Zarządzenie Nr 178/2011
Wójta Gminy Zagnańsk
z dnia 02 grudnia 2011r.

w sprawie zasad ochrony danych osobowych przetwarzanych w Urzędzie Gminy Zagnańsk

Na podstawie art. 33 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U. z 2001r., nr 142, poz. 1591 t. j. z późn. zm.), art. 36 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U z 2002 r., nr 101, poz. 926 t. j. z późn. zm.),§ 3 ust.1 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, w jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U.Nr 100, poz. 1024) zarządza się co następuje:

§ 1

Wprowadza się zasady ochrony danych osobowych przetwarzanych w Urzędzie Gminy Zagnańsk obejmujące:

1) Politykę bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Zagnańsk – stanowiącą załącznik Nr 1 do zarządzenia;
2) Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych – stanowiącą załącznik nr 2 do zarządzenia.

§ 2

Zobowiązuje się pracowników Urzędu Gminy do stosowania zasad określonych w „Polityce" i „Instrukcji"

§ 3

Wykonanie zarządzenia powierza się Administratorowi Bezpieczeństwa Informacji.

§ 4

Traci moc Zarządzenie nr 1/99 Wójta Gminy Zagnańsk z dnia 20 sierpnia 1999 r. w sprawie wykonania ustawy o ochronie danych osobowych w Urzędzie Gminy.

§ 6

Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT GMINY
Szczepan Skorupski

Przygotował:
L. Niciejewski

Załącznik Nr 1
do Zarządzenia Nr 178/2011
Wójta Gminy Zagnańsk
z dnia 02 grudnia 2011r.

Polityka bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy Zagnańsk

Rozdział 1

Postanowienia ogólne

1. Polityka bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy Zagnańsk, zwana dalej „Polityką", jest dokumentem, którego celem jest określenie podstawowych reguł dotyczących zapewnienia bezpieczeństwa w zakresie danych osobowych przetwarzanych w zbiorach danych:
   1) tradycyjnych, w szczególności w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych;
   2) w systemach informatycznych, także w przypadku przetwarzania danych poza zbiorem danych osobowych.
2. Urząd Gminy w Zagnańsku, zwany dalej „Urzędem", realizując Politykę dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia, aby dane te były:
   1) przetwarzane zgodnie z prawem;
   2) zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane przetwarzaniu niezgodnemu z tymi celami;
   3) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane;
   4) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.
3. Urząd 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 nieuprawnioną, 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 2002 r. 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 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).

Rozdział 2

Ewidencja zasobów

1. Wyjaśnienia używanych pojęć:
   1) administrator bezpieczeństwa informacji – osoba wyznaczona przez administratora danych, nadzorująca przestrzeganie bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych;

2) administrator baz danych – osoba odpowiedzialna za sprawne działanie baz danych zawierających zbiory danych osobowych oraz zarządzająca uprawnieniami użytkowników do tych baz w Urzędzie ;
3) administrator sieci – osoba odpowiedzialna za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych, służących do przetwarzania danych osobowych w Urzędzie;
4) 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;
5) nośniki danych osobowych – dyskietki, płyty CD lub DVD, pamięć flash, dyski twarde, taśmy magnetyczne lub inne urządzenia/materiały służące do przechowywania plików z danymi;
6) osoba upoważniona (użytkownik) – osoba posiadająca upoważnienie wydane przez administratora danych osobowych lub osobę przez niego wyznaczoną i dopuszczona, w zakresie wskazanym w tym upoważnieniu do przetwarzania danych osobowych w systemie informatycznym danej komórki organizacyjnej Urzędu;
7) personel pomocniczy – osoby wykonujące prace w zakresie utrzymania czystości oraz wykonujące naprawy urządzeń technicznych w określonych pomieszczeniach (strefach);
8) strefy – pomieszczenia, w których są przetwarzane dane osobowe w sposób określony w art. 7 pkt 2 ustawy o ochronie danych osobowych.

2. Dane osobowe w Urzędzie przetwarzane są w systemie tradycyjnym (papierowym) i informatycznym funkcjonującym w budynku przy ul. Spacerowej 8.

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

4. Polityka zawiera:
1) wykaz zbiorów danych osobowych przetwarzanych w Urzędzie wraz z opisem struktury zbiorów danych wskazującym zawartość poszczególnych pól informacyjnych, ze wskazaniem programów stosowanych do przetwarzania tych danych, stanowiący załącznik nr 1 do Polityki;
2) wykaz pomieszczeń tworzących obszary, w których przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego, stanowiący załącznik nr 2 do Polityki;
3) wykaz osób odpowiedzialnych za stosowanie poszczególnych środków zabezpieczeń, stanowiący załącznik nr 3 do Polityki.

