ZARZĄDZENIE NR 74/2013

Burmistrza Łochowa

z dnia 3 grudnia 2013 r.

w sprawie polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miejskim w Łochowie

Na podstawie art. 31 i art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2013 r. poz. 594 z późn. zm.) oraz art. 36 ust. 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.), a także § 4 i § 5 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), zarządzam, co następuje:

§ 1 .

Wprowadza się do użytku służbowego „Politykę Bezpieczeństwa” w zakresie przetwarzania danych osobowych w Urzędzie Miejskim w Łochowie stanowiącą załącznik nr 1 do niniejszego zarządzenia oraz „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Łochowie”, stanowiącą załącznik nr 2 do zarządzenia.

§ 2 .

Zobowiązuje się wszystkich pracowników Urzędu Miejskiego w Łochowie oraz strony trzecie świadczące usługi na rzecz Urzędu Miejskiego w Łochowie do przestrzegania przepisów zawartych w dokumentach, o których mowa w § 1.

§ 3 .

Zobowiązuje się Kierowników Jednostek Organizacyjnych do sprawowania nadzoru nad ich ochroną oraz do współpracy z Administratorem Bezpieczeństwa Informacji w tym zakresie.

§ 4 .

Wyłącza się jawność dokumentów, o których mowa w § 1 na podstawie art. 36 ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. Dokumenty te mogą być rozpowszechniane bez żadnych ograniczeń wyłącznie wewnątrz Urzędu Miejskiego w Łochowie, o udostępnianiu tych dokumentów na zewnątrz decyduje Administrator Bezpieczeństwa Informacji.

§ 5 .

Wykonanie zarządzenia powierza się Sekretarzowi Gminy.

§ 6 .

Traci moc zarządzenie Nr 14/2005 Burmistrza Łochowa z dnia 16 maja 2005 r. w sprawie: polityki bezpieczeństwa Urzędzie Miejskiego w Łochowie w zakresie przetwarzania danych osobowych oraz instrukcji zarządzenia systemami służącymi do przetwarzania danych osobowych

§ 7 .

Zarządzenie wchodzi w życie z dniem podpisania.

Z up. Burmistrza
Urszula Anna Kalinowska

Elektronicznie podpisany przez:
URSZULA KALINOWSKA
Data: 2013.12.11 09:05:06
Odcisk palca certyfikatu: 8b49 476b e52
c2b7 6b78 8b40 2bb0 5ab8 36ca 911f

ZAŁĄCZNIK 1 do Zarządzenia Nr 74/2013
Burmistrza Łochowa
z dnia 03.12.2013
w sprawie polityki bezpieczeństwa przetwarzania
danych osobowych w Urzędzie Miejskim w Łochowie

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH URZĘDU MIEJSKIEGO W ŁOCHOWIE

Dokumenty powiązane:

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych Urzędu Miejskiego w Łochowie.

§ 1 .

Postanowienia ogólne

1 . 1. Polityka bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miejskim w Łochowie zwana dalej „Polityką”, została wydana w związku z § 3 ust. 1 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. z 2004r., Nr 100, poz. 1024). Celem Polityki jest stworzenie podstaw dla właściwego wykonania obowiązków Administratora

2 . Danych w zakresie zabezpieczenia i prawidłowej ochrony przetwarzanych danych osobowych

3 . Polityka określa zasady przetwarzania danych osobowych oraz ich zabezpieczania, jako zestaw praw, reguł i zaleceń, regulujących sposób ich zarządzania, ochrony i dystrybucji wewnątrz Urzędu.

4 . Polityka zawiera informacje dotyczące rozpoznawania procesów przetwarzania danych osobowych oraz wprowadzonych zabezpieczeń technicznych i organizacyjnych, zapewniających ochronę przetwarzanych danych osobowych.

5 . Niniejszą Politykę stosuje się do:

1) Danych osobowych:

a) przetwarzanych w systemach informatycznych,

b) zapisanych się na zewnętrznych nośnikach informacji,

c) przetwarzanych tradycyjnie.

2) Informacji dotyczących bezpieczeństwa przetwarzania danych osobowych:

a) służących do uwierzytelnienia w systemach informatycznych, w których są przetwarzane dane osobowe,

b) dotyczących wdrożonych zabezpieczeń technicznych i organizacyjnych.

6 . Bez względu na zajmowane stanowisko, miejsce wykonywanej pracy oraz charakter stosunku pracy, zasady określone w niniejszej Polityce oraz w dokumentach powiązanych powinny być znane i stosowane przez pracowników oraz w niezbędnym zakresie przez współpracowników przetwarzających dane osobowe, których administratorem jest Urząd Miejski w Łochowie.

§ 2 .

Definicje

1 . **Administrator Danych Osobowych** – podmiot który decyduje o środkach i celach przetwarzania danych osobowych, reprezentowany przez Burmistrza Łochowa.

2 . **Administrator Bezpieczeństwa Informacji** – osoba wyznaczona przez Burmistrza Łochowa, odpowiedzialna za nadzorowanie stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, w tym w szczególności za przeciwdziałanie dostępowi osób trzecich do systemu, w którym przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie ochrony danych osobowych

3 . **Administrator Systemów Informatycznych** – wyznaczona przez ADO osoba, odpowiedzialna za funkcjonowanie infrastruktury informatycznej na którą składa się cały sprzęt informatyczny oraz systemów i aplikacji informatycznych, za ich przeglądy, konserwację oraz za stosowanie technicznych i organizacyjnych środków bezpieczeństwa w systemach informatycznych.

4 . **Bezpieczeństwo przetwarzania danych osobowych** - zachowanie poufności, integralności i rozłączalności danych osobowych; dodatkowo, mogą być brane pod uwagę inne własności, takie jak dostępność, autentyczność, niezaprzeczalność i niezawodność.

5 . **Dane Osobowe** - każda informacja dotycząca żyjącej osoby fizycznej, która pozwala na bezpośrednią lub pośrednią identyfikacje tej osoby.

6 . **GIODO** – Generalny Inspektor Ochrony Danych Osobowych.

7 . **Integralność danych** – właściwość zapewniająca, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany.

8 . **Naruszenie ochrony danych osobowych** – zamierzone lub przypadkowe naruszenie środków technicznych i organizacyjnych zastosowanych w celu ochrony danych osobowych. W szczególności, gdy stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszanie ochrony danych osobowych.

9 . **Poufność** – właściwość zapewniająca, że informacja (np. dane osobowe) jest dostępna jedynie osobom upoważnionym.

10 . **Przetwarzanie danych osobowych** - jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

11. **Rozporządzenie** - 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).
12. **Rozliczalność** – właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
13. **System informatyczny** – zespół współpracujących urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
14. **Urząd** – Urząd Miejski w Łochowie, ul. Al. Pokoju 75, 07-130 Łochów
15. **Ustawa** – Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz. U. z 2002 r. Nr 101, poz. 926 z poźn. zm.).
16. **Użytkownik systemu** – osoba upoważniona do bezpośredniego dostępu do danych osobowych przetwarzanych w systemie informatycznym, która posiada ustalony identyfikator i hasło
17. **Użytkownik zewnętrznym** - należy przez to rozumieć osobę nie będącą pracownikiem lub stażystą Urzędu Gminy Łochów, posiadającą uprawnienia do przetwarzania informacji w związku z wykonywaniem czynności na rzecz Urzędu.
18. **Właściciel zasobów danych osobowych** – osoba kierująca komórką organizacyjną, odpowiedzialna za ochronę danych osobowych przetwarzanych w podległej komórce. Jest ona zobowiązana zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy o ochronie danych osobowych oraz nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.
19. **Zbiór danych osobowych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony czy podzielony funkcjonalnie.
20. **Zbiór nieinformatyczny** - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony lub podzielony funkcjonalnie, prowadzony poza systemem informatycznym, w szczególności w formie kartoteki, skorowidza, księgi, wykazu lub innego zbioru ewidencyjnego.

§ 3.

Deklaracja Administratora Danych Osobowych

1. ADO zobowiązuje się do podjęcia odpowiednich kroków, mających na celu zapewnienie prawidłowej ochrony danych osobowych, w szczególności do zapewnienia, że przez cały okres ich przetwarzania, dane będą:
   1) Przetwarzane zgodnie z prawem.

2) Zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami.

3) Merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane.

4) Przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania

5) Zabezpieczone środkami technicznymi i organizacyjnymi, które zapewniają rozliczalność, integralność oraz poufność danych

2 . Przy przetwarzaniu danych osobowych w systemach informatycznych Urzędu Gminy Łochów należy stosować wysoki poziom bezpieczeństwa w rozumieniu § 6 ust. 4 Rozporządzenia.

§ 4 .

Przegląd dokumentacji z zakresu ochrony danych osobowych

1 . Niniejsza Polityka oraz dokumenty z nią powiązane powinny być aktualizowane wraz ze zmieniającymi się przepisami prawnymi o ochronie danych osobowych oraz zmianami faktycznymi w ramach Gminy, które mogą powodować, że zasady ochrony danych osobowych określone w obowiązujących dokumentach będą nieaktualne lub nieadekwatne.

2 . Przegląd Polityki ma na celu stwierdzenie, czy postanowienia Polityki odpowiadają aktualnej i planowanej działalności Gminy oraz stanowi prawnemu aktualnemu w momencie dokonywania przeglądu.

3 . Fakty wystąpienia poważnych naruszeń ochrony danych osobowych powinny skutkować zmianami w dokumencie niniejszej Polityki i dokumentach powiązanych

4 . Zmiany niniejszej Polityki wymagają przeglądu innych dokumentów obowiązujących w Gminie dotyczących ochrony danych osobowych

5 . Wszelkie znaczące zmiany Polityki powinny być zatwierdzane przez Burmistrza Łochowa.

§ 5 .

Zarządzanie ochroną danych osobowych

1 . Realizację zamierzeń w celu zwiększenia skuteczności ochrony danych osobowych powinny zagwarantować następujące założenia:

a) Przeszkolenie pracowników dopuszczonych do przetwarzania danych w zakresie bezpieczeństwa danych osobowych.

b) Przypisanie użytkownikom określonych atrybutów pozwalających na ich identyfikację w systemach informatycznych (np. hasła, identyfikatory), umożliwiających im dostęp do danych osobowych - stosownie do zakresu upoważnienia i indywidualnych poziomów uprawnień.

c) Okresowe sprawdzanie przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych osobowych.

d) Podejmowanie niezbędnych działań, w celu likwidacji słabych ogniw w systemie ochrony danych osobowych.

e) Śledzenie osiągnięć w dziedzinie bezpieczeństwa systemów informatycznych i w miarę możliwości organizacyjnych i techniczno-finansowych - wdrażanie nowych narzędzi i metod pracy oraz sposobów zarządzania systemami informatycznymi, służących wzmocnieniu bezpieczeństwa przetwarzanych danych osobowych.

2 . Na każdym etapie przetwarzania danych osobowych należy brać pod uwagę, w niezbędnym zakresie, integralność, poufność oraz rozliczalność dla przetwarzanych danych osobowych.

