Zarządzenie nr 49/2016

Wójta Gminy Iwaniska

z dnia 28 października 2016

W sprawie : **wprowadzenia polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych oraz informacji niejawnych w Urzędzie Gminy w Iwaniskach.**

Działając na podstawie

- art. 31 ustawy z dnia 08 marca 1990 r o samorządzie gminnym (j.t. Dz.U.2016/ poz.446)

- ustawy z dnia 29 sierpnia 1997r o ochronie danych osobowych (j.t. Dz. U. 2016/ poz. 922)

- ustawy z dnia 5 sierpnia 2010 r o ochronie informacji niejawnych (j.t. Dz.U.2016.1167)

- rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 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. 2004, nr 100, poz. 1024) zarządzam co następuje.

§1) Wprowadzam do bezwzględnego stosowania „Politykę bezpieczeństwa i instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych oraz informacji niejawnych w Urzędzie Gminy w Iwaniskach" stanowiącą załącznik nr 1 do niniejszego zarządzenia.

§2) Za wdrożenie, realizację, i nadzór nad spełnieniem zadań i procedur wprowadzonych wyżej wymienionym dokumentem odpowiedzialni są Sekretarz Gminy, kierownicy referatów i osoby zajmujące samodzielne stanowiska pracy.

§3) Pracownicy, w tym także praktykanci i stażyści, Urzędu Gminy w Iwaniskach są zobowiązani do realizacji obowiązków wynikających dla nich z treści załącznika nr 1 do „polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Iwaniska", o której mowa w §1.

§4) 1.Ustanawiam p. Grzegorza Bezdzietnego Administratorem Bezpieczeństwa Informacji (ABI) oraz Administratorem Systemu Informatycznego (ASI).

2.Nadzór nad realizacją obowiązków ABI i ASI wykonuje Wójt jako administrator danych osobowych i informacji niejawnych.

§5) 1. Uchylam zarządzenie nr 51/08 z dnia 31 lipca 2008r.

2. Zarządzenie wchodzi w życie w dniu podpisania

RADCA PRAWNY
mgr Adam J. Meks

Wójt Gminy Iwaniska
mgr Marek Stawiak

Załącznik nr 1 do Zarządzenia Nr 46/2016
Wójta Gminy Iwaniska z dnia
28 października 2016r.

Polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Iwaniska

Opracował Administrator Bezpieczeństwa Informacji
Iwaniska, październik 2016 r.

SPIS TREŚCI

WPROWADZENIE

Ninicjszy dokument zgodny jest z następującymi aktami prawnymi:

- ustawą z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2016r., poz. 922),
- ustawą o ochronie informacji niejawnych z dnia 5 sierpnia 2010r. (tekst jednolity Dz. U. z 2016, poz. 1167),
- rozporządzenia 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),

Dokument ten reguluje sprawy ochrony danych osobowych zawartych w systemie informatycznym eksploatowanym w lokalnej sieci komputerowej Urzędu Gminy oraz zbiorów danych zapisanych w postaci dokumentacji papierowej.
Instrukcja dotyczy następujących baz danych i kartotek:

Granice obszarów w których przetwarzane są dane osobowe oraz ich zakres zostały opisane w Załączniku Nr 4.
Opisane reguły określają granice dopuszczalnego zachowania wszystkich użytkowników systemów informatycznych wspomagających pracę Urzędu. Dokument zwraca uwagę na konsekwencje, jakie mogą ponosić osoby przekraczające określone granice oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń. Odpowiednie zabezpieczenia, ochrona przetwarzanych danych oraz niezawodność funkcjonowania są podstawowymi wymogami stawianymi współczesnym systemom informatycznym. Dokument „Polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Iwaniska", zwany dalej „Polityką bezpieczeństwa", wskazujący sposób zabezpieczenia systemów informatycznych postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych w systemach informatycznych, przeznaczony jest dla osób zatrudnionych przy przetwarzaniu tych danych. Potrzeba jego opracowania wynika z §3 rozporządzenia Prezesa Rady Ministrów z dnia 20 lipca 2011 roku w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz.U. z 2011 Nr 159, poz. 948) oraz § 3 i 4 rozporządzenia 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).

