Załącznik nr 2 do Zarządzenia Nr 62/2014
Wójta Gminy Zaleszany z dnia 27 maja 2014 r.
w sprawie polityki bezpieczeństwa informacji
oraz instrukcji zarządzania systemami informatycznymi
służącymi do przetwarzania danych osobowych

Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Gminy w Zaleszanach

Opracował: Sebastian Nabrzeski

Rozdział 1

Zastosowane pojęcia i definicje

Określenia i skróty użyte w Instrukcji zarządzania systemami informatycznymi w Urzędzie Gminy w Zaleszanach oznaczają:

1) Ustawa - należy przez to rozumieć ustawę z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.),
2) Urząd - należy przez to rozumieć Urząd Gminy w Zaleszanach,
3) Polityka bezpieczeństwa - należy przez to rozumieć załącznik nr 1 do Zarządzenia nr 62/2014 Wójta Gminy Zaleszany z dnia 247 maja 2014 r. w sprawie polityki bezpieczeństwa informacji oraz instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych,
4) Instrukcja – należy przez to rozumieć Instrukcję zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych, czyli niniejszy dokument,
5) ADO – należy przez to rozumieć Administratora Danych Osobowych, którym jest Urząd reprezentowany przez Wójta,
6) ABI - należy przez to rozumieć Administratora Bezpieczeństwa Informacji, czyli Sekretarza Gminy, który w imieniu ADO wykonuje czynności z zakresu ochrony danych osobowych,
7) ASI – należy przez to rozumieć Administratora Systemu Informatycznego, czyli:
    a. upoważnionego przez ABI do administrowania Elektronicznym Systemem Obiegu Spraw i Dokumentów lub innym systemem informatycznym, w którym przetwarzane są dane osobowe pracownika Referatu Organizacyjnego odpowiedzialnego za wdrożenie i stosowanie zasad bezpieczeństwa danych osobowych w zakresie technicznych i logicznych zabezpieczeń systemu,
    b. innego pracownika Urzędu, który otrzymał stosowne upoważnienie od ABI albo od podmiotu będącego administratorem systemu (oprogramowania), albo któremu podmiot będący administratorem systemu (oprogramowania) nadał takie upoważnienie w drodze zawartej umowy.
8) LABI – należy przez to rozumieć Lokalnego Administratora Bezpieczeństwa Informacji, czyli: Skarbnika, kierownika referatu oraz samodzielne stanowisko kierownicze lub urzędnicze, wyszczególnione w schemacie organizacyjnym Urzędu stanowiącym załącznik do Regulaminu organizacyjnego, posiadającego powierzenie obowiązków udzielone przez ABI,
9) Użytkownik – należy przez to rozumieć osobę posiadającą upoważnienie do przetwarzania danych w Urzędzie,

10) Użytkownik systemu – należy przez to rozumieć osobę posiadającą upoważnienie do przetwarzania danych w systemie informatycznym w Urzędzie,
11) Identyfikator – należy przez to rozumieć ciąg znaków literowych, cyfrowych lub innych specjalnych, jednoznacznie identyfikujących Użytkownika systemu,
12) Hasło dostępu – należy przez to rozumieć ciąg znaków literowych, cyfrowych lub innych specjalnych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym,
13) Logowanie się do systemu – należy przez to rozumieć meldowanie się użytkownika systemu do systemu za pomocą własnego identyfikatora i hasła dostępu,
14) System informatyczny – należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
15) Stacja robocza – należy przez to rozumieć zestaw komputerowy przypisany do pracownika – stanowisko komputerowe,
16) Serwer – należy przez to rozumieć specjalistyczny komputer przystosowany do pracy ciągłej z zainstalowanym oprogramowaniem serwerowym, świadczący usługi dla stacji roboczych,
17) Program antywirusowy – należy przez to rozumieć specjalistyczne oprogramowanie służące do ochrony stacji roboczej i serwera przed szkodliwym oprogramowaniem,
18) Informatyk – należy przez to rozumieć pracownika zatrudnionego w Referacie Organizacyjnym na stanowisku ds. sieci informatycznej i komputerowej.

Rozdział 2
Postanowienia ogólne

1. Instrukcja opisuje sposoby nadawania uprawnień Użytkownikom systemów, określa sposób pracy w systemach informatycznych, procedury zarządzania oraz czynności mające wpływ na zapewnienie bezpieczeństwa systemów informatycznych.
2. Instrukcja realizuje Politykę bezpieczeństwa.
3. Instrukcja dotyczy systemów gromadzących dane podlegające ochronie, z wyjątkiem systemów posiadających administratora innego, niż Urząd.
4. Do stosowania niniejszej Instrukcji zobowiązani są wszyscy Użytkownicy systemów.

