POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH SYSTEMU INFORMATYCZNEGO STAROSTWA POWIATOWEGO W LIPNIE

Spis treści

WPROWADZENIE

Niniejszy dokument opisuje reguły dotyczące bezpieczeństwa danych osobowych zawartych w systemach informatycznych w Starostwie Powiatowym w Lipnie z wyłączeniem Systemów **„POJAZD”** i **„KIEROWCA”** użytkowanych w Wydziale Komunikacji, dla których „Instrukcje bezpieczeństwa” zostały opracowane przez PWPW w Warszawie (administratora systemu) oraz z wyłączeniem **Elektronicznego Krajowego Systemu Monitoringu Orzekania o Niepełnosprawności** dla którego opracowana jest osobna Polityka Bezpieczeństwa Informacji.

Opisane reguły określają granice dopuszczalnego zachowania wszystkich użytkowników systemów informatycznych wspomagających pracę Urzędu. Dokument zwraca uwagę na konsekwencje jakie mogą ponosić osoby przekraczające określone granice oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń.

Odpowiednie zabezpieczenia, ochrona przetwarzanych danych oraz niezawodność funkcjonowania są podstawowymi wymogami stawianymi współczesnym systemom informatycznym.

1. Podstawa prawna

-rozporządzenie 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);

-ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.).

2. Podstawowe definicje polityki bezpieczeństwa

1. **Bezpieczeństwo informacji –** to jasno, jednoznacznie i powszechnie sprecyzowane oraz stosowane procesy, procedury, struktury organizacyjne i funkcje nazywane **Polityką Bezpieczeństwa Informacji.**

2. Polityka Bezpieczeństwa Informacji gwarantuje:
   - **poufność informacji** -tylko uprawnieni pracownicy mają dostęp do informacji;
   - **integralność informacji** - dokładność i kompletność informacji oraz metod jej przetwarzania;
   - **dostępność informacji**- osoby upoważnione mają dostęp do aktywów.

3. Bezpieczeństwo informacji wiąże się z :
   - **rozliczalnością** - dostęp użytkownika do informacji może być przypisany jednoznacznie tylko uprawnionemu użytkownikowi ;
   - **autentycznością** - możliwość weryfikacji tożsamości podmiotów;
   - **niezawodnością-** zachowanie i skutki działania są takie jak zamierzone.

4. Poniższe nazwy należy rozumieć następująco:
    a) **Urząd** - Starostwo Powiatowe w Lipnie;
    b) **Główny Administrator Informacji**- Starosta Lipnowski;
    c) **Administrator Bezpieczeństwa Informacji**- pracownik urzędu wyznaczony do nadzorowania przestrzegania zasad ochrony określonych w niniejszym dokumencie oraz wymagań w zakresie ochrony wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych;
    d) **Administrator Systemu Informatycznego –** pracownik urzędu odpowiedzialny za funkcjonowanie systemu informatycznego urzędu oraz stosowanie technicznych i organizacyjnych środków ochrony;
    e) **Użytkownik systemu-** osoba upoważniona do przetwarzania danych osobowych w systemie informatycznym urzędu. Użytkownikiem może być pracownik urzędu, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno - prawnej, osoba odbywająca staż w urzędzie lub wolontariusz;
    f) **Sieć lokalna** - połączenie systemów informatycznych urzędu wyłącznie dla własnych jego potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych;
    g) **Dane osobowe-** informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
    h) **Zbiór danych** - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów;
    i) **Wykaz zbiorów danych osobowych** - wykaz zarejestrowanych, oraz nie podlegających rejestracji zbiorów danych osobowych;
    j) **Przetwarzanie danych** - operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;
    k) **System informatyczny** - zespół współpracujących ze sobą

urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

3. Cele Urzędu Starostwa Powiatowego w Lipnie w Dziedzinie bezpieczeństwa informacji:

a) ochrona wizerunku, zasobów informacyjnych oraz zapewnienie ciągłości działań procesów Urzędu;
b) tworzenie odpowiednio wysokiego poziomu bezpieczeństwa zasobów Urzędu (zapewnienie poufności, integralności i dostępności zasobów oraz zapewnienie rozliczalności podejmowanych działań);
c) zapewnienie zgodności z prawem podejmowanych działań;
d) umożliwianie rozwoju systemu informatycznego;
e) podnoszenie kultury informatycznej.

