Zarządzenie Nr 103/2011

Wójta Gminy Grodziczno

z dnia 30 grudnia 2011 r.

w sprawie: polityki bezpieczeństwa w Urzędzie Gminy w Grodzicznie oraz instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy w Grodzicznie.

Na podstawie: art. 36 ustawy z dnia 29 października 1997 r. o ochronie danych osobowych (jt. Dz. U. z 2002 r. Nr 101 poz. 926 z późniejszymi zmianami) oraz przepisów 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. z 2004 Nr 100 poz. 1024)

zarządza się co następuje:

§ 1

Wprowadza się do stosowania w Urzędzie Gminy w Grodzicznie politykę bezpieczeństwa wraz instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych stanowiącą załącznik do polityki bezpieczeństwa zgodnie z załącznikiem Nr 1 do niniejszego zarządzenia.

§ 2

Traci moc Zarządzenie Nr 104/2009 Wójta Gminy Grodziczno z dnia 31 grudnia 2009 r. w sprawie: polityki bezpieczeństwa w Urzędzie Gminy w Grodzicznie oraz Zarządzenie Nr 105/2009 Wójta Gminy Grodziczno z dnia 31 grudnia 2009 r. w sprawie ustalenia instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy w Grodzicznie.

§ 3

Zarządzenie wchodzi w życie z dniem podpisania.

Załącznik nr 1 do Zarządzenia Wójta Gminy Grodziczno Nr 103/2011
Z dnia 30 grudnia 2011 r.

Polityka Bezpieczeństwa dla Urzędu Gminy w Grodzicznie

Polityka bezpieczeństwa określa sposób prowadzenia i zakres dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.

Podstawa prawna

- Konstytucja Rzeczypospolitej Polskiej art. 47, 51;
- Ustawa z dnia 29 sierpnia 1997 o ochronie danych osobowych (Dz. U. Nr 101 poz. 926 z 2002 r.);
- 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 z 2004).

Polityka bezpieczeństwa została oparta również na zapisach Polskiej Normy PN-ISO/IEC 17799, PN-I-02000 oraz PN-I-13335-1 określających praktyczne zasady zarządzania bezpieczeństwem informacji w obszarze technik informatycznych, która jako cel polityki bezpieczeństwa wskazuje „zapewnienie kierunków działania i wsparcie kierownictwa dla bezpieczeństwa informacji". W zaleceniach dotyczących dokumentu określającego politykę bezpieczeństwa informacji wskazuje się tam, że dokument polityki bezpieczeństwa powinien być zatwierdzony przez kierownictwo, opublikowany i udostępniony w odpowiedni sposób wszystkim pracownikom.

Definicje

- **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden z kilku specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne;
- **Zbiór danych osobowych** - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony (jego części znajdują się w różnych miejscach) lub podzielony funkcjonalnie (przetwarzany za pomocą programów realizujących różne funkcje);
- **Przetwarzanie danych osobowych** – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, przenoszenie, transport opracowywanie, udostępnianie i usuwanie; zwłaszcza takie, które wykorzystuje się w systemach informatycznych;
- **System informatyczny** – system przetwarzania informacji wraz ze związanymi z nimi ludźmi oraz zasobami technicznymi i finansowymi, które dostarcza i rozprowadza informacje. W szczególności systemem informacyjnym może być system, w którym nie będzie żadnego

komputera, a wyłącznie dokumenty papierowe, skoroszyty oraz ludzie tam pracujący, wyposażenie pokoi, czy też organizacja pracy. Ochronie podlegają nie tylko informacje osobowe, ale także ludzie, zasoby techniczne i finansowe;

- **Bezpieczeństwo systemu informatycznego** – wdrożenie stosowanych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą;
- **Administrator Danych Osobowych (ADO)** – organ, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania danych osobowych. Administratorem danych jest Wójt Gminy, który ponosi pełnię odpowiedzialności wynikającej z przepisów ustawy o ochronie danych osobowych w odniesieniu do zbiorów danych osobowych znajdujących się w jego ustawowej dyspozycji;
- **Administrator Bezpieczeństwa Informacji (ABI)** – należy przez to rozumieć pracownika urzędu wyznaczonego przez Administratora Danych Osobowych do nadzorowania przestrzegania zasad ochrony oraz wymagań w zakresie ochrony, wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych;
- **Administrator Systemów Informatycznych (ASI)** – należy przez to rozumieć pracownika lub pracowników Informatyki odpowiedzialnych za stosowanie technicznych i organizacyjnych środków ochrony danych osobowych,
- **Osoba upoważniona lub użytkownik systemu** – osoba posiadająca upoważnienie wydane przez ADO lub osoba uprawniona przez niego i dopuszczona jako użytkownik do przetwarzania danych osobowych w systemie informatycznym danej komórki organizacyjnej, w zakresie wskazanym w upoważnieniu, zwana dalej użytkownikiem;
- **Osoba uprawniona** – osoba posiadająca uprawnienie wydane przez ADO na mocy którego wykonuje w jego imieniu określone czynności;
- **Sieć Lokalna (LAN)** – Lokalna sieć teleinformatyczna;
- **Sieć rozległa (WAN)** – Rozległa sieć teleinformatyczna;
- **Identyfikator użytkownika (LOGIN)** – ciąg znaków literowych i cyfrowych, lub innych, jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
- **Hasło (Password)**– ciąg znaków literowych cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
- **Serwer** – wydzielony komputer świadczący usług w udostępnianiu zasobów (pliki, bazy danych, systemy informatyczne) innym komputerom lub pośredniczący w przekazywaniu danych między komputerami.
- **Osprzęt sieciowy** - modemy, routery, koncentratory, przełączniki, punkty dostępowe.
- **Zalogowanie** – uwierzytelnienie czyli działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
- **Odbiorcy danych** – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:
  - osoby, której dane dotyczą,
  - osoby, upoważnionej do przetwarzania danych,

