Załącznik do Zarządzenia 0050.59.2016
Burmistrza Łobżenicy z dnia 23 czerwca 2016 r.

Obowiązki Administratora Systemu Informatycznego

Administrator Systemu Informatycznego realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym administratora danych, w tym w szczególności:

1. ściśle współpracuje z Administratorem Danych Osobowych, Administratorem Bezpieczeństwa Informacji;
2. zarządza systemem informatycznym, w którym są przetwarzane dane osobowe, posługując się hasłem dostępu do wszystkich stacji roboczych z pozycji administratora;
3. przeciwdziała dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe;
4. wnioskuje do ABI o przydział każdemu użytkownikowi identyfikatora oraz dokonuje ewentualnych modyfikacji uprawnień, a także usuwa konta użytkowników zgodnie z zasadami określonymi w instrukcji zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych;
5. opracowuje działanie mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych;
6. podejmuje działania w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego;
7. wyrejestrowuje użytkowników w uzgodnieniu lub na polecenie administratora danych;
8. zmienia w poszczególnych stacjach roboczych hasła dostępu, ujawniając je wyłącznie danemu użytkownikowi oraz, w razie potrzeby, Administratorowi Bezpieczeństwa Informacji lub Administratorowi Danych;
9. w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego informuje Administratora Bezpieczeństwa Informacji o naruszeniu i współdziała z nim przy usuwaniu skutków naruszenia;
10. prowadzi szczegółową dokumentację naruszeń bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym;
11. jest odpowiedzialny i sprawuje nadzór nad wykonywaniem napraw, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe, nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod katem ich dalszej przydatności do odtwarzania danych w przypadki

awarii systemu informatycznego;

12. podejmuje działania, służące zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji.
13. czuwa nad właściwą archiwizacją dokonywanych zapisów w systemie, sporządza kopie danych zapisanych w systemie w taki sposób, aby utracone dane w przypadkach losowych i innych zdarzeń można było odtworzyć;
14. zapewnia awaryjne zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania. Komputery oraz urządzenia, o których mowa wyżej, powinny być zasilane poprzez zastosowanie specjalnych urządzeń podtrzymujących zasilanie.
15. dopilnowuje, aby komputery przenośne, w których przetwarzane są dane osobowe, były zabezpieczone hasłem dostępu przed nieautoryzowanym uruchomieniem oraz aby mikrokomputery te nie były udostępniane osobom nieupoważnionym do przetwarzania danych osobowych. Osoby posiadające mikrokomputery przenośne z zapisanymi w nich danymi osobowymi należy przeszkolić w kierunku zachowania szczególnej uwagi podczas ich transportu oraz uczulić na to, aby mikrokomputery te przechowywane były we właściwie zabezpieczonym pomieszczeniu.
16. ponosi odpowiedzialność w zakresie :
    a) napraw, konserwacji oraz likwidacji urządzeń komputerowych, na których zapisane są dane osobowe. Dyski i inne informatyczne nośniki danych, zawierające dane osobowe przeznaczone do likwidacji, należy pozbawić zapisu tych danych, a jeśli nie jest to możliwe, należy uszkodzić w sposób uniemożliwiający ich odczyt. Urządzenia przekazywane do naprawy należy pozbawić zapisu danych osobowych lub naprawiać w obecności osoby upoważnionej przez administratora danych.
    b) przestrzegania procedur określających częstotliwość zmiany haseł zgodnie z wytycznymi Instrukcji określającej sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.
    c) sprawdzania systemu pod kątem obecności wirusów komputerowych, częstości ich sprawdzania oraz nadzorowanie wykonywania procedur uaktualniania systemów antywirusowych i ich konfiguracji.
    d) wykonywania kopii awaryjnych, ich przechowywania oraz okresowego sprawdzania pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu,
    e) dokonywania wymaganych okresowych przeglądów, konserwacji oraz uaktualniania systemów służących do przetwarzania danych osobowych oraz dokonywanie wszystkich innymi czynności wykonywanych na bazach danych osobowych.
    f) komunikacji w sieci komputerowej oraz przesyłaniem danych za pośrednictwem urządzeń teletransmisji
    g) właściwego funkcjonowania mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzających dane osobowe oraz kontroli dostępu do danych osobowych a w szczególności poprzez:
        - ustalenie identyfikatorów użytkowników i ich haseł (identyfikatory użytkowników należy wpisać do ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych),
        - dopilnowanie, aby dostęp do danych osobowych przetwarzanych w systemie

był możliwy wyłącznie po podaniu identyfikatora i właściwego hasła,

- dopilnowanie, aby hasła użytkowników były trzymane w tajemnicy (również po upływie terminu ich ważności),
- dopilnowanie, aby identyfikatory osób, które utraciły uprawnienia do przetwarzania danych osobowych, zostały natychmiast wyrejestrowane, a ich hasła unieważnione.

