WÓJT GMINY
CISNA

Zarządzenie Nr 55/2012

Wójta Gminy Cisna

z dnia 16 stycznia 2012r.

w sprawie wprowadzenia Polityki bezpieczeństwa przetwarzania danych osobowych oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Na podstawie art. 36 ust. 1 i 2 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych /Dz. U z 2002r. Nr 101 poz. 926 z późn. zm./ oraz § 3, 4 i 5 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 oraz systemy informatyczne służące do przetwarzania danych osobowych /Dz. U Nr 100 poz. 1024/

zarządzam

co następuje:

§ 1.

1. Ustala się Politykę bezpieczeństwa przetwarzania danych osobowych stanowiącą załącznik Nr 1 do niniejszego zarządzenia.
2. Ustala się Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych stanowiącą załącznik Nr 2 do niniejszego zarządzenia.

§ 2.

Kierowników komórek organizacyjnych zobowiązuje się do zapoznania pracowników z powyższymi dokumentami.

§ 3.

Traci moc Zarządzenie Nr 99 Wójta Gminy Cisna z dnia 23 września 1999r. w sprawie zabezpieczenia zbioru danych osobowych prowadzonych w Urzędzie Gminy w Cisnej.

§ 4.

Zarządzenie wchodzi w życie z dniem podjęcia.

WÓJT GMINY CISNA
mgr Renata Szczepańska

Załącznik Nr 1

Do Zarządzenia Nr 55/2012

Wójta Gminy Cisna z dnia 16.01.2012r.

Polityka bezpieczeństwa przetwarzania danych osobowych.

Rozdział I

Postanowienia ogólne.

1. Polityka bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Cisna zwana dalej „polityką" jest dokumentem, którego celem jest określenie podstawowych reguł dotyczących zapewnienia bezpieczeństwa w zakresie danych osobowych przetwarzanych w zbiorach danych:
   a. tradycyjnych, w szczególności w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych
   b. w systemach informatycznych, także w przypadku przetwarzania danych poza zbiorem danych osobowych.
2. Urząd Gminy Cisna realizując Politykę dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia, aby dane te były:
   a. przetwarzane zgodnie z prawem,
   b. zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane przetwarzaniu niezgodnemu z tymi celami,
   c. merytorycznie poprawne i adekwatne do celów, w jakich są przetwarzane,
   d. przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.
3. Urząd Gminy Cisna realizując Politykę dąży do systematycznego unowocześniania stosowanych na jego terenie informatycznych, technicznych i organizacyjnych środków ochrony tych danych w celu zabezpieczenia danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieupoważnioną, przetwarzaniem z naruszeniem przepisów o ochronie danych osobowych, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.
4. Polityka została opracowana zgodnie z ustawą z dnia 29 sierpnia 1997r. o ochronie danych osobowych /Dz. U. z 2002r. Nr 101 poz. 926 z późn. zm./ zwaną dalej "ustawą o ochronie danych osobowych" oraz rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzanych danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać systemy informatyczne służące do przetwarzania danych osobowych /Dz. U. Nr 100 poz. 1024/.

Rozdział II

Ewidencja zasobów.

1. Wyjaśnienie używanych pojęć:
   - - dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
   - - baza danych osobowych – każdy posiadający strukturę zbiór danych o charakterze osobowym, dostępny według określonych kryteriów,
   - - przetwarzanie danych – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,
   - - administrator bezpieczeństwa informacji – osoba nadzorująca przestrzeganie bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych,
   - - administrator systemu informatycznego – pracownik odpowiedzialny za funkcjonowanie systemu teleinformatycznego, oraz stosowanie technicznych i organizacyjnych środków ochrony w tym systemie,
   - - bezpieczeństwo systemu informatycznego – wdrożenie przez administratora danych osobowych lub inną osobę przez niego wyznaczoną środków organizacyjnych i technicznych w celu zabezpieczenia oraz ochrony danych osobowych przed dostępem, modyfikacją, ujawnieniem, pozyskiwaniem lub zniszczeniem,
   - - nośniki danych osobowych – dyskietki, płyty CD lub DVD, pamięć flash, dyski twarde lub inne urządzenia służące do przechowywania plików z danymi,
   - - osoba upoważniona /użytkownik/ - osoba posiadająca upoważnienie wydane przez administratora danych osobowych i dopuszczona, w zakresie wskazanym w tym upoważnieniu, do przetwarzania danych osobowych w systemie informatycznym Urzędu Gminy,
   - - personel pomocniczy – osoby mające prawo pobierać klucze do pomieszczeń – pracownicy obsługi.