- przedstawiciela, o którym mowa w art. 31a ustawy o ochronie danych osobowych,
- podmiotu, o którym mowa w art. 31 ustawy o ochronie danych osobowych,
- organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

Cele

Celem przeprowadzonej analizy bezpieczeństwa jest ochrona systemu informatycznego jako całości, jego poszczególnych elementów, przetwarzanego przez system zbioru danych, obszaru, w którym przetwarzane są dane oraz osób, a przede wszystkim zapewnienie technicznych i organizacyjnych uwarunkowań mających wpływ na zarządzanie systemami informatycznymi, w których przetwarzane są dane osobowe.

Niniejsza polityka bezpieczeństwa zawiera:

1) wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w których przetwarzane są dane osobowe (załącznik 1);
2) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych lub w inny sposób (załącznik 2);
3) opis struktury zbiorów danych i sposób przepływu danych pomiędzy poszczególnymi systemami (załącznik 3);
4) środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych (załącznik 4);
5) instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych (załącznik 5)
6) instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych (załącznik 6);
7) wzór upoważnienia o nadanych uprawnieniach do przetwarzania danych osobowych (załącznik 7)
8) wzór ewidencji osób upoważnionych do przetwarzania danych osobowych (załącznik 8)

Załącznik Nr 1

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe

Wykaz pomieszczeń lub częsci pomieszczeń, w których przetwarzane są danc

Lp.	Nr pokoju	Określenie w strukturze organizacyjnej urzędu	Uwagi

Załącznik Nr 2

Wykazy zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych lub w inny sposób

Wykaz zbiorów przetwarzanych elektronicznie wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

Lp.	Nazwa zbioru	Program zastosowany do przetwarzania	Nr pomieszczenia w którym przetwarza się dane	Nazwa urządzenia w którym przetwarza się dane osobowe

Wykaz zbiorów przetwarzanych w inny sposób niż elektronicznie

Lp.	Nazwa zbioru	Program zastosowany do przetwarzania	Nr pomieszczenia w którym przetwarza się dane

Załącznik Nr 3

Opis struktury zbiorów danych i sposób przepływu danych pomiędzy poszczególnymi systemami

Opis struktury zbioru danych i sposób przepływu danych pomiędzy poszczególnymi systemami dla zbiorów danych osobowych przetwarzanych elektronicznie

Opis struktury zbioru danych i sposób przepływu danych pomiędzy poszczególnymi systemami znajduje się w dokumentacjach poszczególnych systemów dla poszczególnych zbiorów danych, które są załącznikami w wersji elektronicznej do niniejszej polityki bezpieczeństwa.

Wykaz dokumentacji systemów informatycznych dla poszczególnych zbiorów:

1. Dane kadrowo-płacowe pracowników: x:/zbior1
2. Ewidencja ludności i dowody osobiste: x:/zbior2
3. Rejestr kontrahentów: x:/zbior3
4. Ewidencja podatników, podatków i opłat oraz dłużników: x:/zbior4
5. Ewidencja działalności gospodarczej: x:/zbior5

Gdzie x oznacza literę napędu CDROM

Opis struktury zbioru danych dla zbioru danych osobowych przetwarzanych w inny sposób niż elektronicznie.

1. Rejestr skarg i wniosków. Struktura zbioru: Lp – Data wpływu – Imię i nazwisko petenta Nazwa instytucji, redakcji itp. – Adres petenta, instytucji, redakcji itp. – Przedmiot odwołania skargi, zażalenia – Data zlecenia załatwienia – Komu zlecono załatwienie (do kogo skargę skierowano) – Termin załatwienia – Data wpływu po załatwieniu – Sposób załatwienia – Data wysłania zawiadomienia – Kogo zawiadomiono – Uwagi
2. Ewidencja osób oczekujących na przydział mieszkania komunalnego. Struktura zbioru: Nazwisko i imię oraz adres zamieszkania, ilość osób w gospodarstwie domowym, Uwagi, data przyjęcia wniosku do realizacji.
3. Rejestr zezwoleń na wykonanie regularnych specjalnych przewozów osób w krajowym transporcie drogowym. Struktura zbioru: numer zezwolenia, nazwa przedsiębiorcy (nazwa firmy), siedziba – adres, numer druku, data ważności zezwolenia, data udzielenia zezwolenia.
4. Ewidencja dzierżawców gruntów. Struktura zbioru: imię, nazwisko i adres zamieszkania dzierżawców nieruchomości gminy miejskiej wraz z określeniem numeru umowy, daty zawarcia umowy, kwoty czynszu, termin zapłaty czynszu, numer faktury, datę uiszczenia opłaty.
5. Lista stawiennictwa osób do kwalifikacji wojskowej. Struktura zbioru: imię (imiona) i nazwisko, nazwisko rodowe, numer ewidencyjny pesel, miejsce urodzenia, seria i numer dowodu osobistego, miejsce pobytu stałego lub pobytu czasowego, adres do korespondencji
6. Rejestr mężczyzn/kobiet objętych rejestracją. Struktura zbioru: imię i nazwisko, nazwisko rodowe, imiona i nazwiska rodowe rodziców, imiona i nazwiska poprzednie, data i miejsce urodzenia, stan cywilny, numer pesel, adres i data zameldowania na pobyt stały, poprzednie adresy zameldowania na pobyt stały wraz z określeniem okresu zameldowania, tryb wymeldowania z pobytu stałego, adres zameldowania na pobyt czasowy wraz z określeniem okresu zameldowania, tryb wymeldowania z pobytu czasowego, data ujęcia w rejestrze, data zgłoszenia się do rejestracji, pokwitowanie odbioru potwierdzenia, stopień wojskowy, nazwa i