3 . Administrator Danych Osobowych powinien być zapewniony, że pracownicy, wykonawcy oraz użytkownicy zewnętrzni

a) Są odpowiednio wprowadzani w swoje obowiązki i odpowiedzialności związane z ochroną danych osobowych i ich przetwarzaniem przed przyznaniem im dostępu do danych osobowych.

b) Otrzymali zalecenia określające wymagania w zakresie bezpieczeństwa danych osobowych związane z ich obowiązkami w Gminie.

c) Wypełniali zalecenia i warunki zatrudnienia, które uwzględniają zasady ochrony danych osobowych oraz właściwe metody pracy.

d) W sposób ciągły utrzymywali odpowiednie umiejętności i kwalifikacje.

4 . Za bieżącą, operacyjną ochronę danych osobowych odpowiada każda osoba przetwarzająca te dane w zakresie zgodnym z zakresem upoważnienia, kompetencjami lub rolą sprawowaną w procesie przetwarzania danych.

§ 6 .

Dokumenty powiązane

Na dokumentacje ochrony danych osobowych w Urzędzie Gminy Łochów składają się;

1 . **Ewidencja osób upoważnionych przez Administratora Danych Osobowych do przetwarzania danych osobowych. (wzór Zał. Nr 1)**

- prowadzona przez Administratora Bezpieczeństwa Informacji

2 . **Ewidencja zbiorów danych osobowych przetwarzanych w Urzędzie Gminy Łochów oraz programów zastosowanych do ich przetwarzania. (wzór Zał. Nr 2)**

- prowadzona przez Administratora Bezpieczeństwa Informacji

3 . **Opisy struktur zbiorów danych osobowych**

- prowadzone przez Administratora Systemów Informatycznych

4 . **Opisy sposobów przepływu danych pomiędzy systemami**

- prowadzone przez Administratora Systemów Informatycznych

5 . **Oryginały i Kopie dokumentów dotyczących ochrony danych osobowych (w tym kopie wniosków o rejestrację/aktualizacje zbiorów danych osobowych do GIODO oraz uchwały, zarządzenia, polityki itd. dotyczące ochrony danych osobowych)**

- prowadzone przez Administratora Bezpieczeństwa Informacji

6. **Protokoły z przeprowadzonych kontroli wewnętrznych i zewnętrznych w zakresie ochrony danych osobowych**
   - prowadzone przez Administratora Bezpieczeństwa Informacji
7. **Plany archiwizacji danych osobowych i programów służących do ich przetwarzania**
   - prowadzone przez Administratora Systemów Informatycznych
8. **Ewidencje przenośnych nośników danych używanych w poszczególnych komórkach organizacyjnych Urzędu**
   - prowadzone przez Właścicieli zasobów.

§ 7.

Odpowiedzialność Administratora Danych Osobowych

1. Administrator Danych Osobowych jest odpowiedzialny za przetwarzanie i ochronę danych osobowych zgodnie z przepisami prawa, w tym wprowadzenie do stosowania procedur postępowania zapewniających prawidłowe przetwarzanie danych osobowych, rozumiane jako ochronę danych przed ich udostępnieniem osobom nieupoważnionym, zmianą lub zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem Ustawy oraz utratą, uszkodzeniem lub zniszczeniem.
2. Do kompetencji Administratora Danych Osobowych należy w szczególności:
   a) Wyznaczenie Administratora Bezpieczeństwa Informacji.
   b) Wyznaczanie Właścicieli zasobów danych osobowych.
   c) Określenie celów i strategii ochrony danych osobowych
   d) Podział zadań i obowiązków związanych z organizacją ochrony danych osobowych.
3. Do obowiązków Administratora Danych Osobowych należy:
   a) Zapewnienie szkoleń dla pracowników w zakresie przepisów o ochronie danych osobowych oraz zagrożeń związanych z ich przetwarzaniem.
   b) Przyjmowanie i zatwierdzanie niezbędnych, wymaganych przez przepisy prawa dokumentów regulujących ochronę danych osobowych w Urzędzie
   c) Nadawanie upoważnień pracownikom Urzędu oraz użytkownikom zewnętrznym do przetwarzania danych osobowych.
   d) Zapewnienie środków finansowych na ochronę fizyczną pomieszczeń, w których przetwarzane są dane osobowe.
   e) Zapewnienie środków finansowych niezbędnych do ochrony danych osobowych przetwarzanych w systemach informatycznych oraz w zbiorach nieinformatycznych.
   f) Zapewnienie środków finansowych na merytoryczne przygotowanie osób odpowiedzialnych za nadzór nad ochroną danych osobowych.
   g) Zapewnienie realizacji obowiązku zgłoszenia i aktualizacji zbiorów danych osobowych do rejestracji GIODO.

§ 8 .

Odpowiedzialność Administratora Bezpieczeństwa Informacji

1 . Administrator Danych Osobowych wyznacza Administratora Bezpieczeństwa Informacji, który nadzoruje przestrzeganie zasad ochrony danych osobowych zarówno w systemach informatycznych, jak również w zbiorach danych osobowych prowadzonych w formie papierowej i elektronicznej **(wzór Zał. Nr 3)**

2 . Do kompetencji Administratora Bezpieczeństwa Informacji należy:

a) Określenie zasad ochrony danych osobowych.

b) Wnioskowanie o ukaranie osób winnych naruszenia przepisów i zasad dotyczących ochrony danych osobowych.

3 . Do obowiązków Administratora Bezpieczeństwa Informacji należy:

a) Nadzór nad wdrożeniem stosownych środków organizacyjnych, technicznych i fizycznych w celu ochrony przetwarzanych danych osobowych.

b) Nadawanie, zmienianie oraz cofanie uprawnień do przetwarzania danych osobowych na wniosek Właścicieli zasobów po akceptacji Administratora Danych Osobowych dla pracowników oraz użytkowników zewnętrznych.

c) Nadzór nad zapewnieniem przez Właścicieli zasobów danych osobowych dostosowania funkcjonalności systemów przetwarzających dane osobowe do wymagań określonych w Rozporządzeniu.

d) Prowadzenie dokumentacji opisującej zastosowaną ochronę danych osobowych (niniejsza Polityka oraz wynikające z niej instrukcje i procedury) w tym zapewnienie ich publikacji i dystrybucji oraz prowadzenia dokumentacji, o której mowa w § 6 w zakresie ABI

e) Zapoznawanie pracowników oraz współpracowników Urzędu Gminy z przepisami i zasadami ochrony danych osobowych oraz informowanie o zagrożeniach związanych z ich przetwarzaniem.

f) Reprezentowanie Gminy w kontaktach z Biurem GIODO.

g) Przygotowywanie zgłoszeń zbiorów danych osobowych do rejestracji w Biurze GIODO.

h) Reagowanie na zgłaszane incydenty związane z naruszeniem ochrony danych osobowych oraz analizowanie ich przyczyn i kierowanie wniosków dotyczących ukarania winnych naruszeń.

i) Sprawdzanie wypełnienia obowiązków technicznych i organizacyjnych związanych z ochroną danych osobowych.

4 . Administrator Bezpieczeństwa Informacji w zakresie realizacji swoich obowiązków, ma prawo żądania od pozostałych osób, bez względu na rangę ich stanowiska udzielania natychmiastowej pomocy w razie stwierdzenia, Że doszło do naruszenia przepisów o ochronie danych osobowych, które może skutkować postawieniem Urzędu albo Administratora Danych popełnienia jednego z przestępstw, wskazanych ww. Rozdziale 8 Ustawy.

5. Sprawowanie nadzoru nad przestrzeganiem zastosowanych środków technicznych i organizacyjnych zapewniających ochronę przetwarzanym danym osobowym odpowiednią do zagrożeń oraz kategorii danych objętych ochroną powinno być głównym zadaniem Administratora Bezpieczeństwa Informacji.

§ 9.

Odpowiedzialność Administratora Systemów Informatycznych

1. Rolę ASI pełni pracownik wyznaczony przez Administratora Danych Osobowych
2. Do kompetencji Administratora Systemów Informatycznych należy:
   a) Zabezpieczenie systemów przetwarzania danych osobowych zgłoszonych ASI, w zależności od kategorii przetwarzanych w tym systemie danych.
   b) Zapewnienie poufności, integralności, dostępności i rozliczalności danych przetwarzanych w systemach informatycznych
3. Do obowiązków Administratora Systemów Informatycznych należy:
   a) Bieżący nadzór oraz zapewnianie optymalnej ciągłości działania systemu informatycznego w tym opracowanie procedur określających zarządzanie systemem informatycznym przetwarzającym dane osobowe.
   b) Reagowanie bez zbędnej zwłoki, w przypadku naruszenia bądź powstania zagrożenia bezpieczeństwa danych osobowych.
   c) Przeciwdziałanie próbom naruszenia bezpieczeństwa danych osobowych
   d) Analizę raportów wszelkich zdarzeń w tym incydentów związanych z bezpieczeństwem systemów przetwarzania danych
   e) Zapewnienie zgodności wszystkich wdrażanych systemów przetwarzania danych osobowych z Ustawą oraz z niniejszą Polityką bezpieczeństwa i Instrukcją Zarządzania Systemem Informatycznym w Urzędzie Gminy Łochów.
   f) Instalację i konfigurację oprogramowania i sprzętu, sieciowego i serwerowego używanego do przetwarzania danych osobowych.
   g) Konfigurację i administrację oprogramowaniem systemowym i sieciowym zabezpieczającym dane osobowe przed nieupoważnionym dostępem.
   h) Nadzór nad czynnościami związanymi ze sprawdzaniem systemu pod kątem obecności szkodliwego oprogramowania.
   i) Nadzór nad systemem komunikacji w sieci komputerowej oraz przesyłaniem danych za pośrednictwem urządzeń teletransmisji.
   j) Nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe.
   k) Przyznawanie na wniosek Właściciela zasobów, za zgodą Administratora Danych i zatwierdzeniu przez Administratora Bezpieczeństwa Informacji ściśle określonych praw dostępu do danych osobowych w danym systemie.

l) Świadczenie pomocy technicznej w ramach oprogramowania a także serwis sprzętu komputerowego będącego na stanie Urzędu Gminy Łochów, służącego do przetwarzania danych osobowych.

m) Diagnozowanie i usuwanie awarii sprzętu komputerowego oraz realizacje umów z firmami świadczącymi usługi pogwarancyjnego sprzętu komputerowego.

n) Wykonywanie i zarządzanie kopiami awaryjnymi oprogramowania systemowego (w tym danych osobowych oraz zasobów umożliwiających ich przetwarzanie) i sieciowego

o) Wykonywanie i przechowywanie dokumentacji o której mowa w § 6 należącej do kompetencji ASI.

p) Nadzór nad wdrożeniem i zarządzanie aplikacjami (przeglądanie, nadawanie i odbieranie uprawnień użytkownikom, itp.), w których przetwarza się dane osobowe.

q) Zatwierdzanie wniosków zgłoszeń do rejestracji zbiorów danych osobowych w części E i F.

r) Umożliwienie przeprowadzenia kontroli systemu informatycznego przez służby Biura Generalnego Inspektora Ochrony Danych Osobowych.

§ 10 .

Odpowiedzialność Właścicieli zasobów danych osobowych.