4. Strategia dzięki której można zrealizować powyższe cele:

a) właściwa organizacja Systemu Zarządzania Bezpieczeństwem Informacji;
b) właściwa ochrona informacji, a w szczególności informacji prawnie chronionych;
c) właściwa ochrona informacji związanych z zawartymi umowami;
d) zarządzanie ryzykiem w celu ograniczenia go do bezpiecznego poziomu;
e) zapewnienie wsparcia Zarządzających dla Systemu Bezpieczeństwa Informacji;
f) zapewnienie niezawodności systemów informatycznych;
g) zapewnienie odpowiedniego poziomu dostępności informacji;
h) użytkowanie systemów zgodnie z zasadami bezpieczeństwa;
i) stała edukacja użytkowników systemu informacyjnego.

5. Przetwarzanie informacji

Informacje systemu informacyjnego Urzędu służą do wykonywania zadań z zakresu administracji publicznej i rozwoju instytucjonalnego, przetwarzane i składowane są w postaci manualnej jak i elektronicznej.

Rodzaj informacji ze względu na to czego dotyczą;

a) Informacje publiczne;

b) Dane osobowe;

c) Informacje stanowiące tajemnicę Urzędu;

d) Informacje prawnie chronione.

Grupy informacji stworzone są aby lepiej zarządzać bezpieczeństwem informacji.

Cechy grup informacji:

a) każda grupa ma zdefiniowane zasoby uczestniczące w przetwarzaniu danej informacji;

b) każda grupa ma zdefiniowane zasady bezpieczeństwa, oszacowane jest dla niej ryzyko i na tej podstawie dobrane są odpowiednie zabezpieczenia.

6. Odpowiedzialność za bezpieczeństwo informacji

Za bezpieczeństwo informacji odpowiedzialny jest każdy pracownik Urzędu. Nad przestrzeganiem postanowień Polityki Bezpieczeństwa Informacji i rozwojem Systemu Zarządzania Bezpieczeństwem czuwa Grupa Zarządzania Bezpieczeństwem. Grupa Zarządzania bezpieczeństwem składa się z dwóch pionów:

a) pionu administracyjnego - zarządzającego informacją,

b) pionu bezpieczeństwa - zarządzającego bezpieczeństwem informacji.

Powyższe piony spełniają następujące role:

1. Na poziomie Polityki Bezpieczeństwa Informacji:

    a. Główny Administrator Informacji (GAI)
    b. Administratora Bezpieczeństwa Informacji (ABI).

2. Na poziomie Grupy Informacji:

    a. Administratora Informacji– właściciela informacji (AI),
    b. Administratora Bezpieczeństwa Informacji (ABI).

3. Na poziomie Systemu Przetwarzania:

    a. Administratora Systemu i Sieci (ASS),
    b. Administratora Bezpieczeństwa Informacji (ABI).

Główny Adminstrator Informacji

Głównym Administratorem Informacji (GAI) jest Starosta Lipnowski

odpowiada za:

1. realizację ustawy o ochronie danych osobowych w zakresie dotyczącym Administratora Danych;
2. określenie jaki rodzaj informacji może być przetwarzany w Urzędzie ;
3. określenie grupy informacji przetwarzanych w Urzędzie;
4. określenie czy Urząd jest właścicielem grupy informacji, czy też należy ona do innego podmiotu;
5. ustalenie wykazu informacji stanowiących tajemnicę urzędu.

Administrator Bezpieczeństwa Informacji

Administratora Bezpieczeństwa Informacji ABI powołuje Główny

Administrator Informacji ABI odpowiedzialny jest za:

1. realizację ustawy o ochronie danych osobowych w zakresie dotyczącym Administratora Bezpieczeństwa Informacji;

2. nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których przetwarza są dane osobowe oraz kontrola przebywających w nim osób;
3. określenie stopnia poziomu zabezpieczeń;
4. nadawanie uprawnień pobierania kluczy osobom upoważnionym;
5. określenie zasad i sposobów przechowywania kluczy do pomieszczeń, w których znajdują się newralgiczne elementy sieci komputerowych;
6. nadzór nad działaniami od momentu otrzymania zgłoszenia o naruszeniu bezpieczeństwa systemu ochrony danych osobowych;

Administartor Informacji (AI)

Rolę Administratora Informacji (AI) pełnią Naczelnicy Wydziałów, w których przetwarzana jest dana grupa informacji.