seria wojskowego dokumentu osobistego, oznaczenie wojskowego komendanta uzupełnień, w ewidencji której osoba pozostaje.

7. Wykaz osób o nieuregulowanym stosunku do powszechnego obowiązku obrony. Struktura zbioru: imię i nazwisko, imię ojca, rok urodzenia, miejsce zamieszkania na pobyt stały i pobyt czasowy, wyznaczona data stawienia się do kwalifikacji wojskowej, przyczyna niezgłoszenia się, faktyczna data zgłoszenia się do kwalifikacji wojskowej, miejsce zgłoszenia się do kwalifikacji wojskowej, numer wojskowego dokumentu osobistego, sankcje karne, podstawa wykreślenia z rejestru.

8. Wykaz osób reklamowanych od obowiązku pełnienia czynnej służby wojskowej w razie ogłoszenia mobilizacji i w czasie wojny. Struktura zbioru: imię i nazwisko, imię ojca, stopień wojskowy, rocznik, adres zamieszkania, rodzaj reklamacji, tytuł reklamowania z urzędu lub kwalifikacje i zajmowane stanowisko, numer zawiadomienia lub wykazu imiennego, numer pisma uchylającego reklamacji

9. Wykaz stanowisk i prac zleconych oraz osób dopuszczonych do pracy lub służby na stanowiskach, z którymi wiąże się dostęp do informacji niejawnych stanowiących tajemnicę służbową oznaczonych klauzulą „zastrzeżone" . Struktura zbioru: imię i nazwisko, imię ojca, data i miejsce urodzenia, adres zamieszkania, nazwa jednostki organizacyjnej, zajmowane stanowisko, numer i data wydania poświadczenia bezpieczeństwa, sygnatura akt postępowania sprawdzającego, określenie rodzaju informacji niejawnych, termin ważności poświadczenia bezpieczeństwa, data przeprowadzenia szkolenia, termin powtórzenia postępowania sprawdzającego .

10. Ewidencja wydanych zaświadczeń stwierdzających odbycie przeszkolenia w zakresie ochrony informacji niejawnych. Struktura zbioru: imię i nazwisko, data urodzenia, nazwa komórki organizacyjnej, numer i data wydania zaświadczenia, data przeprowadzenia szkolenia.

11. Książka ewidencja osób wyznaczonych do pełnienia służby w formacji obrony cywilnej – Samodzielny Pluton Ratownictwa Ogólnego. Struktura zbioru: imię i nazwisko, numer pesel, imię ojca, stopień wojskowy, adres zamieszkania, miejsce pracy, numer telefonu kontaktowego, numer karty przydziału do formacji OC.

12. Książka ewidencji kart przydziału do formacji obrony cywilnej. Struktura zbioru: imię i nazwisko, rok urodzenia, miejsce zamieszkania, numer karty przydziału, data wydania karty przydziału, data unieważnienia karty przydziału.

13. Rejestr wykonanych świadczeń osobistych. Struktura zbioru: imię i nazwisko, adres wykonawcy świadczenia, jednostka na rzecz której wykonano świadczenia, rodzaj i zakres wykonanych prac, numer decyzji, numer wezwania, nazwa organu nakładającego obowiązek wykonania świadczenia, czas trwania świadczenia.

14. Rejestr wykonanych świadczeń rzeczowych. Struktura zbioru: imię i nazwisko, adres wykonawcy świadczenia, jednostka na rzecz której wykonano świadczenia, rodzaj i zakres wykonanych prac, numer decyzji, numer wezwania, nazwa organu nakładającego obowiązek wykonania świadczenia, czas trwania świadczenia.

15. Rejestr wydanych decyzji administracyjnych w sprawach świadczeń osobistych. Struktura zbioru: imię i nazwisko, nazwa i adres zakładu pracy, miejsce zamieszkania, określenie wnioskodawcy, numer decyzji, numer wezwania .

16. Rejestr wydanych świadczeń administracyjnych w sprawach świadczeń rzeczowych. Struktura zbioru: imię i nazwisko, nazwa i adres zakładu pracy, miejsce zamieszkania, określenie wnioskodawcy, numer decyzji, numer wezwania.