1 . Administrator Danych Osobowych wyznacza Właścicieli zasobów danych osobowych, którzy są odpowiedzialni za ochronę przypisanych i przetwarzanych zbiorów danych osobowych w podległej komórce organizacyjnej.

2 . Do kompetencji Właścicieli zasobów danych osobowych należy:

a) Określanie celów w jakich mają być przetwarzane dane osobowe, zakresu oraz czasu trwania przetwarzania danych osobowych.

b) Określenie sposobu przetwarzania danych osobowych (czy w systemach informatycznych, czy w zbiorach nieinformatycznych).

c) Ustalenie, czy dane przetwarzane dla określonego celu mają mieć charakter poufny.

3 . Do obowiązków Właścicieli zasobów danych osobowych należy:

a) Zapewnienie podstaw prawnych do przetwarzania danych osobowych od chwili zebrania danych osobowych do chwili ich usunięcia.

b) Zapewnienie aktualności, adekwatności oraz merytorycznej poprawności danych osobowych przetwarzanych w określonym przez nich celu.

c) Realizację obowiązku informowania o przetwarzaniu danych osobowych osób, których dane osobowe są pozyskiwane.

d) Zapewnienie na żądanie uprawnionych osób, udostępnianie informacji o przetwarzanych danych osobowych oraz podmiotach, którym zostały one udostępnione.

e) Zapewnienie złożenia przez pracowników oświadczenia o znajomości przepisów o ochronie danych osobowych oraz zobowiązania do zachowania w tajemnicy danych osobowych oraz informacji na temat zabezpieczania danych osobowych.

f) Zapewnienie uzyskania przez pracowników przetwarzających dane osobowe, formalnego upoważnienia do przetwarzania danych osobowych.

g) W przypadku utworzenia nowego zbioru danych osobowych ustalenie, kogo dotyczą dane osobowe, jaki jest ich zakres (np. imię i nazwisko, adres zamieszkania, NIP, PESEL itp.), cel przetwarzania oraz komu dane osobowe mają być udostępniane. Wszystkie te informacje powinny zostać przekazane do Administratora Bezpieczeństwa Informacji oraz Administratora Systemu Informatycznego.

h) Przygotowanie wniosku do rejestracji/zmiany zbioru do GIODO w części A-D

i) Wnioskowanie do Administratora Danych Osobowych o nadanie upoważnień dla pracowników podległej komórki organizacyjnej.

j) Prowadzenie ewidencji, o której mowa w § 6 w odniesieniu do Właścicieli zasobów.

§ 11 .

Odpowiedzialność pracowników i użytkowników systemu

1 . W celu osiągnięcia i utrzymania wysokiego poziomu bezpieczeństwa przetwarzania danych osobowych konieczne jest zaangażowanie ze strony każdego pracownika i użytkownika zewnętrznego w zakresie ochrony danych osobowych.

2 . Pracownicy Urzędu Gminy oraz użytkownicy zewnętrzni są zobowiązani do informowania o wszelkich podejrzeniach naruszenia lub zauważonych naruszeniach oraz słabościach systemu przetwarzającego dane osobowe bezpośrednio do Administratora Bezpieczeństwa Informacji.

3 . Pracownicy / użytkownicy zewnętrzni są zobowiązani do:

a) Postępowania zgodnie z Polityką.

b) Zachowania w tajemnicy danych osobowych oraz informacji o sposobach ich zabezpieczenia.

c) Ochrony danych osobowych oraz środków przetwarzających dane osobowe przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem.

d) Wykonywania konkretnych działań i procesów w celu zapewnienia ochrony danych osobowych.

4 . Pracownicy / użytkownicy zewnętrzni powinni mieć świadomość możliwości zaistnienia sytuacji naruszenia ochrony danych osobowych. W tym celu powinni:

a) Przestrzegać procedur związanych z otwieraniem i zamykaniem pomieszczeń, a także z wejściem do obszarów przetwarzania danych osobowych osób nieupoważnionych.

b) Informować Administratora Bezpieczeństwa Informacji lub pracowników ochrony o podejrzanych osobach

c) Pracownicy / użytkownicy zewnętrzni powinni na podstawie dokonanej identyfikacji ewentualnych zagrożeń, przedkładać Administratorowi Bezpieczeństwa Informacji projekty i propozycje nowych rozwiązań, których celem jest zwiększenie poziomu ochrony danych osobowych.

§ 12 .

Sankcje za naruszenie zasad ochrony danych osobowych

1. Naruszenie zasad ochrony danych osobowych przez pracownika / użytkownika zewnętrznego może skutkować postawieniem mu zarzutu popełnienia, jednego z przestępstw określonych w Rozdziale 8 Ustawy lub przestępstwa określonego w art. 266 Kodeksu Karnego.
2. Zgodnie z art. 100 § 2 pkt 5 Kodeksu Pracy, pracownik jest obowiązany przestrzegać tajemnicy określonej w odrębnych przepisach. Dane osobowe, którym urząd nadaje charakter poufny mają charakter takiej tajemnicy, a jej ujawnienie w zależności od zakresu ujawnionych danych osobowych oraz nastawienia pracownika dopuszczającego się nieuprawnionego ujawnienia danych, może mieć charakter naruszenia lub ciężkiego naruszenia obowiązków pracowniczych.
3. Pracownik dopuszczający się nieuprawnionego ujawnienia lub wykorzystania danych osobowych w sposób sprzecznych z ich przeznaczeniem (np. wykorzystania danych osobowych do celów prywatnych) czy też ich przetwarzania w sposób niezgodny z przyjętymi w Urzędzie procedurami może zostać ukarany karą upomnienia lub karą nagany.
4. W razie ciężkiego naruszenia obowiązku zachowania danych osobowych w tajemnicy lub przetwarzania ich w sposób rażąco sprzeczny z przyjętymi zasadami i procedurami, Administrator Danych Osobowych może rozwiązać bez wypowiedzenia umowę o pracę z winy pracownika.
5. Sankcje dotyczące ujawnienia poufnych danych osobowych stosuje się analogicznie do ujawnienia przez pracownika informacji dotyczących zabezpieczenia danych osobowych w Urzędzie.

§ 13 .

Szkolenia w zakresie ochrony danych osobowych

1. Przed rozpoczęciem przetwarzania danych osobowych pracownik powinien zostać przeszkolony przez Administratora Bezpieczeństwa Informacji. Szkolenie powinno obejmować następujące zagadnienia:
   a) Przepisy o ochronie danych osobowych.
   b) Zasady przetwarzania danych osobowych.
   c) Procedury dotyczące bezpiecznego przetwarzania danych osobowych w systemach informatycznych .
   d) Zasady użytkowania urządzeń i systemów informatycznych służących do przetwarzania danych osobowych.
   e) Zagrożenia na jakie może być narażone przetwarzanie danych osobowych, a w szczególności te związane z przetwarzaniem danych osobowych w systemach informatycznych.
   f) Zasady dostępu do pomieszczeń, w których przetwarzane są dane osobowe.
   g) Sposób postępowania w przypadku naruszenia ochrony danych osobowych lub systemu informatycznego.
   h) Odpowiedzialność z tytułu naruszenia ochrony danych osobowych.
2. Szkolenia powinny być powtarzane okresowo lub na żądanie, gdy zaistnieje taka potrzeba.

3. Użytkownicy reprezentujący osoby trzecie (tam, gdzie jest to wskazane) powinni przechodzić przeszkolenie w zakresie:
   a) Odpowiednich zasad wynikających z Polityki
   b) Odpowiednich procedur dotyczących bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych.
   c) Poprawnego użytkowania urządzeń i systemów informatycznych służących do przetwarzania danych osobowych.

§ 14.

Wymiana informacji dotyczących danych osobowych

1. Pracownicy Urzędu Gminy oraz użytkownicy zewnętrzni w celu ochrony wymienianych informacji dotyczących danych osobowych powinni podczas przetwarzania uwzględniać następujące zasady:
   a) Wykorzystywanie technik kryptograficznych do ochrony poufności, integralności i rozliczalności danych osobowych przesyłanych publicznymi sieciami telekomunikacyjnymi.
   b) Ochrona wymienianych danych osobowych przed przechwyceniem, kopiowaniem, modyfikacją, błędnym wyborem drogi komunikacji i zniszczeniem.
   c) Zabezpieczenia i ograniczenia związane z możliwościami przekazywania wiadomości za pomocą środków komunikacji, np. automatyczne przekazywania poczty elektronicznej na zewnątrz.
   d) Zakaz pozostawiania informacji zawierających dane osobowe przy urządzeniach drukujących, np. kopiarkach, drukarkach, faksach, do których mogą mieć dostęp osoby nieupoważnione.
   e) Upewnienie się przed przekazaniem danych osobowych, czy rozmówca jest osobą upoważnioną do uzyskania określonych danych osobowych.
   f) Zachowania szczególnej ostrożności w trakcie rozmów telefonicznych, unikając podsłuchania danych osobowych przez osoby nieupoważnione.
   g) Nie pozostawianie wiadomości zawierających dane osobowe w automatycznych sekretarkach.
   h) Właściwe postępowanie z faksami i fotokopiarkami, ponieważ mają one podręczną pamięć i przechowują w niej strony zawierające np. dane osobowe na wypadek błędów transmisji.
2. Transport danych osobowych w formie elektronicznej i papierowej pomiędzy obszarami, w których są przetwarzane dane osobowe powinien być prowadzony przez osoby upoważnione w sposób ograniczający możliwość ich pozyskanie i odczyt przez osoby nieupoważnione.

§ 15.

Przetwarzanie danych osobowych w obszarach bezpiecznych

1. Dane osobowe w Urzędzie Gminy mogą być przetwarzane wyłącznie w pomieszczeniach przetwarzania danych osobowych.
2. Na pomieszczenia przetwarzania danych osobowych składają się pomieszczenia biurowe oraz części pomieszczeń, gdzie Urząd Miejski prowadzi działalność.

a) Serwerownia.

b) Pomieszczenia biurowe, w których zlokalizowane są stacje robocze.

c) Pomieszczenia, w których przechowywane są sprawne oraz uszkodzone elektroniczne nośniki informacji, kopie zapasowe.

d) Pomieszczenia, w których przechowuje się dokumenty źródłowe oraz wydruki z systemu informatycznego.

e) Pomieszczenia, w których zlokalizowane są zbiory nieinformatyczne.

3 . Przebywanie wewnątrz obszarów, o których mowa w ust. 3, osób nieuprawnionych do przetwarzania danych osobowych jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania tych danych lub za zgodą Właściciela zasobów danych osobowych.

4 . Budynki lub pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane podczas nieobecności osób upoważnionych do przetwarzania danych osobowych, w sposób ograniczający możliwość dostęp do nich osobom nieupoważnionym.