AI odpowiedzialni są za :

1. poprawność merytoryczną danych gromadzonych w Zbiorach Danych za pomocą Aplikacji;
2. określenie miejsca i czasu przetwarzania, przechowywania, tworzenia i niszczenia informacji należącej do danej grupy;
3. określenie budynków, pomieszczeń, lub części pomieszczeń tworzących obszar w którym przetwarzane są dane;
4. ewidencjonowanie lokalnych zbiorów danych osobowych wykorzystywanych w Urzędzie;
5. określenie rodzaju Aplikacji oraz Urządzeń Komputerowych, które są niezbędne do realizacji zadań w Wydziale;
6. określenie wrażliwości grupy informacji ze względu na jej poufność, integralność i dostępność;

7. określanie, które osoby i na jakich prawach mają dostęp do danych informacji;
8. powiadomienie Administratora Bezpieczeństwa Informacji o zakładaniu zbiorów danych na lokalnych urządzeniach komputerowych oraz w formie manualnej;
9. określenie czasu rozpoczęcia i zakończenia pracy Użytkowników;
10. zapewnienie Użytkownikowi stanowiska pracy zgodnie z powierzonymi obowiązkami;
11. przygotowanie zgłoszenia rejestracji Zbiorów Danych do Generalnego Inspektoratu Danych Osobowych, jeżeli mają one charakter danych osobowych i przekazanie do Administratora Bezpieczeństwa Informacji.

Praca Administratorów Informacji jest nadzorowana pod względem bezpieczeństwa przez Administratora Bezpieczeństwa Informacji.

Administartor Systemu i Sieci (ASS)

Rolę Administratora Systemu i Sieci (ASS) pełni pracownik, informatyk Urzędu. ASS odpowiedzialny jest za:

1. bieżący monitoring oraz zapewnianie ciągłości działania systemu informatycznego ;
2. optymalizacja wydajności systemu informatycznego;
3. instalacje i konfiguracje sprzętu sieciowego i serwerowego;
4. instalacje i konfiguracje oprogramowania systemowego i sieciowego;
5. konfigurację i administrację oprogramowaniem systemowym i sieciowym zabezpieczającym dane chronione przed nieupoważnionym dostępem do danych;

6. prowadzenie rejestru osób dopuszczonych do systemu (rejestr powinien zawierać: imię i nazwisko osoby, pełnioną rolę, grupę informacji, czas trwania dostępu);

7. współpracę z dostawcami Usług i sprzętu sieciowego, serwerowego oraz zapewnienie zapisów dotyczących ochrony danych osobowych;

8. weryfikację możliwości integracji systemów informatycznych;

9. zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego i sieciowego;

10. zarządzanie kopiami awaryjnymi danych w tym danych osobowych oraz zasobów umożliwiających ich przetwarzanie;

11. opracowanie procedur określających zarządzanie systemem informatycznym;

12. przeciwdziałanie próbom naruszenia bezpieczeństwa informacji;

13. przyznawanie na wniosek Administratora Informacji, za zgodą Administratora Bezpieczeństwa informacji ściśle określonych praw dostępu do informacji w danym systemie;

14. udostępnianie danych zgromadzonych w Systemie Informatycznym, na wniosek Administratora Danych (w rozumieniu ustawy o ochronie danych osobowych) za zgodą Administrator Bezpieczeństwa Informacji;

15. prowadzenie zakupów urządzeń sieciowych i serwerowych;

16. prowadzenie zakupów oprogramowania sieciowego i serwerowego;

17. wnioskowanie do Administratora bezpieczeństwa informacji w sprawie procedur bezpieczeństwa i standardów zabezpieczeń.

Praca Administratora Systemu i Sieci jest nadzorowana pod względem bezpieczeństwa przez Administratora Bezpieczeństwa Informacji.