17. Ewidencja zezwoleń na sprzedaż napojów alkoholowych przeznaczonych do spożycia poza miejscem sprzedaży –detal i w miejscu sprzedaży–gastronomia. Struktura zbioru: numer kolejny punktu sprzedaży, dokładny adres punktu sprzedaży (miejscowość, ulica, numer), rodzaj punktu sprzedaży (stoisko, dział, branża sklepu lub nazwa i kategoria zakładu gastronomicznego), nazwa (imię i nazwisko) oraz adres otrzymującego zezwolenie, rodzaj i nr zezwolenia (A, B, C), data wystawienia, termin ważności, godziny sprzedaży napojów alkoholowych (od-do), data zwrotu w przypadku utraty ważności lub cofnięcia zezwolenia, data i pokwitowanie odbioru, uwagi.

18. Ewidencja osób, w stosunku do których podjęto działania przeciwalkoholowe. Struktura zbioru: data wpływu wniosku, imię i nazwisko, adres zamieszkania, wnoszący wniosek (członek rodziny, osoby postronne, sąd, prokuratura, GOPS, Komenda Powiatowa Policji, zakład pracy i inn.), data posiedzenia Gminnej Komisji Rozwiązywania Problemów Alkoholowych, data skierowania na leczenie dobrowolne, data skierowania do sądu, przebieg postępowania.

19. Rejestr wydanych decyzji o warunkach zabudowy i zagospodarowania przestrzennego. Struktura zbioru: nr decyzji, przedmiot decyzji, oznaczenie nieruchomości, której dotyczy decyzja i nr działki, imię, nazwisko oraz adres zamieszkania wnioskodawcy, termin ważności decyzji;

20. Zbiór danych osobowych uczestników projektu „Przedszkole wokół Nas". Struktura zbioru: uczestnik (imię i nazwisko, PESEL, wiek, adres zamieszkania, nr telefonu kontaktowego). Rodzic/opiekun prawny (imię i nazwisko, adres zamieszkania, nr i seria dowodu osobistego). Nauczyciel prowadzący zajęcia (imię i nazwisko, imiona rodziców, PESEL, nr i seria dowodu osobistego, adres zamieszkania, nr telefonów kontaktowych, nr kont bankowych).

21. Akta stanu cywilnego. Struktura zbioru: imię i nazwisko, PESEL, data urodzenia, data zgonu, miejsce urodzenia, adres, dokument tożsamości, stan cywilny, imiona rodziców.

22. Zbiór osób którym udzielono zezwolenia na wycinkę drzew. Struktura zbioru: imię i nazwisko, adres zamieszkania

Załącznik Nr 4

Środki Techniczne i Organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

1. Obszar, w których przetwarza się, dane osobowe zabezpieczony jest przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania tych danych poprzez zamykanie tych pomieszczeń na dwa zamki.
2. Dodatkowo obszar, w których przetwarza się dane osobowe znajdujący się na parterze budynku jest wyposażony w okna antywłamaniowe.
3. Obszar, w którym znajdują się serwery i osprzęt sieciowy wyposażony jest w gaśnicę przeciwpożarową, system alarmowy i klimatyzację.
4. Serwery i osprzęt sieciowy znajdują się w specjalnym wydzielonym pomieszczeniu zamykanym na klucz, do której dostęp posiada administrator bezpieczeństwa informacji lub osoba przez niego upoważniona.
5. Przebywanie osób nieuprawnionych w pomieszczeniach, w których przetwarza się dane osobowe, jest dopuszczalne za zgodą administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.
6. Dostęp do danych osobowych mają tylko i wyłącznie pracownicy posiadający pisemne, imienne upoważnienia podpisane przez Administratora Danych Osobowych.
7. Każdy z pracowników zachowuje szczególną ostrożność przy przetwarzaniu wszelkich danych osobowych.
8. Dostęp do pomieszczeń możliwy jest tylko i wyłącznie w godzinach pracy urzędu. W wypadku, gdy jest wymagany poza godzinami pracy - możliwy jest tylko na podstawie pisemnego zezwolenia administratora danych osobowych.
9. Szafy, w których przechowywane są dane osobowe są zamykane na klucz.
10. Klucze do tych szaf posiadają upoważnieni pracownicy i Administrator Danych.
11. Szafy z danymi są otwarte tylko na czas potrzebny na dostęp do danych, a następnie są zamykane.
12. Dane osobowe w formie papierowej mogą znajdować się na biurkach tylko na czas niezbędny na dokonanie czynności służbowych, a następnie są chowane do szaf.
13. Dostęp do komputerów, na których są przetwarzane dane osobowe mają tylko upoważnieni pracownicy urzędu.
14. Stacje komputerowe, na których przetwarzane są dane osobowe mają tak ustawione monitory, aby nie miały wglądu w dane osoby nieupoważnione.
15. W przypadku użytkowania komputera przenośnego poza obszarem, w którym przetwarza się dane osobowe, należy zachować szczególną ostrożność i stosować środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.
16. W przypadku potrzeby przeniesienia danych osobowych pomiędzy komputerami należy dokonać tego z zachowaniem szczególnej ostrożności.
17. Nośniki użyte do tego należy wyczyścić (skasować nieodwracalnie), aby nie zostały na nich dane osobowe.
18. W wypadku niemożliwości skasowania danych z nośnika (płyta CD-ROM) należy taki nośnik zniszczyć fizycznie.
19. W przypadku wykorzystania do przenoszenia dysków, dane należy kasować z tych dysków.
20. Danych osobowych nie należy przesyłać drogą elektroniczną bez ochrony kryptograficznej.

