ZARZĄDZENIE NR 0050.132.2011

WÓJTA GMINY KRZYŻANOWICE – KIEROWNIKA URZĘDU GMINY

z dnia 14.12.2011 roku.

w sprawie : wprowadzenia Instrukcji Zarządzania Systemem Informatycznym w Urzędzie Gminy Krzyżanowice.

§ 1

Instrukcja Zarządzania Systemem Informatycznym w Urzędzie Gminy Krzyżanowie, określa sposób zarządzania systemem informatycznym wykorzystywanym do przetwarzania danych osobowych przez Administratora Danych.

§ 2

Stosownie do § 6 ust. 1 pkt. 3 rozporządzenia, po uwzględnieniu kategorii przetwarzanych danych osobowych oraz zagrożenia ich bezpieczeństwa wprowadza się wysoki poziom bezpieczeństwa przetwarzanych danych osobowych w systemie informatycznym Administratora Danych.

§ 3

1.Dostęp do systemu informatycznego służącego do przetwarzania danych osobowych może uzyskać wyłącznie osoba upoważniona do przetwarzania danych osobowych po zarejestrowaniu jej w systemie informatycznym Administratora Danych jako użytkownika.
2. Rejestracja użytkownika, o której mowa w pkt 1, polega na nadaniu osobie upoważnionej do przetwarzania danych osobowych identyfikatora i przydzieleniu hasła.
1) Identyfikator użytkownika jest to ciąg znaków literowo-cyfrowych**.** W identyfikatorze pomija się polskie znaki diakrytyczne. Identyfikator użytkownika:
a) jest jego nazwą w systemie informatycznym,
b) nie może być zmieniony bez wiedzy użytkownika,
c) nie jest przyznany innemu użytkownikowi. W wypadku zbieżności nadawanego identyfikatora z identyfikatorem wcześniej zarejestrowanego użytkownika Administrator Bezpieczeństwa Informacji nadaje inny identyfikator.
2) Hasło to co najmniej czteroznakowy ciąg znaków literowych lub cyfrowych, znany jedynie osobie, której nadano identyfikator użytkownika.
3. Wyrejestrowanie czasowe użytkownika z systemu informatycznego Administratora Danych polega na zablokowaniu dostępu do identyfikatora użytkownika do czasu ustania przyczyny uzasadniającej wyrejestrowanie i może nastąpić z powodu:

1) zawieszenia w pełnieniu obowiązków służbowych;

2) wypowiedzenia umowy o pracę;
3) wszczęcia postępowania dyscyplinarnego.

4. Wyrejestrowanie trwałe użytkownika polega na usunięciu identyfikatora użytkownika z systemu informatycznego i następuje z powodu:

1) rozwiązania lub wygaśnięcia stosunku pracy lub innego stosunku prawnego, w ramach którego zatrudniony był użytkownik,
2) z innej ważnej przyczyny.

5. Administrator Bezpieczeństwa Informacji na polecenie Administratora Danych rejestruje i wyrejestrowuje użytkownika z systemu.

§ 4

1.Każdy użytkownik systemu informatycznego posługuje się wyłącznie swoim identyfikatorem i hasłem.

2.Zabrania się użytkownikom:

1) udostępniania swojego identyfikatora i hasła innym osobom,
2) korzystania z identyfikatora lub hasła innego użytkownika,
3) zapisywania identyfikatora i hasła w miejscach i na nośnikach, dających możliwość zapoznania się z nimi przez osoby nieupoważnione.

3. Administrator Bezpieczeństwa Informacji może w uzasadnionych sytuacjach polecić dokonanie zmiany hasła przez użytkownika.

§ 5

1.Rozpoczęcie pracy na komputerze stacjonarnym następuje po włączeniu zasilania stacji, a następnie wprowadzeniu identyfikatora i hasła.