1. „Polityka bezpieczeństwa" określa tryb postępowania w przypadku, gdy:
   - stwierdzono naruszenie zabezpieczenia systemu informatycznego,
   - stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci informatycznej mogą wskazywać na naruszenie zabezpieczeń tych danych.
2. „Polityka bezpieczeństwa" obowiązuje wszystkich pracowników Urzędu Gminy.
3. Wykonywanie postanowień tego dokumentu ma zapewnić właściwą reakcję, ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa systemów oraz zapewnić właściwy tryb działania w celu przywrócenia bezpieczeństwa danych przetwarzanych w systemie informatycznym Urzędu.
4. Administrator Danych, którym jest Wójt, swoją decyzją wyznacza Administratora Bezpieczeństwa Informacji danych zawartych w systemach informatycznych Urzędu,

zwanego dalej „Administratorem Bezpieczeństwa" oraz osobę upoważnioną do zastępowania „Administratora Bezpieczeństwa".

5. „Administrator Bezpieczeństwa" realizuje zadania w zakresie ochrony danych, a w szczególności:
- ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach systemów informatycznych Urzędu,
- podejmowania stosownych działań zgodnie z niniejszą „Polityką bezpieczeństwa" w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia danych znajdujących się w systemie informatycznym,
- niezwłocznego informowania Administratora Danych lub osoby przez niego upoważnionej o przypadkach naruszenia przepisów ustawy o ochronie danych osobowych,
- nadzoru i kontroli systemów informatycznych służących do przetwarzania danych osobowych i osób przy nim zatrudnionych.
6. Osoba zastępująca Administratora Bezpieczeństwa powyższe zadania realizuje w przypadku nieobecności Administratora Bezpieczeństwa.
7. Osoba zastępująca składa Administratorowi Bezpieczeństwa relację z podejmowanych działań w czasie jego zastępstwa.

Rozdział 1. OPIS ZDARZEŃ NARUSZAJĄCYCH OCHRONĘ DANYCH OSOBOWYCH

1. Podział zagrożeń:
- zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych,
- zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora systemu, awarie sprzętowe, błędy oprogramowania), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych,
- zagrożenia zamierzone, świadome i celowe - najpoważniejsze zagrożenia, naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na: nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu), nieuprawniony dostęp do systemu z jego wnętrza, nieuprawniony przekaz danych, pogorszenie jakości sprzętu i oprogramowania, bezpośrednie zagrożenie materialnych składników systemu.
2. Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe to głównie:
- sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.,
- niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,

- awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru,
- pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,
- jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
- nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,
- stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
- nastąpiła niedopuszczalna manipulacja danymi osobowymi w systemie,
- ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń,
- praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych - np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.,
- ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. „bocznej furtki", itp.,
- podmieniono lub zniszczono nośniki z danymi osobowymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane osobowe,
- rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.).

3. Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, dyskietkach w formie niezabezpieczonej itp.

Rozdział 2. ZABEZPIECZENIE DANYCH OSOBOWYCH

§ 1. Cele i zasady ogólne

1. Administratorem danych osobowych zawartych i przetwarzanych w systemach informatycznych Urzędu Gminy jest Wójt.
2. Administrator danych osobowych jest obowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w systemach informatycznych Urzędu, a w szczególności:
- zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym,
- zapobiegać zabraniu danych przez osobę nieuprawnioną,
- zapobiegać przetwarzaniu danych z naruszeniem ustawy oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych.

3. Administrator danych zobowiązany jest do zapewnienia, aby dane osobowe były:
- przetwarzane zgodnie z prawem,

- zbierane dla oznaczonych, zgodnych z prawem celów,
- merytorycznie poprawne i adekwatne w stosunku do celów.