Administartor Systemu Baz Danych (ASBD)

Rolę Administratora Systemu Baz Danych (ASBD) pełni pracownik , Informatyk Urzędu. ASBD odpowiedzialny jest za:

1. bieżący monitoring oraz zapewnianie ciągłość działania systemów baz danych;
2. optymalizację wydajności systemów baz danych;
3. instalacje i konfiguracje oprogramowania bazodanowego;
4. konfigurację i administrację oprogramowaniem bazodanowym zabezpieczającym dane chronione przed nieupoważnionym dostępem;
5. prowadzenie rejestru osób dopuszczonych do systemu baz danych (rejestr powinien zawierać: imię i nazwisko osoby, pełnioną rolę, grupę informacji, czas trwania dostępu);
6. przyznawanie na wniosek Administratora Informacji, za zgodą Administratora Bezpieczeństwa Informacji ściśle określonych prawa dostępu do Informacji w danym systemie bazodanowym;
7. udostępnianie danych zgromadzonych w systemie bazodanowym, na wniosek Administratora Danych (w rozumieniu ustawy o ochronie danych osobowych) za zgodą Administratora Bezpieczeństwa Informacji;
8. współpracę z dostawcami Aplikacji;

9. nadzór nad wdrożonymi Aplikacjami (przeglądanie, nadawanie i odbieranie uprawnień użytkownikom, definiowanie słowników itp.);

10. weryfikację możliwości integracji aplikacji bazodanowych;

11. zapewnienie przeszkolenia Użytkowników w zakresie prawidłowego korzystania z aplikacji bazodanowych zgodnie z powierzonymi im obowiązkami;

12. zarządzanie kopiami awaryjnymi danych w tym danych osobowych oraz zasobów umożliwiających ich przetwarzanie;

13. opracowanie procedur określających zarządzanie systemem bazodanowym;

14. wykorzystywanie narzędzi baz danych dla tworzenia zestawień;

15. świadczeniu pomocy technicznej w ramach aplikacji bazodanowych dla użytkowników;

16. przeciwdziałanie próbom naruszenia bezpieczeństwa informacji;

17. wnioskowanie do Administratora Bezpieczeństwa informacji w sprawie procedur bezpieczeństwa i standardów zabezpieczeń;

Użytkownik

Użytkownik odpowiedzialny jest za:

1. zachowanie szczególnej staranności przy gromadzeniu danych;
2. zadbanie aby dane przetwarzane były zgodnie z prawem;
3. zadbanie aby dane były zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu

przetwarzaniu niezgodnemu z tymi celami;

4. zadbanie o to by dane były merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane;
5. poprawne korzystanie z aplikacji zgodnie z powierzonymi obowiązkami służbowymi ;
6. informowanie Administratora Systemu o wszelkich nieprawidłowościach działania Aplikacji;
7. ustalenie hasła, okresowe zmiany haseł;
8. utrzymywanie w ścisłej tajemnicy haseł, którymi się posługuje zmianę hasła w przypadku powzięcia przez użytkownika podejrzenia lub stwierdzenia, że z hasłem mogły zapoznać się osoby trzecie i powiadomienie o tym fakcie Administratora Bezpieczeństwa Informacji;
9. zgłaszanie Administratorowi Informacji wszelkich zauważonych nieprawidłowości danych gromadzonych w Aplikacji ;
10. zgłaszanie awarii Urządzeń komputerowych, Oprogramowania Systemowego, Sieci Komputerowej

7. Polityka Bezpieczeństwa określa

-Wykaz budynków i pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe;
-Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;
-Opis struktury zbiorów danych oraz powiązań między - Sposób przepływu danych pomiędzy poszczególnymi systemami;
- Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Obszar przetwarzania danych osobowych

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe wyznacza Administrator Bezpieczeństwa Informacji.

1. Przetwarzanie informacji, w tym informacji osobowych odbywa, się we wszystkich lokalizacjach Urzędu to jest: w Lipnie w budynkach przy ulicy

Sierakowskiego 10B , pomieszczenia zajmowane przez:

- Wydział Komunikacji i Transportu;
- Wydział Geodezji, Kartografii, Katastru i Gospodarki Nieruchomościami;
-Biuro Organów Powiatu;
-Biuro Radcy Prawnego i Przewodniczącego Rady Powiatu;
-Wydział Organizacyjny, Spraw Obywatelskich i Rozwoju Lokalnego;
-Pomieszczenie w którym znajduje się serwer;
-Sekretariat;
-Biuro Starosty Powiatu Lipnowskiego;
-Biuro Wicestarosty Powiatu Lipnowskiego;
-Biuro Sekretarza Powiatu Lipnowskiego;
-Kadry;
-Wydział Finansów i Budżetu;
-Wydział Środowiska, Rolnictwa i Leśnictwa;

oraz przy ulicy Mickiewicza 58 , pomieszczenia zajmowane przez:

-Wydział Oświaty, Kultury, Sportu i Zdrowia;
-Powiatowy Zespół ds. Orzekania o Stopniu Niepełnosprawności;
-Wydział Architektury i Budownictwa;
-Referat Administracyjno – Gospodarczy i Zamówień Publicznych;
-Centrum Kryzysowe, Sprawy Obywatelskie, Radca prawny;

2. Część informacji przetwarzana jest również na komputerach przenośnych.

3. Większość informacji składowana i przetwarzana jest w budynku przy ulicy Sierakowskiego 10B. Tam też zlokalizowano większość systemów informatycznych Urzędu.

