ZARZĄDZENIE Nr 22/2016
BURMISTRZA ZWOLENIA
z dnia 15 lutego 2016r.

w sprawie wprowadzenia Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Miejskim w Zwoleniu

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990r. o samorządzie gminnym (Dz.U. z 2015r. poz.1515, z późn. zm.), art.36 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz.U. z 2015r. poz. 2135, z późń. zm.)zarządzam, co następuje:

§1.

Wprowadzam Instrukcję zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Miejskim w Zwoleniu stanowiącą załącznik do niniejszego zarządzenia .

§2.

Wykonanie zarządzenia powierzam Administratorowi Bezpieczeństwa Informacji.

§3.

Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ
mgr inż. Bogusława Jaworska

RADCA PRAWNY
mgr Anna Kołłątaj
KL - R - 238

Załącznik do zarządzenia nr 22/2016
Burmistrza Zwolenia z dnia 15 lutego 2016 r.

Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Miejskim w Zwoleniu

Spis treści

§ 1.
Wstęp

Instrukcja stanowi zestaw procedur opisujących zasady zapewnienia bezpieczeństwa danych osobowych w systemach i aplikacjach informatycznych.

Zawarte są w niej ogólne zasady zarządzania każdym systemem informatycznym służącym do przetwarzania danych osobowych w **Urzędzie Miejskim w Zwoleniu.**

Ponadto stanowi ona podstawę do opracowania instrukcji szczegółowych uwzględniających specyfikę poszczególnych systemów informatycznych.

§ 2.
Bezpieczeństwo eksploatacji sprzętu i oprogramowania

1. Sprzęt służący do przetwarzania danych osobowych składa się z komputerów klasy PC, notebooków oraz serwerów.
2. Sieć komputerowa służąca do przetwarzania danych osobowych posiada zapewnione prawidłowe zasilanie energetyczne gwarantujące właściwe i zgodne z wymaganiami producenta działanie sprzętu komputerowego.
3. Główne węzły są podtrzymywane przez UPS zapewniający odpowiedni czas pracy systemu.
4. Programy zainstalowane na komputerach obsługujących przetwarzania danych osobowych są użytkowane z zachowaniem praw autorskich i posiadają licencje.
5. ASI odpowiada za wyposażenie systemu informatycznego w mechanizmy uwierzytelnienia użytkownika oraz za stosowanie kontroli dostępu do danych osobowych jedynie osób upoważnionych.
6. Ekrany monitorów są wyposażone w wygaszacze zabezpieczone hasłem, które aktywuje się automatyczne po upływie określonego czasu od ostatniego użycia komputera.
7. Ekrany monitorów, są ustawione w taki sposób, żeby w miarę możliwości uniemożliwić odczyt wyświetlanych informacji osobom nieupoważnionym.

§ 3.
Procedura nadawania uprawnień do przetwarzania danych osobowych

1. Do przetwarzania danych osobowych w systemie informatycznym mogą być dopuszczone wyłącznie osoby posiadające upoważnienia do przetwarzania danych osobowych.
2. ABI składa do ASI wniosek o przyznanie uprawnień.