Rozdział 3
Nadawanie i rejestrowanie uprawnień do przetwarzania danych osobowych w systemie informatycznym

1. Do przetwarzania danych osobowych w systemie informatycznym mają dostęp wyłącznie Użytkownicy systemu posiadający aktualne upoważnienie do przetwarzania danych osobowych, posiadają konto Użytkownika systemu i posiadają prawo do logowania się do systemu przy pomocy własnego identyfikatora i hasła dostępu.
2. Każdy Użytkownik systemu posiada odrębny Identyfikator.
3. Identyfikator jest niepowtarzalny w obrębie danego systemu, a po zablokowaniu nie może zostać przydzielony innemu Użytkownikowi systemu.
4. Identyfikator jest nadawany i blokowany przez ASI na wniosek LABI w trybie i na zasadach opisanych w Polityce bezpieczeństwa oraz odnotowany w ewidencji osób upoważnionych do przetwarzania danych osobowych, prowadzonej przez ABI.

Rozdział 4
Zasady posługiwania się hasłem

1. W Urzędzie stosuje się uwierzytelnianie dwustopniowe: na poziomie dostępu do systemu operacyjnego oraz na poziomie dostępu do systemu informatycznego, w którym przetwarzane są dane osobowe.
2. Bezpośredni dostęp do systemu może mieć miejsce wyłącznie po podaniu przez Użytkownika systemu własnego identyfikatora i/lub hasła dostępu.
3. Hasło dostępu ustanowione podczas przyznawania w systemie uprawnień Użytkownik systemu ma obowiązek zmienić podczas pierwszego logowania się do systemu na indywidualne hasło dostępu.
4. Użytkownik systemu ponosi pełną odpowiedzialność za wszystkie operacje wykonane przy użyciu identyfikatora i/lub hasła dostępu.
5. Hasło Użytkownika systemu musi być zmieniane nie rzadziej niż co 30 dni. W systemach, w których istnieje taka możliwość, Użytkownik systemu ma obowiązek dokonywać takiego ustawienia, aby system wymuszał dokonanie zmiany we wskazanym terminie.
6. Użytkownik systemu jest zobowiązany do zachowania poufności swoich haseł dostępu – również po upływie terminu ich ważności.
7. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie. W sytuacji, kiedy zachodzi podejrzenie, że poza Użytkownikiem systemu inna osoba poznała jego hasło, Użytkownik systemu zobowiązany jest do jego natychmiastowej zmiany.
8. Przy wyborze hasła Użytkownika systemu obowiązują następujące zasady:

1) minimalna długość hasła dostępu: 8 znaków, w tym znaki alfanumeryczne, znaki specjalne oraz wielkie i małe litery,
2) zabrania się stosowania haseł dostępu, których treść odpowiada informacjom o Użytkowniku powszechnie znanym lub znanym szerszej grupie osób, w szczególności takich, jak: identyfikator w systemie, imię, nazwisko, data urodzenia, numer rejestracyjny samochodu, a także przewidywalnych sekwencji znaków z klawiatury.

9. Zmiany hasła nie wolno zlecać innym osobom.
10. W systemach, które umożliwiają opcję zapamiętywania hasła dostępu nie wolno korzystać z tego uprawnienia.

Rozdział 5

Procedury rozpoczynania, zawieszania i kończenia pracy z komputerem i w systemie

1. Przed rozpoczęciem pracy przy komputerze należy zalogować się do systemu operacyjnego przy użyciu własnego identyfikatora i/lub hasła dostępu.
2. Przed rozpoczęciem pracy w systemie informatycznym należy zalogować się do systemu przy użyciu własnego identyfikatora i/lub hasła dostępu.
3. Każde stanowisko komputerowe, z wyłączeniem sekretariatu, musi mieć zainstalowaną opcję wygaszacza ekranu, która zostaje uruchomiona po upływie co najwyżej 10 minut z obowiązkowym użyciem hasła dostępu przy wznowieniu pracy komputera.
4. Stanowisko komputerowe zlokalizowane w sekretariacie musi mieć zainstalowaną opcję wygaszacza ekranu, która zostaje uruchomiona po upływie co najwyżej 3 minut z obowiązkowym użyciem hasła dostępu przy wznowieniu pracy komputera. Komputer ten musi być przytwierdzony do stanowiska pracy linką zabezpieczającą.
5. Przed wyłączeniem komputera należy bezwzględnie zakończyć pracę uruchomionych programów i wylogować się z systemów, do których Użytkownik systemu był zalogowany.
6. Każdy Użytkownik systemu ma obowiązek wykonywać kopie zapasowe ważnych dokumentów w celu ochrony przed utratą, co najmniej raz w tygodniu, a w przypadku dokumentów lub systemów informatycznych zawierających zbiory danych osobowych – codziennie.
7. Po wyłączeniu komputera należy wyłączyć listwę zasilającą komputer lub UPS.
8. Użytkownik systemu udostępniający stanowisko komputerowe innemu upoważnionemu Użytkownikowi systemu, zobowiązany jest, przed udostępnieniem mu komputera, do zakończenia pracy zgodnie z zasadami wskazanymi w ust. 5.

