BURMISTRZ MIASTA
NIESZAWA

Zarządzenie Nr ...7.../2013
BURMISTRZA MIASTA NIESZAWA
z dnia ...12...02.....2013 r.

w sprawie: wprowadzenia w życie Polityki Bezpieczeństwa Informacji w Urzędzie Miasta Nieszawa

Na podstawie art. 36 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity: Dz. U. 2002 r. Nr 101 poz. 926, z póź. zm.) oraz § 3 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 (Dz. U. Nr 100, poz. 1024) zarządzam, co następuje:

§ 1

Dla zapewnienia ochrony przetwarzanych informacji wprowadza się Politykę Bezpieczeństwa Informacji i zarządzania systemem informatycznym służącym do ich przetwarzania w Urzędzie Miasta w Nieszawie stanowiącą załącznik do niniejszego zarządzenia.

§ 2

Polityka Bezpieczeństwa i Instrukcja Zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Miejskim Ośrodku Pomocy Społecznej w Nieszawie ma zastosowanie na wszystkich stanowiskach pracy.

§ 3

Zobowiązuję się pracowników do stosowania zasad określonych w Polityce Bezpieczeństwa i Instrukcji Zarządzania.

§ 4

Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ
mgr Marian Błodziecki

Załącznik nr 1
do Zarządzenia nr 7/2013
z dnia 13.02.2013

Polityka Bezpieczeństwa Informacji i Instrukcja Zarządzania Systemem Informatycznym w Urzędzie Miasta w Nieszawie.

Definicje

§ 1

Określenia i skróty użyte w Polityce Bezpieczeństwa Informacji oznaczają:

1. **Urząd** – Urząd Miejski w Nieszawie,
2. **Administrator Danych Osobowych** – Burmistrz miasta Nieszawy **(dalej ADO)**
3. **Administrator Bezpieczeństwa Informacji** - osoba wyznaczona przez Burmistrza Nieszawy, odpowiedzialna za bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych oraz za sprawność i konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych w przetwarzanych zbiorach danych osobowych **(dalej ABI).**
4. **Administrator Systemów Informatycznych** – osoba wyznaczona przez Burmistrza Miasta (dalej ASI)
5. **Zarządzający oprogramowaniem** – osoba wyznaczona przez Burmistrza Miasta, odpowiedzialna za zarządzanie oprogramowaniem komputerowym w Urzędzie Miejskim w Miasta.
6. **u.o.d.o.** – ustawę z dnia 29 sierpnia 19997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, ze zm.),
7. **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),
8. **Bezpieczeństwo systemu informatycznego** – wdrożenie przez **ADO** lub osobę przez niego uprawnioną środków organizacyjnych i technicznych w celu zabezpieczenia oraz ochrony danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz nieuprawnioną zmianą, utratą, uszkodzeniem lub zniszczeniem.
9. **Przetwarzanie danych osobowych** – wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie.
10. **Osoba upoważniona lub użytkownik systemu** – osoba posiadająca upoważnienie wydane przez ADO lub uprawnioną przez niego osobę i dopuszczona jako użytkownik do przetwarzania danych osobowych w systemie informatycznym danej komórki organizacyjnej w zakresie wskazanym w upoważnieniu, zwana dalej **użytkownikiem.**
11. **Osoba uprawniona** – osoba posiadająca upoważnienie wydane przez ADO do wykonywania w jego imieniu określonych czynności.
12. **Użytkownik uprzywilejowany** – osoba posiadająca najwyższy stopień uprawnień do zarządzania systemem informatycznym.

Polityka bezpieczeństwa danych osobowych
w Urzędzie Miasta w Nieszawie.

Postanowienia ogólne

Polityka bezpieczeństwa w zakresie zarządzania systemem informatycznym służącym do przetwarzania danych osobowych określa reguły postępowania i czynności praktyczne dotyczące zarządzania, ochrony i dystrybucji informacji podlegającej ochronie (danych osobowych).
Polityka bezpieczeństwa w zakresie zarządzania systemem informatycznym służącym do przetwarzania danych osobowych zawiera:

1. identyfikację zasobów systemu informatycznego,
2. wykaz pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe,
3. wykaz zbiorów danych osobowych oraz programów zastosowanych do przetwarzania tych danych,
4. środki techniczne i organizacyjne służące zapewnieniu poufności, integralności i rozliczalności przetwarzanych danych.