Wykaz zbiorów danych osobowych przetwarzanych w systemie informatycznym

1. W skład systemu wchodzą:

-dokumentacja papierowa (korespondencja, wnioski, deklaracje, itd.) ;
-urządzenia i oprogramowanie komputerowe służące do przetwarzania informacji oraz procedury przetwarzania danych w tym systemie, w tym procedury awaryjne, wydruki komputerowe.

2. Wykaz zbiorów danych osobowych przetwarzanych w systemie

informatycznym wraz z opisem i wydziałem w którym są przetwarzane prowadzi Administrator Bezpieczeństwa Informacji wykaz ten stanowi **Załącznik nr 1.**

Struktury zbiorów danych osobowych i ich powiązań oraz sposób przepływu danych.

Opisy struktur zbiorów danych osobowych i ich powiązań **Załącznik A** oraz sposób przepływu danych pomiędzy poszczególnymi systemami **Załącznik B** prowadzi Administrator Bezpieczeństwa Informacji .

Środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

1. Środki ochrony fizycznej

1.1 Budynki urzędu, zamykane po zakończeniu pracy, posiadają system alarmowy .

1.2 Urządzenia służące do przetwarzania danych osobowych znajdują się w pomieszczeniach zabezpieczonych zamkami patentowymi.

1.3 Przebywanie osób nieuprawnionych w pomieszczeniach tworzących obszar przetwarzania danych osobowych dopuszczalne jest tylko w obecności osoby zatrudnionej przy przetwarzaniu danych lub w obecności Administratora Bezpieczeństwa Informacji.

1.4 Pomieszczenia, o których mowa wyżej, powinny być zamykane na czas nieobecności pracownika zatrudnionego przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich.

1.5 W przypadku przebywania interesantów bądź innych osób postronnych w pomieszczeniach, o których mowa wyżej, monitory stanowisk dostępu do danych osobowych powinny być ustawione w taki sposób, aby uniemożliwić tym osobom wgląd w dane.

1.6 Do przebywania w pomieszczeniu serwera uprawnieni są: Administrator Bezpieczeństwa Informacji, osoba odpowiedzialna za obsługę informatyczną urzędu oraz Administrator Danych.

1.7 Przebywanie w pomieszczeniu serwera osób nieuprawnionych (konserwator, elektryk, sprzątaczka) dopuszczalne jest tylko w obecności jednej

z osób upoważnionych)

2. Środki sprzętowe, informatyczne i telekomunikacyjne

2.1 Każdy dokument papierowy zawierający dane osobowe przeznaczony do wyrzucenia powinien być zniszczony w sposób uniemożliwiający jego odczytanie, przy pomocy niszczarki, która umożliwia cięcie poprzeczne.

2.2 Urządzenia wchodzące w skład systemu informatycznego podłączone są do odrębnego obwodu elektrycznego, zabezpieczonego na wypadek zaniku napięcia albo awarii w sieci zasilającej UPS-em.

2.3 Siec lokalna podłączona do Internetu , oddzielona sprzętowym firewallem (zaporą).

2.4 Na stanowiskach pracy, w których przetwarzane są dane osobowe stosuje się oprogramowanie do tworzenia kopii zapasowych.

2.5 Na serwerze oraz w poszczególnych stacjach roboczych zainstalowano oprogramowanie antywirusowe. Poczta elektroniczna wpływająca do Urzędu skanowana jest programem antywirusowym przed przesłaniem jej do użytkownika.

2.6 Kopie awaryjne wykonywane są w cyklach:
- tygodniowa na płytach CD,DVD,
- miesięczna na płytach CD,DVD ,
- kwartalna na płytach DVD-R .