2. Dane osobowe w Urzędzie Gminy przetwarzane są w systemie informatycznym funkcjonującym w budynku pod numerem 49 w Cisnej.

3. Szczegółowe zasady ochrony danych osobowych przetwarzanych w zbiorach Urzędu Gminy określa „Instrukcja zarządzania systemem informatycznym" służącym do przetwarzania danych osobowych.

Rozdział III

Opis zdarzeń naruszających ochronę danych osobowych

I. Rodzaje zagrożeń naruszających ochronę danych osobowych:
   1. zagrożenia losowe

a. zewnętrzne /np. klęski żywiołowe, przerwy w zasilaniu/ - ich wystąpienie może prowadzić do utraty integralności danych lub ich zniszczenia lub uszkodzenia infrastruktury technicznej systemu, ciągłość systemu zostaje zakłócona, jednak nie dochodzi do naruszenia poufności danych,
b. wewnętrzne /np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania/ - w wyniku ich wystąpienia może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych.

2. Zagrożenia zamierzone/świadome i celowe naruszenie poufności danych/ - w wyniku ich wystąpienia zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy, w ramach tej kategorii wyróżnia się:
   - - nieuprawniony dostęp do systemu z zewnątrz / włamanie do systemu/,
   - - nieuprawniony dostęp do systemu z jego wnętrza,
   - - nieuprawnione przekazanie danych,
   - - bezpośrednie zagrożenie materialnych składników systemu /np. kradzież sprzętu/.

II.. Okoliczności zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego , w którym przechowywane są dane osobowe, to w szczególności:

a. sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu / np. pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne/,

b. niewłaściwe parametry środowiska /np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego/,

c. awarie sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych,

d. pojawienie się odpowiedniego komunikatu alarmowego od części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,

e. pogorszenie jakości danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenie systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,

f. naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,

g. modyfikacja danych lub zmiana w strukturze danych bez odpowiedniego upoważnienia,

h. ujawnienie osobom nieuprawnionym danych osobowych lub objętych tajemnicą procedur ochrony ich przetwarzania albo innych strzeżonych elementów systemu zabezpieczeń,

i. praca w systemie informatycznym, wykazująca nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych / np. praca na komputerze osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu/,

j. podmienienie lub zniszczenie nośników z danymi osobowymi bez odpowiedniego upoważnienia lub skasowanie bądź skopiowanie w sposób niedozwolony danych osobowych,

k. rażące naruszenie obowiązków w zakresie przestrzegania procedur bezpieczeństwa informacji / niewylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce lub kserokopiarce, niezamknięcie pomieszczenia z komputerem, niewykonanie w określonym terminie kopii zapasowych, 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, znajdujących się na dyskietkach, pamięciach flash, płytach CD, DVD lub wydrukach komputerowych w formie niezabezpieczonej / otwarte szafy, biurka, regały itp./

4. Szczegółowe zasady postępowania w przypadku stwierdzenia naruszenia ochrony danych osobowych reguluje Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Rozdział IV

Środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych.

1. Formy zabezpieczeń pomieszczeń, w których przetwarzane są dane osobowe:
   - - wszystkie pomieszczenia, w których przetwarza się dane osobowe są zamykane na klucz, w przypadku opuszczenia przez ostatnią osobę upoważnioną do przetwarzania danych osobowych także w godzinach pracy,
   - - dane osobowe przechowywane w wersji tradycyjnej /papierowej/ lub elektronicznej po zakończeniu pracy są przechowywane w zamykanych na klucz meblach biurowych, a tam gdzie to jest możliwe w szafach metalowych lub pancernych. Klucze od szafek należy zabezpieczyć przed dostępem osób nieupoważnionych do przetwarzania danych osobowych,
   - - nieaktualne lub błędne wydruki zawierające dane osobowe niszczone są w niszczarkach.

