ZARZĄDZENIE NR 5/10
Wójta Gminy Stargard Szczeciński
z dnia 5 stycznia 2010 roku

w sprawie ustalenia Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym systemów informatycznych służącym do przetwarzania danych osobowych w Urzędzie Gminy w Stargardzie Szczecińskim.

Na podstawie § 3 rozporządzenia Prezesa Rady Ministrów z dnia 25 lutego 1999 roku w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych (Dz.U. Nr 18 poz. 162) oraz § 3 ust.3 oraz § 4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U.Nr 100, poz.1024 z 2004r.), zarządza się co następuje:

§ 1. Ustala się „Politykę bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy w Stargardzie Szczecińskim zwaną dalej „Polityką bezpieczeństwa", która stanowi załącznik do niniejszego zarządzenia.

§ 2. Zobowiązuje się pracowników Urzędu Gminy Stargard Szczeciński do stosowania zasad określonych w „Polityce bezpieczeństwa".

§ 3. Wykonanie zarządzenia powierza się Administratorowi Bezpieczeństwa Informacji.

§ 4. Traci moc zarządzenie nr 105/05 Wójta Gminy Stargard Szczeciński z dnia 19 września 2005 r. w sprawie ustalenia Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym systemów informatycznych służącym do przetwarzania danych osobowych w Urzędzie Gminy w Stargardzie Szczecińskim.

§ 5. Zarządzenie wchodzi w życie z dniem podpisania

WÓJT
Kazimierz Szarżanowicz

WPROWADZENIE

Zbiór danych osobowych – rozumie się przez to każdy posiadający strukturę zestawów danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy jest zestaw ten rozproszony lub podzielony funkcjonalnie.

Dane osobowe mogą być przechowywane w systemach informatycznych lub kartotekach, księgach, wykazach i innych zbiorach ewidencyjnych.

Przetwarzanie danych może odbywać się tylko w obszarze przetwarzania danych osobowych Urzędu Gminy określonym w niniejszej polityce bezpieczeństwa.

Pracownicy Urzędu Gminy zobowiązani są do dołożenia szczególnej staranności w celu ochrony danych osobowych przed dostępem osób nieuprawnionych.

Pracownicy Urzędu Gminy zobowiązani do zbierania danych osobowych mogą udostępnić te dane tylko tej osobie, której one dotyczą w sposób uniemożliwiający wejście w ich posiadanie przez osoby trzecie, chyba że otrzymały na to zgodę osoby, której te dane dotyczą.

Niniejszy dokument opisuje reguły dotyczące bezpieczeństwa danych osobowych zawartych w systemach informatycznych w Urzędzie Gminy w Stargardzie Szczecińskim. Opisane reguły określają granice dopuszczalnego zachowania wszystkich użytkowników systemów informatycznych wspomagających pracę Urzędu Gminy. 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 systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Stargard Szczeciński"**, zwany dalej **„Polityką bezpieczeństwa"**, określa dane osobowe (zbiory i ich strukturę), miejsce przetwarzania (obszar przetwarzania danych), sposób przetwarzania (sposób przepływu danych pomiędzy systemami) oraz podaje procedury uwierzytelnienia i dostępu do danych osobowych, archiwizacji i przechowywania oraz wskazuje sposób postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych w systemach informatycznych w Urzędzie Gminy Stargard Szczeciński.

„Polityka bezpieczeństwa" zawiera:

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

   OBSZAR PRZETWARZANIA DANYCH OSOBOWYCH
   -stanowi załącznik nr 1 do „Polityki Bezpieczeństwa.

2. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do ich przetwarzania.

   WYKAZ ZBIORÓW DANYCH OSOBOWYCH
   -stanowi załącznik nr 2 do „Polityki Bezpieczeństwa.

3. Opis struktury zbiorów danych osobowych wskazujących zawartość poszczególnych pól informacyjnych i powiązań między nimi.

   OPIS STRUKTURY ZBIORÓW DANYCH OSOBOWYCH
   oraz SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY SYSTEMAMI
   -stanowi załącznik nr 3 do „Polityki Bezpieczeństwa.