3. Środki ochrony w ramach oprogramowania systemu

3.1 Dostęp fizyczny do baz danych osobowych zastrzeżony jest wyłącznie dla osoby zajmującej się obsługą informatyczną urzędu, Administratora Bezpieczeństwa Informacji.

3.2 Konfiguracja systemu umożliwia użytkownikom końcowym dostęp do danych osobowych jedynie za pośrednictwem aplikacji.

3.3 System informatyczny z jakiego korzystają pracownicy urzędu pozwala zdefiniować odpowiednie prawa dostępu do zasobów informatycznych systemu.

4. Środki ochrony w ramach narzędzi baz danych i innych narzędzi programowych

4.1 Zastosowano identyfikator i hasło dostępu do danych na poziomie aplikacji.

4.2 Dla każdego użytkownika systemu jest ustalony odrębny identyfikator.

4.3 Zdefiniowano użytkowników i ich prawa dostępu do danych osobowych na poziomie aplikacji (unikalny identyfikator i hasło).

5. Środki ochrony w ramach systemu użytkowego

5.1 Zastosowano wygaszanie ekranu w przypadku dłuższej nieaktywności użytkownika.

5.2 Komputer, z którego możliwy jest dostęp do danych osobowych zabezpieczony jest hasłem uruchomieniowym (BIOS), hasłem wejściowym do systemu operacyjnego oraz hasłem do każdej aplikacji przy pomocy której przetwarzane są dane osobowe.

6. Środki organizacyjne

6.1 Osoby upoważnione do przetwarzania danych osobowych przed dopuszczeniem do pracy zostaną przeszkolone w zakresie obwiązujących przepisów o ochronie danych osobowych, procedur przetwarzania danych, oraz poinformowane o podstawowych zagrożeniach związanych z przetwarzaniem danych w systemie informatycznym.

6.2 Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych Osobowych.

6.3 Wprowadzono instrukcję zarządzania systemem informatycznym.

6.4 Zdefiniowano procedury postępowania w sytuacji naruszenia ochrony danych osobowych.

6.5 Wprowadzono obowiązek rejestracji wszystkich przypadków awarii systemu, działań konserwacyjnych w systemie oraz naprawy systemu.

6.6 Określono sposób postępowania z nośnikami informacji.

8. Opis zdarzeń naruszających ochronę danych osobowych

1. Podział zagrożeń:
    1) Zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu) - ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu; ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych.
    2) Zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania, pogorszenie jakości sprzętu i oprogramowania) - może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych.
    3) Zagrożenia zamierzone - świadome i celowe działania powodujące naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na:
        - nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu),
        - nieuprawniony dostęp do systemu z jego wnętrza,
        - nieuprawnione przekazanie danych,
        - bezpośrednie zagrożenie materialnych składników systemu (np. kradzież sprzętu).
2. Naruszenie lub podejrzenie naruszenia systemu informatycznego, w którym przetwarzane są dane osobowe następuje w sytuacji:

1) losowego lub nieprzewidzianego oddziaływania czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, itp.,
2) niewłaściwych parametrów środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,
3) awarii sprzętu lub oprogramowania, które wyraźnie wskazuje na umyślne działanie w kierunku naruszenia ochrony danych,
4) pojawienia się odpowiedniego komunikatu alarmowego,
5) podejrzenia nieuprawnionej modyfikacji danych w systemie lub innego odstępstwa od stanu oczekiwanego,
6) naruszenia lub próby naruszenia integralności systemu lub bazy danych w tym systemie,
7) pracy w systemie wykazującej odstępstwa uzasadniające podejrzenie przełamania lub zaniechania ochrony danych osobowych - np. praca osoby, która nie jest formalnie dopuszczona do obsługi systemu,
8) ujawnienia nieautoryzowanych kont dostępu do systemu,
9) naruszenia dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (np. nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, itp.).

3. Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia fizycznego miejsc przechowywania i przetwarzania danych osobowych np.
   - niezabezpieczone pomieszczenia,
   - nienadzorowane, otwarte szafy, biurka, regały,
   - niezabezpieczone urządzenia archiwizujące,

pozostawianie danych w nieodpowiednich miejscach – kosze, stoły itp

Znajomość polityki bezpieczeństwa systemu informatycznego

Do zapoznania się z niniejszym dokumentem oraz stosowania zawartych w nim zasad zobowiązani są wszyscy pracownicy Urzędu upoważnieni do przetwarzania danych w systemie informatycznym.