2. Formy zabezpieczeń przed nieautoryzowanym dostępem do baz danych Urzędu Gminy:

- - podłączenie urządzenia końcowego / komputera, terminala, drukarki/ do sieci komputerowej dokonywane jest przez administratora systemu informatycznego,
- - udostępnianie użytkownikowi zasobów sieci zawierających dane osobowe /programów i baz danych/ przez administratora systemu informatycznego następuje na podstawie upoważnienia do przetwarzania danych osobowych,
- - identyfikacja użytkownika w systemie poprzez zastosowanie uwierzytelnienia,
- - udostępnianie kluczy i uprawnień do wejścia do pomieszczeń, gdzie przetwarzane są dane osobowe tylko pracownikom do tego upoważnionym,
- - stosowanie programu antywirusowego z zaporą antywłamaniową na komputerach ze środowiskiem MS Windows,
- - zabezpieczenie hasłami kont na komputerach,
- - ustawienie monitorów stanowisk przetwarzania danych osobowych w sposób uniemożliwiania wgląd w dane osobom upoważnionym.

3. Formy zabezpieczeń przed nieautoryzowanym dostępem do baz danych Urzędu Gminy poprzez Internet:

a. logiczne oddzielenie sieci wewnętrznej LAN od sieci zewnętrznej, uniemożliwiające uzyskanie połączenia z bazą danych spoza sytemu informatycznego, jak również uzyskanie dostępu do sieci rozległej Internet,

b. zastosowanie dwóch poziomów zabezpieczenia sieci:

- - pierwszy poziom ochrony stanowi lokalna brama sieciowa z zainstalowanym systemem typu firewall – z funkcją analizy charakteru ruchu sieciowego – uniemożliwiającym nawiązanie połączenia z chronionymi komputerami oraz blokującym ruch o charakterze niepożądanym lub takim, który może zostać uznany za szkodliwy,
- - drugi poziom zabezpieczeń stanowią listy dostępu na głównym routerze uniemożliwiające nawiązanie połączenia z jakimkolwiek niewskazanym jawnie komputerem w sieci.

4. Formy zabezpieczeń przed utratą danych osobowych w wyniku awarii:

- - odrębne zasilanie sprzętu komputerowego,
- - ochrona serwerów przed zanikaniem zasilania poprzez stosowanie zasilaczy zapasowych UPS,
- - ochrona przed utratą zgromadzonych danych osobowych poprzez cykliczne wykonywanie kopii zapasowych, z których w przypadku awarii odtwarzane są dane i system operacyjny,

- - zastosowanie ochrony przeciwpożarowej poprzez umieszczenie gaśnic oraz czujników dymu.

5, Organizacyjną ochronę danych i ich przetwarzania realizuje się przez:

- - zapoznanie każdej osoby z przepisami dotyczącymi ochrony danych osobowych przed dopuszczeniem jej do pracy przy ich przetwarzaniu,
- - przeszkolenie osób w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochrona danych oraz form zabezpieczeń pomieszczeń i budynku,
- - kontrolowanie pomieszczeń budynku,
- - prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,
- - wyznaczenie administratora bezpieczeństwa informacji.

Rozdział V

Postanowienia końcowe.

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu, w szczególności przez osobę, która wobec naruszenia ochrony danych osobowych lub uzasadnionego domniemania takiego naruszenia, nie podjęła działań określonych w niniejszym dokumencie, mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych.
2. Wobec osoby uchylającej się od powiadomienia administratora bezpieczeństwa informacji o wystąpieniu naruszenia lub zagrożenia bezpieczeństwa systemu informatycznego stosuje się karę dyscyplinarną.
3. Zastosowanie kary dyscyplinarnej, o której mowa w ust. 2, nie wyklucza odpowiedzialności karnej ani cywilnej.
4. W sprawach nie uregulowanych niniejszym dokumentem mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych /Dz. U. z 2002r. Nr 101 poz.926 / . rozporządzenie 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. Nr 100 poz. 1024/ oraz rozporządzenie Ministra Sprawiedliwości z dnia 28 kwietnia 2004r. 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/.

