Burmistrz Sośnicowic

ZARZĄDZENIE NR 91/2016

BURMISTRZA SOŚNICOWIC

z dnia 10.10.2016

w sprawie: ***wprowadzenia Analizy zagrożeń i ryzyka przetwarzania danych osobowych w Urzędzie Miejskim w Sośnicowicach***

Na podstawie: art. 30 ust. 1 oraz art. 33 ust.2 ustawy z dnia 8 marca 1990 o samorządzie gminnym i art. 36 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U.2016.922. z późn. zm.) oraz § 4 ust. 5 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku 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) zarządza się, co następuje:

§ 1

Wprowadzam ***Analizę zagrożeń i ryzyka przetwarzania danych osobowych w Urzędzie Miejskim w Sośnicowicach***, stanowiącą załącznik do niniejszego zarządzenia.

§ 2

Nadzór nad wykonaniem zarządzenia powierzam Administratorowi Bezpieczeństwa Informacji

§ 3

Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ SOŚNICOWIC

Z upoważnienia Burmistrza
SEKRETARZ GMINY
Kazimiera Kaczmar

Uzasadnienie :

Celem opracowania i wdrożenia dokumentu, jakim jest ***Analiza zagrożeń i ryzyka przetwarzania danych osobowych w Urzędzie Miejskim w Sośnicowicach*** jest uwzględnienie norm, wymaganych ustawą i rozporządzeniem, odnoszących się do wdrożenia systemu zarządzania bezpieczeństwem informacji, jak i analizy ryzyka przetwarzanych informacji, w tym danych osobowych.

Na Administratorze spoczywa obowiązek zapewnienia środków, zapewniających odpowiednią dla zagrożeń ochronę przetwarzania danych osobowych.
Z punktu widzenia wymienionych norm, oznacza to spełnienie trzech reguł:
1) **reguły poufności informacji**, polegającej na zapewnieniu, że informacja jest udostępniona jedynie osobom upoważnionym;
2) **reguły rozliczalności informacji**, polegającej na tym, że osoby upoważnione mają dostęp do informacji i związanych z nią aktów tylko wtedy, gdy istnieje taka potrzeba oraz istnieje możliwość identyfikacji takiej osoby;
3) **reguły integralności informacji**, polegającej na zapewnieniu dokładności i kompletności informacji oraz metod jej przetwarzania.

Bezpieczeństwo wiąże się z ograniczeniem ryzyka, czyli wyeliminowanie nieakceptowanego ryzyka utraty zasobów Urzędu Miejskiego w Sośnicowicach.
Niniejszy dokument jest podstawą do zarządzania bezpieczeństwem informacji rozumianym jako identyfikacja, ocena i ustalenie priorytetów wystąpienia ryzyka. Następnie podjęcie takiego działania, aby zminimalizować, monitorować i kontrolować prawdopodobieństwo wystąpienie zjawisk niepożądanych.

Załącznik nr 1 do Zarządzenia 91/2016 z dnia 10.10.2016
Dokument nadzorowany w wersji elektronicznej

Z upoważnienia Burmistrza
SEKRETARZ GMINY
Kazimierz Kaczmar

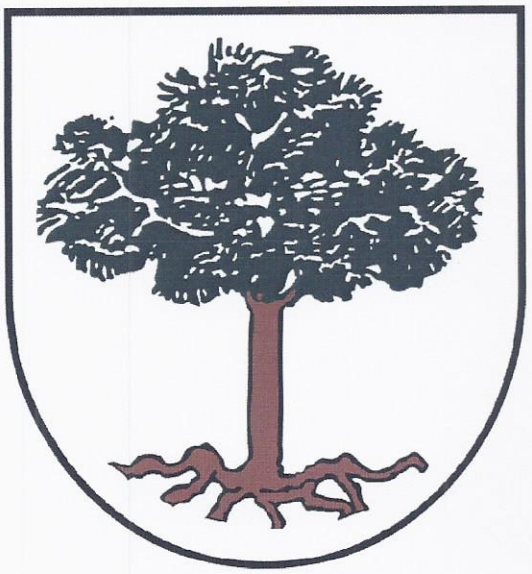
ZATWIERDZAM

.....

podpis Administratora Danych Osobowych

ANALIZA ZAGROŻEŃ I RYZYKA

przy przetwarzaniu danych osobowych w Urzędzie Miasta i Gminy Sośnicowice



Opracował:

Inspektor ds. Administracji Bezpieczeństwa Informacji
Adam Szczęsny

Administrator Bezpieczeństwa Informacji

SPIS TREŚCI

1. Podstawy prane opracowanej dokumentacji.

- Art. 36 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych
  Dz. U. 2016.922 z późn. zm
- § 4 p.5 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków techniczny i organizacyjnych , jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych Dz. U. Nr 100, poz. 1024

2. WYMOGI OGÓLNE BEZPIECZEŃSTWA

W czasie przetwarzania danych osobowych w Urzędzie Miasta i Gminy Sośnicowice , informacje występują w postaci :

- plików lub informacji przechowywanych na dysku twardym komputera,
- plików lub informacji przechowywanych pamięci operacyjnej komputera ,
- plików lub informacji zapisanych na nośnikach pamięci,
- wersji roboczych lub gotowych dokumentów w formie papierowej.

Bezpieczeństwo przetwarzanych lub przechowywanych informacji zawierające dane osobowe wymaga :

- zapewnienia ochrony fizycznej stanowiska komputerowego przed nieuprawnionym dostępem,
- ochrony nośników technicznych i wydruków dokumentów wytwarzanych przy pomocy sprzętu komputerowego w tym określenia zasad postępowania z nimi przed nieuprawnionym dostępem,
- zabezpieczenia przed nieupoważnionym dostępem do danych osobowych znajdujących się w zasobach systemu informatycznego,
- zapewnienia dostępności do danych osobowych znajdujących się na technicznych nośnikach informacji oraz w pamięci systemu informatycznego dla upoważnionych użytkowników,
- zapewnienia możliwości kontroli nośników , na których przetwarzano lub przechowywano dane osobowe.

3. ZAGROŻENIA DLA SYSTEMU

Biorąc pod uwagę specyfikację prac wykonywanych przy pomocy systemu informatycznego, przeznaczonego do przygotowania dokumentów zawierających dane osobowe , podstawowe zagrożenia to: utrata poufności , integralności i rozliczalności.

- poufność to zapewnienie , że dane osobowe nie są udostępnianie nieupoważnionym podmiotom,
- integralność to zapewnienie , aby wszelkie zmiany wykonywane w systemie informatycznym, w systemie jego katalogów oraz poszczególnych plikach zawierających dane osobowe były skutkiem zaplanowanych działań użytkowników systemu ; właściwość zapewniająca , że dany nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
- rozliczalność to właściwość zapewniająca , że działania podmiotu przetwarzającego dane mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

Zagrożenia w zakresie poufności obejmują :

- nieuprawniony dostęp do pomieszczenia , w którym przetwarzane są dane osobowe ,
- ujawnienie haseł dostępu do stanowiska komputerowego na którym przetwarzane są dane osobowe,
- nieuprawnione przeniesienie informacji zawierających dane osobowe na inny nośnik,
- utrata nośnika zawierającego dane osobowe,
- klęska żywiołowa , w wyniku której utracono dane osobowe,
- nieuprawnione wyniesienie danych osobowych zawartych na nośniku elektronicznym,

Zagrożenia w zakresie rozliczalności obejmują :

- brak kontroli nad dokumentami wykonanymi na stanowisku komputerowym w zakresie ich kopiowania i drukowania,
- wyparcie się pracy na stanowisku komputerowym , gdzie przetwarza się dane osobowe,
- wprowadzenie zmian w treści dokumentu zawierającego dane osobowe
- błędy oprogramowania lub sprzętu.

Zagrożenia w zakresie integralności obejmują :

- nielegalny dostęp danych osobowych, w tym do stanowiska komputerowego,
- błędy, pomyłki,
- brak mechanizmów uniemożliwiających skasowanie lub zmianę loginów przez administratora lub innego użytkownika,
- wirus,
- brak w wykorzystywanych aplikacjach mechanizmów zapewniających integralność danych.

