Załącznik Nr 3 do Zarządzenia Burmistrza
Nr 0050.58.2016 z dnia 23 czerwca 2016 r.

URZĄD MIEJSKI GMINY W ŁOBŻENICY

INSTRUKCJA POSTĘPOWANIA

W SYTUACJI NARUSZENIA BEZPIECZEŃSTWA

DANYCH OSOBOWYCH

W URZĘDZIE MIEJSKIM GMINY ŁOBŻENICA

ZATWIERDZAM
BURMISTRZ
Piotr Łosoś (2)
.....

OPRACOWAŁ:

Administrator Bezpieczeństwa Informacji

w Urzędzie Miejskim Gminy w Łobżenicy

Łobżenica , dnia 23 czerwca 2016 roku.

§ 1.

POSTANOWIENIA OGÓLNE

Instrukcja postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych przeznaczona jest dla osób działających przy przetwarzaniu danych osobowych w Urzędzie Miejskim Gminy w Łobżenicy i należy stosować ja w powiązaniu z Polityką bezpieczeństwa przetwarzania danych osobowych oraz Instrukcją zarządzania systemami informatycznymi w Urzędzie Miejskim Gminy Łobżenica.

Celem instrukcji jest ustalenie jednolitych zasad postępowania w przypadku, gdy:

1) stwierdzono naruszenie lub istnieje podejrzenie naruszenia ochrony danych osobowych, zgromadzonych w systemach informatycznych lub na innych nośnikach informacji, w tym nośnikach papierowych;
2) stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zasad ochrony danych.

§ 2.

NARUSZENIE BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Za naruszenie bezpieczeństwa danych osobowych i systemów informatycznych uważa się w szczególności:

1) nieupoważniony dostęp, modyfikację, kopiowanie lub zniszczenie/usunięcie danych osobowych, zarówno w systemie informatycznym, jak i na nośnikach papierowych i elektronicznych;
2) udostępnianie danych osobowych nieuprawnionym podmiotom lub osobom;
3) nielegalne bądź nieświadome ujawnienie danych osobowych;
4) pozyskiwanie danych osobowych z nielegalnych źródeł;
5) nieautoryzowany dostęp do danych przez połączenie sieciowe;
6) niedopełnienie obowiązku ochrony danych osobowych przez umożliwienie dostępu do danych (np. pozostawienie danych na nośnikach papierowych, niezablokowanie dostępu do systemu, brak nadzoru nad serwisantami i innymi osobami nieuprawnionymi przebywającymi w pomieszczeniach, gdzie przetwarza się dane osobowe);
7) naruszenie zasad ochrony fizycznej pomieszczeń, w których przetwarza się dane osobowe;
8) wykrycie niezabezpieczonego kanału dystrybucji danych osobowych;
9) przetwarzanie danych osobowych niezgodnie z uprawnionym celem i zakresem;

10) zainfekowanie systemów informatycznych wirusami lub instalacja innych programów godzących w integralność systemu informatycznego;
11) ujawnienie indywidualnych haseł dostępu do systemu;
12) przesyłanie danych osobowych przez Internet bez zabezpieczenia;
13) przesyłanie nośników elektronicznych z danymi osobowymi bez zabezpieczenia;
14) zniszczenie sprzętu stanowiącego wyposażenie systemów informatycznych w wyniku pożaru, kradzieży lub celowego uszkodzenia;
15) kradzież sprzętu służącego do przetwarzania danych osobowych oraz nośników danych lub oprogramowania;
16) brak aktualnych kopii bezpieczeństwa danych osobowych lub brak odpowiednich nośników do sporządzania kopii;
17) niewłaściwe niszczenie nośników z danymi osobowymi pozwalające na ich odczyt;
18) inne sytuacje wskazujące lub potwierdzające naruszenie bezpieczeństwa danych osobowych w Urzędzie.

§ 3.
MOŻLIWE PRZYPADKI NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

O możliwości zaistnienia incydentu naruszenia bezpieczeństwa danych osobowych może świadczyć m.in.

1) nadmierne, w stosunku do wykonywanych zadań (zakres upoważnienia), uprawnienia użytkownika do zasobów systemu;
2) korzystanie z zasobów systemu poza godzinami pracy (bez zgody przełożonego);
3) wysoka aktywność kont, które długo pozostawały niewykorzystane lub ich aktywność była niska;
4) zanotowanie, w krótkim czasie dużej liczby nieudanych prób logowania do systemu;
5) naruszenie lub wadliwe funkcjonowanie zabezpieczeń fizycznych budynku i pomieszczeń, w których przetwarza się dane osobowe (włamanie lub zacinające się zamki, niedomykające się okna itp.);
6) obecność osób nieupoważnionych w pomieszczeniu, w którym przetwarzane są dane osobowe.

§ 4.