3. Użytkownikom systemu, którzy przetwarzają dane osobowe w systemie informatycznym na podstawie upoważnienia, o którym mowa w ust. 1 przyznawane są indywidualne identyfikatory z hasłem inicjującym.
4. ADI na podstawie upoważnienia, o którym mowa w ust. 1, rejestruje użytkownika w systemie oraz nadaje mu identyfikator.
5. Identyfikator użytkownika wraz z jego imieniem i nazwiskiem ASI przekazuje ABI w celu wpisania do Ewidencji osób upoważnionych do przetwarzania danych osobowych.
6. Dostęp do danych osobowych przetwarzanych w systemie informatycznym jest możliwy wyłącznie po wpisaniu identyfikatora i hasła.
7. Identyfikator użytkownika systemu stanowi ciąg znaków jednocześnie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym
8. Hasło użytkownika systemu stanowi ciąg znaków literowych, cyfrowych lub innych, przypisane do identyfikatora użytkownika systemu, znane jedynie jemu.
9. W przypadku zmiany przez użytkownika uprawnień do obsługi danego systemu ABI występuje z wnioskiem do ASI o modyfikację uprawnień.
10. W przypadku utraty przez użytkownika uprawnień do obsługi danego systemu informatycznego (np. rozwiązanie stosunku pracy, nieobsługiwania systemu z powodu zmiany stosunku pracy) ABI występuje do ASI z wnioskiem o anulowanie upoważnienie do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych.
11. Identyfikator użytkownika systemu nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego nie powinien być przydzielony innej osobie.
12. ASI posiada przydzielony przez ADO w systemie informatycznym identyfikator użytkownika uprzywilejowanego.
13. Użytkownikom systemu zabrania się:
    - ujawniania własnego identyfikatora i hasła współpracownikom i osobom z zewnątrz,
    - udostępniania stanowisk pracy z danymi osobowymi osobom nieuprawnionym,
    - pozostawianie własnych haseł w miejscach, do których mogą mieć dostęp inne osoby,
    - korzystanie z komputerów nie związanych z własnym miejscem pracy,
    - udostępnianie osobom nieuprawnionym jakichkolwiek informacji na temat programów komputerowych zainstalowanych w systemie.

§ 4.
Metody i środki uwierzytelnienia.

1. Pierwsze hasła dla system przydziela ASI przy wprowadzaniu identyfikatora użytkownika systemu.
2. Użytkownik systemu jest zobowiązany do natychmiastowej zmiany hasła inicjującego.
3. ASI wymusza zmianę haseł inicjujących wszystkim użytkownikom systemu.
4. Hasło użytkownika systemu powinno mieć minimum 8 znaków i być zmieniane co 30 dni oraz niezwłocznie w przypadku podejrzenia, że hasło mogło zostać ujawnione.
5. Hasło użytkownika systemu zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.
6. Hasło wpisywane z klawiatury nie może pojawiać się na ekranie monitora w formie jawnej.
7. Za systematyczną zmianę hasła odpowiada użytkownik systemu.
8. W systemie, w którym nie następuje automatyczne wymuszenie zmiany hasła, hasło zmienia użytkownik systemu.
9. Użytkownik systemu niezwłocznie ustala swoje, znane tylko jemu hasło dostępu.
10. Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako hasło wykorzystywać: dat, imion, nazwisk, inicjałów itp.
11. Właścicielem hasła jest użytkownik systemu.
12. Zabronione jest zapisywanie haseł w sposób jawny oraz przekazywanie ich innym osobom.
13. Osoba odpowiedzialna za przydział haseł i częstotliwość ich zmian, a także w zakresie rejestrowania i wyrejestrowania użytkowników jest ASI
14. Za wszelkie operacje w systemie wykonywane z wykorzystaniem indywidualnego identyfikatora oraz haseł odpowiada właściciel identyfikatora.
15. W przypadku, gdy zaistnieje podejrzenie, że dane hasło poznała osoba nieuprawniona, użytkownik systemu jest zobowiązany do niezwłocznego powiadomienia o powyższym fakcie ABI celem wszczęcia i zastosowania przewidzianych w takich sytuacjach procedur, a także do natychmiastowej zmiany hasła powiadomienia ASI.

§ 5.
Hasła ASI

1. ASI zobowiązany jest zmieniać swoje hasło nie rzadziej niż co 30 dni.

2. Hasło skład się z co najmniej 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.
3. Hasła administratora wymieniane powinny być spisane oraz umieszczone w zamkniętych kopertach odrębnych dla każdego z systemów w miejscach uniemożliwiających dostęp do nich osób nieupoważnionych, chroniącym przed utratą lub zniszczeniem oraz gwarantujących ich odczytania upoważnionemu użytkownikowi, a także ADO w przypadku nadzwyczajnym.
4. Zarejestrowane hasła administratora, oprócz treści haseł winny posiadać adnotację o dacie ich wprowadzenia do systemu oraz być przechowywane przez okres 5 lat.
5. W przypadku utraty uprawnień przez osobę administrującą systemem należy niezwłocznie zmienić hasło, do których miała dostęp.