Źródłami zagrożeń dla stanowisk komputerowych, gdzie przetwarza się dane osobowe mogą być:

- siły natury - zdarzenia , które nie wynikają z działalności człowieka, tzn.
    - uderzenia pioruna,
    - pożar będący konsekwencją uderzenia pioruna,

- starzenie się sprzętu,
- starzenie się nośników pamięci ,
- kurz,
- katastrofy budowlane,
- ulewny deszcz,
- ekstremalne temperatury, wilgoć,

- ludzie - mogą to być pracownicy lub osoby z zewnątrz , którzy działają w sposób celowy lub przypadkowy ; zagrożenia te to przede wszystkim:
  - błędy i pomyłki użytkowników
  - błędy i pomyłki administratorów
  - błędy utrzymania systemu w poufności , integralności i rozliczalności,
  - zaniedbania użytkowników przy przesyłaniu , udostępnianiu i kopiowaniu,
  - zgubienie nośnika zawierającego dane osobowe,
  - niewłaściwe zniszczenie nośnika,
  - nielegalne użycie oprogramowania
  - choroba ważnych osób i nieuprawnione zastępstwo
  - epidemia kadry i brak osób do dostępu,
  - podpalenie obiektu,
  - zalanie wodą,
  - katastrofa budowlana będąca konsekwencją przypadkowego działania człowieka,
  - zakłócenia elektromagnetyczne , radiotechniczne,
  - podłożenie i wybuch bomby, ładunku wybuchowego,
  - użycie broni,
  - zmiany napięcia w sieci,
  - utrata prądu,
  - zbieranie się ładunków elektrostatycznych,
  - utrata kluczowych pracowników,
  - niedobór pracowników,
  - defektu oprogramowania,
  - szpiegostwo,
  - terroryzm,
  - wandalizm,
  - destrukcja zbiorów i programów impulsem elektromagnetycznym,
  - kradzież,
  - włamanie do systemu,
  - wyłudzenie, fałszowanie dokumentów,
  - podszycie się pod uprawnionego użytkowania,
  - podsłuch,
  - użycie złośliwego oprogramowania,

Każde z ww. zagrożeń wynikających z działalności człowieka może być ograniczone poprzez:

- rygorystyczne przestrzeganie zasad postępowania z danymi osobowymi,
- fizyczne zabezpieczenie obiektu, w którym działa system,
- wdrożenie systemu kontroli użytkowników,

- brak połączenia stanowisk komputerowych systemu z siecią internetową.

Zagrożenia wynikające z działania sił natury można ograniczyć poprzez właściwe zabezpieczenie budynków i pomieszczeń, w których znajdują się stanowiska komputerowe , na których przetwarza się dane osobowe.

Potencjalne ataki mogą być wykonane poprzez: podsłuch, wyłudzenie , fałszowanie dokumentów, wykorzystanie promieniowania ujawniającego.

4. STOPIEŃ WAŻNOŚCI INFORMACJI

Stopień ważności informacji zawierających dane osobowe określa poziom ochrony oraz zastosowanie właściwych środków bezpieczeństwa. W Urzędzie Miasta i Gminy Sośnicowice przetwarza się dane osobowe zwykłe i wrażliwe - merytorycznie związane z zakresem obowiązków użytkownika.

Ponieważ przewarzająca część danych osobowych w Urzędzie Miasta i Gminy Sośnicowice przetwarzana jest za pomocą komputerów , wielkość potencjalnych skutków ujawnienia/utraty informacji w nich zawartych jest stosunkowo duża, dlatego też należy oszacować poziom utraty poufności , jako wysoki (8 w skali od 1 do 10). Dotyczy to każdej kategorii przetwarzanych zasobów danych osobowych.

Dokładność i kompletność realizowanych czynności w zakresie prowadzonych spraw administracyjnych są zapewnione przez odpowiednie usytuowanie stanowisk komputerowych, na których się przetwarza dane osobowe (stanowiska jednoosobowe). Wymagania związane z potrzebą zachowania integralności informacji zawierających dane osobowe w systemie są średnie (4-6 w skali od 1 do 10). Dotyczy to każdej kategorii ww. przetwarzanych zasobów danych osobowych.

Wytwarzane dokumenty zawierające dane osobowe są rejestrowane , przechowywane do wglądu a następnie niszczone lub archiwizowane przez osoby posiadające stosowne upoważnienie. Raz w roku tworzone są kopie archiwalne na nośnikach pamięci. Można, zatem określić wymagania związane z zachowaniem rozliczalności , jako średnie (4-6 w skali od 1 do 10).