OBOWIĄZKI OSOBY STWIERDZAJĄCEJ NARUSZENIE BEZPIECZEŃSTWA DANYCH OSOBOWYCH

1. Osoba, która podejrzewa lub stwierdzi zagrożenie lub naruszenie zasad ochrony danych osobowych ma obowiązek niezwłocznie:

1) powiadomić o zaistniałym zdarzeniu Administratora Bezpieczeństwa Informacji oraz swojego bezpośredniego przełożonego;
2) określić (opisać) symptomy świadczące o możliwości naruszenia lub naruszeniu zasad ochrony danych;
3) określić sytuację i czas w jakim je zauważono;
4) podać wszelkie istotne informacje mogące pomóc w ustaleniu przyczyny naruszenia zasad ochrony danych osobowych.

2. Administratorowi Bezpieczeństwa Informacji zgłasza się w szczególności przypadki:

1) użytkowania stacji roboczej przez osobę nie będącą użytkownikiem systemu;
2) usiłowania logowania się do systemu (sieci) przez osobę nieuprawnioną;
3) usuwania, dodawania lub modyfikowania bez wiedzy i zgody użytkownika jego dokumentów (rekordów);
4) udostępniania osobom nieuprawnionym stacji roboczej lub komputera przenośnego, służących do przetwarzania danych osobowych;
5) niezabezpieczenia hasłem dostępu do komputera służącego do przetwarzania danych osobowych;
6) hasła do systemów przyklejone są w pobliżu komputera lub zapisane są w sposób jawny dla innych osób przebywających w pomieszczeniu biurowym;
7) przechowywania kopii awaryjnych w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych eksploatowane na bieżąco;
8) przechowywania nośników informacji oraz wydruków z danymi osobowymi, nieprzeznaczonymi do udostępniania, w warunkach umożliwiających do nich dostęp osobom nieuprawnionym,
9) pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów;
10) kradzież komputerów, twardych dysków, pendrive lub CD z danymi osobowymi;
11) przebywania osób nieuprawnionych w obszarze, w którym przetwarzane są dane osobowe, w trakcie nieobecności osoby zatrudnionej przy przetwarzaniu tych danych i bez zgody Administratora Danych;

12) pozostawiania bez nadzoru otwartych pomieszczeń, w których przetwarzane są dane osobowe;
13) pozostawiania po godzinach pracy dokumentów nie zabezpieczonych w szafach lub w innych przeznaczonych do tego celu urządzeniach biurowych, posiadających odpowiednie zabezpieczenia, czyli nie stosowania „polityki czystego biurka";
14) ślady na drzwiach, oknach i szafach wskazują na próbę włamania;
15) dokumentacja zawierająca dane osobowe jest niszczona bez użycia niszczarki.

§ 5.
OBOWIĄZKI ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI W PRZYPADKU NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

1. Administrator Bezpieczeństwa Informacji, który stwierdził lub uzyskał informację wskazującą na naruszenie zasad ochrony tych danych zobowiązany jest do niezwłocznego:
1) poinformować o zaistniałym przypadku Administratora Systemu Informatycznego;
2) zapisania wszelkich informacji i okoliczności związanych z danym zdarzeniem, a w szczególności dokładnego czasu uzyskania informacji o naruszeniu zasad ochrony danych osobowych lub czasu samodzielnego wykrycia tego faktu;
3) jeżeli zasoby systemu na to pozwalają, wygenerowania i wydrukowania wszystkich dokumentów i raportów, które mogą pomóc w ustaleniu wszelkich okoliczności zdarzenia, opatrzenia ich datą i podpisania;
4) przystąpienia do zidentyfikowania rodzaju zaistniałego zdarzenia, w tym do określenia skali zniszczeń, metody dostępu osoby niepowołanej do danych itd.;
5) podjęcia odpowiednich kroków w celu powstrzymania lub ograniczenia dostępu osoby niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów naruszenia ochrony danych.

2. Po dokonaniu powyższych zadań ABI dokonuje następujących czynności:
1) przeprowadza szczegółową analizę, w celu określenia przyczyn naruszenia ochrony danych osobowych lub podejrzenia takiego naruszenia, oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości;
2) sprawdza stan urządzeń wykorzystywanych do przetwarzania danych osobowych;
3) kontroluje zawartość zbioru danych osobowych;
4) analizuje skalę zniszczeń i zagrożeń;

5) przygotowuje szczegółowy raport o przyczynach, przebiegu i wnioskach ze zdarzenia, dołączając ewentualne kopie dowodów dokumentujących to zdarzenie oraz w terminie nie przekraczającym 14 dni od daty zaistnienia zdarzenia przekazuje go Administratorowi Danych Osobowych. Wzór raportu z naruszenia bezpieczeństwa danych osobowych stanowi załącznik Nr 1 do niniejszej Instrukcji.

3. Realizacja działań korygujących i zapobiegawczych ABI wynikających z zaistnienia incydentów bezpieczeństwa lub zagrożeń systemu ochrony danych osobowych:

1) w przypadku stwierdzenia konieczności podjęcia działań korygujących lub zapobiegawczych, określa: źródło powstania incydentu lub zagrożenia, zakres działań korygujących lub zapobiegawczych, termin realizacji, osobę odpowiedzialną;
2) prowadzi nadzór nad poprawnością i terminowością wdrażanych działań korygujących lub zapobiegawczych;
3) ocenia efektywność przeprowadzonych działań.