Cele

Celem polityki bezpieczeństwa, o której mowa w pkt. 1, jest wskazanie działań, jakie należy podejmować oraz ustanowienie zasad, jakie należy stosować, aby prawidłowo były realizowane obowiązki ADO w zakresie zabezpieczenia danych osobowych.

Identyfikacja zasobów systemu informatycznego

Struktura teleinformatyczna Urzędu Miasta Nieszawa składa się z przewodowej, strukturalnej sieci lokalnej dołączonej do sieci Internet. W ramach tej struktury funkcjonuje system informatyczny służący do rejestrowania i przetwarzania danych osobowych. Podlega on ochronie, zgodnie z przepisami ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2002r. Nr 101, poz. 926 z późn. zm.), zwanej dalej "ustawą".

W ramach tej infrastruktury funkcjonuje system usług sieciowych. Zawierają one dane podlegające ochronie ze względu na powyższą ustawę oraz są strategiczne dla ciągłości pracy i funkcjonowania Urzędu.

Podstawowymi systemami informatycznymi w Urzędzie są:

- Płatnik - program wymagany do rozliczenia z Zakładem Ubezpieczeń Społecznych
- Gratyfikant GT
- KSZOB
- PODATKI
- BESTI@

Ze względu na różnorodność systemów i przetwarzanych danych oraz fakt połączenia z globalną siecią Internet, zapewnienie właściwej ochrony systemu informatycznego jest zagadnieniem złożonym.

Wykaz pomieszczeń tworzących obszar przetwarzania danych osobowych

Przetwarzanie danych osobowych jest wykonywaniem jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zamienianie, udostępnianie i usuwanie, a zwłaszcza takich, które wykonuje się w systemach informatycznych. Biorąc pod uwagę przepisy ustawy, nakazujące jej stosowanie także w przypadkach przetwarzania danych poza zbiorem danych, przetwarzanie danych osobowych może wystąpić w większości pomieszczeń Urzędu Miasta. Ze względu jednak na szczególne nagromadzenia danych osobowych, szczególnie chronione powinny być pomieszczenia, w których znajdują się elementy struktury informatycznej przechowujące, przetwarzające i udostępniające dane osobowe (jak serwery baz danych), przechowujące i składujące kopie zapasowe.

Wykaz zbiorów danych osobowych

- Dokumentacja papierowa (korespondencja, wnioski, deklaracje, itp.),
- Wydruki komputerowe,
- Bazy wykorzystywane przez oprogramowanie wskazane w rozdziale drugim.

Środki techniczne i organizacyjne służące zapewnieniu poufności, integralności i rozliczalności przetwarzania danych

System informatyczny, ze względu na połączenie z siecią publiczną, musi zapewniać środki bezpieczeństwa określone dla wysokiego poziomu bezpieczeństwa (§ 6 ust. 4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dania 29 kwietnia 2004r. 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).

1. Bezpieczeństwo fizyczne

Gwarancją zapewnienia bezpieczeństwa systemu informatycznego oraz przetwarzanych i przechowywanych danych jest zapewnienie bezpieczeństwa fizycznego. Warunkiem zapewnienia bezpieczeństwa fizycznego systemu jest kontrola dostępu do wszystkich stacji roboczych. W związku z tym szczególną ochroną obejmuje się pomieszczenia, w których znajdują się węzły sieci oraz te, w których przechowywane są i składowane dane. Wymienione pomieszczenia powinny być stale zamknięte, a dostęp do nich powinny mieć tylko upoważnione osoby.

2. Zarządzanie oprogramowaniem

ADO wyznacza ASI, który posiada najwyższe uprawnienia w systemie informatycznym. Tylko ASI jest

osobą uprawnioną do instalowania i usuwania oprogramowania systemowego i narzędziowego. Dopuszcza się instalowanie tylko legalnie pozyskanych programów, niezbędnych do wykonywania ustawowych zadań Urzędu i posiadających ważną licencję użytkowania.