23. Komputer y, na których przetwarza się dane osobowe podłączone są do systemów przeciwdziałającym awariom zasilania i zakłóceniom w sieci zasilającej.
24. Zabe zpieczenie sieci komputerowej LAN. Sieć komputerowa musi być zabezpieczona przed dostępem od sieci WAN. Do zabezpieczenia sieci stosuje się:
    a) router wyposażony w firewall, który ma za zadanie uwierzytelnianie źródła przychodzących wiadomości oraz filtrowanie pakietów w oparciu o adres IP, numer portu i inne parametry. Router składa się z bezpiecznego systemu operacyjnego i filtra pakietów. Ruch pakietów, który firewall przepuszcza jest określony przez administratora.
    b) adresowanie stacji roboczych tylko adresami statycznymi,
    c) systemy antywirusowe,
    d) dostęp do klienta poczty elektronicznej tylko na serwerach dedykowanych przez urząd
    e) okablowanie sieciowe wykonane jest z kabla spełniającego „normę" co najmniej kategorii 5
25. W systemie informatycznym służącym do przetwarzania danych osobowych stosuje się mechanizm kontroli dostępu do tych danych poprzez wprowadzenie identyfikatora i dokonaniu uwierzytelnienia poprzez hasło.
26. Do zasilania serwera i osprzętu sieciowego jest odrębna sieć zasilająca.
27. W systemach informatycznych, w których przetwarza się dane osobowe zastosowano podwójną autoryzację użytkownika. Pierwszej autoryzacji należy dokonać w momencie uzyskania dostępu do komputera, podając login użytkownika i hasło. Drugiej autoryzacji należy dokonać uruchamiając program użytkowy, podając login użytkownika i hasło. Dostęp do danych osobowych znajdującej się w systemie informatycznym uzyskuje się dopiero po poprawnym podwójnym zalogowaniu się do systemu Informatycznego.
28. Dostęp do konsoli serwera i osprzętu sieciowego zabezpieczony jest hasłem.
29. W przypadku zastosowania osprzętu sieciowego działającego bezprzewodowo, dostęp do usług świadczonych przez ten osprzęt musi być zabezpieczony metodą kryptograficzną.
30. Dane osobowe zawarte w systemie informatycznym zabezpiecza się poprzez sporządzanie ich kopii zapasowych. Kopie te sporządza się na dysku twardym serwera lub na nośniki zewnętrzne. Kopie na nośnikach zewnętrznych przechowuje się w zabezpieczonym pojemniku w szafie metalowej w pomieszczeniu nr 9 Urzędu. Po ustaniu użyteczności kopii zapasowych są one niszczone lub usuwane w zależności od typu nośnika.

Załącznik Nr 5

INSTRUKCJA

zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

Procedura nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności.

Nadawanie uprawnień.

1. Administrator Danych lub bezpośredni przełożony określa wymagane dla pracownika uprawnienia do zbiorów danych osobowych.
2. Administrator danych analizuje te wymagania i podejmuje decyzję o nadaniu uprawnień we wnioskowanym zakresie, ograniczeniu nadania uprawnień bądź odmowie nadania uprawnień.
3. Wpisu informacji o nadanych uprawnieniach do ewidencji osób upoważnionych do przetwarzania danych osobowych na podstawie pisemnego upoważnienia, który określa załącznik nr 7 do polityki bezpieczeństwa dokonuje administrator bezpieczeństwa informacji.
4. Ewidencję osób upoważnionych do przetwarzania danych osobowych prowadzi administrator bezpieczeństwa informacji wg wzoru, który stanowi załącznik nr 8 do polityki bezpieczeństwa.
5. Rejestracji uprawnień do przetwarzania danych osobowych w systemie informatycznym dokonuje administrator bezpieczeństwa informacji, lub osoba przez niego upoważniona.

Odbieranie uprawnień.

1. Odbieranie uprawnień może odbyć się:

a) w przypadku zmiany zakresu obowiązków pracownika,

b) w przypadku zmiany stanowiska pracy,

c) w przypadku rozwiązania umowy o pracę,

d) w przypadku naruszenia zasad ochrony danych osobowych pracownika

2. Administrator Danych lub bezpośredni przełożony odbiera uprawnienie do przetwarzania danych osobowych.
3. Wpisu informacji o odebranych uprawnieniach do ewidencji osób upoważnionych do przetwarzania danych osobowych na podstawie pisemnego upoważnienia, który określa załącznik nr 7 do polityki bezpieczeństwa dokonuje administrator bezpieczeństwa informacji.
4. Rejestracji odebrania uprawnień administrator bezpieczeństwa informacji dokonuje niezwłocznie.
5. Identyfikator byłego użytkownika nie jest powtórnie nadawany innej osobie.

Stosowane metody i środki uwierzytelniające oraz procedury związane z ich zarządzaniem i użytkowaniem

1. W systemie informatycznym służącym do przetwarzania danych osobowych stosuje się mechanizm kontroli dostępu do tych danych poprzez wprowadzenie identyfikatora i dokonaniu uwierzytelnienia poprzez hasło.