2. Użytkownik zobowiązany jest chronić dane osobowe przed dostępem osób nieupoważnionych w szczególności poprzez:

1) ustawienie monitora komputera w sposób uniemożliwiający podgląd,
2)zabezpieczenie nośników elektronicznych i sprzętu komputerowego, zwłaszcza nie pozostawianie ich bez nadzoru.
3) nie dopuszczanie do używania sprzętu komputerowego przez osoby inne niż użytkownicy, którym zostały powierzone do wykonywania obowiązków i zadań u Administratora Danych.

3.Monitory komputerów wyposażone są we włączające się po 20 minutach od przerwania pracy wygaszacze ekranu. Wznowienie wyświetlenia następuje dopiero po wprowadzeniu stosownego hasła.

4.W razie opuszczenia stanowiska pracy użytkownik obowiązany jest aktywizować wygaszacz ekranu lub w inny sposób zablokować stację roboczą.

5.Zakończenie pracy na stacji roboczej następuje po prawidłowym wylogowaniu się użytkownika i wyłączeniu komputera oraz zasilania.

§ 6

1.Przy przetwarzaniu danych osobowych na komputerach przenośnych obowiązują procedury określone w niniejszej Instrukcji dotyczące pracy na komputerach stacjonarnych, z zastrzeżeniem ust. 2.

2.Użytkownicy, którym zostały powierzone komputery przenośne powinni:

1) chronić je przed uszkodzeniem, kradzieżą i dostępem osób nieupoważnionych. Szczególną ostrożność należy zachować podczas transportu.
2) pliki zawierające dane osobowe należy przechowywać w chronionych kontenerach, zaszyfrowanych oraz chronionych hasłem dostępu.

3. Zakazuje się przetwarzania na komputerach przenośnych całych zbiorów danych lub obszernych

z nich wypisów, nawet w postaci zaszyfrowanej.

§ 7

1.Automatyczne kopie danych znajdujących się na serwerach należy wykonać codziennie od poniedziałku do piątku po godzinach pracy Urzędu Gminy tak aby nie miało to wpływu na bieżącą pracę Urzędu.
2. Zabronione jest wykonywanie kopii awaryjnych na PenDrivach,
3. Nośniki zawierające kopie, o których mowa w ust. 1,
1) muszą być opisane i zarejestrowane w rejestrze, którego wzór stanowi załącznik do niniejszego Zarządzenia. Odpowiedzialnym za prowadzenie rejestru jest użytkownik wykonujący kopie,
2) poddawane bezzwłocznemu zniszczeniu po ustaniu ich użyteczności, przydatności lub stwierdzenia uszkodzenia. Zniszczenia nośników dokonuje komisja powołana przez Administratora Danych.

§ 8

1. W przypadku posługiwania się nośnikami danych pochodzącymi od podmiotu zewnętrznego użytkownik jest zobowiązany do sprawdzenia go programem antywirusowym.
2. Zakazuje się przesyłania danych osobowych pocztą elektroniczną.
3. Zbiory danych osobowych przechowywane są na serwerze obsługującym system informatyczny Administratora Danych.

§ 9

1. Komputery PC chronione są przed wirusami komputerowymi w następujący sposób:
1) Administrator Bezpieczeństwa Informacji instaluje na każdym stanowisku komputerowym oprogramowanie antywirusowe,
2) za bezpieczeństwo antywirusowe odpowiada użytkownik komputera,
3) zabrania się używania przenośnych nośników danych nie sprawdzonych na obecność wirusów komputerowych,
4) fakt znalezienia wirusa należy zgłaszać Administratorowi Bezpieczeństwa Informacji,
5) zabrania się samodzielnego instalowania oprogramowania bez wiedzy Administratora Bezpieczeństwa Informacji,
6) zabrania się przeglądania stron internetowych nie związanych z wykonywanymi czynnościami służbowymi.
2. Ochrona komputerów PC przed nieautoryzowanym dostępem do systemu informatycznego następuje poprzez:
1) zabezpieczenie systemu informatycznego przed nieautoryzowanym dostępem z sieci INTERNET za pomocą urządzenia typu FIREWALL,
2) codzienną aktualizację oprogramowania antywirusowego oraz okresowe skanowanie dysków komputera programem antywirusowym,
3) skanowanie poczty elektronicznej przez skaner antywirusowy.
3. Użytkownik jest obowiązany zawiadomić Administratora Bezpieczeństwa Informacji o pojawiających się komunikatach wskazujących na wystąpienie zagrożenia wywołanego szkodliwym oprogramowaniem.
4. Administrator Bezpieczeństwa Informacji z własnej inicjatywy lub na wniosek Administratora Danych w ramach posiadanych możliwości technicznych dokonuje zmiany ustawień systemu w celu uniemożliwienia przeglądania wskazanych stron www.