5 . W celu ograniczenia dostępu osób nieupoważnionych do pomieszczeń , w których zlokalizowano przetwarzanie danych osobowych, należy zapewnić:

a) Jasne określenie granic obszaru przetwarzania danych osobowych oraz umiejscowienie dostosowane do wymagań bezpieczeństwa w odniesieniu do aktywów znajdujących się wewnątrz obszaru.

b) Jednolite granice budynków lub pomieszczeń, gdzie zlokalizowano środki przetwarzania danych osobowych (tzn. aby granice nie miały luk lub punktów, przez które łatwo się włamać).

c) Ściany zewnętrzne pomieszczeń solidnej konstrukcji oraz wszystkie drzwi zewnętrzne odpowiednio zabezpieczone przed nieautoryzowanym dostępem za pomocą mechanizmów zabezpieczeń, np. alarmów, zamków itp.

d) Zamykanie drzwi i okien w pomieszczeniach pozostawianych bez dozoru oraz należy rozważyć zastosowanie mechanizmów zewnętrznej ochrony dla okien, szczególnie tych położonych na poziomie gruntu.

e) System wykrywania włamań zgodnych z normami w strefach bezpieczeństwa oraz regularne jego testowanie.

6 . Obszary bezpieczne powinny być odpowiednio zabezpieczone przed skutkami pożaru.

7 . Ochrona obszarów bezpiecznych powinna być zapewniona poprzez odpowiednie fizyczne zabezpieczenia wejścia zapewniające, że tylko osoby upoważnione mogą uzyskać dostęp, w tym celu należy zapewnić:

a) Nadzorowanie pobytu osób nie będących pracownikami Urzędu Gminy w obszarach bezpiecznych, chyba że ich dostęp został wcześniej zaakceptowany.

b) Kontrolowanie i ograniczenie dostępu do obszarów, gdzie są przetwarzane dane osobowe tylko dla uprawnionego personelu.

c) Regularne przeglądanie praw dostępu do obszarów bezpiecznych i jeśli zachodzi potrzeba, uaktualnianie ich lub odbieranie.

8. Przetwarzanie danych osobowych jest zakazane w tych pomieszczeniach , w których osoby trzecie wykonują prace techniczne.

9. Nośniki elektroniczne zawierające dane osobowe powinny być ewidencjonowane i należy przechowywać w zamykanych szafach , które znajdują się w obszarach przetwarzania danych osobowych.

10. Każdorazowe uchybienie zabezpieczeń fizycznych chroniących dane osobowe powinno być zgłaszane do Administratora Bezpieczeństwa Informacji.

§ 16 .

Dopuszczenie osób do przetwarzania danych osobowych

1. Przetwarzanie danych osobowych jest możliwe wyłącznie po uzyskaniu przez pracownika / użytkownika zewnętrznego formalnego upoważnienia do przetwarzania danych osobowych zaakceptowanego przez Administratora Danych Osobowych i wystawianego przez Administratora Bezpieczeństwa Informacji, w tym celu przełożony pracownika / użytkownika zewnętrznego przed dopuszczeniem pracownika do pracy przy przetwarzaniu danych osobowych:
   a) Zapoznaje pracownika / użytkownika zewnętrznego z przepisami dotyczącymi ochrony danych osobowych oraz uregulowaniami wewnętrznymi obowiązującymi w tym zakresie w Urzędzie.
   b) Przyjmuje od pracownika / użytkownika zewnętrznego podpisane oświadczenie o zachowaniu danych osobowych i sposobów ich zabezpieczania w tajemnicy, przetwarzania danych osobowych zgodnie z przepisami oraz oświadczenia o znajomości niniejszego dokumentu a także o znajomości „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Łochów", którego wzór stanowi **(wzór Zał. Nr 4)** niniejszej Polityki.
   c) Wnioskuje do Administratora Bezpieczeństwa Informacji o formalne upoważnienie **(wzór zał. Nr 5)** pracownika do przetwarzania danych osobowych
2. Oświadczenia i upoważnienia, o których mowa w ust. 1 przechowuje się w aktach osobowych pracownika.
3. Przełożony pracownika / użytkownika zewnętrznego jest zobowiązany niezwłocznie po ustaniu potrzeby przetwarzania danych osobowych przez pracownika / użytkownika zewnętrznego złożyć rezygnację do Administratora Bezpieczeństwa Informacji dotyczącą jego dostępu do danych osobowych.

§ 17 .

Ewidencja osób upoważnionych do przetwarzania danych osobowych

1. Osoby upoważnione do przetwarzania danych osobowych powinny być wpisywane do ewidencji. Ewidencja osób upoważnionych do przetwarzania danych osobowych (ewidencja) powinna być prowadzona przez Administratora Bezpieczeństwa Informacji.
2. Jakakolwiek zmiana w zakresie informacji zawartych w ewidencji powinna podlegać natychmiastowemu odnotowaniu.

3. Właściciele zasobów danych osobowych, przełożeni pracowników / użytkowników zewnętrznych odpowiadają za natychmiastowe zgłoszenie do Administratora Bezpieczeństwa Informacji osób, które utraciły uprawnienia dostępu do danych osobowych.
4. Administrator Bezpieczeństwa Informacji w oparciu o informacje, o których mowa w ust. 3 powinien podjąć działania, których celem jest uniemożliwienie tym osobom dostępu do danych osobowych i wyrejestrować z ewidencji, o której mowa w ust. 1.
5. Elektroniczne nośniki informacji, na których gromadzone są wykazy zawierające ewidencję osób upoważnionych do przetwarzania danych osobowych powinny być przechowywane w szafie zamykanej, do której ma dostęp Administrator Bezpieczeństwa Informacji lub osoba przez niego upoważniona.

§ 18 .

Dostęp zdalny

1. Zastosowane przez Urząd rozwiązania techniczne umożliwiające dostęp zdalny do danych osobowych powinny zapewniać integralność, poufność i rozliczalność przetwarzanych danych osobowych oraz ochronę kryptograficzną wobec danych służących do uwierzytelnia a przesyłanych publicznymi łączami telekomunikacyjnymi.
2. Nadawanie uprawnień w celu dostępu zdalnego do systemów informatycznych przetwarzających dane osobowe realizowane jest przez Administratora Systemów Informatycznych po spełnieniu wymagań określonych w ust. 1 oraz po uzyskaniu akceptacji Administratora Danych Osobowych
3. Dostęp do systemów informatycznych dla użytkowników zewnętrznych powinien być monitorowany pod kątem bezpieczeństwa przez Administratorów Systemów Informatycznych w celu zapewnienia poufności, rozliczalności i integralności danych osobowych.

§ 19 .

Rejestracja zbiorów danych osobowych

1. Upoważnieni pracownicy są zobowiązani do wnioskowania Administratorowi Bezpieczeństwa Informacji zamiaru utworzenia nowego zbioru danych osobowych wraz z wskazaniem podstawy przetwarzania danych, uzasadnieniem celowości, zakresu i sposobu zbierania danych osobowych.
2. Administratora Bezpieczeństwa Informacji weryfikuje wniosek o utworzenie nowego zbioru danych osobowych oraz analizuje nowy zbiór danych pod kątem obowiązku zgłoszenia zasobu, jako zbioru danych do rejestracji w GIODO.
3. W sytuacji, jeżeli rejestracja nowo powstałego zbioru lub zbioru wymagającego aktualizacji danych osobowych jest ustawowo wymagana, Właściciel zasobu przygotowuje projekt zgłoszenia zbioru danych osobowych / zgłoszenia zmian do rejestracji / zmiany w GIODO . w części A-D
4. Zgłoszenie / zmiana wniosku zgłoszenia zbioru do rejestracji przez GIODO w części E – F jest przygotowywana przez Administratora Systemów Informatycznych odpowiedzialnego za odpowiednie zabezpieczenie danych w systemie informatycznym Urzędu.

5. Administrator Bezpieczeństwa Informacji sprawdza opisane zgłoszeniu rejestracyjnym warunki techniczne o organizacyjne dotyczące zabezpieczeń w systemie informatycznym, a w przypadku niewystarczającego poziomu zabezpieczeń występuje z wnioskiem do Administratora Danych Osobowych o podniesienie poziomu tych zabezpieczeń.
6. Sprawdzony przez Administratora Bezpieczeństwa Informacji projekt zgłoszenia zbioru danych osobowych do rejestracji w GIODO jest przedstawiany Administratorowi Danych Osobowych do podpisu.
7. Administrator Danych Osobowych zgłasza wniosek o rejestrację zbioru danych osobowych do GIODO i wyznacza Właściciela zasobów danych osobowych dla zarejestrowanego zbioru danych osobowych.
8. Administrator Bezpieczeństwa Informacji uzupełnia Politykę, dokumenty z nią powiązane oraz pozostałe dokumenty obowiązujące w Urzędzie w zakresie ochrony danych osobowych informacje na temat nowego zbioru.
9. Pismo jest wysyłane przez Administratora Bezpieczeństwa Informacji do GIODO.

§ 20 .

Udostępnianie danych osobowych

1. Dane osobowe mogą być udostępniane podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa, osobom, których dotyczą oraz w szczególnych przypadkach na podstawie art. 29 ust. 2 Ustawy.
2. Udostępnianie danych osobowych osobie nieupoważnionej do przetwarzania danych osobowych może nastąpić wyłącznie za zgodą Właściciela zasobów danych osobowych. Zgoda może dotyczyć również udostępniania danych osobowych w przyszłości. Zarówno wniosek jak i zgoda powinny być wystosowane z zachowaniem formy pisemnej
3. Udostępniając dane osobowe należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
4. Na pisemny wniosek pochodzący od osoby, której dane dotyczą, informacje o osobie powinny być udzielone w terminie 30 dni od daty złożenia wniosku.
5. Za przygotowanie danych osobowych do udostępnienia w zakresie wskazanym we wniosku jest odpowiedzialny Właściciel zasobów danych osobowych.
6. Odpowiedź na wniosek o udostępnienie danych osobowych przed wysłaniem jest akceptowana i parafowana przez Właściciela zasobów danych osobowych oraz Administratora Bezpieczeństwa Informacji a następnie podpisywana przez Administratora Danych Osobowych.
7. W przypadku odpowiedzi na wniosek, o którym mowa w ust. 2, nie od osoby, której dane dotyczą, Właściciel zasobów danych osobowych przekazuje kopię odpowiedzi do Administratora Bezpieczeństwa Informacji.
8. Informacje zawierające dane osobowe są przekazywane uprawnionym podmiotom lub osobom za potwierdzeniem odbioru, np. w następujący sposób:

a) Listem poleconym za pokwitowaniem odbioru.

b) Teletransmisji danych zgodnie z zasadami wymiany informacji opisanymi w § 14 niniejszej Polityki.

c) Innym bezpiecznym, określonym wymogiem prawnym lub umową.

d) Informacja o udostępnieniu danych osobowych podlega odnotowaniu jeśli dane osobowe udostępniane są ze zbioru danych osobowych. W takim przypadku, odnotowaniu podlega informacja o zakresie danych podlegających udostępnieniu, dacie udostępnienia odbiorcy, celu udostępnienia oraz danych osób, które ze strony Urzędu udostępniły dane osobowe. Nie dotyczy to sytuacji, gdy przepisy prawa zezwalają na zbieranie danych osobowych bez konieczności ujawniania adresata danych.

§ 21 .

Powierzanie przetwarzania danych osobowych

1 . Powierzenie przetwarzania danych osobowych występuje wówczas, gdy podmioty zewnętrzne współpracujące z Urzędem mają dostęp do danych osobowych przetwarzanych przez Urząd.