4. Wyznacza osobę, zwaną dalej Administratorem Bezpieczeństwa Informacji, odpowiedzialnym za bezpieczeństwo danych osobowych w systemie informatycznym, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe, oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń.
5. Opracowuje instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych, przeznaczoną dla osób zatrudnionych przy przetwarzaniu tych danych którą jest Rozdział 3. POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Iwaniska.
6. Określa budynki, pomieszczenia lub części pomieszczeń, tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego.
7. Opracowuje instrukcję, określającą sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji którą jest § 3. Zabezpieczenia, Rozdział 2. ZABEZPIECZENIE DANYCH OSOBOWYCH polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Iwaniska.
8. Prowadzi ewidencję osób uprawnionych do przetwarzania danych osobowych w poszczególnych systemach.
9. Organizuje szkolenia mające na celu zaznajomienie każdej osoby przetwarzającej dane osobowe z przepisami dotyczącymi ich ochrony.
10. Odpowiada za to by zakres czynności osoby zatrudnionej przy przetwarzania danych osobowych określał odpowiedzialność tej osoby za:

- ochronę danych przed niepowołanym dostępem,
- nieuzasadnioną modyfikację lub zniszczenie danych,
- nielegalne ujawnienie danych. w stopniu odpowiednim do zadań realizowanych w procesie przetwarzania danych osobowych.

11. Rejestruje zbiory danych osobowych w Biurze Generalnego Inspektora Ochrony Danych Osobowych.

§ 2. Cele ochrony i zasady ogólne

1. Celem wprowadzonych niniejszą Polityką zabezpieczeń i obostrzeń jest ochrona danych osobowych zawartych w eksploatowanym w systemie. Określone niżej sposoby zabezpieczeń dotyczą:

- zabezpieczeń przed dostępem do danych osób nieupoważnionych na etapie eksploatacji systemu tj. wprowadzanie danych, aktualizacji lub usuwania danych, wyświetlania lub drukowania zestawień,
- ochrony danych zarchiwizowanych na nośnikach zewnętrznych, procedur niszczenia niepotrzebnych wydruków lub nośników danych.
- systemu zabezpieczeń przed dostępem osób niepowołanych do pomieszczeń, w których są eksploatowane urządzenia oraz sposobów dostępu do tych pomieszczeń pracowników, personelu pomocniczego Urzędu oraz serwisu zewnętrznego,
- monitorowania systemu zabezpieczeń,
- zakresu obowiązków pracowników – w części dotyczącej bezpieczeństwa danych.

2. Strategia ochrony danych osobowych opiera się na następujących zasadach:
- podstawowym sposobem zabezpieczenia danych i dostępu do nich jest system definiowania użytkowników, grup użytkowników oraz haseł. Są to zabezpieczenia programowe wmontowane w eksploatowane systemy uniemożliwiające dostęp do systemu osobom nieupoważnionym.
- dodatkowym systemem zabezpieczenia jest stosowanie kryptograficznej ochrony danych, jaką oferuje system operacyjny.
- kopie danych zarchiwizowanych na nośnikach magnetycznych lub płytach CD są przechowywane w ognioodpornym sejfie – chronią w ten sposób dane na wypadek pożaru, klęski żywiołowej lub katastrofy. Prowadzona jest ścisła ewidencja tych nośników,
- w pomieszczeniach, w których zainstalowany jest serwer i komputery zawierające bazy danych jest zainstalowany system alarmowy i przeciwpożarowy,
- zagadnienia związane z ochrona danych i obowiązki stąd wynikające są ujęte w zakresach czynności pracowników::
  1. Pracownik zobowiązany jest dbać o bezpieczeństwo powierzonych mu do przetwarzania, archiwizowania lub przechowywania danych zgodnie z obowiązującą w Urzędzie Polityką Bezpieczeństwa, regulaminami i instrukcjami wewnętrznymi, w tym m. in.:
     - Chronić dane przed dostępem osób nieupoważnionych,
     - Chronić dane przed przypadkowym lub nieumyślnym zniszczeniem, utratą lub modyfikacją,
     - Chronić nośniki magnetyczne i optyczne oraz wydruki komputerowe przed dostępem osób nieupoważnionych oraz przed przypadkowym zniszczeniem,
     - Utrzymywać w tajemnicy powierzone identyfikatory, hasła, częstotliwość ich zmiany oraz szczegóły technologiczne systemów także po ustaniu zatrudnienia w Urzędzie.
     - Archiwizować dane zgodnie z instrukcją technologiczną,
     - Prowadzić niezbędną, przewidzianą instrukcją technologiczną dokumentację pracy z systemem, archiwizowania danych itp.
  2. Zabrania się pod rygorem odpowiedzialności służbowej i karnej:
     - Ujawniać dane – w tym dane osobowe zawarte w obsługiwanych systemach,
     - Kopiować bazy danych lub ich części poza przewidzianymi instrukcją technologiczną kopiami bezpieczeństwa,
     - Zabrania się przetwarzania danych w sposób inny niż opisany instrukcją technologiczną.
- każdy pracownik Urzędu, podpisze oświadczenie stanowiące Załącznik Nr 1,
- za całość polityki bezpieczeństwa odpowiada Administrator Bezpieczeństwa Informacji.