Uwierzytelnianie użytkowników

Dostęp do systemu informatycznego służącego do przetwarzania danych osobowych może uzyskać wyłącznie osoba (użytkownik) zarejestrowana w tym systemie przez ASI na wniosek ABI.
Dostęp do systemów operacyjnych serwerów i stacji roboczych powinien być chroniony przez nazwę użytkownika i hasło. Zespół ten tworzy jedną z głównych linii obrony przed intruzami. Dlatego należy uświadamiać użytkownikom rolę, jaką w systemie ochrony odgrywa dobrze wybrane i trudne hasło o odpowiednio dobranym czasie życia (wygaśnięcia). Jednocześnie należy wdrożyć mechanizmy systemowe kontrolujące składnię i czas życia haseł. System powinien mieć wbudowane mechanizmy ograniczające liczbę błędnych prób logowania oraz umożliwiające wskazanie stacji roboczych, na których dany użytkownik może pracować. Zalecane jest ustawienie blokady konta użytkownika na 3 do 5 prób logowania.

Hasło powinno składać się z unikalnego zestawu co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne. Hasło nie może być identyczne z identyfikatorem użytkownika, ani jego imieniem lub nazwiskiem. Hasła powinny być okresowo zmieniane (co 30-90 dni).Użytkownikowi systemu nie wolno udostępniać swojego identyfikatora ani hasła innym osobom.

Redundancja sprzętowa i programowa

Dla zapewnienia wysokiej niezawodności systemu ASI opracowuje i wprowadza procedury awaryjne (np. w wypadku uszkodzenia głównego serwera/komputera/urządzenia gromadzącego dane).
Należy rygorystycznie przestrzegać wymogu przechowywania nośników zawierających awaryjne kopie danych i systemów w pomieszczeniach innych niż pomieszczenia, w których przechowywane są dane przeznaczone do bieżącego użytku.

Zapewnienie stałego zasilania energią

Ciągłe zasilanie serwerom zapewniać powinno stosowanie zasilaczy awaryjnych UPS. W przypadku stacji roboczych, UPS stosuje się w zależności od potrzeb i możliwości finansowych.

Procedury awaryjne i procedury na wypadek klęsk żywiołowych i ewakuacji

Zapewnieniu ciągłej dostępności informacji służą procedury postępowania w przypadku wydarzeń losowych (np. awaria serwera, zalanie pomieszczenia, pożar, itp.). Procedury takie powinny obejmować uruchomienie systemu w minimalnej konfiguracji udostępniającej zasoby systemu. Komputery przewidywane na awaryjne serwery powinny stać w pomieszczeniach innych niż serwery na bieżąco eksploatowane. W przypadku ewakuacji należy w pierwszej kolejności zapewnić bezpieczeństwo danym.

Profilaktyka antywirusowa

Wszystkie serwery a także wszystkie stacje robocze uczestniczące w przetwarzaniu danych osobowych muszą posiadać zainstalowany i aktualny system antywirusowy sprawdzający w trybie rzeczywistym wszystkie pliki zapisywane i odczytywane, a także monitorować połączenia internetowe oraz pocztę elektroniczną. Baza definicji wirusów powinna być aktualizowana możliwie jak najczęściej. Zabronione jest blokowanie pracy tego programu. Dla zapewnienia ochrony przed wirusami serwer oraz stacje robocze powinny być okresowo (nie rzadziej niż co dwa miesiące) objęte pełnym testem antywirusowym.

Przeciwdziałanie nowym technikom łamania zabezpieczeń oraz eliminacja luk wykrytych w zabezpieczeniach systemów

W związku z dynamicznym rozwojem technik służących do atakowania systemów informatycznych, ASI powinien na bieżąco śledzić informacje na temat wykrytych luk i wprowadzać zalecane zabezpieczenia (jak łaty dla systemów operacyjnych i aktualizacja oprogramowania).

Procedury postępowania z nośnikami informacji i wydrukami (wytwarzanie, rejestrowanie, kasowanie, niszczenie

Dla zachowania wysokiego poziomu bezpieczeństwa informacji w systemie informatycznym określa się procedury postępowania z nośnikami (dyskietki, płyty CD/DVD, nośniki papierowe) zawierającymi informacje od chwili wytworzenia do chwili skasowania lub zniszczenia. Dla zapewnienie szczelności systemu powinno się dążyć do pełnego ewidencjonowania i opisu nośników zawierających newralgiczne dane.