2 . Wskazane w ust. 1 powierzenie przetwarzania danych osobowych może się odbywać wyłącznie w trybie przewidzianym w art. 31 Ustawy poprzez zawarcie na piśmie umowy powierzenia przetwarzania danych osobowych, pomiędzy Urzędem a danym podmiotem, któremu zleca się czynności związane z przetwarzaniem danych osobowych lub uwzględnienie kwestii powierzenia w umowach.

3 . W sytuacji powierzenia przetwarzania danych osobowych podmiotowi zewnętrznemu, w umowie powierzenia przetwarzania danych osobowych określa się przede wszystkim:

a) Cel i zakres przetwarzania danych osobowych.

b) Obowiązek zachowania w tajemnicy danych osobowych oraz informacji o zabezpieczeniach tych danych.

c) Konsekwencje prawne i kary finansowe wynikające z niestosowania się do warunków umowy (z punktu widzenia ochrony danych osobowych).

d) Wymagania bezpieczeństwa dla procesu przetwarzania danych osobowych.

4 . Zalecane jest aby w umowach powierzenia przetwarzania danych osobowych oraz w umowach, na podstawie których dochodzi do wymiany informacji uwzględnić następujące elementy:

a) Definicję informacji, która ma być chroniona.

b) Spodziewany czas trwania umowy, włączając w to przypadki, w których obowiązek zachowania poufności może być bezterminowy.

c) Wymagane działania w momencie zakończenia umowy.

d) Odpowiedzialność i działania sygnatariuszy podejmowane w celu uniknięcia nieupoważnionego ujawnienia informacji.

e) Własność informacji.

f) Dozwolone użycie danych osobowych oraz praw sygnatariusza do jej użycia.

g) Prawa do audytu i monitorowania działań związanych z ochroną danych osobowych.

h) Proces powiadamiania i raportowania nieuprawnionego ujawnienia lub naruszenia poufności i integralności danych osobowych.

i) Zasady zwrotu lub niszczenia danych osobowych przy zakończeniu umowy.

j) Działania podejmowane w przypadku naruszenia warunków umowy.

5 . Właściciele zasobów danych osobowych są zobowiązani do wnioskowania do Administratora Bezpieczeństwa Informacji o przygotowanie projektu umowy powierzenia danych osobowych dla zasobów danych osobowych, za które są odpowiedzialni.

6 . Projekt umowy powierzenia przetwarzania danych osobowych innemu podmiotowi przygotowuje zespół powołany przez Administratora Bezpieczeństwa Informacji.

7 . Powierzenie przetwarzania danych osobowych poza granice Rzeczpospolitej Polskiej wymaga zgody Administratora Danych Osobowych i odbywa się po sprawdzeniu wymagań prawnych obowiązujących w tym zakresie.

§ 22 .

Postępowanie w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych

1 . Poniższe postanowienia mają zastosowanie zarówno w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych przetwarzanych w systemach informatycznych, jak i w zbiorach nieinformatycznych.

2 . Przed przystąpieniem do pracy pracownicy / użytkownicy zewnętrzni zobowiązani są dokonać sprawdzenia stanu urządzeń informatycznych oraz oględzin swojego stanowiska pracy, w tym zwrócić szczególną uwagę, czy nie zaszły okoliczności wskazujące na naruszenie lub próby naruszenia ochrony danych osobowych.

3 . Za okoliczności, które uznaje się za naruszenie lub podejrzenie naruszenia ochrony systemu przetwarzającego dane osobowe, uważa się w szczególności:

a) Nieuprawniony dostęp lub próbę dostępu do danych osobowych lub pomieszczeń, w których się one znajdują.

b) Nieuprawnione naruszenie lub próby naruszenia poufności, integralności i rozliczalności danych i systemu.

c) Niezamierzoną zmianę lub utratę danych zapisanych na kopiach zapasowych.

d) Nieuprawniony dostęp do danych osobowych (sygnał o nielegalnym logowaniu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu).

e) Udostępnienie osobom nieupoważnionym danych osobowych lub ich części.

f) Inny stan systemu informatycznego lub pomieszczeń, niż pozostawiony przez użytkownika po zakończeniu pracy.

g) Wydarzenia losowe, obniżające poziom ochrony systemu (np. brak zasilania lub pożar).

h) Kradzież sprzętu informatycznego lub nośników zewnętrznych zawierających dane osobowe (np. wydruków komputerowych, dyskietek, płyt CD-ROM, dysków twardych, pamięci zewnętrznych, itp.).

4. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych pracownicy zobowiązani są do bezzwłocznego powiadomienia o tym fakcie Administratora Bezpieczeństwa Informacji.

5. Do czasu przybycia Administratora Bezpieczeństwa Informacji, zgłaszający:
   a) Powstrzymuje się od rozpoczęcia lub kontynuowania pracy, jak również od podejmowania jakichkolwiek czynności, mogących spowodować zatarcie śladów naruszenia bądź innych dowodów.
   b) Zabezpiecza elementy systemu informatycznego lub kartotek, przede wszystkim poprzez uniemożliwienie dostępu do nich osobom nieupoważnionym.
   c) Podejmuje, stosownie do zaistniałej sytuacji, wszelkie niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych.
   d) Wykonuje polecenia Administratora Bezpieczeństwa Informacji.

6. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych Administrator Bezpieczeństwa Informacji, po przybyciu na miejsce:
   a) Ocenia zastałą sytuację, biorąc pod uwagę w szczególności stan pomieszczeń, w których przetwarzane są dane osobowe oraz stan urządzeń, a także szacuje wielkość negatywnych następstw incydentu.
   b) Wysłuchuje relacji osoby, która dokonała powiadomienia oraz innych osób związanych z incydentem.
   c) Podejmuje decyzje o toku dalszego postępowania, stosownie do zakresu naruszenia lub zasadności podejrzenia naruszenia ochrony danych osobowych.

7. Administrator Bezpieczeństwa Informacji sporządza raport z przebiegu zdarzenia, w którym powinny się znaleźć w szczególności informacje o:
   a) Dacie i godzinie powiadomienia.
   b) Godzinie pojawienia się w pomieszczeniach, w których przetwarzane są dane.
   c) Sytuacji, jaką zastał.
   d) Podjętych działaniach i ich uzasadnieniu.
   e) Stanie systemu po podjęciu działań naprawczych.
   f) Wnioskach w sprawie ograniczenia możliwości ponownego wystąpienia naruszenia ochrony danych osobowych.

8. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych, użytkownik może kontynuować pracę dopiero po otrzymaniu pozwolenia od Administratora Bezpieczeństwa Informacji.

9. W przypadku, gdy naruszenie ochrony danych osobowych jest wynikiem uchybienia obowiązującej w Urzędzie dyscypliny pracy, Administrator Bezpieczeństwa Informacji wyjaśnia wszystkie okoliczności incydentu i podejmuje stosowne działania wobec osób, które dopuściły się wskazanego naruszenia.

10. Po zakończeniu czynności naprawczych system powinien utrzymać poziom ochrony nie niższy niż przed wystąpieniem incydentu związanego z naruszeniem ochrony danych osobowych.

§ 23 .

Wykaz zbiorów danych osobowych

1 . Urząd Miejski w Łochowie - reprezentowana przez Burmistrza Łochowa - jest administratorem danych osobowych wymienionych „Ewidencji zbiorów danych osobowych", prowadzonej przez Administratora Bezpieczeństwa Informacji

2 . Dane osobowe gromadzone we wskazanych zbiorach są przetwarzane w systemach informatycznych oraz w kartotekach ewidencyjnych, które są zlokalizowane w pomieszczeniach lub części pomieszczeń przetwarzania danych osobowych.

3 . Administrator Systemów Informatycznych w oparciu o informacje uzyskane od Właścicieli zasobów, prowadzi wykaz systemów i aplikacji zastosowanych do przetwarzania danych osobowych.

§ 24 .

Opis struktury zbiorów danych osobowych

1 . Opis struktury zbiorów danych osobowych prowadzi Administrator Systemu Informatycznego.

2 . Zakresy danych osobowych przetwarzanych w poszczególnych zbiorach danych osobowych są ustalone w oparciu o strukturę zbiorów danych osobowych prowadzonych w systemach informatycznych oraz powiązania pól informacyjnych utworzonych w tych systemach.

3 . Aktualny opis struktury ww. zbiorów danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi powinien być prowadzony przez Administratora Systemów Informatycznych.

§ 25 .

Sposób przepływu danych pomiędzy poszczególnymi systemami

Administratorów Systemów Informatycznych, prowadzi dokumentację systemów informatycznych, zawierającą opis współpracy pomiędzy różnymi systemami informatycznymi oraz sposób przepływu danych pomiędzy systemami, w których te dane są przetwarzane.

§ 26 .

Zasady ochrony danych osobowych w zbiorach nieinformatycznych

1 . Zbiory nieinformatyczne powinny być odpowiednio zabezpieczone przed nieuprawnionym dostępem i zniszczeniem.

2 . Dokumenty i wydruki, zawierające dane osobowe, należy przechowywać w zamykanych pomieszczeniach, do których dostęp mają jedynie uprawnione osoby.

3 . Na czas nie użytkowania, dokumenty i wydruki zawierające dane osobowe powinny być zamykane w szafach biurowych lub zamykanych szufladach.

4. Wydruki robocze, błędne lub zdezaktualizowane powinny być niezwłocznie niszczone przy użyciu niszczarki do papieru lub w inny sposób zapewniający skuteczne ich usunięcie lub zanonimizowane

5. Dla udokumentowania czynności dokonywanych w celu likwidacji zbiorów archiwalnych, powinny być stosowane odpowiednie przepisy dot. zasad archiwizacji i brakowania dokumentacji Urzędu.

§ 27.

Postanowienia końcowe

1. Niezależnie od odpowiedzialności określonej w przepisach prawa powszechnie obowiązującego, naruszenie zasad określonych w niniejszej Polityce może być podstawą rozwiązania stosunku pracy bez wypowiedzenia z osobą, która dopuściła się naruszenia.

2. W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r., o ochronie danych osobowych (t.j. Dz.U. z 2002 r., Nr 101, poz. 926 z późn. zm.) oraz przepisy wykonawcze do tej Ustawy.

Elektronicznie podpisany przez:
URSZULA KALINOWSKA
Data: 2013.12.11 09:05:06
Odcisk palca certyfikatu: 8b49 476b e52
c2b7 6b78 8b40 2bb0 5ab8 36ca 911f

ZAŁĄCZNIK 2 do Zarządzenia Nr 74/2013
Burmistrza Łochowa
z dnia 03.12.2013
w sprawie polityki bezpieczeństwa przetwarzania
danych osobowych w Urzędzie Miejskim w Łochowie

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych Urzędu Miejskiego w Łochowie.

Dokumenty powiązane:

Polityka bezpieczeństwa przetwarzania danych osobowych Urzędu Miejskiego w Łochowie.

§ 1 .

Postanowienia ogólne

1 . Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych Urzędu Miejskiego w Łochowie, zwana dalej „Instrukcją" określa zasady, tryb postępowania i zalecenia Administratora Danych, które muszą być stosowane przez osoby przez niego upoważnione do przetwarzania danych osobowych w systemach informatycznych.