5. PODATNOŚĆ SYSTEMU NA ZAGROŻENIA

Podatność systemu na zagrożenia może wynikać z :

- dostępności systemu wynikającego np. z braku ochrony fizyczne budynku lub znacznej liczby personelu , mającego potencjalnie dostęp do systemu oraz wiedzę jak obsługiwać system,
- dostępność informacji znajdujących się w systemie za pośrednictwem połączeń zewnętrznych,
- możliwość celowego wprowadzenia luk w sprzęcie i oprogramowaniu lub wprowadzenia wirusów komputerowych,
- możliwość awarii sprzętu lub oprogramowania za względu na uszkodzenia ,błędy projektowe lub umyślną interwencję,
- przesyłanie informacji przez niezabezpieczone łącza telekomunikacyjne.

Podatność systemu na zagrożenia została ograniczona poprzez:

- ochronę fizyczną stanowisk komputerowych,
- kontrolę dostępu do pomieszczeń , gdzie przetwarzane są dane osobowe,
- wydzielenie stref ochronnych,
- ograniczenie liczby personelu, mającego potencjalnie dostęp do stanowisk komputerowych oraz wiedzę jak je obsługiwać ,
- zbudowanie stabilnej sieci zasilającej,
- przeglądy okresowe nośników,
- kontrolę zmian konfiguracji,
- testowanie oprogramowania,
- audyt,
- zabezpieczenie haseł,
- użycie oprogramowania antywirusowego,
- backupy,

W celu oszacowania potencjalnych strat wynikających z utraty (ujawnienia) danych osobowych przetwarzanych na stanowiskach komputerowych wykonano analizę ryzyka na podstawie przewidywanych zagrożeń dla zasobów. Analiza ryzyka musi być wykonana okresowo przez Administratora Bezpieczeństwa Informacji i Administratora Systemu Informatycznego; raz do korku na tej podstawie aktualizowana jest tabela ryzyka znajdująca się na stronie Urzędu Miasta Sośnicowice : **http://www.sosnicowice.pl/**

6. ANALIZA ZAGROŻEŃ I RYZYKA

Analiza zagrożeń i ryzyka polega na identyfikacji ryzyka wystąpienia niepożądanego czynnika (ujawnienia , przechwycenia itd.), określenia jego wielkości i zidentyfikowania obszarów wymagających zabezpieczeń tak, aby to ryzyko zminimalizować lub całkowicie go zlikwidować.
Aby przeprowadzić poprawnie analizę ryzyka na początku należy określić :

- zasoby które należy chronić ;
- zagrożenia - czynnik, który może powodować wystąpienie incydentu;
- podatność - słabość zasobów , która może być wykorzystana przez potencjalne zagrożenie
- skutki - jaki wpływ będzie miał zaistniały incydent na system informatyczny.

Zasobami systemu są wszelkie elementy służące do przetwarzania , przechowywani lub przekazywania informacji oraz do zapewnienia im właściwego poziomu bezpieczeństwa, tzn.:

- sprzęt komputerowy przechowujący dane - dysk twardy,
- pracownicy Urzędu , przetwarzający dane osobowe,
- aplikacje , w których przetwarzane są dane osobowe,
- pomieszczenia, w których pracują osoby przetwarzające dane osobowe,
- koszty dodatkowych zabezpieczeń obudowy systemu po incydencie.

Zagrożenia systemu to wszystkie niekorzystne czynniki mogące przyczynić się w trakcie pracy z danymi osobowymi do wystąpienia incydentu, mogącego mieć wypływ na ich ujawnienie bądź utratę, tzn. :

- poufność - właściwość polegająca na tym, że informacja nie jest dostępna lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom, tj. nieuprawiony dostęp do informacji , kradzież, pomyłka, sabotaż, itp.
- rozliczalność - właściwość pozwalająca na rozliczanie osoby pracującej na stanowisku komputerowym systemu przetwarzającego dane osobowe w zakresie dostępu do pomieszczenia , w którym ono jest zainstalowane oraz rozliczenie czynności wykonanych przy pomocy tego stanowiska komputerowego, w systemie katalogów oraz pojedynczych zbiorach.
- integralność - właściwość polegająca na zapewnieniu dokładności i kompletności aktywów tj. atak wirusów, pożar itp.