„Polityka bezpieczeństwa" określa:

1. Procedury nadawania i rejestrowania uprawnień do przetwarzania danych osobowych.
2. Procedury i metody uwierzytelniające dostęp informacji zawierających dane osobowe.
3. Procedury rozpoczęcia, zawieszenia i zakończenia pracy systemów przetwarzających dane osobowe.
4. Procedury tworzenia, przechowywania i likwidowania kopii zapasowych zbiorów danych i narzędzi do przetwarzania danych osobowych.
5. Tryb postępowania w przypadku, gdy:
   1) stwierdzono naruszenie zabezpieczenia systemu informatycznego,
   2) 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.

„Polityka bezpieczeństwa" obowiązuje wszystkich pracowników Urzędu Gminy w Stargardzie Szczecińskim.

Wykonywanie postanowień tego dokumentu ma określić miejsca, zakresy, sposoby, i uprawnienia przetwarzania oraz ma zapewnić właściwą reakcję, ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa systemów i zapewnić właściwy tryb działania w celu przywrócenia bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych.

Rozdział 1

ADMINISTRATOR DANYCH

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 osobowych Urzędu Gminy, a w szczególności:
   1) zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym,
   2) zapobiegać przed zabraniem danych przez osobę nieuprawnioną,
   3) zapobiegać przetwarzaniu danych z naruszeniem ustawy oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych.

Rozdział 2

ADMINISTRATOR BEZPIECZEŃSTWA INFORMACJI

1. Administrator danych, swoją decyzją wyznacza Administratora Bezpieczeństwa Informacji danych zawartych w systemach informatycznych, zwanego dalej "Administratorem Bezpieczeństwa" oraz osobę upoważnioną do zastępowania „Administratora Bezpieczeństwa".
2. "Administrator bezpieczeństwa" realizuje zadania w zakresie ochrony danych, a w szczególności:
   1) przyznawania unikalnych identyfikatorów użytkownikom przetwarzającym dane osobowe w systemie informatycznym oraz prowadzenia ich rejestru
   2) przyznawania, zmiany i wycofania uprawnień użytkownikom w zakresie dostępu do systemu informatycznego oraz prowadzenia ich rejestru
   3) ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach systemów informatycznych,
   4) podejmowania stosownych działań w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia danych znajdujących się w systemie informatycznym,
   5) niezwłocznego informowania Administratora danych lub osoby przez niego upoważnionej o przypadkach naruszenia przepisów ustawy o ochronie danych osobowych,
   6) nadzoru i kontroli systemów informatycznych służących do przetwarzania danych osobowych i osób przy nim zatrudnionych.

Administrator Bezpieczeństwa Informacji uprawniony jest do kontroli wszystkich użytkowników systemów informatycznych przetwarzających dane osobowe w Urzędzie Gminy w Stargardzie Szczecińskim.

Osoba zastępująca Administratora Bezpieczeństwa powyższe zadania realizuje w przypadku nieobecności Administratora Bezpieczeństwa.

Osoba zastępująca składa Administratorowi Bezpieczeństwa relację z podejmowanych działań w czasie jego zastępstwa.

Rozdział 3

ZABEZPIECZENIE DANYCH OSOBOWYCH

Środki techniczne:

1. Przetwarzanie danych osobowych w wydzielonych pomieszczeniach położonych w strefie administracyjnej,
2. Zabezpieczenie wejścia do pomieszczeń, o których mowa w pkt. 1,
3. Szczególne zabezpieczenie centrum przetwarzania danych (komputer centralny, serwerownia) poprzez zastosowanie systemu kontroli dostępu,
4. Wyposażenie pomieszczeń w szafy dające gwarancję bezpieczeństwa dokumentacji.