4. Administrator Bezpieczeństwa Informacji prowadzi Rejestr incydentów bezpieczeństwa oraz działań korygujących i zapobiegawczych zgodnie z wzorem przedstawia załącznik Nr 2 do Instrukcji.

§ 6.
OBOWIĄZKI ADMINISTRATORA SYSTEMU INFORMATYCZNEGO W PRZYPADKU NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

1. Administrator Systemu Informatycznego w przypadku naruszenia bezpieczeństwa danych osobowych w systemie informatycznym zobowiązany jest do:

1) podjęcia działań w celu zminimalizowania szkód i zabezpieczenia przed usunięciem śladów naruszenia ochrony danych, w tym między innymi:
   a) fizycznego odłączenia urządzeń i segmentów sieci, które mogły umożliwić dostęp do bazy danych osobie niepowołanej;
   b) wylogowania użytkownika podejrzanego o naruszenie zasad ochrony danych;
   c) zmianę hasła użytkownika (na konto administratora), poprzez którego uzyskano nielegalny dostęp, w celu uniknięcia ponownej próby uzyskania takiego dostępu.
2) przeprowadzenia analizy stanu systemu informatycznego w celu potwierdzenia lub wykluczenia faktu naruszenia zasad ochrony danych osobowych.

2. Po wyeliminowaniu bezpośredniego zagrożenia ASI podejmuje działania, a w szczególności:

1) przywraca normalne działanie systemu, przy czym, jeżeli nastąpiło uszkodzenie bazy danych, odtwarza ją z ostatniej kopii awaryjnej z zachowaniem wszelkich środków ostrożności mających na celu uniknięcie ponownego uzyskania dostępu przez osobę nieupoważnioną, tą samą drogą;
2) jeżeli przyczyna zdarzenia był błąd osoby zatrudnionej przy przetwarzaniu danych osobowych w systemie informatycznym, przeprowadza dodatkowe szkolenie wszystkich osób biorących dział przy przetwarzaniu danych;
3) jeżeli przyczyną zdarzenia było uaktywnienie wirusa, ustala w miarę możliwości źródło jego pochodzenia oraz wykonuje dodatkowe testy i zabezpieczenia antywirusowe;
4) jeżeli przyczyną zdarzenia było włamanie w celu pozyskania danych osobowych, dokonuje szczegółowej analizy wdrożonych środków zabezpieczających, w celu zapewnienia skutecznej ochrony bazy danych;
5) jeżeli przyczyną zdarzenia był zły stan urządzenia lub sposób działania programu, przeprowadza kontrolne czynności serwisowo-programowe.

§ 7.

OBOWIĄZKI ADMINISTRATORA DANYCH OSOBOWYCH W PRZYPADKU NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Administrator Danych Osobowych w przypadku naruszenia danych osobowych podejmuje działania:

1) zasięga porady prawnej i ewentualnie sformułowanie zawiadomienia o przestępstwie;
2) wszczyna postępowanie wyjaśniające, a w uzasadnionych przypadkach postępowanie dyscyplinarne.

§ 8.

SANKCJE KARNE

1. Nieprzestrzeganie zasad postępowania określonych w niniejszej instrukcji stanowi naruszenie obowiązków pracowniczych i może być przyczyną odpowiedzialności dyscyplinarnej określonej w Kodeksie Pracy.

2. Jeżeli skutkiem działania określonego w pkt 1 jest ujawnienie informacji osobie nieupoważnionej, sprawca może zostać pociągnięty do odpowiedzialności karnej wynikającej z przepisów Kodeksu Karnego.

3. Jeżeli skutkiem działania określonego pkt 1 jest szkoda, sprawca ponosi odpowiedzialność materialną na warunkach określonych w przepisach Kodeksu Pracy oraz Prawa Cywilnego.

Załącznik Nr 1 do Instrukcji – Raport o sytuacji naruszenia bezpieczeństwa danych osobowych

Raport
z naruszenia bezpieczeństwa danych osobowych

1. Data: ..... (dd.mm.rrrr) Godzina: ..... (00:00)

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

   .....
   (imię, nazwisko, stanowisko służbowe, nazwa użytkownika – jeśli występuje)

3. Lokalizacja zdarzenia:

   .....
   (np. nr pokoju, nazwa pomieszczenia)

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

   .....

   .....

5. Podjęte działania:

   .....

   .....

6. Przyczyny wystąpienia zdarzenia:

   .....

   .....

7. Postępowanie wyjaśniające:

   .....

   .....

.....
(data, podpis Administratora Bezpieczeństwa Informacji)

Załącznik Nr 2 do Instrukcji – Rejestr incydentów bezpieczeństwa oraz działań korygujących i zapobiegawczych

REJESTR INCYDENTÓW BEZPIECZEŃSTWA ORAZ DZIAŁAŃ KORYGUJĄCYCH I ZAPOBIEGAWCZYCH

Lp.	Zadanie / problem / incydent	Źródło zgłoszenia	Data rozpoczęcia	Data zakończenia	Odpowiedzialny za realizację	Przyczyna niezgodności	Działania korygujące / zapobiegawcze	Ocena skuteczności