Rozdział 6
Tworzenie kopii zapasowych systemów serwerowych

1. Kopie zapasowe systemów serwerowych są wykonywane automatycznie pod nadzorem informatyka, zgodnie z ustalonym przez ASI harmonogramem.
2. Cykliczne wykonywanie kopii zapasowych danych jest wykonywane za pomocą narzędzi systemowych bądź dedykowanych dla danego systemu.

Rozdział 7
Przechowywanie nośników informacji i kopii zapasowych

1. Nośniki informacji są przechowywane w obszarach przetwarzania danych w sposób opisany w Polityce bezpieczeństwa. Z nośnikami danych zawierającymi dane osobowe, zbędnymi do realizacji zadań należy postępować zgodnie z zasadami opisanymi w Polityce bezpieczeństwa.
2. Kopie zapasowe są przechowywane na macierzy dyskowej.

Rozdział 8
Sposób zabezpieczania systemu informatycznego

1. Ochronę przed zanikaniem zasilania w energię elektryczną serwera oraz stacji roboczych, na których przetwarzane są dane osobowe, zapewniają zasilacze UPS lub baterie w laptopach.
2. Ochronę antywirusową stacji roboczych zapewnia program antywirusowy.
3. W przypadku wykrycia przez Użytkownika systemu wirusa na stacji roboczej, należy wstrzymać pracę na stanowisku komputerowym i niezwłocznie poinformować o tym fakcie informatyka.
4. Przed użyciem zewnętrznego nośnika danych należy sprawdzić, czy nie jest on zainfekowany wirusem.
5. W przypadku pracy w systemie wykazującym jakiekolwiek odstępstwa, w szczególności w przypadku pojawienia się komunikatu alarmowego, Użytkownik systemu ma obowiązek zaprzestać pracy w systemie i poinformować o tym fakcie informatyka.

Rozdział 9
Sposób oprowadzenia informacji o odbiorcach

1. Dane osobowe z systemów informatycznych mogą być udostępniane wyłącznie uprawnionym odbiorcom w trybie i na zasadach opisanych w Ustawie.
2. Aplikacje wykorzystywane do obsługi baz danych osobowych powinny zapewniać odnotowanie informacji o udzielonych odbiorcom danych. Zakres informacji powinien obejmować co najmniej: dane odbiorcy, datę wydania, zakres udostępnionych danych.
3. Rejestr wniosków o udostępnienie danych osobowych prowadzony i realizowany jest w ramach każdego Referatu pod nadzorem LABI.

Rozdział 10
Wykonywanie przeglądów i konserwacji

1. Przeglądy i konserwacje systemów i nośników informacji, dla których administratorem systemu jest Urząd, wykonywane są wyłącznie przez ASI.
2. W przypadku gdy uszkodzenie systemu informatycznego, dla którego administratorem jest Urząd wykracza poza możliwości ASI, naprawy dokonuje na zlecenie Urzędu podmiot zewnętrzny.

Rozdział 11
Procedura postępowania w przypadku stwierdzenia awarii systemów

1. Procedura dotyczy systemów i serwerów należących do Urzędu, zlokalizowanych:
   1) przy ul. Tadeusza Kościuszki 16,
   2) przy placu Kościuszki 5.
2. Za realizację czynności opisanych w niniejszej procedurze odpowiada ASI.
3. W przypadku pojawienia się problemów z działaniem serwera i/lub systemu operacyjnego należy:
   1) w miarę możliwości sprawdzić stan logów systemowych,
   2) sprawdzić stan ostatniej kopii systemu,
   3) zdiagnozować przyczynę problemu,
   4) wyłączyć serwer,
   5) po zdiagnozowaniu usterki przystąpić do naprawy serwera i/lub systemu.