Zabezpieczenia medium transmisyjnego

Połączenia z sieci wewnętrznej do sieci zewnętrznej (Internet) mogą być wykonywane tylko za pośrednictwem routerów wyposażonych w odpowiednio skonfigurowaną zaporę firewall. Zasada konfigurowania zapory ogniowej powinna uwzględniać blokowanie wszelkich usług nie będących niezbędnymi do prawidłowego funkcjonowania. Powinny być także blokowane wszelkie połączenia przychodzące z sieci zewnętrznej, które nie są powiązane zapoczątkowanymi połączeniami wychodzącymi z sieci wewnętrznej (established/related).

Postanowienia ogólne

§1

Niniejsza „ Polityka Bezpieczeństwa Informacji", ma zastosowanie do ochrony zbiorów danych osobowych przetwarzanych w Urzędzie Miasta w Nieszawie, w celu ich bezpiecznego wykorzystania oraz określa zasady korzystania z systemów informatycznych.

§2

Niniejsza "Polityka Bezpieczeństwa Informacji" określa:

1. sposób przydziału haseł dla użytkowników i częstotliwość ich zmiany oraz osoby odpowiedzialne za te czynności,
2. sposób rejestrowania i wyrejestrowywania użytkowników oraz osoby odpowiedzialne za te czynności,
3. procedury rozpoczynania i kończenia pracy,
4. metodę i częstotliwość tworzenia kopii awaryjnych,
5. metodę i częstotliwość sprawdzania obecności wirusów komputerowych oraz metodę ich usuwania,
6. sposób i czas przechowywania nośników informacji, w tym kopii informatycznych i wydruków,
7. sposób dokonywania przeglądów i konserwacji systemu i zbioru danych osobowych, sposób postępowania w zakresie komunikacji w sieci komputerowej.

§2

Podstawowe zasady przetwarzania danych osobowych;

1. Przetwarzanie danych osobowych może odbywać się zgodnie z obowiązującą ustawą o ochronie danych osobowych oraz wykonawczymi dokumentami normatywnymi.
2. Osobą odpowiedzialną za bezpieczeństwo danych w systemach informatycznych przetwarzających dane osobowe jest ABI.
3. Przetwarzanie danych osobowych jest możliwe tylko przez uprawnione osoby w wyznaczonym przez ADO obszarze (budynku, pomieszczeniu lub części pomieszczenia) podlegającym szczególnej ochronie bezpieczeństwa.
4. Udostępnianie danych osobowych może odbywać się tylko za zgodą ADO na wniosek przygotowany w oparciu o art. 29 ust. 1 ustawy o ochronie danych osobowych oraz wg wzoru określonego w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998r. (Dz. U. Nr 80, poz. 522), chyba, że przepis innej ustawy stanowi inaczej.
5. Zgodnie z ustawą o ochronie danych osobowych, udostępniane dane mogą być wykorzystane wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione (art. 29 ust 4) a przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania (art. 26 ust. 1 pkt. 4).

§3

1. Dostęp do systemu informatycznego służącego do przetwarzania danych osobowych, zwanego dalej "systemem" może uzyskać wyłącznie osoba (użytkownik) zarejestrowana w tym systemie przez ABI.
2. Rejestracja, o której mowa w ust. 1, polega na nadaniu identyfikatora i przydziale hasła oraz wprowadzeniu tych danych do bazy użytkowników systemu.

§4

1. Hasło powinno składać się z unikalnego zestawu co najmniej ośmiu znaków, zwierać małe i wielkie litery oraz cyfry lub znaki specjalne.
2. Hasło nie może być identyczne z identyfikatorem użytkownika ani jego imieniem lub nazwiskiem.
3. Zmiana hasła następuje w okresach od 30 do 90 dni.
4. Zabrania się użytkownikom systemu udostępniania swojego identyfikatora i hasła innym osobom.

