUMENTY I ZAPISY ZWIĄZANE

Załącznik nr 1 – Karta uprawnień
Załącznik nr 2 - Schemat tworzenia kopii baz danych
Załącznik nr 3 - Lista kontrolna kopii zapasowych

WICESTAROSTA
Krzysztof Dziwisz