Załącznik Nr 2

do Zarządzenia Nr 55/2012

Wójta Gminy Cisna

z dnia 16.01.2012r.

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Rozdział I

Postanowienia ogólne.

1. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwana dalej „instrukcją", określa procedury dotyczące zasad bezpieczeństwa przetwarzania danych osobowych oraz zasady postępowania administratora danych osobowych, osób wyznaczonych przez niego i użytkowników przetwarzających dane osobowe w Urzędzie Gminy Cisna, zwanym dalej „Urzędem Gminy".
2 Instrukcja została opracowana zgodnie z ustawą z dnia 29 sierpnia 1997r. o ochronie danych osobowych /Dz. U. z 2002r. Nr 101 poz. 926 z późn. zm./ zwaną dalej "ustawą o ochronie danych osobowych" oraz rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzanych danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać systemy informatyczne służące do przetwarzania danych osobowych /Dz. U. Nr 100 poz. 1024/.
3 Wójt Gminy Cisna wykonuje obowiązki administratora danych osobowych i administratora systemów informatycznych z funkcję administratora bezpieczeństwa informacji sprawuje referent ds. informatyki w odniesieniu do prowadzonych w Urzędzie Gminy zbiorów danych.
4 W systemach informatycznych służących do przetwarzania danych osobowych w Urzędzie Gminy stosuje się środki bezpieczeństwa na poziomie wysokim.

Rozdział II

Nadanie uprawnień do przetwarzania danych osobowych oraz ich rejestrowanie w systemie informatycznym.

1. Przed przystąpieniem do pracy przy przetwarzaniu danych osobowych, każdy użytkownik powinien zostać zapoznany przez administratora bezpieczeństwa informacji z przepisami dotyczącymi ochrony danych osobowych oraz obowiązującymi w Urzędzie Gminy wewnętrznymi regulacjami w tym zakresie.

2. Do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służący do przewarzania danych osobowych, mogą zostać dopuszczone wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych wydane przez administratora danych osobowych. Oryginał upoważnienia zostaje przekazany użytkownikowi za potwierdzeniem odbioru, kopia zostaje włączona do akt osobowych użytkownika.
3. Przyznanie uprawnień do przetwarzania danych osobowych w systemie informatycznym polega na wprowadzeniu do systemu dla każdego użytkownika identyfikatora, hasła oraz ustanowienia zakresu dostępnych danych i operacji.
4. Za wygenerowanie identyfikatora i hasła użytkownika odpowiada administrator bezpieczeństwa informacji.
5. Przełożeni użytkowników zobowiązani są pisemnie poinformować administratora danych osobowych o każdej zmianie dotyczącej użytkowników mającej wpływ na zakres posiadanych uprawnień do przetwarzania danych osobowych.
6. Administrator bezpieczeństwa informacji jest zobowiązany do prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych.

Rozdział III

Stosowane metody i środki uwierzytelniania użytkownika oraz procedury związane z ich zarządzaniem i użytkowanie.

1. Użytkownik uzyskuje dostęp do danych osobowych p[przetwarzanych w systemie informatycznym wyłącznie po podaniu identyfikatora i hasła.
2. Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi. Użytkownik jest odpowiedzialny za wszystkie czynności wykonywane przy użyciu swojego identyfikatora.
3. Użytkownik otrzymuje hasło początkowe z chwilą przystąpienia do pracy w systemie informatycznym i jest zobowiązany zmienić je natychmiast po rozpoczęciu pracy na sobie tylko znany ciąg znaków.
4. Hasło składa się co najmniej z 6 znaków.
5. Hasło powinno zawierać małe i wielkie litery oraz cyfry.
6. Hasło nie może być zapisane w miejscu dostępnym dla osób nieuprawnionych i należy je zachować w tajemnicy, również po upływie jego ważności.
7. Użytkownik nie może udostępniać osobom nieuprawnionym swojego identyfikatora oraz hasła. Po uwierzytelnieniu w systemie użytkownik nie może udostępniać osobom nieuprawnionym swojego stanowiska pracy.
8. W przypadku, gdy istnieje podejrzenie, że hasło mogła poznać osoba nieuprawniona, użytkownik zobowiązany jest niezwłocznie zmienić hasło oraz powiadomić o tym fakcie administratora bezpieczeństwa informacji.