§5

1. Wyrejestrowania użytkownika z systemu informatycznego dokonuje ABI.
2. Wyrejestrowanie, o którym mowa w ust. 1, może mieć charakter tymczasowy lub stały.
3. Wyrejestrowanie następuje poprzez:

1. zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe),
2. usunięcie danych użytkownika z bazy użytkowników systemu (wyrejestrowanie trwałe).

4. Przyczyną czasowego wyrejestrowania użytkownika z systemu informatycznego jest:
   1. nieobecność w pracy trwająca dłużej niż 31 dni kalendarzowych,
   2. zawieszenie w pełnieniu obowiązków służbowych,
   3. zwolnienie z pełnienia obowiązków służbowych.
5. Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy użytkownika.

§6

Rozpoczęcie pracy w systemie odbywa się poprzez:
1. przygotowanie stanowiska pracy,
2. włączenie stacji roboczej,
3. wprowadzenie swojego identyfikatora i hasła.

§7

Zakończenie pracy w systemie odbywa się poprzez:
1. zamknięcie aplikacji,
2. odłączenie od zasobów systemowych,
3. zamknięcie połączenia z serwerem,
4. zamknięcie systemu operacyjnego,
5. wyłączenie stacji roboczej.

§8

Zabrania się użytkownikom:
1. udostępniania stacji roboczej osobom niezarejestrowanym w systemie w trybie określonym w §1 ust. 2,
2. udostępniania stacji roboczej do konserwacji lub naprawy bez porozumienia z ABI,
3. użytkowania nielicencjonowanego oprogramowania,
4. samodzielnego instalowania oprogramowania,
5. używania w stacjach roboczych własnych, niezatwierdzonych przez ADO (dyskietki, płyty CD/DVD, urządzenia masowe USB, itp.),
6. używania stacji roboczych do czynności innych niż służbowe.

§9

1. Każdy przypadek naruszenia ochrony danych osobowych podlega zgłoszeniu do ABI, a w szczególności:
   1. naruszenie bezpieczeństwa systemu informatycznego,
   2. stwierdzenie objawów (stanu urządzeń, sposobu działania programu lub jakości komunikacji w sieci), które mogą wskazywać na naruszenie bezpieczeństwa.
2. ABI 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 lub rekordów,
   4. przebywania osób nieupoważnionych w obszarze, w którym przetwarzane są dane osobowe, w trakcie nieobecności osoby zatrudnionej przy przetwarzaniu tych danych i bez zgody ADO, pozostawiania bez nadzoru otwartych pomieszczeń, w których przetwarzane są dane osobowe,

5. udostępniania osobom nieuprawnionym stacji roboczej lub komputera przenośnego, służących do przetwarzania danych osobowych,
6. niezabezpieczenia hasłem dostępu do komputera służącego do przetwarzania danych osobowych,
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.

3. Obowiązek dokonania zgłoszenia, o którym mowa w ust. 1, spoczywa na każdym pracowniku, który powziął wiadomość o naruszeniu ochrony danych osobowych.
4. W przypadku naruszenia integralności bezpieczeństwa sieciowego, obowiązkiem ABI jest natychmiastowe wstrzymanie udostępniania zasobów dla użytkowników i odłączenie magazynów danych od sieci.
5. ASI w porozumieniu z ABI ustalają przyczyny naruszenia integralności bezpieczeństwa sieciowego.
6. Przywrócenie udostępniania zasobów użytkownikom może nastąpić dopiero po ustaleniu i usunięciu przyczyny naruszenia integralności bezpieczeństwa sieciowego.

§10

1. Za sporządzanie kopii bezpieczeństwa informacji znajdujących się na serwerach odpowiada ASI. Wykonywanie kopii bezpieczeństwa danych znajdujących się na stacjach roboczych należy do użytkowników. Dopuszcza się wykonywanie kopii bezpieczeństwa przy wykorzystaniu dyskietek, płyt CD/DVD, streamerów, dysków twardych i innych urządzeń zapewniających odpowiednią trwałość przechowywanych danych. Zaleca się korzystanie z udostępnionego na każdej maszynie dysku sieciowego. Zaleca się zapisywanie istotnych zbiorów danych na udostępnionych przez ASI dyskach sieciowych dostępnych na serwerze.
2. Zabrania się przechowywania kopii awaryjnych w pomieszczeniach przeznaczonych do przechowywania zbiorów danych pozostających w bieżącym użytku.
3. ASI przegląda okresowo kopie awaryjne i ocenia ich przydatność do odtworzenia zasobów systemu w przypadku jego awarii.
4. Stwierdzenie utraty przez kopie awaryjne waloru przydatności do celu, o którym mowa w ust. 4, upoważnia ASI do ich zniszczenia.