§ 3. Zabezpieczenia

Wprowadza się następujące zabezpieczenia danych w systemie informatycznym:
1. Na wszystkich stacjach roboczych, na których przetwarzane są dane osobowe wprowadza się **wysoki** poziom zabezpieczeń.
2. Pomieszczenia, w których stoi serwer i komputery zawierające dane osobowe i kartoteki osobowe są zabezpieczone poprzez system alarmowy i przeciwpożarowy. Wykaz tych pomieszczeń zawiera Załącznik Nr 4.
3. Ochronę przed awariami zasilania oraz zakłóceniami w sieci energetycznej serwera i urządzeń sieci informatycznej zapewniają zasilacze UPS. Stacje robocze przetwarzające

dane osobowe gromadzone lokalnie i mogące utracić integralność danych w wyniku awarii zasilania mają ochronę w formie zasilacza UPS.

4. Zalogowanie się do systemu wymaga podania nazwy użytkownika i hasła. Każdy użytkownik ma przypisane uprawnienia do wykonywania operacji. Logowanie do systemu możliwe jest w godzinach pracy Urzędu.
5. Oprogramowanie wykorzystywane do przetwarzania danych posiada własny system kont (zabezpieczonych hasłami) i uprawnień.
6. Administrator Bezpieczeństwa Informacji ma uprawnienia do definiowania kont użytkowników i haseł.
7. W celu ochrony przed dostępem do danych komputera z sieci publicznej wykorzystuje się system zapory ogniowej dostępnej w systemie operacyjnym.
8. Stosuje się aktywną ochronę antywirusową w czasie rzeczywistym na każdym komputerze, na którym przetwarzane są dane osobowe. Aktualizacja bazy wirusów wykonuje się codziennie automatycznie.
9. Wydruki zawierające dane osobowe powinny znajdować się w miejscu, które uniemożliwia dostęp osobom postronnym.
10. Kopia bezpieczeństwa danych zgromadzonych na serwerach wykonywana jest automatycznie każdego wieczora, a danych zawartych wyłącznie na komputerach lokalnych wykonują okresowo pracownicy w ramach swoich obowiązków.
11. Kartoteki papierowe znajdują się w meblowych szafach, zamykanych na zamki meblowe w pokojach, w których przetwarzane są dane osobowe.
12. Stosuje się następujące zabezpieczenia organizacyjne przed dostępem do danych osób niepowołanych:

- dostęp do danych mają wyłącznie pracownicy wyznaczeni przez Administratora Danych. Administrator Danych prowadzi ścisły rejestr tych pracowników obejmujący listę nazwisk użytkowników posiadających dostęp do danych, łącznie z ich identyfikatorami w systemie.
- w pokoju, do którego dostęp mają petenci monitory komputerowe ustawione są w ten sposób, by petenci nie widzieli zapisów na ekranie,
- na stanowiskach których system operacyjny na to pozwala w przypadku dłuższej bezczynności uruchamiane są tzw. wygaszacie ekranu, których deaktywacja jest możliwa po podaniu prawidłowego hasła użytkownika.
- częstotliwość tworzenia kopii bezpieczeństwa określa instrukcja archiwowania zasobów. Za wykonanie tych kopii odpowiedzialne są osoby przetwarzające dane osobowe.
- tworzenie kopii bezpieczeństwa nadzoruje informatyk poprzez monitorowanie ewidencji kopii.