Rozdział IV

Rozpoczęcie, zawieszenie i zakończenie pracy przez użytkowników systemu.

1. Użytkownik rozpoczynając pracę na komputerze loguje się do sytemu informatycznego.
2. Dostęp do danych osobowych możliwy jest jedynie po dokonaniu uwierzytelnienia użytkownika.
3. W sytuacji opuszczenia stanowiska pracy przez użytkownika na odległość uniemożliwiającą jego obserwacje należy wylogować się z systemu.
4. Monitory stanowisk komputerowych, na których przetwarzane są dane osobowe, znajdujące się w pomieszczeniach, gdzie przebywają osoby nieposiadające uprawnień do przetwarzania danych osobowych, należy ustawić tak, aby uniemożliwić osobom nieupoważnionym wgląd w dane.
5. Przebywanie osób nieuprawnionych w pomieszczeniach znajdujących się na obszarze, w którym przetwarzane są dane osobowe, jest dopuszczalne tylko w obecności osoby upoważnionej do ich przetwarzania.
6. Pomieszczenia, w których przetwarzane są dane osobowe, należy zamykać na czas nieobecności osób upoważnionych, w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym.
7. Przed opuszczeniem stanowiska pracy użytkownik obowiązany jest:
   a. wylogować się z systemu informatycznego albo
   b. wywołać wygaszacz ekranu.
8. Kończąc pracę użytkownik zobowiązany jest:
   a. wylogować się z systemu informatycznego a następnie wyłączyć sprzęt komputerowy,
   b. zabezpieczyć stanowisko pracy.

Wszelką dokumentację oraz nośniki magnetyczne i optyczne, na których znajdują się dane osobowe, przechowuje się w szafkach zamykanych na klucz.

Rozdział V

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

1. Dane osobowe przetwarzane w systemie informatycznym podlegają zabezpieczeniu poprzez tworzenie kopii zapasowych.
2. Za tworzenie kopii zapasowych zbiorów danych osobowych odpowiedzialny jest administrator systemu informatycznego.
3. W przypadku lokalnego przetwarzania danych osobowych na komputerach służbowych użytkownicy systemu informatycznego obowiązani są do wykonywania kopii zapasowych zbiorów danych raz w tygodniu.

4. Kopie zapasowe zbiorów danych są tworzone co najmniej dwa razy w roku. W szczególnych przypadkach – przed aktualizacją lub zmiana w systemie.
5. Kopie zapasowe zbiorów danych należy okresowo sprawdzić pod kątem ich przydatności do odtwarzania w przypadku awarii systemu informatycznego. Za przeprowadzanie tej procedury odpowiedzialny jest administrator sytemu informatycznego.
6. Kopie zapasowe przechowywane są w szafkach zamykanych na klucz.

Rozdział VI

Sposób, miejsce i okres przechowywania wydruków, elektronicznych nośników danych zawierających dane osobowe oraz kopii zapasowych.