§ 6.
Procedura rozpoczęcia, zawieszenia i zakończenia pracy

1. Rozpoczęcie pracy na komputerze przez użytkownika systemu następuje po poprawnym zalogowaniu się do systemu informatycznego (uwierzytelnieniu).
2. Rozpoczęcie pracy w aplikacji musi być prowadzone zgonie z instrukcją zawartą w dokumentacji technicznej aplikacji, a w przypadku braku takiej dokumentacji według zasad opracowanych przez ASI.
3. Przed opuszczeniem stanowiska pracy, użytkownik systemu obowiązany jest wylogować się z systemu lub wywołać blokadę wygaszaczem ekranu.
4. Kontynuacja pracy po powrocie powinna być możliwa jedynie po ponownym uwierzytelnieniu lub po wprowadzeniu hasła.
5. Zakończenie pracy w systemie informatycznym polega na przeprowadzeniu operacji wylogowania z systemu, a także poprzez uruchomienie odpowiedniej dla systemu wersji jego zamknięcia, w przypadku braku takiej dokumentacji według zasad opracowanych przez ASI oraz po wyłączeniu systemu komputerowego.
6. Użytkownik systemu jest zobowiązany upewnić się czy proces wylogowania zakończył się pomyślnie.
7. Po zakończeniu pracy w systemie informatycznym użytkownik systemu jest zobowiązany zabezpieczyć stanowisko pracy a w szczególności wszelką dokumentację oraz nośniki magnetyczne i optyczne, na których znajdują się dane osobowe.
8. Jakiekolwiek stanowiska komputerowe nie mogą pozostawać z uruchomionym i dostępnym systemem bez dozoru pracującego na nim użytkownika systemu.

9. Każdy użytkownik systemu w przypadku podejrzenia fizycznej ingerencji w przetwarzane dane osobowe, używane narzędzia programowe, a także sprzętowe zobowiązany jest do natychmiastowego zaprzestania pracy i wyłączenie sprzętu.
10. Każdy użytkownik systemu niezwłocznie o faktach w ust. 9 powiadamia ABI, a także ASI.
11. Każdy użytkownik systemu niezwłocznie powiadamia ASI w przypadku braku możliwości zalogowania się na swoje konto lub o jakichkolwiek trudnościach i występujących przy tym trudnościach.
12. ABI lub ASI monitoruje rozpoczęcie i zakończenie pracy systemu informatycznego.
13. ABI lub ASI ma prawo do monitorowania pracy urządzeń przyłączonych do sieci informatycznej w zakresie przesyłania i przetwarzania danych, rejestracji zdarzeń związanych z przesyłaniem i przetwarzaniem danych w oprogramowaniu oraz prawidłowości wykorzystania powierzonego użytkownikom systemu sprzętu i oprogramowania.
14. Informacje pozyskane w wyniku monitorowania działań użytkowników systemu oraz pracy urządzeń mogą zostać wykorzystane wyłącznie do celów służbowych, związanych z bezpieczeństwem przetwarzania danych osobowych w systemach informatycznych.

§ 7.
Procedura tworzenia kopii zapasowych

1. Zbiory danych osobowych przetwarzanych w systemie informatycznym, są dodatkowo zabezpieczone przed utratą lub uszkodzeniem za pomocą centralnego UPS-a zabezpieczającego przed awarią zasilania lub zakłóceń w sieci. Dodatkowo są tworzone kopie bezpieczeństwa danych na serwerze i komputerach gdzie przechowywane są bazy danych.
2. Za tworzenie kopii zapasowych systemu informatycznego odpowiedzialny jest ASI.
3. Kopie są wykonywane raz dziennie po zakończeniu dziennej obsługi systemu.

§ 8.
Sposób, miejsce i okres przechowywania elektronicznych nośników informacji, kopii zapasowych i wydruków

1. Wszelkie nośniki informatyczne zawierające dane osobowe, przeznaczone do przekazania innemu podmiotowi, nieupoważnionemu do otrzymania danych osobowych, pozbawia się zapisu tych danych.
2. Urządzenia, dyski lub inne informatyczne nośniki zawierające dane osobowe przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych,

a w przypadku gdy nie jest to możliwe, nośniki niszczy się trwale w sposób uniemożliwiający odczyt danych.