§11

1. Sprawdzanie obecności wirusów komputerowych w systemie oraz ich usuwanie odbywa się przy wykorzystaniu licencjonowanego oprogramowania w oparciu o serwer dystrybucji aktualnych sygnatur i wersji oprogramowania.
2. Oprogramowanie, o którym mowa w ust. 1, sprawuje ciągły nadzór nad pracą systemu i jego zasobami oraz serwerami i stacjami roboczymi.
3. Za sprawdzenie obecności wirusów na stacjach roboczych odpowiedzialni są użytkownicy systemu. Sprawdzenie nie powinno być wykonywane rzadziej niż raz na dwa miesiące.
4. W przypadku pozytywnego wyniku testu (wykrycie wirusa), o którym mowa w ust. 4, użytkownik systemu zobowiązany jest niezwłocznie powiadomić o tym fakcie ASI i zaprzestać przetwarzania danych osobowych do czasu usunięcia problemu.
5. Do obowiązków ASI należy aktualizacja oprogramowania służącego do sprawdzania w systemie oraz na serwerach obecności wirusów komputerowych.
6. W przypadku problemów z wykonaniem aktualizacji, o której mowa w ust. 7, użytkownik systemu zobowiązany jest do natychmiastowego powiadomienia o tym fakcie ASI.

§12

1. System i urządzenia informatyczne służące do przetwarzania danych osobowych, zasilanie energią elektryczną, zabezpiecza się przed utratą danych osobowych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.
2. Minimalne zabezpieczenie systemu i urządzeń informatycznych, o których mowa w ust. 1, polega na wyposażeniu serwerów oraz stacji roboczych w zasilacze awaryjne (UPS).

§13

1. Urządzenia informatyczne służące do przetwarzania danych osobowych można przekazać:
    1. do naprawy,
    2. podmiotowi nieuprawnionemu do otrzymania tych danych,
    3. do likwidacji dopiero po uprzednim uzyskaniu zgody ABI.
2. Urządzenia, o których mowa w ust. 1, przed ich przekazaniem pozbawia się zapisu danych osobowych.
3. Jeżeli nie jest możliwe pozbawienie urządzenia przekazywanego do likwidacji zapisu danych osobowych, urządzenie - przed przekazaniem - uszkadza się w sposób uniemożliwiający odczytanie tych danych.

§14

1. Przeglądu i konserwacji systemu dokonuje ASI doraźnie.
2. Przeglądu plików zawierających raport dotyczący działalności aplikacji bądź systemu (log systemowy) ASI dokonuje nie rzadziej niż raz na dwa tygodnie.
3. Przeglądu i sprawdzenia poprawności zbiorów danych zawierających dane osobowe dokonuje użytkownik systemu przy współudziale ASI nie rzadziej niż raz na dwa tygodnie.

§15

1. Bezpieczeństwo komunikacji w obrębie systemów przetwarzających dane osobowe ASI zapewnia przy użyciu narzędzi w obrębie systemu.
2. W systemach działających sieciowo, na zasadzie udostępniania zasobów na serwerze, ASI powinien uwzględniać dedykowane przyzwolenia dostępu.

§16

1. Przesyłanie danych osobowych w komunikacji wewnętrznej (LAN) musi być wykonane w sposób umożliwiający dostęp tylko użytkownikom uprawnionym i wyznaczonym przez ASI, przy użyciu narzędzi zabezpieczeń w obrębie systemu informatycznego.
2. W sytuacji, gdy dostępne narzędzia informatyczne nie będą wystarczające do działania w komunikacji wewnętrznej, ASI wyznacza sposób postępowania, mając w szczególności na uwadze ochronę danych osobowych.

§17

Do przesyłania danych przy połączeniach w sieci publicznej (Internet), z uwagi na przekazywane dane osobowe, powinny być wykorzystywane tylko kanały transmisji wykorzystywane przez autoryzowane programy wykorzystywane również w innych urzędach oraz instytucjach państwowych z uwzględnieniem przepisów prawnych uwzględniających wysyłanie tych danych.