Podatność systemu to słabości zasobów , które mogą być wykorzystane do ujawnienia informacji niejawnych lub ich utraty.
Skutki określają wysokość start w systemie informatycznym po zainstalowaniu incydentu.
SKALA:
- identyfikacja sutków utraty zasobów, dla atrybutu poufności danych osobowych <0-10>

Wartość	Skutki
<0>	Brak skutków utraty poufności
<1-3>	Niski skutek utraty poufności
<4-7>	Średni skutek utraty poufności
<8-9>	Wysoki skutek utraty poufności
<9-10>	Całkowita utrata poufności

- identyfikacja sutków utraty zasobów, dla atrybutu rozliczalności danych osobowych <0-10>

Wartość	Skutki
<0>	Utrata dostępności nie występuje
<1-3>	Niski skutek utraty rozliczalności
<4-7>	Średni skutek utraty rozliczalności
<8-9>	Wysoki skutek utraty rozliczalności
<9-10>	Absolutny skutek utraty rozliczalności

- identyfikacja sutków utraty zasobów, dla atrybutu integralności danych osobowych <0-10>

Wartość	Skutki
<0>	Utrata integralności nie występuje
<1-3>	Niski skutek utraty integralności
<4-7>	Średni skutek utraty integralności
<8-9>	Wysoki skutek utraty integralności
<9-10>	Bezwzględny skutek utraty integralności

- identyfikacja podatności systemu informatycznego na określenie zagrożenia <0-10>

Wartość	Skutki
<0>	Brak podatności
<1-3>	Niski poziom
<4-7>	Średni poziom
<8-9>	Wysoki poziom
<9-10>	Ekstremalny poziom

Ryzyko = iloczyn wartości skutków i podatności zasobów systemu (max 100)
- skala poziomu ryzyka <1-100>

Wartość	**Poziom ryzyka**
<1-20>	Niski poziom ryzyka utraty bezpieczeństwa danych osobowych
<21-60>	Średni poziom ryzyka utraty bezpieczeństwa danych osobowych
<61-80>	Wysoki poziom ryzyka utraty bezpieczeństwa danych osobowych
<81-100>	Maksymalny poziom ryzyka utraty bezpieczeństwa danych osobowych

Ryzyko ogólne (średnio) = 30,28/ 100

Występuje *średnie* ryzyko utraty bezpieczeństwa danych osobowych

7. Wnioski

Ww. analiza przeprowadzona dla wszystkich chronionych zasobów oraz wszystkich możliwych zagrożeń dała pełny obraz, na co zwrócić szczególną uwagę w Urzędzie Miasta i Gminy Sośnicowice, jakie zastosować dodatkowe środki bezpieczeństwa występującego systemu informatycznego, w którym przetwarzane są dane osobowe. Dodatkowo ułatwia też stworzenie stosownej dokumentacji.

W związku z powyższym na podstawie ww. analizy największym potencjalnym zagrożeniem występującym w Urzędzie Miasta i Gminy Sośnicowice dla bezpieczeństwa danych osobowych jest:

- nieuprawniony dostęp,
- kradzież (włamanie do systemu),

Innymi zagrożeniami są :

- awaria sprzętu,
- atak wirusa,
- pożar obiektu Urzędu Miasta i Gminy Sośnicowice,

W celu zmniejszenia ww. zagrożeń szczególną uwagę należy zwrócić na :

- przetwarzanie danych osobowych tylko przez osoby upoważnione,
- zabezpieczenie obiektu i systemu informatycznego w zakresie ochrony antywłamaniowej oraz przestrzeganie ustalonych zasad w tym zakresie,
- przestrzeganie instrukcji obsługi sprzętu i zasad posługiwania się nim,
- stosowanie nowoczesnych zabezpieczeń antywłamaniowych.

Aby skutecznie wyeliminować ww. zagrożenia należy wprowadzić następujące dodatkowe zabezpieczenia:

- przestrzegać zasad korzystania ze sprzętu informatycznego określonych w Polityce Bezpieczeństwa *(PB)* i Instrukcji Zarządzania Systemem informatycznym (*IZSI*), ze zwróceniem szczególnej uwagi na dostęp osób postronnych,
- przestrzegać rygorystycznie przepisów w zakresie ochrony danych osobowych,
- przestrzegać zasad posługiwania się sprzętem komputerowym (kopiowanie, przesyłanie, udostępnianie),
- stosować procedury (PB i IZSI)korzystania z systemu informatycznego w którym przetwarzane są dane osobowe.