§ 4. Monitorowanie zabezpieczeń

1. Do monitorowania systemu zabezpieczeń, stosownie do swojego zakresu czynności zobligowani są:

- Administrator Danych
- Administrator Bezpieczeństwa Informacji

2. W ramach monitoringu należy przeprowadzać następujące działania:

- okresowe sprawdzanie kopii bezpieczeństwa pod względem przydatności do odtworzenia danych,
- sprawdzania częstotliwości zmian haseł,

3. Administrator Bezpieczeństwa sporządza roczne plany kontroli zatwierdzone przez Administratora Danych i zgodnie z nimi przeprowadza kontrole oraz dokonuje kwartalnych ocen stanu bezpieczeństwa danych osobowych.

§ 5. Szkolenia

1. Szkolenie podstawowe dotyczące bezpieczeństwa danych obejmuje wszystkich pracowników Urzędu Gminy.
2. System szkoleń szczegółowych obejmuje pracowników zatrudnionych bezpośrednio przy przetwarzaniu danych, w tym danych osobowych.
3. Tematyka szkoleń obejmuje:

- Przepisy i instrukcje wewnętrzne dotyczące ochrony danych archiwizacji zasobów i przechowywania nośników, niszczenie wydruków i zapisów na nośnikach magnetycznych i optycznych,
- Zakresy obowiązków pracowników związanych bezpośrednio z bezpieczeństwem danych i ochroną systemów na poszczególnych stanowiskach.

§ 6. Archiwowanie danych

1. Dane zgromadzone na serwerze kopiowane są w trybie jednodniowym. Kopie awaryjne danych zapisywanych w programach wykonywane są automatycznie.
2. Dane zgromadzone na komputerach lokalnych wykonywane są co najmniej w trybie tygodniowym, a za wykonanie kopii danych odpowiedzialny jest pracownik obsługujący dane stanowisko przetwarzające dane.
3. Okresową weryfikację kopii bezpieczeństwa pod kątem ich przydatności do odtworzenia danych przeprowadza informatyk.

§ 7. Niszczenie wydruków i zapisów na nośnikach magnetycznych

1. Nośniki magnetyczne przekazywane na zewnątrz powinny być pozbawione zapisów zawierających dane osobowe. Niszczenie poprzednich zapisów powinno odbywać się poprzez wymazywanie informacji oraz formatowanie nośnika.
2. Uszkodzone nośniki magnetyczne przed ich wyrzuceniem należy fizycznie zniszczyć (przeciąć, przełamać itp.).
3. Po wykorzystaniu wydruki zawierające dane osobowe powinny być niszczone w niszczarkach lub przez spalenie w piecu c. o. znajdującym się w kotłowni budynku Urzędu.

Rozdział 3. POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Każdy pracownik Urzędu Gminy, który powezmie wiadomość w zakresie naruszenia bezpieczeństwa danych przez osobę przetwarzającą dane osobowe bądź posiada informację o mogącą mieć wpływ na bezpieczeństwo danych osobowych jest zobowiązany fakt ten niezwłocznie zgłosić Administratorowi Bezpieczeństwa.
2. W razie niemożliwości zawiadomienia Administratora Bezpieczeństwa lub osoby przez niego upoważnionej, należy powiadomić bezpośredniego przełożonego
3. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych Administratora Bezpieczeństwa lub upoważnionej przez niego osoby, należy:

- niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców,

- rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
- zaniechać - o ile to możliwe - dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,
- podjąć inne działania przewidziane i określone w instrukcjach technicznych i technologicznych stosownie do objawów i komunikatów towarzyszących naruszeniu,
- podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej,
- zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku,
- udokumentować wstępnie zaistniałe naruszenie,
- nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora Bezpieczeństwa lub osoby upoważnionej.

4. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych, Administrator Bezpieczeństwa lub osoba go zastępująca:
- zapoznaje się z zaistnialą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy Urzędu,
- może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
- rozważa celowość i potrzebę powiadamia o zaistniałym naruszeniu Administratora danych,
- nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba, ze specjalistami spoza Urzędu.

5. Administrator Bezpieczeństwa dokumentuje zaistniały przypadek naruszenia oraz sporządza raport, który powinien zawierać w szczególności:
- wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub podejrzanych w związku z naruszeniem,
- określenie czasu i miejsca naruszenia i powiadomienia,
- określenie okoliczności towarzyszących i rodzaju naruszenia,
- wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania,
- wstępną ocenę przyczyn wystąpienia naruszenia,
- ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.

6. Raport, o którym mowa w pkt. 5, Administrator Bezpieczeństwa niezwłocznie przekazuje Administratorowi Danych (Wójtowi), a w przypadku jego nieobecności osobie uprawnionej.
7. Po wyczerpaniu niezbędnych środków doraźnych po zaistnialym naruszeniu Administrator Bezpieczeństwa zasięga niezbędnych opinii i proponuje postępowanie naprawcze, a w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych.
8. Zaistniałe naruszenie może stać się przedmiotem szczegółowej, zespołowej analizy prowadzonej przez Kierownictwo urzędu, Administratora Bezpieczeństwa Informacji, Pełnomocnika ds. Ochrony Informacji Niejawnych.
9. Analiza, o której mowa w ust. 8, powinna zawierać wszechstronną ocenę zaistniałego naruszenia, wskazanie odpowiedzialnych, wnioski co do ewentualnych przedsięwzięć proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.

Rozdział 4. POSTANOWIENIA KOŃCOWE

1. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie dyscyplinarne.
2. Administrator Bezpieczeństwa zobowiązany jest prowadzić ewidencję osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych wg wzoru stanowiącego Załącznik Nr 3 do niniejszego dokumentu.
3. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, w szczególności przez osobę, która wobec naruszenia zabezpieczenia systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym Administratora Bezpieczeństwa.
4. Orzeczona kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia Administratora Bezpieczeństwa Informacji nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity Dz. U. z 2016r., poz. 922) oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
5. W sprawach nie uregulowanych niniejszym dokumentem mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity Dz. U. z 2016r., poz. 922), rozporządzenia 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) oraz rozporządzenie Ministra Sprawiedliwości z dnia 28 kwietnia 2004 r. w sprawie sposobu technicznego przygotowania systemów i sieci do przekazywania informacji - do gromadzenia wykazów połączeń telefonicznych i innych przekazów informacji oraz sposobów zabezpieczenia danych informatycznych (Dz. U. Nr 100, poz. 1023).
6. Niniejsza „Polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Iwaniska" wchodzi w życie z dniem jej podpisania przez Wójta.

RADCA PRAWNY
mgr Adam J. Meks
KI/K-411

Załącznik Nr 1 do „Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Iwaniska

Iwaniska, dn. .....

.....
(imię i nazwisko pracownika)

.....
(adres)

.....

OŚWIADCZENIE

(tekst oświadczenia podpisanego przez pracowników Urzędu Gminy oraz służb pomocniczych)