Środki organizacyjne:

1. zapoznanie każdej osoby z przepisami dotyczącymi ochrony danych osobowych, przed dopuszczeniem jej do pracy przy przetwarzaniu danych osobowych,
2. przeszkolenie osób, o których mowa w pkt. 1, w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochroną danych osobowych,
3. kontrolowanie otwierania i zamykania pomieszczeń, w których są przetwarzane dane osobowe, polegające na otwarciu pomieszczenia przez pierwszą osobę, która rozpoczyna pracę oraz zamknięciu pomieszczenia przez ostatnią wychodzącą osobę.

Niezależnie od niniejszych zasad opisanych w dokumencie „Polityka bezpieczeństwa w Urzędzie Gminy w Stargardzie Szczecińskim." w zakresie bezpieczeństwa mają zastosowanie wszelkie wewnętrzne regulaminy lub instrukcje dotyczące bezpieczeństwa ludzi i zasobów informacyjnych oraz indywidualne zakresy zadań osób zatrudnionych przy przetwarzaniu danych osobowych w określonym systemie.

Zabezpieczenia:

1) *Zabezpieczenia przed utratą zasilania z sieci energetycznej i utratą danych:*
   a) *odrębne zasilanie sprzętu komputerowego,*
   b) *ochrona serwerów przed zanikiem zasilania poprzez stosowanie zasilaczy zapasowych UPS,*
   c) *ochrona przed utratą zgromadzonych danych przez robienie kopii zapasowych na nośnikach CD i DVD, z których w przypadku awarii odtwarzane są dane i system operacyjny*
   d) *ochrona przed awarią podsystemu dyskowego przez używanie macierzy dyskowych.*

2) *Zabezpieczenia przed nieautoryzowanym dostępem do baz danych Urzędu:*
   a) *wszystkie gniazdka lokalnej sieci komputerowej są galwanicznie oddzielone od szkieletu sieci komputerowej. Podłączenie (zkrosowanie) danego użytkownika do sieci komputerowej dokonuje Administrator Bezpieczeństwa Informacji.*
   b) *aby uzyskać dostęp do zasobów sieci, należy zwrócić się do Administratora Bezpieczeństwa z odpowiednim wnioskiem w którym podane będą dane nowego użytkownika oraz zasoby jakie ma on mieć udostępnione.*
   c) *w systemie informatycznym zastosowano podwójną autoryzację użytkownika. Pierwszej autoryzacji należy dokonać w momencie uzyskania dostępu do serwera, podając login użytkownika i hasło. Drugiej autoryzacji należy dokonać uruchamiając program użytkowy, podając login użytkownika i hasło. Dostęp do wybranej bazy danych uzyskuje się dopiero po poprawnym podwójnym zalogowaniu się do systemu informatycznego.*

3) *Zabezpieczenia przed nieautoryzowanym dostępem do baz danych poprzez internet.*
W zakresie dostępu z sieci wewnętrznej do sieci rozległej Internet zastosowano środki ochrony przed podsłuchiwaniem, penetrowaniem i atakiem z zewnątrz. Zastosowano firewall, który ma za zadanie uwierzytelnianie źródła przychodzących wiadomości oraz filtrowanie pakietów w oparciu o adres IP, numer portu i inne parametry. Ściana ogniowa składa się z bezpiecznego systemu operacyjnego i filtra pakietów. Ruch pakietów, który firewall przepuszcza jest określony przez administratora.

Firewall zapisuje do logu fakt zaistnienia wyjątkowych zdarzeń i śledzi ruch pakietów przechodzących przez nią. Dostęp do sieci jest ustalony indywidualnie dla każdego użytkownika na podstawie wniosku.
Oprócz filtra pakietów zastosowano również system wykrywający obecność wirusów w poczcie elektronicznej.

W efekcie zapewnione jest:

a) zabezpieczenie sieci przed atakiem z zewnątrz poprzez blokowanie wybranych portów,

b) filtrowanie pakietów i blokowanie niektórych usług,

c) objęcie ochroną antywirusową wszystkich danych ściąganych z internetu na stacjach lokalnych,

d) zapisywanie logów połączeń użytkowników z siecią Internet

Postanowienia końcowe.