3. Usuwanie danych z systemu musi być zrealizowane przy pomocy właściwego oprogramowania przeznaczonego do bezpiecznego usuwania danych z nośnika informacji. Za wskazany proces odpowiada ASI.
4. W przypadku nośników informacji, przez ich zniszczenie rozumie się ich trwałe i nieodwracalne zniszczenie do stanu nie dającego możliwości odzyskania danych.
5. Decyzję o likwidacji danych osobowych przetwarzanych bezpośrednio w systemie informatycznym oraz danych osobowych przechowywanych w kopiach zapasowych podejmuje osoba nadzorująca pracę na określonym zbiorze danych osobowych w porozumieniu z ABI.
6. Dla udokumentowania likwidacji danych osobowych, o których mowa w ust. 5 likwidujący sporządza protokół zawierający niezbędne informacji o usunięciu danych.
7. Fakt zniszczenia kopii zapasowych, ASI odnotowuje w rejestrze kopii zapasowych.
8. Przechowywanie w systemie informatycznym, na kopiach zapasowych lub w postaci wydruków dane osobowe, które przestały być użyteczne podlegają usunięciu lub zniszczeniu w sposób trwały uniemożliwiający ich odczytanie.
9. Kopie zapasowe zbioru danych osobowych są wykonywane na serwerze plików i są przechowywane w pomieszczeniu innym niż te, w którym przechowuje się zbiory danych osobowych wykorzystywane do bieżących prac związanych z ich przetwarzaniem.
10. Wydruki oraz elektroniczne nośniki informacji z danymi osobowymi pochodzącymi z systemu informatycznego, które nie są przeznaczone do udostępnienia, przechowuje się w zamkniętych szafach i pomieszczeniach, do których dostęp mogą mieć wyłącznie uprawnieni użytkownicy systemu.
11. Zabrania się pozostawienia dokumentów, kopii dokumentów, wydruków z danymi osobowymi w drukarkach, kserokopiarkach itd. Każdy pracownik ma absolutnie przestrzegać „zasady czystego biurka" polegającej na niepozostawieniu pracy.
12. Wydruki i dokumenty wykorzystywane w pracach kancelaryjno-biurowych należy zniszczyć w stopniu uniemożliwiającym ich odczytanie w niszczarkach dokumentów.
13. Pomieszczenia, w których przetwarzane są dane osobowe na czas nieobecności osób zatrudnionych należy zamykać, w sposób uniemożliwiający dostęp do nich osobom postronnym. Kategorycznie zabrania się pozostawienia kluczy w drzwiach, szafach, biurkach a także pozostawienia otwartych lub nieprawidłowo zamkniętych drzwiach pomieszczeń, w których przetwarzane są dane osobowe.

§ 9.
Procedura zabezpieczenia systemu informatycznego, w tym przed wirusami komputerowymi

1. Komputery zainstalowane w sieci informatycznej posiadają zainstalowany firewall i program antywirusowy.
2. Program antywirusowy powinien być uaktywniony cały czas podczas pracy danego systemu.
3. Za ochronę antywirusową odpowiada ASI.
4. Wszystkie pliki otrzymane z zewnątrz, jak również wysyłane na zewnątrz należy sprawdzać pod kątem wystąpienia wirusów najnowszą wersją programu antywirusowego. Sprawdzanie odbywa się automatycznie przez system antywirusowy lub ręcznie przez użytkowników systemu.
5. Zabrania się użytkownikom systemu wyłączania, odinstalowywania programów zabezpieczających komputer (firewall, program antywirusowy).
6. W przypadku, gdy użytkownik systemu zauważy komunikat wskazujący na zaistnienie zagrożenia zobowiązany jest do natychmiastowego zaprzestania jakichkolwiek czynności w systemie.
7. W przypadku wskazanym w ust. 6 użytkownik systemu zobligowany jest do natychmiastowego powiadomienia ASI i ABI.
8. ASI zobowiązany jest do dopilnowania, aby zainstalowany program antywirusowy był tak skonfigurowany, by dokonywał aktualizacji bazy wirusów, a także by było zagwarantowane automatyczne sprawdzanie każdego komputera pod kątem ewentualnej obecności wirusów komputerowych.
9. Osoby użytkujące komputer przenośny, dopuszczony do przetwarzania danych osobowych, zobowiązane są w szczególności do:
   - zachowania szczególnej ostrożności podczas transportu i przechowywania komputera,
   - stosowania odpowiedniego hasła do systemu,
   - szyfrowania danych prawnie chronionych w celu zapobieżenia dostępowi do danych osobowych osobom nieupoważnionym.