2 . Instrukcja została opracowana zgodnie z wymogami § 5 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).

3 . Podstawowymi celami zabezpieczeń systemów informatycznych służących do przetwarzania danych osobowych, jest zapewnienie jak najwyższego poziomu bezpieczeństwa przetwarzanych danych osobowych w systemach informatycznych.

4 . Za priorytet uznano zagwarantowanie zgromadzonym danym osobowym, przez cały okres ich przetwarzania w systemach, charakteru poufnego wraz z zachowaniem ich integralności i rozliczalności.

5 . Administrator Bezpieczeństwa Informacji powinien posiadać stosowne uprawnienia w nadzorowanych systemach informatycznych, gwarantujące skuteczne wykonywanie zadań z zakresu nadzoru wszędzie tam, gdzie jest to możliwe. Nie oznacza to automatycznego prawa dostępu do danych osobowych przetwarzanych w tych systemach.

§ 2 .

Obowiązki w zakresie ochrony danych osobowych

1 . Do obowiązków osób zaangażowanych w przetwarzanie danych osobowych w systemach informatycznych należy:

a) Podejmowanie współpracy przy ustaleniu przyczyn naruszenia ochrony danych osobowych oraz usuwania skutków tych naruszeń, w tym zapobieganie ich ewentualnemu ponownemu wystąpieniu.

b) Przetwarzanie danych osobowych wyłącznie w celach określonych przez swoich przełożonych.

2 . Do kompetencji osób zarządzających pracownikami należy w szczególności wnioskowanie do Administratora Danych Osobowych dla bezpośrednio podległych pracowników o nadanie, zmianę lub cofnięcie uprawnień do systemów informatycznych, w których są przetwarzane dane osobowe.

3 . Użytkownicy powinni podlegać okresowym szkoleniom, stosownie do potrzeb wynikających ze zmian w systemie informatycznym (wymiana sprzętu na nowszej generacji, zmiana oprogramowania) oraz w związku ze zmianą przepisów o ochronie danych osobowych lub zmianą wewnętrznych regulacji.

§ 3 .

Obowiązki Administratora Bezpieczeństwa Informacji

1 . Do obowiązków Administratora Bezpieczeństwa Informacji w zakresie ochrony danych osobowych przetwarzanych w systemach informatycznych należy w szczególności:

a) Nadzór nad stosowaniem środków ochrony.

b) Nadzór nad przestrzeganiem przez Administratora Systemów Informatycznych i użytkowników systemu - procedur bezpieczeństwa.

c) Wskazywanie zagrożeń oraz reagowanie na naruszenia ochrony danych osobowych i usuwanie ich skutków.

d) Prowadzenie ewidencji użytkowników systemów informatycznych, w których przetwarzane są dane osobowe, stanowiącej część ewidencji osób upoważnionych do przetwarzania danych osobowych oraz wszelkiej dokumentacji opisującej sposób realizacji i stopień ochrony danych osobowych w Urzędzie.

e) Kontrolowanie nadanych w systemach informatycznych uprawnień do przetwarzania danych osobowych pod kątem ich zgodności z wpisami umieszczonymi w ewidencji osób upoważnionych do przetwarzania danych osobowych.

f) Prowadzenie szkoleń dla użytkowników w zakresie stosowanych w systemach informatycznych środków ochrony danych osobowych.

g) Uzgadnianie z Administratorem Systemów Informatycznych szczególnych procedur regulujących wykonywanie czynności w systemach lub aplikacjach służących do przetwarzania danych osobowych.

h) Zapewnienie doradztwa w zakresie przestrzegania przez użytkowników zewnętrznych zasad ochrony danych osobowych przyjętych w Urzędzie.

§ 4 .

Obowiązki Administratora Systemów Informatycznych

1 . Do obowiązków Administratora Systemów Informatycznych w zakresie ochrony danych osobowych przetwarzanych w systemach informatycznych należy w szczególności:

a) Realizacja zadań określonych w §8, §24 i §25 Polityki bezpieczeństwa przetwarzania danych osobowych Urzędu Miejskiego w Łochowie

b) Operacyjne zarządzanie systemami informatycznymi w sposób zapewniający ochronę danych osobowych w nich przetwarzanych.

c) Przestrzeganie opracowanych dla systemu procedur operacyjnych i bezpieczeństwa.

d) Kontrola przepływu informacji pomiędzy systemem informatycznym a siecią publiczną oraz kontrola działań inicjowanych z sieci publicznej a systemem informatycznym.

e) Zarządzanie stosowanymi w systemach informatycznym środkami uwierzytelnienia, w tym rejestrowanie i wyrejestrowywanie użytkowników oraz dokonywanie zmiany uprawnień na podstawie zaakceptowanych wniosków przez osobę do tego upoważnioną.

f) Utrzymanie systemu w należytej sprawności technicznej.

g) Regularne tworzenie kopii zapasowych zasobów danych osobowych oraz programów służących do ich przetwarzania oraz okresowe sprawdzanie poprawności wykonania kopii zapasowych.

h) Wykonywanie lub nadzór nad wykonywaniem okresowych przeglądów i konserwacji, zgodnie z odrębnymi procedurami, sprzętu IT, systemów informatycznych, aplikacji oraz elektronicznych nośników informacji, na których zapisane są dane osobowe.

§ 5 .

Obowiązki Właścicieli zasobów danych osobowych

1 . Do obowiązków Właścicieli zasobów danych osobowych w zakresie ochrony danych osobowych przetwarzanych w systemach informatycznych należy w szczególności:

a) Zapewnienie właściwego poziomu ochrony danych osobowych w systemach, dla danych za które są odpowiedzialni.

b) Informowanie Administratora Bezpieczeństwa Informacji o zmianie celu przetwarzania danych osobowych w systemie lub poszerzeniu zakresu zbieranych danych osobowych.

c) Udostępnianie danych osobowych wyłącznie osobom upoważnionym lub uprawnionym do ich uzyskania

§ 6 .

Obowiązki użytkowników

1 . Do obowiązków użytkowników systemu informatycznego w zakresie ochrony danych osobowych w systemach informatycznych należy w szczególności

a) Przestrzeganie opracowanych dla systemu zasad przetwarzania danych osobowych.

b) Przestrzeganie opracowanych dla systemu procedur operacyjnych i bezpieczeństwa.

c) Uniemożliwienie dostępu lub podglądu danych osobowych w systemie dla osób nieupoważnionych.

d) Informowanie Administratora Bezpieczeństwa Informacji o wszelkich naruszeniach, podejrzeniach naruszenia i nieprawidłowościach w sposobie przetwarzania i ochrony danych osobowych.

e) Wykonywania bez zbędnej zwłoki poleceń Administratora Bezpieczeństwa Informacji w zakresie ochrony danych osobowych jeśli są one zgodne z przepisami prawa powszechnie obowiązującego.

§ 7 .

Bezpieczna eksploatacja systemów informatycznych

1 . Bezpieczna eksploatacja systemów informatycznych przetwarzających dane osobowe, zostaje zapewniona poprzez przestrzeganie następujących zasad:

a) Użytkownikom zabrania się, wprowadzania zmian do oprogramowania, sprzętu informatycznego poprzez jego samodzielne konfigurowanie i wyposażanie.

b) Użytkownikom zabrania się, umożliwiania stronom trzecim uzyskiwania nieupoważnionego dostępu do systemów informatycznych.

c) Użytkownikom nie wolno instalować nowego lub aktualizować już zainstalowanego oprogramowania.

d) Użytkownikom nie wolno korzystać z systemów informatycznych dla celów innych niż związane z wykonywaniem obowiązków służbowych.

e) Użytkownikom nie wolno korzystać z prywatnego sprzętu informatycznego, w tym oprogramowania oraz nośników pamięci.

f) Użytkownikom nie wolno podejmować prób testowania, modyfikacji i naruszenia zabezpieczeń systemów informatycznych lub jakichkolwiek działań noszących takie znamiona.

g) Informacje przetwarzane przy użyciu współdzielonych aplikacji sieciowych na stacjach roboczych muszą być zapisywane na dyskach serwera.

h) Wszystkie aplikacje sieciowe, współdzielone zasoby użytkowe muszą być ulokowane na przeznaczonych do tego celu serwerach.

i) Nieautoryzowane podłączenie własnego lub strony trzeciej urządzenia teleinformatycznego do systemu informatycznego Urzędu jest zabronione.

§ 8 .

Nadawanie uprawnień do przetwarzania danych osobowych

1 . Użytkownicy systemu przetwarzającego dane osobowe przed przystąpieniem do przetwarzania danych osobowych w tym systemie informatycznym, zobowiązani są zapoznać się z:

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

b) Polityką bezpieczeństwa przetwarzania danych osobowych Urzędu Miejskiego w Łochowie.

2 . Użytkownicy przed dopuszczeniem do obsługi systemu informatycznego, w którym przetwarzane są dane osobowe powinni podlegać przeszkoleniu w zakresie obsługi sprzętu informatycznego, oprogramowania systemowego oraz oprogramowania do obsługi aplikacji, którą będą wykorzystywali.

3. Pierwsze zarejestrowanie użytkownika w systemie i nadanie odpowiednich uprawnień do systemu przetwarzającego dane osobowe musi być poprzedzone złożeniem przez użytkownika oświadczenia o:

a) Zachowaniu w tajemnicy danych osobowych i sposobów ich zabezpieczania oraz przetwarzaniu danych osobowych zgodnie z przepisami.

b) Uzyskanie formalnego upoważnienia do przetwarzania danych osobowych.

c) Wzory oświadczenia oraz upoważnienia stanowi załącznik nr 4 do Polityki bezpieczeństwa przetwarzania danych osobowych Urzędu Miejskiego w Łochowie

d) Po spełnieniu wymagań określonych w ust. 3, rejestrowanie użytkowników i nadawanie uprawnień w systemach informatycznych realizowane zgodnie z procedurą określoną w § 16 Polityki bezpieczeństwa przetwarzania danych osobowych Urzędu Miejskiego w Łochowie.

e) Identyfikator oraz zakres dostępu użytkownika powinien być rejestrowany w ewidencji osób upoważnionych do przetwarzania danych osobowych, określonej w §17 Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędu Miejskiego w Łochowie.

f) Administrator Systemów Informatycznych powinien przekazywać użytkownikom tymczasowe hasła dostępowe w sposób bezpieczny.

g) Procedurę nadawania uprawnień do przetwarzania danych osobowych w systemach należy stosować odpowiednio, w przypadku zmiany uprawnień w systemach lub w przypadku odebrania uprawnień w systemach.

h) Zmiany dotyczące użytkownika, takie jak rozwiązanie umowy o pracę lub utrata upoważnienia, są przesłanką do natychmiastowego wyrejestrowania użytkownika z systemu oraz unieważnienia hasła i odnotowanie tego faktu w ewidencji osób upoważnionych do przetwarzania danych osobowych.

i) Prawa dostępu przyznane użytkownikom zewnętrznym powinny mieć charakter czasowy i mogą być przyznawane na okres odpowiadający wykonywanemu zadaniu.

j) Dostęp do systemu informatycznego a także do poszczególnych aplikacji i baz danych przetwarzających dane osobowe powinien być możliwy tylko po podaniu identyfikatora odrębnego dla każdego użytkownika i poufnego hasła.