Rozdział 12

Zasady zabezpieczania pomieszczeń serwerowych

1. Zasady opisane w niniejszym rozdziale dotyczą pomieszczeń serwerowych zlokalizowanych w:
   1) budynku przy ul. Tadeusza Kościuszki 16 – pokój na parterze,
   2) budynku przy placu Kościuszki 5 – pokój na I piętrze (Referat Gospodarki i Ochrony Środowiska).
2. Każde pomieszczenie serwerowe oznaczone jest napisem „Serwerownia".
3. Dostęp do pomieszczeń serwerowych posiadają tylko osoby upoważnione, wymienione w Polityce bezpieczeństwa, z zastrzeżeniem przepisów Rozdziału 15 niniejszej Instrukcji. Ponadto rejestr osób posiadających dostęp do pomieszczeń serwerowych znajduje się u ABI.
4. Klucze do pomieszczeń serwerowych wydawane są tylko osobom upoważnionym.
5. Wszelkie prace w pomieszczeniach serwerowych wymienionych w ust. 1, realizowane przez firmy zewnętrzne prowadzone są pod nadzorem ASI, a wejście do serwerowni odnotowane jest w rejestrze wejść prowadzonym przez ASI.
6. W przypadku nieobecności ASI w pomieszczeniach serwerowych, drzwi pomieszczeń muszą być zamykane.
7. W przypadku widocznych śladów wejścia do serwerowni przez osoby postronne, ASI sporządza protokół oraz powiadamia przełożonego.

Rozdział 13

Procedura wykonywania kopii bezpieczeństwa

1. Za realizację czynności opisanych w niniejszej procedurze odpowiada ASI.
2. Kopie wszystkich serwerów wykonywane są automatycznie i poza godzinami pracy Urzędu.
3. W pierwszym etapie kopia przenoszona jest na zewnętrzną macierz back-up'ową.
4. W kolejnym etapie kopia przenoszona jest na drugą macierz dyskową.
5. ASI w dniu roboczym sprawdzają status wykonanej kopii.

Rozdział 14

Procedura testu sprawności działania UPS w serwerowniach

1. Za realizację czynności opisanych w niniejszej procedurze odpowiada ASI.

2. Stan sprawności UPS będzie wykonywany nie rzadziej niż 1 raz na pół roku w dniach wolnych od pracy.
3. Przed testem należy wyłączyć wszystkie serwery i odpiąć od UPS.
4. Do UPS należy podpiąć zastępcze urządzenie, np. komputer, który znacząco obciąży prądowo badany UPS.
5. Aby przystąpić do testu należy:
   1) włączyć zasilacz awaryjny,
   2) włączyć urządzenie obciążające UPS,
   3) wyłączyć UPS z prądu i sprawdzić, jak długo będzie następowało podtrzymanie urządzenia obciążającego.
6. Każdorazowo wynik badania, tj. czas działania UPS ASI wpisuje do rejestru testów UPS, który znajduje się w pok. nr 12, w budynku przy ul. Tadeusza Kościuszki 16.
7. Po wykonanym teście należy odłączyć urządzenie obciążające, załączyć UPS oraz podpiąć serwery i je uruchomić.

Rozdział 15
Procedura wejścia do serwerowni zlokalizowanej w budynku przy ul. Tadeusza Kościuszki 16

W przypadku podejrzenia wystąpienia niebezpieczeństwa i konieczności wejścia pracownika Urzędu do pomieszczenia serwerowni w czasie nieobecności ASI, należy:

1. Otworzyć drzwi kluczem znajdującym się w sekretariacie.
2. Po wyjściu z serwerowni należy ją ponownie zabezpieczyć, poprzez prawidłowe zamknięcie drzwi.
3. Zwrócić niezwłocznie klucz w sekretariacie.
4. Powiadomić o awaryjnym wejściu do pomieszczeń serwerowni przełożonego.
5. Każdorazowe wejście należy odnotować w rejestrze wejść do serwerowni.

Rozdział 16
Procedura bezpieczeństwa w razie włamań do sieci komputerowej

1. Nadzór nad sieciami zlokalizowanymi w budynkach Urzędu przy ul. Tadeusza Kościuszki 16 oraz Placu Kościuszki 5 sprawuje ASI.
2. Sieć komputerowa Urzędu wyposażona jest w firewall oraz logowanie pakietów i IDS.
3. Wszystkie stanowiska komputerowe wyposażone są w program antywirusowy, który automatycznie pobiera najnowszą bazę sygnatur.
4. Serwer email powiadamia ASI o potencjalnym niebezpieczeństwie.

5. W przypadku widocznych śladów wejścia (włamania) do sieci, wykryciu wirusa lub widocznej luki bezpieczeństwa należy:
   1) zabezpieczyć i odłączyć serwer od sieci,
   2) sprawdzić logi systemowe,
   3) podjąć kroki zmierzające do usunięcia luki lub zagrożenia.
6. Naruszenie bezpieczeństwa sieci wewnętrznej i kradzieży danych należy zgłosić przełożonemu oraz sporządzić notatkę, którą należy przekazać Wójtowi.