§18

Nośniki informatyczne zawierające dane osobowe powinny być opisane w sposób czytelny i zrozumiały dla użytkownika, a zarazem nie powinny ułatwiać rozpoznania zawartości przez osoby nieupoważnione.

§19

1. Nośniki informatyczne przechowywane są w miejscach, do których dostęp mają wyłącznie osoby upoważnione.
2. W pomieszczeniach, gdzie nie jest możliwe ograniczenie dostępu osób postronnych, monitory stanowisk dostępu do danych osobowych ustawia się w taki sposób, aby uniemożliwić tym osobom wgląd w dane.
3. Ekrany monitorów stanowisk dostępu do danych osobowych są zaopatrzone w wygaszacze z ustawioną opcją wymagania hasła, które po upływie maksymalnie 10 minut nieaktywności użytkownika automatycznie wyłączają funkcję eksploatacji ekranu.

§20

Osoby użytkujące przenośne nośniki informatyczne, służące do przetwarzania danych osobowych, obowiązane są niezwłocznie informować na piśmie ABI o zakresie, rodzaju zbieranych danych osobowych oraz celu ich przetwarzania. ABI może żądać usunięcia danych, co do których zachodzi uzasadnione podejrzenie, że nie są przetwarzane zgodnie z zasadami określonymi w przepisach o ochronie danych osobowych.

§21

Osoba użytkująca przenośny komputer, służący do przetwarzania danych osobowych, obowiązana jest zachować szczególną ostrożność podczas transportu i przechowywania tego komputera poza obszarem ochrony danych w celu zapobieżenia dostępowi do tych danych osobie niepowołanej.

§22

1. Wszystkie komputery (serwery i stacje robocze) biorące udział w przetwarzaniu danych osobowych są wyposażone w oprogramowanie antywirusowe. Zabrania się wyłączania tego oprogramowania. Dane zawarte na nośnikach zewnętrznych (np. dyskietki) muszą być sprawdzone przez program antywirusowy przed wprowadzeniem ich do systemu. W przypadku jakichkolwiek wątpliwości odnośnie zagrożenia wirusowego należy sprawdzić zawartość całego dysku twardego programem antywirusowym. W przypadku dalszych niejasności należy kontaktować się z ASI.
2. Użytkownicy stacji roboczych nie mają prawa dokonywać samodzielnie jakichkolwiek instalacji oprogramowania zarówno na stacjach roboczych, jak i na serwerach sieci. Za instalację i konfigurację oprogramowania odpowiadają wyznaczone osoby zajmujące się administracją. ASI i ABI są odpowiedzialni za instalację uaktualnień oprogramowania.
3. ASI przygotowuje a ADO zatwierdza listę oprogramowania dopuszczoną do użytkowania na stacjach roboczych w zależności od typu prac na nich wykonywanych.
4. Zabrania się wszelkich prac z wykorzystaniem oprogramowania, na które użytkownik nie ma ważnej licencji (zakaz nie dotyczy programów, na użytkowanie których licencja nie jest wymagana) lub niewiadomego pochodzenia.
5. Przy wprowadzaniu do systemu nowych programów lub danych zawsze należy kierować się zasadą ograniczonego zaufania.

§23

Wykonywanie prac pozasłużbowych na komputerach dopuszcza się w wyjątkowych przypadkach - za zgodą przełożonych.

§24

Zabrania się pozostawiania sprzętu komputerowego niezabezpieczonego przed dostępem osób

nieuprawnionych, bez nadzoru osoby odpowiedzialnej za jego użytkowanie. Zalecane jest stosowanie wygaszaczy ekranu zabezpieczonych hasłem.

§25

1. Użytkownik systemu sporządzający wydruki, które zwierają dane osobowe jest odpowiedzialny za zachowanie szczególnej ostrożności przy korzystaniu z nich, a zwłaszcza za zabezpieczenie ich przed dostępem osób nie posiadających imiennego upoważnienia oraz nieuprawnionych do wglądu na podstawie indywidualnego zakresu czynności.
2. Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.