§ 9.

Metody i środki uwierzytelniania w systemie

1. Identyfikatory i hasła są sposobem zagwarantowania rozliczalności, poufności i integralności danych osobowych przetwarzanych w systemach informatycznych. Służą do weryfikowania tożsamości użytkownika, uzyskania dostępu do określonych zasobów, kont uprzywilejowanych lub uruchomienia określonej funkcjonalności.

2. Mając na uwadze zagwarantowanie wysokiego poziomu bezpieczeństwa przetwarzania danych osobowych oraz zagwarantowania użytkownikom pełnej rozliczalności wykonywanych przez nich operacji w systemach informatycznych, wszyscy użytkownicy przy uwierzytelnianiu do systemów informatycznych powinni stosować się do poniższych zasad:

a) Użytkownik systemu powinien posiadać unikalny identyfikator do swojego osobistego i wyłącznego użytku.

b) Hasła dostępu do systemów informatycznych powinny być tworzone przez użytkownika i stanowią tajemnicę służbową, znaną wyłącznie temu użytkownikowi z zastrzeżeniem § 8 ust. 7

c) Użytkownik ponosi pełną odpowiedzialność za utworzenie hasła dostępu oraz jego przechowywanie.

d) Hasła nie mogą być ujawniane lub przekazywane komukolwiek, bez względu na okoliczności.

e) Użytkownik nie powinien przechowywać haseł w widocznych miejscach, nie powinien umieszczać haseł w żadnych automatycznych procesach logowania (skryptach, makrach lub pod klawiszami funkcyjnymi).

3 . Użytkownicy są odpowiedzialni za wszelkie działania w systemach informatycznych prowadzone z użyciem ich identyfikatora i hasła.

4 . Administrator Systemów Informatycznych jest odpowiedzialny za okresowe sprawdzanie, usuwanie lub blokowanie zbędnych identyfikatorów użytkowników oraz kont w systemach, za które są odpowiedzialni.

§ 10 .

Wymogi dotyczące uwierzytelniania

1 . Wszystkie konta dostępowe (identyfikatory) do systemów informatycznych powinny być chronione hasłem lub innym bezpiecznym, zaakceptowanym przez Administratora Bezpieczeństwa Informacji sposobem uwierzytelniania.

2 . Identyfikator oraz nadane uprawnienia powinny umożliwiać wykonywanie czynności wyłącznie zgodnych z zakresem powierzonych obowiązków.

3 . Identyfikator użytkownika powinien być niepowtarzalny a po wyrejestrowaniu się z systemu informatycznego nie powinien być przydzielany innej osobie.

4 . Identyfikator, który utracił ważność nie może być ponownie przydzielony innemu użytkownikowi.

5 . Hasło początkowe, które jest przydzielane przez Administratora Systemów Informatycznych, powinno umożliwiać użytkownikowi zarejestrowanie się w systemie tylko jeden raz i powinno być natychmiast zmienione przez użytkownika.

6 . Użytkownicy powinny wybierać hasła dobrej jakości.

7 . Hasła nie mogą być takie same jak identyfikator użytkownika oraz nie mogą być zapisywane w systemach w postaci jawnej.

8 . Hasła powinny być utrzymywane w tajemnicy również po upływie ich ważności.

9 . Należy unikać ponownego lub cyklicznego używania starych haseł.

10 . Hasła dla użytkowników o wysokich uprawnieniach (np. root, administrator) mogą być wykorzystywane tylko w uzasadnionych przypadkach i fakt ten powinien być udokumentowany.

11. Hasła użytkowników o wysokich uprawnieniach powinny być przechowywane w miejscu zabezpieczonym przed dostępem osób nieupoważnionych.

12. Rutynowe działania użytkownika nie powinny być prowadzone z wykorzystaniem kont uprzywilejowanych.

13. Udostępnienie hasła osobie postronnej należy traktować jako poważny incydent naruszenia ochrony danych osobowych.

§ 11.

Wymogi dotyczące zmiany haseł

1. Użytkownik jest zobowiązany zmieniać hasło, w którego posiadaniu się znajduje:
   a) Okresowo, zgodnie z wymaganiami dla danego systemu informatycznego (przed upływem terminu ważności hasła).
   b) W przypadku ujawnienia lub podejrzenia ujawnienia hasła.
2. W przypadku braku dostępu do konta chronionego hasłem, w którego posiadaniu się znajduje, użytkownik zobowiązany jest wystąpić o zmianę hasła do właściwego Administratora Systemów Informatycznych, w sytuacji:
   a) Zapomnienia/zgubienia hasła.
   b) Wygaśnięcia ważności hasła.
   c) Zablokowania konta spowodowanego nieprawidłowym wprowadzeniem hasła.
   d) Braku uprawnień/interfejsu umożliwiających samodzielną zmianę hasła.
3. Zmiana haseł użytkowników powinna być wymuszana przez system co 30 dni, w przypadku braku wymuszenia przez system, użytkownik sam jest zobowiązany do zmiany hasła co 30 dni.

§ 12.

Procedura bezpiecznego uwierzytelniania

1. Procedura bezpiecznego uwierzytelniania w systemie informatycznym zapewnia minimalizowanie możliwości nieautoryzowanego dostępu do systemu. Procedura powinna ujawniać minimum informacji o systemie informatycznym tak, aby nie pozwolić nieuprawnionemu użytkownikowi na uzyskanie dodatkowych wskazówek w celu ich wykorzystania w sposób niedozwolony. W tym celu należy zapewnić:
   a) Wyświetlanie ogólnego ostrzeżenia, że dostęp do stacji roboczej dozwolony jedynie dla uprawnionych użytkowników.
   b) Zatwierdzanie jedynie kompletnych informacji wejściowych, niezbędnych przy logowaniu jeżeli wystąpi błąd, system nie powinien wskazywać, która część danych jest poprawna, a która niepoprawna.
   c) Ograniczenie liczby nieudanych prób logowania się do systemu, np. do trzech prób, oraz uwzględnić:
      - wykonywanie zapisu nieudanych i udanych prób

- wymuszanie odstępu czasowego przed każdą kolejną próbą logowania się lub odrzucanie wszelkich dalszych prób, jeśli nie mają specjalnej autoryzacji,
- rozłączenie połączeń,
- wysłanie wiadomości alarmowej na konsolę systemową w przypadku, gdy maksymalna liczba prób została osiągnięta,
- ustawienia maksymalnej liczby prób logowania się w połączeniu z minimalną długością hasła oraz wartością chronionego systemu,
- ograniczenie maksymalnego i minimalnego czasu trwania logowania; jeśli zostanie on przekroczony, system powinien przerwać procedurę logowania,

d) Wyświetlanie następujących informacji po pomyślnym zalogowaniu:
- datę i czas ostatniego pomyślnego logowania do systemu,
- szczegółowe dane dotyczące nieudanych prób logowania się, jakie zdarzyły się od chwili ostatniej udanej próby,

e) Blokowanie wyświetlania hasła w trakcie wprowadzania lub ukrywanie wprowadzanych znaków pod symbolami.

f) Blokowanie przesyłania haseł przez sieć jawnym tekstem.

§ 13 .

Wymagania dotyczące sprzętu i oprogramowania

1 . Wygaszacz stacji roboczej powinien być skonfigurowany w taki sposób, aby aktywował się automatycznie po upływie 10 minut od ostatniego użycia stacji roboczej, uruchamiając blokadę stacji roboczej, wymuszającą ponowne zalogowanie.

2 . Ekrany monitorów należy ustawić w taki sposób, by uniemożliwić osobom postronnym wgląd lub spisanie informacji aktualnie wyświetlanej na ekranie monitora.

3 . Programy zainstalowane na stacjach roboczych stacjonarnych i na komputerach przenośnych obsługujących przetwarzanie danych osobowych muszą być użytkowane z zachowaniem praw autorskich i posiadać licencje.

4 . Oprogramowanie może być używane tylko zgodnie z prawami licencji. Oprogramowanie typu Freewere, Shareware lub inne oprogramowanie dostarczane bez opłat jest uznawane jako nieautoryzowane, jeżeli nie otrzyma stosownej aprobaty Administratora Systemów Informatycznych.

5 . Przed zainstalowaniem nowego oprogramowania Administrator Systemów Informatycznych lub inna upoważniona osoba, zobowiązana jest sprawdzić jego działanie pod kątem bezpieczeństwa całego systemu.

6 . Sieć teleinformatyczna wykorzystywana do przetwarzania danych osobowych powinna mieć zapewnione prawidłowe zasilanie energetyczne gwarantujące właściwe i zgodne z wymaganiami producenta działanie sprzętu informatycznego.

7. Serwer systemu przetwarzającego dane osobowe powinien być zasilany przez UPS o odpowiednich parametrach, pozwalających na podtrzymanie zasilania przez co najmniej 15 minut oraz na wykonanie, bezpiecznego wyłączenia serwera, tak aby przed ostatecznym zanikiem zasilania zostały prawidłowo zakończone operacje rozpoczęte na zbiorze danych osobowych.

8. Pomieszczenie serwerowi oraz pomieszczenia, w których przetwarzane są dane osobowe powinny być odpowiednio chronione przed skutkami pożaru.

9. Infrastruktura techniczna związana z siecią teleinformatyczną i jej zasilaniem (rozdzielnie elektryczne, skrzynki z bezpiecznikami) powinna być zabezpieczona przed dostępem osób nieupoważnionych.

10. Gniazda zasilania sieci teleinformatycznej powinny być odpowiednio oznakowane, zabezpieczone przed włączeniem do nich innych odbiorników i wykonane w specjalnym standardzie.

11. Wdrażanie aplikacji i oprogramowania eksploatowanych systemów powinno być poprzedzone wyczerpującymi, pozytywnymi i udokumentowanymi testami.

12. Powinna zostać opracowana metoda przywracania poprzedniej wersji, zanim zmiany zostaną wdrożone.

13. Należy przechowywać wszystkie poprzednie wersje oprogramowania jako środek utrzymania ciągłości działania.

14. Należy zapewnić rejestrowanie wszystkich błędów, związanych z problemami przetwarzania danych osobowych, zgłaszanych przez użytkowników lub programy systemowe.

15. Należy zapewnić ograniczenie dostępu do bibliotek źródłowych programów a dostęp i zmiany odnotowywać.

16. Należy chronić informacje zawarte w dziennikach zdarzeń systemów przed manipulacja i nieautoryzowanym dostępem.

17. Należy zapewnić synchronizację zegarów wszystkich stosowanych systemów służących do przetwarzania danych osobowych z uzgodnionym, dokładnym źródłem czasu.

18. Należy zapewnić aby porty i usługi, które nie są wykorzystywane były zablokowane.

§ 14.

Funkcjonalność systemu informatycznego

1. System informatyczny służący do przetwarzania danych osobowych powinien zapewniać dla każdej osoby, której dane osobowe są przetwarzane w tym systemie — z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie — automatyczne odnotowywanie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych, informacji o dacie pierwszego wprowadzenia danych do systemu oraz o identyfikatorze osoby wprowadzającej dane.