1. *do pomieszczeń w których następuje przetwarzanie danych osobowych mają dostęp tylko uprawnione osoby bezpośrednio związane z nadzorem nad serwerami lub aplikacjami.*
2. *zabezpieczenie przed nieuprawnionym dostępem do danych, prowadzone jest przez Administratora Bezpieczeństwa zgodnie z przyjętymi procedurami nadawania uprawnień do systemu informatycznego.*
3. *osoby mające dostęp do danych powinny posiadać zaświadczenie o przebytym szkoleniu z zakresu ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997r. (Dz. U. Nr 133, poz. 883 z późn. zm.).*
4. *w pobliżu wejścia do pomieszczenia z serwerami i innym urządzeniami znajduje się gaśnica, która okresowo jest napełniana i kontrolowana przez specjalistę.*

Rozdział 4

OPIS ZDARZEŃ NARUSZAJĄCYCH OCHRONĘ DANYCH OSOBOWYCH

1. Podział zagrożeń:

1) **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.

2) **zagrożenia losowe wewnętrzne** (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych.

3) **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 których przetwarzane są dane osobowe to głównie:**

   1) **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.,

   2) **niewłaściwe parametry środowiska**, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,

   3) **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,

   4) **pojawienie się** odpowiedniego **komunikatu alarmowego** od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,

   5) **jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu** lub inną nadzwyczajną i niepożądaną modyfikację w systemie,

   6) nastąpiło **naruszenie lub próba naruszenia integralności systemu** lub bazy danych w tym systemie,

   7) **stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),**

   8) nastąpiła **niedopuszczalna manipulacja danymi osobowymi** w systemie,

   9) ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń,

   10) 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.,

   11) ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki", itp.,

   12) podmieniono lub zniszczono nośniki z danymi osobowymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane osobowe,

   13) 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 5

KONTROLA PRZESTRZEGANIA ZASAD ZABEZPIECZENIA DANYCH OSOBOWYCH

1. Administrator danych lub osoba przez niego wyznaczona, którą jest „Administrator Bezpieczeństwa Informacji" sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych wynikających z ustawy o ochronie danych osobowych oraz zasad ustanowionych w niniejszym dokumencie.
2. Administrator Bezpieczeństwa sporządza półroczne plany kontroli zatwierdzone przez Wójta i zgodnie z nimi przeprowadza kontrole oraz dokonuje kwartalnych ocen stanu bezpieczeństwa danych osobowych.
3. Na podstawie zgromadzonych materiałów, o których mowa w ust. 2, Administrator Bezpieczeństwa sporządza roczne sprawozdanie i przedstawia Administratorowi danych.

Rozdział 6

PRACA W SYSTEMACH INFORMATYCZNYCH

Poziom bezpieczeństwa przetwarzania danych

W Urzędzie Gminy Stargard Szczeciński wprowadzony jest podstawowy poziom bezpieczeństwa

Zarządzanie systemem informatycznym

1. System informatyczny służący do przetwarzania danych osobowych może być obsługiwany wyłącznie przez pracowników Urzędu Gminy, w zakresie nadanych im poziomów uprawnień przez administratora po odbyciu szkolenia w zakresie obsługi sprzętu komputerowego i zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych. Każdy użytkownik podpisuje stosowne oświadczenie, którego wzór stanowi załącznik nr 4.
2. W szczególnych wypadkach (np. zapobieżenia utraty zbioru, usunięcie awarii, modyfikacja oprogramowania, itp.) użytkownik może dopuścić do obsługi systemu informatycznego przedstawiciela autora oprogramowania lub serwisu po uprzednim powiadomieniu administratora (ABI) i pod jego nadzorem.
3. Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane są do zachowania ich w tajemnicy w czasie zatrudnienia jak i po jego ustaniu jak też:
   a) nie ujawniać szczegółów technologicznych w przetwarzanych systemach,
   b) nie udostępniać osobom nieupoważnionym nośników magnetycznych i wydruków komputerowych,
   c) kopiować lub przetwarzać danych w sposób inny niż dopuszczony obowiązującą instrukcją.