§ 10

1. System informatyczny Administratora Danych winien umożliwiać automatycznie:
1) przypisanie wprowadzanych danych użytkownikowi (identyfikatorowi użytkownika), który te dane wprowadza do systemu,
2) sygnalizację wygaśnięcia czasu obowiązywania hasła dostępu do programu informatycznego obsługującego zbiór danych,
3) sporządzenie i wydrukowanie dla każdej osoby, której dane są przetwarzane w systemie, raportu zawierającego:
a) datę pierwszego wprowadzenia danych do systemu informatycznego Administratora Danych,
b) identyfikator użytkownika wprowadzającego dane,
c) źródła danych w przypadku zbierania danych nie od osoby, której one dotyczą,
2.Odnotowanie informacji, o których mowa w ust. 1 pkt 3, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.

§ 11

1.Instalacji oprogramowania na stanowiskach komputerowych dokonuje Administrator Systemów Informatycznych.
2.Za każde stanowisko komputerowe znajdujące się w Urzędzie Gminy odpowiedzialny jest wyznaczony przez kierownika jednostki Urzędu Gminy pracownik.

3.Zabrania się użytkownikom stanowisk komputerowych:
1)samodzielnej ingerencji w oprogramowanie i konfigurację powierzonego sprzętu komputerowego,
2) instalowania i użytkowania nielegalnego oprogramowania,
3) przechowywania kopii nielegalnego oprogramowania,
4) instalowania oprogramowania nie przeznaczonego do wykonywania obowiązków służbowych,
5) deinstalowania zainstalowanego na stanowisku komputerowym oprogramowania,
6) przeinstalowania oprogramowania na inne stanowisko,
7) podłączania do sieci komputerowej sprzętu komputerowego nie będącego własnością Urzędu Gminy,
8) dokonywania samodzielnych napraw sprzętu komputerowego,
9) dokonywania samodzielnych zmian miejsca użytkowania sprzętu komputerowego,
10) podłączania do listew podtrzymujących napięcie, przeznaczonych dla sprzętu komputerowego, innych urządzeń, szczególnie tych łatwo powodujących spięcia jak grzejników, czajników, wentylatorów,
11) zasłaniania kratek wentylatorów sprzętu komputerowego meblami, zasłonami lub stawianie ich tuż przy ścianie.
12) przechowywania prywatnych danych użytkowników takich jak zdjęcia, filmy

§ 12

1.Bieżąca konserwacja sprzętu komputerowego prowadzona jest przez Administratora Systemów Informatycznych.
2.Użytkownicy systemu komputerowego zgłaszają Administratorowi Systemów Informatycznych wszelkie awarie sprzętu komputerowego.
3. W przypadku stwierdzenia awarii sprzętu komputerowego zawierającego dane osobowe:
1) naprawa i konserwacja sprzętu winna odbyć się na miejscu,
2) w razie konieczności dokonania naprawy w serwisie Administrator Systemów Informatycznych zabezpiecza dane poprzez wymontowanie nośnika danych lub nadzoruje naprawę.

Z serwisantem należy podpisać umowę powierzenia przetwarzania danych.
4.Zużyty lub uszkodzony sprzęt komputerowy służący do przetwarzania danych osobowych może być zbywany lub przekazywany do utylizacji po fizycznym zniszczeniu nośnika z danymi osobowymi.
5.Zapisy logów systemowych powinny być okresowo przeglądane przez Administratora Systemów Informatycznych oraz każdorazowo po wykryciu naruszenia zasad bezpieczeństwa.
6.Kontrole i testy przeprowadzane przez Administratora Systemów Informatycznych powinny obejmować zarówno dostęp do zasobów systemu oraz uprawnienia poszczególnych użytkowników.