2. Użytkownik systemu informatycznego posiada niepowtarzalny identyfikator oraz pierwsze hasło dostępu nadane przez administratora bezpieczeństwa informacji.

3. Hasło dostępu użytkownika systemu informatycznego musi zawierać, co najmniej 8 znaków, zawiera ono małe i wielkie litery oraz cyfry lub znaki specjalne.

4. Hasło dostępu użytkownika systemu informatycznego nie może być takie samo jak jego identyfikator.

5. Użytkownik systemu informatycznego ma obowiązek zmieniać swoje hasło dostępu nie rzadziej niż co 30 dni.
6. Użytkownikowi sytemu informatycznego nie wolno zapisywać hasła dostępu na nośnikach informacji.
7. Użytkownik sytemu informatycznego jest zobowiązany do utrzymania w tajemnicy hasła dostępu, również po upływie jego ważności.
8. Hasło dostępu przy wpisywaniu go w systemie informatycznym nie może być wyświetlane na ekranie monitora.
9. W przypadku kompromitacji hasła, niezwłocznie jest ono zmieniane przez użytkownika lub administratora bezpieczeństwa informacji.

Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu

1. Administrator danych, ustala czas pracy użytkownikom systemu. Na pracę poza godzinami funkcjonowania urzędu musi wyrazić zgodę na piśmie administrator danych, w formie upoważnienia jednorazowego lub stałego.
2. Rozpoczęcie pracy z systemem informatycznym odbywa się poprzez wprowadzenie identyfikatora i uwierzytelnienie się poprzez hasło, które w trakcie wpisywania go do systemu informatycznego nie może być widoczne.
3. Po uwierzytelnieniu użytkownik sprawdza poprawność działania aplikacji. W przypadku stwierdzenia niezgodności w działaniu aplikacji powiadamia administratora bezpieczeństwa informacji, który podejmuje odpowiednie działania.
4. Zawieszenie pracy polega na zakończeniu realizowanych transakcji, jeśli takowe są w trakcie oraz zamknięciu aplikacji.
5. Zakończenie pracy odbywa poprzez:
a) zakończenie realizowanych transakcji, jeśli takowe są w trakcie.
b) zamknięcie aplikacji służącej do przetwarzania danych osobowych
c) wyłączeniu komputera
c) zabezpieczenia dokumentów i nośników przenośnych zawierających dane osobowe zgodnie z obowiązującymi zasadami.
d) zabezpieczenia obszaru, w którym przetwarzane są dane osobowe przed dostępem osób nieupoważnionych zgodnie z obowiązującymi zasadami.

Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.

1. Za sporządzanie i bezpieczeństwo kopii odpowiedzialny jest administrator bezpieczeństwa informacji, lub osoba przez niego upoważniona.
2. Kopii zapasowych danych osobowych należy dokonywać poprzez kopiowanie całej bazy danych.
3. Kopie zapasowe danych osobowych wykonuje się codziennie w dni robocze na dysku twardym serwera, a raz na miesiąc jedna kopia jest zgrywana na dwa nośniki CD lub DVD.
4. Kopie zapasowe danych osobowych dysk serwera sporządza się programem Cobian Backup, zaś na nośniki CD bądź DVD kopie sporządzane są programem Nero.

5. Kopie zapasowe danych osobowych, umieszcza się w katalogu, którego nazwą fragmentem nazwy jest data utworzenia tej kopii.
6. Nośniki CD lub DVD oznaczone są adnotacją jakiego okresu dotyczą.
7. W czasie tworzenia kopii zapasowych danych osobowych użytkownicy systemów nie mogą pracować z systemami przetwarzającymi dane osobowe.
8. Kopie zapasowe danych osobowych może tworzyć jedynie administrator bezpieczeństwa informacji, lub osoba przez niego upoważniona,
9. Kopie zapasowe programów i narzędzi programowych służących do przetwarzania, danych osobowych wykonywane są przez administratora bezpieczeństwa informacji lub osobę przez niego upoważnioną.
10. Kopie zapasowe programów i narzędzi programowych służących do przetwarzania danych osobowych wykonuje się na 2 nośnikach CD lub DVD programem Nero.
11. Kopie zapasowe programów i narzędzi programowych służących do przetwarzania danych osobowych oznacza się jakiego systemu dotyczą.
12. Kopie zapasowe programów i narzędzi programowych służących do przetwarzania danych osobowych sporządza się niezwłocznie po instalacji nowego oprogramowania lub jego aktualizacji.
13. Kopie zapasowe sprawdza się pod kątem ich dalszej przydatności do odtworzenia danych poprzez weryfikację w systemie służącym do jej sporządzania.

Sposób, miejsce i okres przechowywania kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

1. Kopie zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania przechowywane są w pojemniku w szafie metalowej w pomieszczeniu biura nr 9.
2. Pomieszczenie to wyposażone jest w alarm antywłamaniowy.
3. Kopie zapasowe danych osobowych składowane na dysku serwera, zabezpieczone są konsolą serwera, zabezpieczoną hasłem.
4. Kopie zapasowe zbiorów danych przechowywane są przez ich przydatności, o ile odrębne przepisy nie stanowią inaczej. Zaś po upływie tego okresu są kopie usuwa się, a w przypadku nośników CD lub DVD niszczy się je fizycznie.
5. Kopie zapasowe programów i narzędzi programowych służących do przetwarzania danych osobowych przechowywane są przez okres użytkowania tych programów. Po tym okresie niszczy się je fizycznie.