Rejestr użytkowników

1. Dostęp do danych osobowych w systemie informatycznym ma wyłącznie osoba ujęta w rejestrze użytkowników.
2. Rejestr użytkowników prowadzony jest przez administratora bezpieczeństwa informacji.
3. Rejestr użytkowników zawiera: imię i nazwisko użytkownika, identyfikator oraz datę przydziału i wygaśnięcia identyfikatora.
4. Użytkownikowi, który został zarejestrowany w rejestrze użytkowników administrator (ABI) przyznaje unikalny identyfikator.
5. Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego nie może być przyznany innej osobie.
6. Identyfikator osoby, która utraciła uprawnienia do dostępu do systemu informatycznego, należy niezwłocznie wyrejestrować z systemu informatycznego, w którym są one przetwarzane, unieważnić jej hasło oraz podjąć inne stosowne działania w celu zapobieżenia dalszemu dostępowi tej osoby do danych.
7. Rejestr użytkowników dostępny jest tylko administratorowi danych i bezpieczeństwa informacji i podlega zabezpieczeniu przed dostępem osób nieuprawnionych.

Przydział haseł dla użytkowników

1. Każdy użytkownik systemu informatycznego mający dostęp do danych osobowych musi mieć hasło zabezpieczające wejście do systemu, zwane dalej hasłem.
2. Hasło użytkownika znane jest tylko użytkownikowi, administratorowi danych i administratorowi bezpieczeństwa informacji.
3. Hasło powinno być zmieniane nie rzadziej jak raz w miesiącu, standardowo w ostatnim dniu miesiąca kalendarzowego.
4. Do zmiany hasła upoważnione są użytkownik, administrator danych i administrator bezpieczeństwa informacji.
5. Hasło użytkownika umożliwiające dostęp do systemu informatycznego utrzymuje się w tajemnicy, również po upływie jego ważności.
6. Nadzór nad prawidłowym zabezpieczeniem systemu przez użytkownika sprawuje administrator bezpieczeństwa informacji.

Procedury rozpoczęcia i zakończenia pracy

3. Rozpoczęcie pracy w systemie informatycznym następuje po uprzednim upewnieniu się czy nie uszkodzono sprzętu komputerowego oraz nie naruszono danych osobowych.
4. Bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.
5. W pomieszczeniach gdzie przebywają osoby postronne, monitory stanowisk dostępu do danych osobowych powinny być ustawione w taki sposób, żeby uniemożliwić tym osobom wgląd w dane.
6. Ekrany monitorów stanowisk dostępu do danych osobowych powinny być automatycznie wyłączone po upływie ustalonego czasu nieaktywności użytkownika.
7. Zakończenie pracy na stanowisku dostępu do danych osobowych winno nastąpić w taki sposób, aby osoba nieupoważniona nie mogła mieć dostępu do tych danych.

Zabezpieczenie danych osobowych przed wirusami komputerowymi

1. Dane osobowe przechowywane w systemie informatycznym winny być chronione przed wirusami komputerowymi przy użyciu dostępnych środków technicznych i programów antywirusowych.
2. Użytkownik ma obowiązek dbania i zabezpieczenie danych osobowych przed wirusami komputerowymi.
3. Sprawdzanie danych pod kątem obecności wirusów komputerowych wykonywane jest przez administratora bezpieczeństwa informacji co najmniej raz w tygodniu standardowo w ostatni dzień tygodnia .

Przechowywanie nośników informacji

1. Nośniki informacji oraz wydruki z danymi osobowymi, które nie są przeznaczone do udostępniania przechowywane mają być w kasach pancernych, szafach metalowych lub innych szafach zamykanych na zamki patentowe, znajdujące się w pomieszczeniach specjalnie zabezpieczonych przed dostępem osób niepowołanych.
2. Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia należy zniszczyć w stopniu uniemożliwiającym ich odczytanie, stosując do tego niszczarki typu paskowo-odcinkowe.