1. Stwierdzam własnoręcznym podpisem, że znana mi jest treść przepisów:
   - o ochronie i postępowaniu z wiadomościami, stanowiącymi tajemnicę służbową,
   - o ochronie danych osobowych (tekst jednolity Dz. U. z 2016 poz. 922) oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 28 kwietnia 2004 roku (Dz. U. Nr 100 poz. 1024 z 2004 r.) oraz o odpowiedzialności karnej za naruszenie ochrony danych osobowych.
2. Jednocześnie zobowiązuję się nic ujawniać wiadomości, z którymi zapoznałem / zapoznałam się z racji wykonywanej pracy w Urzędzie Gminy, a w szczególności nie będę:
   - ujawniać danych zawartych w eksploatowanych w Urzędzie systemach informatycznych, zwłaszcza danych osobowych znajdujących się w tym systemach,
   - ujawniać szczegółów technologicznych używanych w Urzędzie systemów oraz oprogramowania,
   - udostępniać osobom nieupoważnionym nośniki magnetyczne i optyczne oraz wydruki komputerowe,
   - kopiować lub przetwarzać danych w sposób inny niż dopuszczony obowiązującą instrukcją technologiczną.

.....
(podpis pracownika)

.....
(podpis przełożonego)

RADCA PRAWNY
mgr Adam J. Meks

Załącznik Nr 2 do „Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Iwaniska

Iwaniska, dn. .....

UPOWAŻNIENIE
DO PRZETWARZANIA DANYCH OSOBOWYCH

Nr .....

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2016r. poz. 922)

UPOWAŻNIAM

Panią/Pana .....

zatrudnioną na stanowisku .....
do przetwarzania danych osobowych oraz do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych w Urzędzie Gminy Iwaniska.

Upoważnienie obowiązuje na czas zatrudnienia w jednostce.

.....
(podpis pracownika)

.....
(podpis przełożonego)

RADCA PRAWNY
mgr Adam J. Meks

Załącznik Nr 3 do „Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Iwaniska

Wzór

Wykaz osób, które zostały zapoznane z „Polityką bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Iwaniska,

przeznaczonej dla osób zatrudnionych przy przetwarzaniu tych danych.

Lp	Nazwisko i imię	Stanowisko	Data	Podpis

Załącznik Nr 4 do „Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Iwaniska

Granice obszarów, w których przetwarzane są dane osobowe

Wykaz budynków i pomieszczeń wchodzących w skład obszaru przetwarzania danych osobowych.	
Adres: ul. Rynek 3	**Pomieszczenia:** **– parter, numery pokojów: 1,2,3,4,5,6** **– 1 piętro, numery pokojów: 10,11,12,17**

Ankieta dotycząca środków ochrony zawartych w programach obsługujących dane osobowe.

Wykaz zbiorów danych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, zlokalizowanych w Iwaniskach, przy ul. Rynek 3				
Lp.	**Zbiór danych**	**Programy zastosowane do przetwarzania / Nazwa zasobu**	**Lokalizacja zbioru/zasobu**	**Miejsce przetwarzania danych**
Referat Organizacyjny				
1 2	DZIENNIK KORESPONDENCYJNY	„EDICTA”	Serwer	Parter pok. 1,2,3,4,5,6, 1 piętro pok. 10,11,12,15,17
3	SKARGI i WNIOSKI	Rejestr skarg i wniosków	Parter pok. 5	Parter pok. 5
4	ARCHIWUM ZAKŁADOWE	Akta	Parter pok. 5	Parter pok. 5
5	Kadry i wynagrodzenia	Akta osobowe	Parter pok.5	Parter pok.5
6	Akta radnych	Akta rady	Parter pok.1	Parter pok.1
7	Akta komisji wyborczych	Rejestr	Parter pok.1	Parter pok.1
8	ROBOTY PUBLICZNE I PRACE INTERWENCYJNE	Rejestr	Parter pok. 5	Parter pok. 5
9	REJESTR STAŻY, PRAKTYK	Rejestr	Parter pok. 5	Parter pok. 5
Urząd Stanu Cywilnego				
8	AKTA STANU CYWILNEGO	Akta Stanu Cywilnego	1 piętro – pok. 11	1 piętro – pok. 11
9		„ŹRÓDŁO”	MSWIA	1 piętro – pok. 11
10	Rejestr członków OSP	Rejestr	1 piętro – pok. 11	1 piętro – pok. 11
10	EWIDENCJA LUDNOŚCI I DOWODY OSOBISTE	„SELWIN”	Serwer	1 piętro – pok. 12
11		„ŹRÓDŁO”	MSWIA	1 piętro – pok. 12
12		Karty mieszkańców	1 piętro – pok. 12	1 piętro – pok. 12
13		Rejestr wyborców	1 piętro – pok. 12	1 piętro – pok. 12
14		Rejestr poborowych i przedpoborowych	1 piętro – pok. 11	1 piętro – pok. 11, 12