1. Użytkownicy nie mogą wynosić z budynku Urzędu Gminy wydruków, nośników danych z zapisanymi danymi osobowymi bez zgody administratora bezpieczeństwa informacji.
2. Wydruki archiwalne lub bieżące przechowywane mogą być wyłącznie w pomieszczeniach uniemożliwiających dostęp do nich osób nieupoważnionych.
3. Kopie zapasowe na nośnikach optycznych i magnetycznych przechowywane są w szafkach zamykanych na klucze, do których dostęp ma wyłącznie administrator bezpieczeństwa informacji.
4. Za bezpieczeństwo danych zapisanych w komputerach przenośnych oraz w innych urządzeniach przenośnych w całości odpowiada użytkownik komputera lub urządzenia przenośnego.
5. Zbędne wydruki zawierające dane osobowe natychmiast po wykorzystaniu muszą zostać zniszczone w niszczarce dokumentów.
6. Przeznaczone do likwidacji elektroniczne i optyczne nośniki informacji, mogące zawierać dane osobowe, pozbawia się w sposób trwały zapisu tych danych, a w przypadku, gdy nie jest to możliwe, niszczy lub uszkadza w sposób trwale uniemożliwiający ich odczytanie.
7. Kopie zapasowe usuwa się niezwłocznie w wypadku ich uszkodzenia lub po upłynięciu terminu przechowywania w sposób trwale uniemożliwiający ich odczytanie.
8. Za zniszczenie zbędnych wydruków i innych zbędnych dokumentów zawierających dane osobowe odpowiedzialny jest kierownik komórki organizacyjnej.
9. Za zniszczenie kopii zapasowych sporządzanych indywidualnie przez użytkownika odpowiada użytkownik.
10. Za skasowanie zbędnych danych lub zniszczenie zbędnych nośników elektronicznych odpowiedzialny jest administrator systemu informatycznego.
11. Kopie zapasowe przechowuje się przez okres dwunastu miesięcy po okresie sporządzenia kopii, dopuszcza się dłuższy okres przechowywania, o ile pozwalają na to warunki.

Rozdział VII

Sposób zabezpieczenia systemu informatycznego przed działaniem oprogramowania, którego celem jest uzyskanie dostępu do systemu informatycznego.

1. Za ochronę antywirusową systemu informatycznego odpowiada administrator systemu informatycznego.
2. System antywirusowy zainstalowany jest w każdym komputerze z dostępem do danych osobowych, za jego wdrożenie odpowiada administrator bezpieczeństwa informacji.
3. Program antywirusowy jest uaktywniony przez cały czas pracy każdego komputera w systemie informatycznym.
4. Wszystkie pliki otrzymane z zewnątrz, jak również wysyłane na zewnątrz, podlegają automatycznemu sprawdzeniu przez system antywirusowy pod kątem występowania zagrożenia wirusowego, z zastosowaniem najnowszej wersji programu antywirusowego.
5. W przypadku pojawienia się wirusa, użytkownik obowiązany jest zaprzestać wykonywania jakichkolwiek czynności w systemie i niezwłocznie powiadomić administratora bezpieczeństwa informacji.
6. Niedozwolone jest otwieranie wiadomości poczty elektronicznej i załączników od nieznanych nadawców.
7. Niedozwolone jest wyłączanie, blokowanie i odinstalowywanie programów zabezpieczających przed oprogramowaniem złośliwym oraz nieautoryzowanym.
8. Administrator bezpieczeństwa informacji jest odpowiedzialny za aktywowanie i poprawne konfigurowanie specjalistycznego oprogramowania monitorującego wymianę danych na styku:
   a. sieci lokalnej,
   b. stanowiska komputerowego użytkownika systemu i pozostałych urządzeń wchodzących w skład sieci lokalnej.

Rozdział VIII

Udostępnianie danych osobowych i sposób odnotowywania informacji o udostępnianiu danych.

1. Dane osobowe przetwarzane w Urzędzie Gminy mogą być udostępnione podmiotom lub osobom uprawnionym do ich otrzymania na mocy ustawy o ochronie danych osobowych oraz innych przepisów powszechnie obowiązujących.
2. Dane osobowe udostępnia się na pisemny, umotywowany wniosek, chyba że przepisy odrębne stanowią inaczej.
3. Dane udostępnione Urzędowi Gminy przez inny podmiot można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

4. Dokładna kopia danych osobowych przesyłanych do ZUS przechowywana jest w bazie danych programu Płatnik w postaci dokumentów i zestawów dokumentów oznaczonych odpowiednim statusem dokumentu lub zestawu, datą utworzenia, datą wysłania.