Konserwacja systemu i zbioru danych osobowych

1. Urządzenia, dyskietki lub inne informatyczne nośniki danych zawierające dane osobowe, przeznaczone do przekazania innemu podmiotowi nie uprawnionemu do otrzymania danych osobowych pozbawia się wcześniej zapisu tych danych.
2. Urządzenia, dyskietki i inne informatyczne nośniki przeznaczone do naprawy pozbawia się przed naprawą zapisu tych danych lub naprawia się je pod nadzorem osoby upoważnionej przez administratora bezpieczeństwa informacji.
3. Przeznaczone do likwidacji urządzenia, dyskietki lub inne nośniki zawierające dane osobowe pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie.

Sposób postępowania w zakresie komunikacji w sieci komputerowej.

1. Dostęp do sieci komputerowej, w której znajdują się dane osobowe mają wyłącznie pracownicy posiadający specjalne upoważnienie administratora danych.
2. Zgodnie z nadanymi przez administratora danych upoważnieniami do przetwarzania danych osobowych, zawartych w zakresie czynności pracownika administrator bezpieczeństwa informacji nadaje odpowiednie uprawnienia w tym zakresie w systemie komputerowym danego pracownika.
3. Przesyłanie danych osobowych za pomocą internetu dopuszczalne jest tylko po uprzednim zakodowaniu tych danych, spakowaniu i zabezpieczeniu hasłem.
4. Poinformowanie odbiorcy danych osobowych przekazywanych za pomocą internetu o treści hasła zabezpieczającego oraz przesył danych nie może nastąpić w czasie tej samej transmisji.

5. Zakazuje się :
   1) kopiowania danych osobowych znajdujących się w sieci na stacjonarne nośniki informatyczne (za wyjątkiem przypadków kopiowania w celu utworzenia kopii awaryjnej) i wynoszenia ich poza teren Urzędu Gminy,
   2) kopiowania danych osobowych znajdujących się w systemie na komputery przenośne (laptopy itp.).

Kopie awaryjne

1. Zbiory danych osobowych winny być zabezpieczone przed ich przypadkową utratą na dodatkowych nośnikach informatycznych (dyskietki, płyty CD, zewnętrzne dyski twarde itp.) zwane dalej kopiami awaryjnymi.
2. Kopie awaryjne wykonywane są przez administratora bezpieczeństwa informacji raz w tygodniu, standardowo w ostatni dzień tygodnia po zakończeniu pracy w systemach informatycznych.
3. Kopie awaryjne powinny być przechowywane w pomieszczeniu wyznaczonych przez administratora danych innym niż pomieszczenie, w którym są zbiory danych osobowych eksploatowane na bieżąco. Pomieszczenie to włączone jest do obszaru, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego.
4. Nadzór nad prawidłowym przechowywaniem kopii awaryjnych sprawuje administrator bezpieczeństwa informacji.
5. Prowadzona jest ewidencja kopii awaryjnych zawierająca datę sporządzenia, datę likwidacji, zakres przechowywanych danych.

Rozdział 7

POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. W przypadku stwierdzenia naruszenia:
   1) zabezpieczenia systemu informatycznego,
   2) technicznego stanu urządzeń,
   3) zawartości zbioru danych osobowych,
   4) ujawnienia metody pracy lub sposobu działania programu,
   5) jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych,
   6) innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. zalanie, pożar, itp.)

każda osoba zatrudniona przy przetwarzaniu danych osobowych jest obowiązana niezwłocznie powiadomić o tym fakcie Administratora 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:
   1) 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,
   2) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
   3) zaniechać - o ile to możliwe - dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,
   4) podjąć inne działania przewidziane i określone w instrukcjach technicznych i technologicznych stosownie do objawów i komunikatów towarzyszących naruszeniu,
   5) podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej,
   6) zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku,
   7) udokumentować wstępnie zaistniałe naruszenie,
   8) 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:
   1) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy Urzędu Gminy,
   2) może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
   3) rozważa celowość i potrzebę powiadamia o zaistniałym naruszeniu Administratora danych ,
   4) nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba, ze specjalistami spoza Urzędu Gminy.
5. Administrator Bezpieczeństwa dokumentuje zaistniały przypadek naruszenia oraz sporządza raport wg wzoru stanowiącego nr 5, który powinien zawierać w szczególności:
   1) wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpytanych w związku z naruszeniem,
   2) określenie czasu i miejsca naruszenia i powiadomienia,
   3) określenie okoliczności towarzyszących i rodzaju naruszenia,
   4) wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania,
   5) wstępną ocenę przyczyn wystąpienia naruszenia,
   6) ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.