Zabezpieczenie przed niebezpiecznym oprogramowaniem

1. Systemy informatyczne zabezpieczone są przed niebezpiecznym oprogramowaniem poprzez stosowanie programów antywirusowych i systemu wykrywania włamań-firewall.
2. Na komputerze, w którym przetwarzane są dane osobowe musi być zainstalowany program antywirusowy, który musi działać w tle.
3. Należy stosować program antywirusowy, który zabezpiecza przed wirusami i innymi zagrożeniami.
4. Użytkownik systemu zobowiązany jest raz na 2 tygodnie aktualizować definicje wirusów i zagrożeń ze strony producenta oprogramowania.

5. W przypadku wykrycia obecności wirusa komputerowego lub innego zagrożenia należy niezwłocznie powiadomić administratora bezpieczeństwa informacji, który podejmuje odpowiednie działania.
6. System wykrywania włamań oparty jest na rozwiązaniu sprzętowym, który ma za zadanie uwierzytelnianie źródła przychodzących pakietów oraz filtrowania pakietów w oparciu o adres IP i numer portu.
7. System wykrywania włamań podłączony jest do sieci komputerowej LAN na styku jej połączenia z siecią WAN.
8. Ruch pakietów, który przepuszcza firewall jest określony przez administratora bezpieczeństwa informacji lub osobę przez niego upoważnioną.

Sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4; Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r.

1. Systemy informatyczne służące do przetwarzania danych osobowych w spełnia wymogi § 7 ust. 1 pkt 4.
2. W przypadku udostępnienia danych osobowych należy ten fakt odnotować w postaci notatki która, musi uwzględniać informacje: komu przekazujemy dane (np. firmie której eksploatujemy oprogramowanie), cel przekazania (np. naprawa struktury danych) kiedy, (data).

Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do ich przetwarzania.

1. Przeglądu i konserwacji dokonuje administrator bezpieczeństwa informacji, lub osoba przez niego upoważniona,
2. W przypadku przekazywania komputera z dyskiem lub innym nośnikiem danych osobowych do naprawy, należy nośnik zdemontować, zabezpieczyć dostęp hasłem lub dokonać naprawy w obecności osoby upoważnionej przez administratora danych, w przypadku przekazania nośnika innemu podmiotowi dane muszą zostać nieodwracalnie skasować,
3. Zabronione jest dokonywanie napraw sprzętu komputerowego samodzielnie przez pracowników urzędu.
4. Nośniki informacji zawierające dane osobowe przeznaczone do likwidacji muszą zostać pozbawione przez administratora bezpieczeństwa informacji lub osobę przez niego upoważnioną zapisu tych danych w sposób uniemożliwiający ich odczytanie.
5. Nośniki informacji zawierające dane osobowe przeznaczone do przekazania podmiotowi nieuprawnionemu do przetwarzania danych pozbawia się je wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie.

Załącznik Nr 6

INSTRUKCJA

postępowania w sytuacji naruszenia ochrony danych osobowych

1. Postanowienia ogólne
   a) Instrukcja określa tryb postępowania w sytuacji naruszenia ochrony danych osobowych gromadzonych i przetwarzanych systemach informatycznych. Instrukcję stosuje się także w przypadku gdy stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń tych danych.
   b) Przez naruszenie ochrony danych osobowych rozumie się niezgodne z przepisami ustawy z dnia 29 października 1997 r. o ochronie danych osobowych (Dz. U. Nr 133 poz. 883 z późn. zm.) przetwarzanie danych oraz usuwanie danych
   c) Osobami bezpośrednio odpowiedzialnymi za zgodną z prawem ochronę danych osobowych i ich zabezpieczenie są użytkownicy systemów informatycznych upoważnieni do przetwarzania danych osobowych oraz administrator bezpieczeństwa informacji w zakresie nadzoru nad zabezpieczeniem systemów informatycznych.
2. Tryb postępowania w sytuacji naruszenia ochrony danych osobowych.
   a) Użytkownik systemu informatycznego, który podejmie wiadomość lub stwierdzi naruszenie ochrony danych osobowych zobowiązany jest do natychmiastowego poinformowania o tym bezpośredniego przełożonego i pisemnie administratora bezpieczeństwa informacji.
   b) Gdy stan urządzeń, zawartość zbioru danych osobowych ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazać na naruszenie zabezpieczenie danych osobowych to fakt ten należy zgłosić pisemnie administratorowi bezpieczeństwa informacji.
   c) Administrator bezpieczeństwa informacji doraźnie usuwa przyczynę naruszenia zabezpieczenia systemu informatycznego, sprawdza ten system i powiadamia administratora danych.
   d) W przypadku naruszenia ochrony danych osobowych administrator bezpieczeństwa informacji sporządza protokół, który powinien zawierać:
      - kto zgłosił, kiedy (data), o której godzinie,
      - na czym polega naruszenie ochrony danych osobowych,
      - zabezpieczone dowody naruszenia danych,
      - propozycje wniosków co do dalszego trybu postępowania, w tym dotyczących zmiany systemu ochrony danych osobowych.
   e) Sporządzony protokół administrator bezpieczeństwa informacji przedstawia administratorowi danych.
   f) Administrator danych przeprowadza postępowanie wyjaśniające. Jeżeli stwierdzone zostanie naruszenie ochrony danych osobowych z winy użytkownika systemu informatycznego wszczyna się postępowanie dyscyplinarne wg odrębnych przepisów. Jeżeli naruszenie ochrony danych wyczerpuje znamiona przestępstwa określone w art. 49- 52 i 54 ustawy z dnia 29 października 1997 r. o ochronie danych osobowych sporządza się doniesienie do odpowiednich organów ścigania.
   g) Administrator bezpieczeństwa informacji przeprowadza niezwłocznie analizę systemu informatycznego i wprowadza dodatkowe zabezpieczenia w celu zmniejszenia zagrożenia i podatności tego systemu na naruszenie zasad bezpieczeństwa danych osobowych.