Rozdział IX

Wykonywanie przeglądów i konserwacji sytemu oraz nośników danych służących do przetwarzania danych.

1. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe wykonywane są przez administratora bezpieczeństwa informacji.
2. Administrator systemu informatycznego okresowo sprawdza możliwość odtwarzania danych z kopii zapasowych.
3. Aktualizacja oprogramowania powinna być przeprowadzana zgodnie z zaleceniami producentów oraz opinią rynkową co do bezpieczeństwa i stabilności nowych wersji.
4. Za terminowość przeprowadzania przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada administrator bezpieczeństwa informacji.
5. Nieprawidłowości w działaniu systemu informatycznego oraz oprogramowania są niezwłocznie usuwane przez administratora bezpieczeństwa informacji a ich przyczyny analizowane.
6. Zmiana konfiguracji sprzętu komputerowego, na którym znajdują się dane osobowe lub zmiana jego lokalizacji, może być dokonana tylko za wiedzą i zgodą administratora bezpieczeństwa informacji.

Rozdział X

Postępowanie w przypadku naruszenia ochrony danych osobowych.

1. Każdy użytkownik, który stwierdzi lub podejrzewa naruszenie ochrony danych osobowych w systemie informatycznym, zobowiązany jest niezwłocznie poinformować o tym administratora bezpieczeństwa informacji.
2. Do czasu przybycia administratora bezpieczeństwa informacji na miejsce naruszenia lub ujawnienia naruszenia ochrony danych osobowych należy:
   a. niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców naruszenia,
   b. rozważyć wstrzymanie bieżącej pracy na komputerze w celu zabezpieczenia miejsca zdarzenia,
   c. zaniechać, o ile to możliwe, dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić jego udokumentowanie i analizę,
   d. udokumentować wstępnie zaistniałe naruszenie,

e. nie opuszczać, bez uzasadnionej potrzeby, miejsca zdarzenia do czasu przybycia administratora bezpieczeństwa informacji.

3. Po przybyciu na miejsce naruszenia lub ujawnienia naruszenia danych osobowych, administrator bezpieczeństwa informacji we współpracy z administratorem systemu informatycznego:
   a. zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania, mając na uwadze ewentualne zagrożenia dla prawidłowości pracy Urzędu Gminy,
   b. może żądać wyjaśnień dotyczących zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać In formacje związane z zaistniałym naruszeniem,
   c. dokonuje zabezpieczenia systemu informatycznego przed dalszym rozprzestrzenianiem się skutków naruszenia,
   d. podejmuje odpowiednie kroki w celu powstrzymania lub ograniczenia dostępu osoby niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów naruszenia.
4. Po wyczerpaniu niezbędnych środków doraźnych, administrator bezpieczeństwa informacji we współpracy z administratorem systemu informatycznego zasięga niezbędnych opinii i proponuje działania mające na celu usunięcie naruszenia i jego skutków.
5. Administrator bezpieczeństwa informacji dokumentuje zaistniały przypadek naruszenia oraz sporządza raport, który zawiera w szczególności:
   a. wskazanie osoby powiadamiającej o naruszeniu oraz innych osób, które złożyły wyjaśnienia w związku z naruszeniem,
   b. określenie czasu i miejsca naruszenia oraz powiadomienia o naruszeniu,
   c. określenie okoliczności towarzyszących i rodzaju naruszenia,
   d. wyszczególnienie uwzględnionych przesłanek wyboru metody postępowania i opis podjętego działania,
   e. wstępną ocenę przyczyn wystąpienia naruszenia,
   f. ocenę przeprowadzonego postępowania wyjaśniającego i działań podjętych w celu usunięcia naruszenia i jego skutków.
6. Po przywróceniu prawidłowego funkcjonowania systemu informatycznego, administrator bezpieczeństwa informacji we współpracy z administratorem systemu informatycznego przeprowadza szczegółową analizę w celu okreslenia przyczyn naruszenia ochrony danych osobowych lub podejrzenia takiego naruszenia oraz podejmuje kroku mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.