17. Zapewnienie osobom przetwarzającym dane osobowe, aby :
    a) ekrany monitorów stanowisk komputerowych, na których przetwarzane są dane osobowe, automatycznie wyłączały się po upływie ustalonego czasu nieaktywności użytkownika. Zalecanym rozwiązaniem powyższego problemu jest zastosowanie takich wygaszaczy ekranowych, które po upływie określonego czasu bezczynności użytkownika wygaszają monitor i jednocześnie uruchamiają blokadę, która uniemożliwia kontynuowanie pracy na komputerze bez podania właściwego hasła. Wygaszacz taki, oprócz ochrony danych, które przez dłuższy czas byłyby wyświetlane na ekranie monitora, chroniłby system przed przechwyceniem sesji dostępu do danych przez nieuprawnioną osobę.
    b) w pomieszczeniach, gdzie przebywają osoby postronne, monitory stanowisk dostępu do danych osobowych były ustawione w taki sposób, aby uniemożliwić tym osobom wgląd w dane.
18. Podjęcie natychmiastowych działań zabezpieczających stan systemu informatycznego w przypadku otrzymania informacji o naruszeniu zabezpieczeń systemu informatycznego lub o zmianach w sposobie działania programu lub urządzeń wskazujących na naruszenie bezpieczeństwa danych. Działania, o których mowa wyżej, powinny mieć na celu wykrycie przyczyny lub sprawcy zaistniałej sytuacji i jej usunięcie. W przypadku gdy, na przykład, istnieje podejrzenie, że naruszenie bezpieczeństwa danych osobowych zostało spowodowane zaniedbaniem lub naruszeniem dyscypliny pracy, zadaniem administratora bezpieczeństwa informacji powinno być przedstawienie wniosku administratorowi danych o wszczęcie postępowania wyjaśniającego i ukaranie odpowiedzialnych za to osób.
19. ASI zobowiązuje się do stosowania przepisów ustawy o ochronie danych osobowych i aktów wykonawczych wydanych na jej podstawie oraz przyjętych standardów i procedur wewnętrznych Urzędu dotyczących polityki bezpieczeństwa i Instrukcji zarządzania systemem przetwarzania danych osobowych przy użyciu systemu informatycznego i w sposób ręczny w Urzędzie.
20. Administrator Systemu Informatycznego przestrzega niżej wymienionej procedury dotyczącej częstotliwości tworzenia kopii zapasowych.
    1) Zbiory danych osobowych oraz programy i narzędzia programowe służące do ich przetwarzania, zapisywanie na nośnikach zewnętrznych (np. dyski: wymienne, magnetyczne, optyczne) tworzące kopie zapasowe kolejnych okresów, powinny być odpowiednio oznakowane i przechowywane w wyznaczonych, odpowiednio zabezpieczonych pomieszczeniach.
    2) Kopie zapasowe określone w pkt.1 powinny być sporządzane regularnie w okresach wyznaczonych niżej w pkt. 3.
    3) Ustala się następującą częstotliwość tworzenia kopii awaryjnych na nośnikach zewnętrznych – magnetycznych i optycznych:
        a) Kopie tygodniowe, wykonywane przez ASI lub użytkowników obejmujące:
            - dane baz serwerów

b) Kopie miesięczne, umieszczane w zapieczętowanych kopertach, deponowane przez ASI w miejscu wyznaczonym i odpowiednio zabezpieczonym obejmują:
   - dane baz serwerów
c) Kopie tygodniowe przechowywane są do czasu zdeponowania kopii miesięcznych,
d) Kopie miesięczne przechowywane są do czasu zdeponowania kopii rocznej.
e) Niszczenie kopii awaryjnych należy wykonać w sposób określony w instrukcji zachowując szczególna ostrożność przed wydostaniem się informacji na zewnątrz lub w niepowołane ręce.
f) W sytuacjach awaryjnych zaistniałych pod nieobecność ASI lub w razie jego niedyspozycji Administrator Danych udostępnia kopie awaryjne osobie przez siebie wyznaczonej i upoważnionej.

BURMISTRZ
Piotr Łosoś (2)