Załącznik 7

Urząd Gminy w Grodzicznie

NR WNIOSKU O NADANIE UPOWAŻNIENIA _____/ r.

nadawany przez Administratora danych w Urzędzie Gminy w Grodzicznie

WNIOSEK O NADANIE/ODWOŁANIE* UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

Upoważniany (imię i nazwisko)	

System/y:										
Identyfikator** :										

okres obowiązywania: od _____ do _____***

ZAKRES UPRAWNIEŃ (DOSTĘPNYCH CZYNNOŚCI) :

Zbiory:

Nazwa zbioru	Zmiana od dnia	Odczyt od dnia	Inne od dnia

*niepotrzebne skreślić
**jeżeli dane są przetwarzane w systemie informatycznym
***nie podanie daty oznacza „do odwołania"

Data i podpis wnioskującego o nadanie upoważnienia (np. przełożony)	
Urząd Gminy w Grodzicznie jako Administrator danych osobowych, w rozumieniu art. 7 pkt 4 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.),a w jej imieniu niniejszym upoważnia Panią/Pana. na mocy art. 37 tej ustawy, do przetwarzania danych. W ramach tego upoważnienia otrzymuje Pani/Pan dostęp do danych osobowych w powyżej określonym zakresie.	
Data i podpis Administratora danych lub osoby wskazanej przez Administratora danych do nadawania upoważnień	
Data i podpis upoważnionego	potwierdzam, iż zostałem zapoznany z przepisamiochrony danych oraz stosowanymi sposobami ich zabezpieczenia .....

Data przyjęcia wniosku i podpis osoby prowadzącej ewidencję upoważnionych do przetwarzania danych	
Podpis administratora bezpieczeństwa informacji (ABI)	

OŚWIADCZENIE (pracownika, zleceniodawcy lub konsultanta)

Ja niżej podpisany: .....

- **Stwierdzam, iż jest mi znana definicja danych osobowych** w rozumieniu art. 6 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.), w myśl której za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej albo możliwej do zidentyfikowania osoby fizycznej.

- **Zobowiązuje Się do zachowania w tajemnicy danych osobowych**, do których mam lub będę miał/a dostęp w związku z wykonaniem zadań służbowych, obowiązków pracowniczych w Urzędzie Gminy w Grodzicznie bądź zadań zleconych przez lub na rzecz Urząd Gminy Grodziczno, a w szczególności nie będę w celach pozasłużbowych bądź niezgodnych ze zleceniem lub powierzeniem przetwarzania wykorzystywał/a danych osobowych, z którymi zapoznałem/Am się w Urzędzie Gminy w Grodzicznie, o ile nie są one powszechnie znane.

- **Zobowiązuje się zachować w tajemnicy** sposoby zabezpieczenia danych stosowane w Urzędzie Gminy w Grodzicznie, o ile nie są one powszechnie znane lub nie wynikają w sposób oczywisty z innych powszechnie znanych informacji. Ponadto **przyjmuje do wiadomości, iż** sposoby zabezpieczenia danych osobowych stosowane w Urzędzie Gminy w Grodzicznie. są tajemnicą przedsiębiorstwa w rozumieniu art. 11 ust. 4 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (tekst jed. Dz. U. z 2003 r. Nr 153, poz. 1503).

- **Przyjmuje do wiadomości, iż postępowanie z powyższymi zobowiązaniami, może być uznane przez administratora danych osobowych za ciężkie naruszenie obowiązków pracowniczych** w rozumieniu art. 52 § 1 pkt 1 Kodeksu Pracy lub za naruszenie przepisów karnych ww. ustawy o ochronie danych osobowych, a także przepisów prawa cywilnego w przypadku umowy zlecenia lub umowy powierzenia przetwarzania.

.....
miejsce i data złożenia oświadczenia

.....
podpis składającego oświadczenie

Oświadczenie podpisano w obecności:

.....
Podpis odbierającego oświadczenie

Załącznik Nr 8

Ewidencja osób zatrudnionych przy przetwarzaniu danych osobowych

Lp.	Nazwisko i Imię	Identyfikator	Nazwa zbioru	Data nadania	Nr	Upoważniający	Data odebrania	Odbierający	Nr

Sporządzono dnia//Data aktualizacji: rrrr/mm/dd//rrrr/mm/dd

Sporządził:.....