§ 10.
Ochrona przed nieautoryzowanym dostępem do sieci lokalnej

1. ASI jest odpowiedzialny aktywowanie i poprawne konfigurowanie specjalistycznego oprogramowania monitorującego wymianę danych na styku sieci lokalnej i sieci zewnętrznej.
2. Użytkownicy systemu obowiązani są do utrzymania stałej aktywności zainstalowanego na ich stanowiskach komputerowych specjalistycznego

oprogramowania monitorującego wymianę danych na styku stanowiska i sieci lokalnej.

§ 11.
Procedury wykonywania przeglądów i konserwacji

3. Przeglądy i konserwacje systemu informatycznego powinny być wykonywane w terminach określonych przez producentów systemu oraz zgodnie z harmonogramem ASI.
4. Aktualizacja oprogramowania powinna być przeprowadzona zgodnie z zaleceniami producentów oraz opinią rynkową co do bezpieczeństwa i stabilności nowych wersji.
5. Za terminowość przeprowadzenia przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada ASI.
6. ASI okresowo sprawdza możliwość odtworzenia danych z kopii zapasowych.
7. Nieprawidłowość w działaniu systemu informatycznego oraz oprogramowania powinny być niezwłocznie usunięte, a ich przyczyny przeanalizowane.
8. Wszelkie prace konserwacyjne i naprawcze sprzętu i naprawcze sprzętu komputerowego oraz uaktualnienia systemu informatycznego, wykonywane przez podmiot zewnętrzny, powinny odbywać się na zasadach określonych w szczegółowej umowie z uwzględnieniem klauzuli dotyczącej ochrony danych.
9. W przypadku naprawy sprzętu komputerowego dane osobowe należy zabezpieczyć, natomiast w przypadku naprawy sprzętu poza terenem danej jednostki, należy zdemontować i zabezpieczyć dyski twarde.
10. Wszelkie naprawy sprzętu na terenie jednostki przez firmy zewnętrzne powinny się odbywać w asyście ASI.
11. Zmiana konfiguracji sprzętu komputerowego, na którym znajdują się dane osobowe lub zmiana jego lokalizacji może być dokonana tylko przy udziale ASI i za zgodą ABI.

§ 12.
Zarządzanie oprogramowaniem

1. W Urzędzie Miejskim w Zwoleniu stosuje się wyłącznie legalne oprogramowanie.
2. Instalacja oprogramowania na stanowiskach pracowniczych mogą być dokonywane z nośników znajdujących się w zasobach Urzędu Miejskiego w Zwoleniu

3. Instalowanie oprogramowania nie będącego w zasobach Urzędu Miejskiego w Zwoleniu ma być konsultowane z ASI.
4. Instalacja i korzystanie z produktów w wersjach ewaluacyjnych, testowych lub w jakichkolwiek inny sposób ograniczony umowami licencyjnymi może być użytkowane zgodnie z ich przeznaczeniem.
5. Za całość zagadnień związanych z instalowaniem, użytkowaniem oprogramowania w Urzędzie Miejskim w Zwoleniu jest odpowiedzialny ASI.
6. Do przechowywania oryginalnych dokumentów licencyjnych (kart rejestracyjnych, narzędzi, nośników dla używanego w Urzędzie Miejskim w Zwoleniu oprogramowania, ABI wyznacza wydzieloną szafę, gdzie dostęp ma wyłącznie ASI.

§ 13.
Postanowienia końcowe

W sprawach nieuregulowanych w niniejszej Instrukcji mają zastosowanie przepisy aktualnej Ustawy o Ochronie Danych Osobowych oraz wydane na jej podstawie akty wykonawcze.

BURMISTRZ
mgr inż. Bogusława Jaworska