§ 13

1.Użytkownik zobowiązany jest zawiadomić Administratora Bezpieczeństwa Informacji o każdym naruszeniu lub podejrzeniu naruszenia bezpieczeństwa systemu, a w szczególności o:
1) naruszeniu hasła dostępu i identyfikatora,
2) częściowym lub całkowitym braku danych albo dostępie do danych w zakresie szerszym niż wynikający z przyznanych uprawnień,
3) braku dostępu do właściwej aplikacji lub zmianie zakresu wyznaczonego dostępu do zasobów serwera,
4) wykryciu wirusa komputerowego,
5)zauważeniu elektronicznych śladów próby włamania do systemu informatycznego Administratora Danych,
6) znacznym spowolnieniu działania systemu informatycznego,
7) podejrzeniu kradzieży sprzętu komputerowego lub dokumentów zawierających dane osobowe,
8) zmianie położenia sprzętu komputerowego,
9) zauważeniu śladów usiłowania lub dokonania włamania do pomieszczeń lub zamykanych szaf.
2. Administrator Bezpieczeństwa Informacji po otrzymaniu zawiadomienia, o którym mowa w ust. 1:
1) przeprowadza postępowanie wyjaśniające w celu ustalenia okoliczności naruszenia ochrony danych osobowych,
2) podejmuje działania chroniące system przed ponownym naruszeniem,
3) w przypadku stwierdzenia faktycznego naruszenia bezpieczeństwa systemu sporządza raport naruszenia bezpieczeństwa systemu informatycznego Administratora Danych, a następnie niezwłocznie przekazuje jego kopię Administratorowi Danych,
4) w uzasadnionych przypadkach może zarządzić odłączenie części systemu dotkniętego incydentem od pozostałej jego części,
5)w razie odtwarzania danych z kopii zapasowych upewnia się, czy odtwarzane dane zapisane zostały przed wystąpieniem incydentu; dotyczy to zwłaszcza przypadków infekcji wirusowej.
3.Administrator Danych po zapoznaniu się z raportem, o którym mowa w ust. 2 pkt. 3, podejmuje decyzje o dalszym trybie postępowania, zwłaszcza powiadomienia właściwych organów oraz podjęciu innych, szczególnych czynności zapewniających bezpieczeństwo systemu informatycznego administratora danych bądź zastosowaniu środków ochrony fizycznej.
4.Administrator Bezpieczeństwa Informacji oraz Administrator Systemów Informatycznych zobowiązany jest do informowania Administratora Danych o awariach systemu informatycznego, zwłaszcza zauważonych przypadkach naruszenia niniejszej instrukcji przez użytkowników, a zwłaszcza o przypadkach posługiwania się przez użytkowników nieautoryzowanymi programami, nieprzestrzegania zasad używania oprogramowania antywirusowego, niewłaściwego wykorzystania sprzętu komputerowego lub przetwarzania danych w sposób niezgodny z procedurami ochrony danych osobowych.

§ 14

Wykonanie Zarządzenia powierzam Administratorowi Bezpieczeństwa Informacji, Administratorowi Systemów Informatycznych a nadzór nad wykonaniem Zarządzenia będę sprawował osobiście.

§ 15

Zarządzenie wchodzi w życie z dniem podpisania.

U Z A S A D N I E N I E

Obowiązek prowadzenia dokumentacji opisującej sposób przetwarzania danych osobowych określony został w art. 36 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. z 2002 r. Dz. U. Nr 101 poz. 926 z późn. zm.).

Sposób wykonania tego obowiązku został skonkretyzowany w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z 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).

Funkcjonowanie wymienionych przepisów pozwoliło na określenie zarówno w doktrynie jak i w praktyce standardów, którym te dokumenty powinny odpowiadać.

Niniejsze Zarządzenie stanowi dostosowanie dotychczas funkcjonujących przepisów wewnętrznych w tym zakresie do obowiązujących wymagań.