2. W przypadku zbierania danych osobowych od osoby, której dane nie dotyczą należy zapewnić w systemie informatycznym odnotowywanie informacji o źródle pochodzenia danych. Proces ten nie musi odbywać się automatycznie.

3. Dla każdego systemu służącego do przetwarzania danych osobowych, z którego udostępniane są dane osobowe odbiorcom danych, należy zapewnić odnotowanie w bazie danych tego systemu informacji, komu, kiedy i w jakim zakresie dane zostały udostępnione, chyba, że dane pochodzą z jawnego zbioru danych osobowych.

4. Należy zapewnić dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym sporządzenie i wydrukowanie:
   a) Zestawień zakresu i treści przetwarzanych na jej temat danych osobowych.
   b) Zestawienia zawierającego informacje wymagane w § 7 ust. 1 Rozporządzenia.

5. W przypadku przetwarzania danych osobowych, w co najmniej dwóch systemach, wymagania, o których mowa w § 7 ust. 1 pkt 4 Rozporządzenia, mogą być realizowane w jednej z nich lub w odrębnej aplikacji przeznaczonej do tego celu.

6. Treść ostatecznego rozstrzygnięcia indywidualnej sprawy osoby, której dane dotyczą, nie może być wyłącznie wynikiem operacji na danych osobowych, prowadzonych w aplikacji lub systemie informatycznym.

7. Zabronione jest nadawanie ukrytych znaczeń elementom numerów porządkowych w aplikacjach ewidencjonujących osoby fizyczne

8. Zaleca się wbudowanie do aplikacji funkcjonalności, zapewniających wymuszanie zmiany haseł po zadanym czasie, badania ich długości, jakości i powtarzalności (z użyciem funkcji skrótu).

§ 15 .

Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie

1. Przed przystąpieniem do pracy z systemem, użytkownik obowiązany jest dokonać sprawdzenia stanu urządzeń informatycznych oraz oględzin swojego stanowiska pracy, ze zwróceniem szczególnej uwagi, czy nie zaszły okoliczności wskazujące na naruszenie ochrony danych osobowych.

2. W przypadku stwierdzenia bądź podejrzenia, iż miało miejsce naruszenie ochrony danych osobowych, użytkownik systemu zobowiązany jest postępować zgodnie z procedurą opisaną w §22 Polityki bezpieczeństwa przetwarzania danych osobowych Urzędu Miejskiego w Łochowie.

3. Przed opuszczeniem stanowiska pracy, użytkownik obowiązany jest zablokować swoją stację roboczą poprzez wciśnięcie klawiszy “ctrl+alt+delete” i wybranie opcji “Zablokuj stację roboczą”.

4. Kończąc pracę, użytkownik obowiązany jest do wylogowania się z systemu informatycznego i zabezpieczenia stanowiska pracy, w szczególności wszelkiej dokumentacji, wydruków oraz wymiennych nośników informacji, na których znajdują się dane osobowe i umieszczenia ich zamykanych szafkach.

§ 16 .

Przetwarzanie, udostępnianie i likwidacja danych osobowych

1 . W przypadku przekazywania urządzeń lub nośników zawierających dane osobowe, poza obszar przetwarzania danych osobowych, zabezpiecza się je w sposób zapewniający poufność, integralność i rozliczalność tych danych, przez co rozumie się:
   a) Ograniczenie dostępu do danych osobowych hasłem zabezpieczającym dane przed osobami nieupoważnionymi.
   b) Stosowanie metod kryptograficznych.
   c) Stosowanie odpowiednich zabezpieczeń fizycznych.
   d) Stosowanie odpowiednich zabezpieczeń fizycznych.
   W zależności od stopnia zagrożenia zalecane jest stosowanie kombinacji wyżej wymienionych zabezpieczeń.
2 . Nieuzasadnione kopiowanie przez użytkowników plików z serwerów na stacje robocze użytkowników i na elektroniczne nośniki informacji jest zabronione bez akceptacji ze strony Administratora Bezpieczeństwa Informacji.
3 . W przypadku udostępniania danych osobowych odbiorcy danych w rozumieniu art. 7 pkt 6 Ustawy, użytkownik ma obowiązek odnotować komu i kiedy udostępniono poszczególne dane.
4 . Jeżeli dane osobowe nie są pozyskane od osoby, której dotyczą, użytkownik zobowiązany jest odnotować w systemie informatycznym źródło pochodzenia danych.
5 . Dla udokumentowania czynności dokonywanych w celu likwidacji zbiorów danych osobowych nie podlegających archiwizacji w odrębnym trybie dla który cel przetwarzania ustał, Administrator Bezpieczeństwa Informacji lub osoby upoważnione sporządzają protokół, w którym zamieszcza następujące informacje:
   a) Datę dokonania likwidacji.
   b) Przedmiot likwidacji (aplikacja, baza).
   c) Podpisy osób dokonujących i obecnych przy likwidacji zbiorów danych osobowych.
6 . Decyzję o likwidacji zbiorów danych osobowych, przetwarzanych w systemach informatycznych podejmują Właściciele zasobów danych osobowych.
7 . W przypadku likwidacji elektronicznych nośników informacji, należy dokonać wcześniej skutecznego usunięcia danych z tych nośników. W przypadku gdy usunięcie danych nie jest możliwe, należy uszkodzić nośniki w sposób uniemożliwiający odczyt tych danych.
8 . Przed przekazaniem elektronicznego nośnika informacji osobie nieuprawnionej, należy usunąć z nośnika dane osobowe.

§ 17 .

Kopie zapasowe

1. Kopie zapasowe zbiorów danych osobowych oraz programów i narzędzi programowych służących do ich przetwarzania powinny być wykonywane na bieżąco przez Administratora Systemów Informatycznych.
2. Kopie zapasowe powinny być tworzone na nośnikach magnetycznych, odpowiednio opisanych, oznakowanych i ewidencjonowanych a każdy proces wykonywania kopii zapasowej powinien być dokumentowany.
3. Kopie zapasowe należy opisywać w sposób umożliwiający szybką i jednoznaczną identyfikację zawartych w nich danych.
4. W celu usystematyzowania procesu wykonywania kopi zapasowej, odpowiedzialny za ten proces Administrator Systemów Informatycznych jest zobowiązany do sporządzenia harmonogramu wykonywania kopi zapasowej, wraz z opisem narzędzi służących do jej wykonywania, nazwą polityk, nazwą systemu, nazwą bazy danych, terminem okresu przechowywania, rodzajem wykorzystywanego nośnika wraz z numerem seryjnym nośnika.
5. Tworzenie, przechowywanie i likwidację kopii zapasowych powinny regulować szczegółowe instrukcje operacyjne dla poszczególnych systemów informatycznych, opracowywane przez Administratora Systemów Informatycznych, z uwzględnieniem niniejszych postanowień.
6. Administrator Systemów Informatycznych odpowiedzialny za tworzenie kopi zapasowych, zobowiązany jest przestrzegać terminów sporządzania kopii zapasowych oraz okresowo dokonywać kontroli możliwości odtworzenia danych zapisanych na tych kopiach, pod kątem ewentualnej przydatności w sytuacji awarii systemu.
7. Kopie zapasowe powinny być tworzone w bezpiecznym systemie archiwizacji, który powinien zapewniać ograniczony dostęp fizyczny do nośników oraz przyznanie uprawnień dostępu tylko wyznaczonemu imiennie Administratorowi Systemów Informatycznych oraz Administratorowi Bezpieczeństwa Informacji.
8. Dane z kopii zapasowych powinny być odtwarzane wyłącznie przez Administratora Systemów Informatycznych
9. Kopie zapasowe, które uległy uszkodzeniu powinny podlegać natychmiastowemu zniszczeniu.
10. Niszczenia kopii zapasowych, na nośnikach magnetycznych dokonuje Administrator Systemów Informatycznych lub inna upoważniona przez Kierownictwo osobą.
11. Proces niszczenia kopi zapasowych powinien odbywać się komisyjnie i powinien być dokumentowany.

§ 18 .

Przechowywanie nośników elektronicznych zawierających dane osobowe

1. Dane osobowe mogą być przechowywane:
   a) Na serwerach zlokalizowanych w obszarach wyznaczonych do przetwarzania danych osobowych.
   b) Na wymiennych nośnikach elektronicznych.

c) Na poszczególnych stacjach roboczych.

2 . Wykorzystanie wymiennych nośników elektronicznych (CD/DVD, pamięć USB, wymienna karta pamięci, dyskietka) powinno być ściśle kontrolowane i dozwolone wyłącznie dla upoważnionych użytkowników.

3 . Wymienne nośniki elektroniczne, o ile nie są użytkowane, powinny być przechowywane w zamykanych szafkach.

4 . Nośniki zawierające kopie zapasowe powinny być przechowywane w innym pomieszczeniu niż to, w którym umieszczony jest serwer przetwarzający dane osobowe.

5 . Kopie zapasowe powinny być przechowywane w odpowiednio zabezpieczonej, ognioodpornej szafie, do której dostęp mogą mieć wyłącznie osoby upoważnione.

6 . Nośniki magnetyczne i optyczne z danymi osobowymi powinny być:

a) Oznaczane i przechowywane w zamykanych szafach lub sejfach.

b) Przechowywane maksymalnie przez okres wskazany dla danego rodzaju danych osobowych przez Administratora Bezpieczeństwa Informacji.

7 . Informację o maksymalnym okresie przechowywania nośników magnetycznych oraz optycznych, na których zapisane są dane osobowe przekazują Właściciele zasobów danych osobowych do Administratora Bezpieczeństwa Informacji.

§ 19 .

Ochrona systemu informatycznego przed działaniem szkodliwego oprogramowania

1 . Na każdej stacji roboczej w sieci oraz serwerze przetwarzającym dane osobowe powinno być zainstalowane oprogramowanie antywirusowe skanujące na bieżąco system informatyczny.

2 . Skaner poczty elektronicznej powinien być stale włączony.

3 . Oprogramowanie antywirusowe powinno być zainstalowane tak aby użytkownik nie był w stanie wyłączyć lub pominąć etapu skanowania.

4 . Kontrola antywirusowa powinna być przeprowadzana na wszystkich nośnikach magnetycznych i optycznych, służących zarówno do przetwarzania danych osobowych w systemie, jak i do celów instalacyjnych.

5 . Należy stosować wersje programów antywirusowych z aktualną bazą sygnatur wirusów.

6 . Nowe wersje oprogramowania antywirusowego oraz uaktualnienia bazy sygnatur wirusów instalują Administrator Systemów Informatycznych niezwłocznie po ich otrzymaniu lub ściągnięciu, uprzednio weryfikując pochodzenie oprogramowania.

7 . W razie zainfekowania systemu Administrator Systemów odpowiada za usunięcie wirusa.

8 . Administrator Systemów Informatycznych ma prawo odłączyć od sieci stację roboczą, na której zostanie zlokalizowany wirus, jeśli uznają, Se dalsze pozostawienie go w sieci zagraża innym stacjom roboczym.

Elektronicznie podpisany przez:
URSZULA KALINOWSKA
Data: 2013.12.11 09:05:06
Odcisk palca certyfikatu: 8b49 476b e52
c2b7 6b78 8b40 2bb0 5ab8 36ca 911f