6. Raport, o którym mowa w ust. 6, Administrator Bezpieczeństwa niezwłocznie przekazuje Administratorowi danych, a w przypadku jego nieobecności osobie uprawnionej.
7. Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym 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. 9, 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 8

MONITOROWANIE ZABEZPIECZEŃ

1. Prawo do monitorowania systemu zabezpieczeń posiadają, zgodnie z zakresem czynności:
   1) Administrator Danych,
   2) Administrator Bezpieczeństwa Informacji.
2. W ramach kontroli należy zwracać szczególna uwagę na:
   1) okresowe sprawdzanie kopii bezpieczeństwa pod względem przydatności do możliwości odtwarzania danych,
   2) kontrola ewidencji nośników magnetycznych,
   3) kontrola właściwej częstotliwości zmiany haseł .

Rozdział 9

SZKOLENIA

1. Wszyscy pracownicy Urzędu Gminy mają obowiązek brać udział w szkoleniach.
2. Szkolenie powinno dotyczyć:
   1) obowiązujących przepisów i instrukcji wewnętrznych dotyczących ochrony danych osobowych, sposobu niszczenia wydruków i zapisów na nośnikach magnetycznych i optycznych,
   2) przedstawienie zasad ochrony danych osobowych dotyczących bezpośrednio wykonywanych obowiązków na stanowisku pracy.

Rozdział 10

NISZCZENIE WYDRUKÓW I ZAPISÓW NA NOŚNIKACH MAGNETYCZNYCH

1. Nośniki magnetyczne przekazywane na zewnątrz powinny być pozbawione zapisów zawierających dane osobowe,
2. Niszczenie poprzednich zapisów powinno odbywać się poprzez wymazywanie informacji oraz formatowanie nośnika,
3. Poprawność przygotowania nośnika magnetycznego powinna być sprawdzona przez Administratora Bezpieczeństwa Informacji,
4. Uszkodzone nośniki magnetyczne przed ich wyrzuceniem należy fizycznie zniszczyć poprzez przecięcie, przełamanie itp.
5. Wydruki po wykorzystaniu należy zniszczyć w mechanicznej niszczarce do papieru.

Rozdział 11

ARCHIWIZACJA DANYCH

1. Dane systemów kopiowane są w systemie tygodniowym.
2. Kopie awaryjne danych zapisywanych w programach wykonywane są codziennie.
3. Odpowiedzialnym za wykonywanie kopii danych i kopii awaryjnych jest Administrator Bezpieczeństwa Informacji.
4. Na koniec danego miesiąca wykonywane są kopie bezpieczeństwa z całego programu przetwarzającego dane.
5. Kopie awaryjne przechowywane są w *(kasa pancerna, szafa metalowa - w wyznaczonym pomieszczeniu)*
6. Dyskietki, na których zapisywane są kopie bezpieczeństwa są każdorazowo wymazywane i formatowane, w taki sposób, by nie można było odtworzyć ich zawartości.
7. Płyty CD, DVD na których przechowuje się kopie awaryjne niszczy się w sposób mechaniczny, tak by nie można było użyć ich ponownie.
8. Administrator Bezpieczeństwa Informacji odpowiedzialny jest za dokonywanie wymiany kopii awaryjnych na aktualne.
9. Administrator Bezpieczeństwa Informacji dokonuje okresowej weryfikacji kopii bezpieczeństwa pod kątem ich przydatności,

Rozdział 12

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.
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 2002 r. Nr 101, poz. 926) 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 2002 r. Nr 101, poz. 926), 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).