15		„ŹRÓDŁO"	MSWIA	1 piętro – pok. 12
16		Koperty dowodowe	1 piętro – pok. 12	1 piętro – pok. 12
17	Kancelaria tajna	Akta	I piętro	I piętro – pok. 12
18	EDG	Kartoteka	MSWIA	1 piętro – pok. 12
19		CEIDG	MR	1 piętro – pok. 12
20	EWIDENCJA ZEZWOLEŃ NA SPRZEDAŻ NAPOJÓW ALKOHOLOWYCH	Kartoteka	1 piętro – pok. 12	1 piętro – pok. 12
21	DODATKI MIESZKANIOWE	Kartoteka	1 piętro – pok. 12	1 piętro – pok. 12
Referat Finansowy				
20		„GMINA2"	Serwer	Parter pok. 3 1 piętro – pok. 10
21		Karty gospodarstw	1 piętro – pok. 10	1 piętro – pok. 10
22		Nakazy płatnicze i decyzje	1 piętro – pok. 10	1 piętro – pok. 10
23	PODATKI I OPŁATY LOKALNE	Akta (ulgi podatkowe)	1 piętro – pok. 10	1 piętro – pok. 10
24		Upomnienia	1 piętro – pok. 10	1 piętro – pok. 10
		Kasa	Serwer	1 piętro – pok. 10
		„Tytuły wykonawcze"	Serwer	1 piętro – pok. 10
25		Tytuły wykonawcze	1 piętro – pok. 10	1 piętro – pok. 10
28		Rejestr zaświadczeń	1 piętro – pok. 10	1 piętro – pok. 10
26	ZWROT PODATKU AKCYZOWEGO	„PALIWO"	Serwer	1 piętro – pok. 10
27		Wnioski i decyzje	1 piętro – pok. 10	1 piętro – pok. 10
29	Kadry i wynagrodzenia	"PŁACE"	Serwer	1 piętro – pok. 17
30		Listy płac	1 piętro – pok. 17	1 piętro – pok. 17
31	Kadry i wynagrodzenia	„Płatnik"	Serwer	1 piętro – pok. 17
32		Rejestr deklaracji ZUS	1 piętro – pok. 17	1 piętro – pok. 17
33	KASA	„GMINA2"	Serwer	1 piętro – pok. 10
Referat Rozwoju Gospodarczego i Promocji Gminy				
34	Czynsze mieszkaniowe	„GMINA2"	Serwer	Parter pok. 3, 1 piętro, pok. 15
35		Akta najemcy	1 piętro, pok. 15	1 piętro, pok. 15
	UŻYTKOWANIE WIECZYSTE	Akta spraw	Parter, pok. 3	Parter, pok. 3
	UMOWY DZIERŻAWY	Akta spraw	Parter, pok. 3	Parter, pok. 3
	Numeracja porządkowa nieruchomości	Akta spraw	Parter, pok. 3	Parter, pok. 3
	Decyzje o zabudowie	Akta spraw	1 piętro, pok. 15	1 piętro, pok. 15
Referat Rolnictwa, Zaopatrzenia w Wodę, Odprowadzania Ścieków i Nieczystości				
	Wycinka drzew	Wnioski	parter – pok. 2	parter – pok. 2
	Zeznania świadków	Zaświadczenia	parter – pok. 2	parter – pok. 2
36	UPRAWA MAKU I KONOPII	Rejestr zezwoleń	parter – pok. 2	parter – pok. 2
37	OPŁATY ZA WODĘ	„WODA"	Serwer, parter – pok. 2	parter – pok. 2
		Kasa	Serwer	1 piętro pok. 9