Rozdział 3

Opis zdarzeń naruszających ochronę danych osobowych

1. 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 systemu, może nastąpić naruszenie poufności danych;

2) zagrożenia zamierzone (świadome i celowe naruszenia poufności danych) – w wyniku ich wystąpienia zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy; w ramach tej kategorii zagrożeń 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).

2. Okoliczności zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe, to w szczególności:
   1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu (np. wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej);
   2) niewłaściwe parametry środowiska (np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych);
   3) awarie sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych;
   4) pojawienie się odpowiedniego komunikatu alarmowego od części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu;
   5) pogorszenie jakości danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie;
   6) naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie;
   7) modyfikacja danych lub zmiana w strukturze danych bez odpowiedniego upoważnienia;
   8) ujawnienie osobom nieuprawnionym danych osobowych lub objętych tajemnicą procedur ochrony ich przetwarzania albo innych strzeżonych elementów systemu zabezpieczeń;
   9) praca w systemie informatycznym, wskazująca nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych (np. praca przy komputerze osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu);
   10) podmienienie albo zniszczenie nośników z danymi osobowymi bez odpowiedniego upoważnienia lub skasowanie bądź skopiowanie w sposób niedozwolony danych osobowych;
   11) rażące naruszenie obowiązków w zakresie przestrzegania procedur bezpieczeństwa informacji (niewylogowania 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 dyskach, dyskietkach, pamięciach flash, płytach CD, DVD, taśmach magnetycznych, kartach pamięci oraz wydrukach komputerowych w formie niezabezpieczonej (otwarte szafy, biurka, regały, urządzenia archiwalne i inne).

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

Rozdział 4

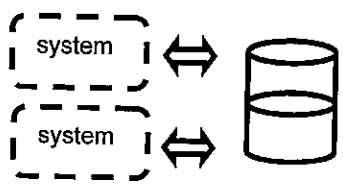
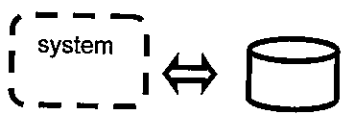
Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych

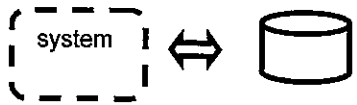
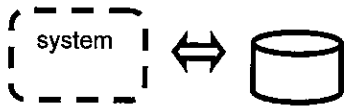
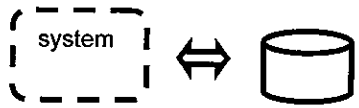
1. Formy zabezpieczeń pomieszczeń, w których przetwarzane są dane osobowe:
   1) wszystkie pomieszczenia, w których przetwarza się dane osobowe są zamykane na klucz, a w przypadku opuszczenia pomieszczenia przez ostatnią osobę upoważnioną do przetwarzania danych osobowych – także w godzinach pracy;
   2) dane osobowe przechowywane w wersji tradycyjnej (papierowej) lub elektronicznej (pamięć flash, płyta CD, DVD, dyskietka) po zakończeniu pracy są przechowywane w zamykanych na klucz meblach biurowych, a tam, gdzie jest możliwe – w szafach metqlowych lub pancernych; klucze od szafek należy zabezpieczyć przed dostępem osób nieupoważnionych do przetwarzania danych osobowych;
   3) nieaktualne lub błędne wydruki zawierające dane osobowe niszczone są w niszczarkach;
   4) siedziba Urzędu, w której zlokalizowane są zbiory danych osobowych jest nadzorowana przez system alarmowy po godzinach pracy;
2. Formy zabezpieczeń przed nieautoryzowanym dostępem do baz danych Urzędu:
   1) podłączenie urządzenia końcowego (komputera, terminala, drukarki) do sieci komputerowej Urzędu dokonywane jest przez administratora sieci lub upoważnionego pracownika Referatu Organizacyjnego;
   2) udostępnianie użytkownikowi zasobów sieci zawierających dane osobowe (programów i baz danych) przez administratora sieci oraz administratora bazy następuje na podstawie upoważnienia do przetwarzania danych osobowych;
   3) identyfikacja użytkownika w systemie poprzez zastosowanie uwierzytelnienia;
   4) przydzielenie indywidualnego identyfikatora każdemu użytkownikowi systemu informatycznego i rejestrowanie przez system czasu logowania użytkownika i rodzaju wprowadzonych przez niego danych;
   5) udostępnianie kluczy i uprawnień do wejścia do centrum przetwarzania danych (serwerowni) tylko pracownikom do tego upoważnionym;
   6) stosowanie programu antywirusowego z zaporą włamaniową na komputerach ze środowiskiem operacyjnym MS Windows;
   7) zabezpieczenie hasłami kont na komputerach oraz używanie kont z ograniczonymi uprawnieniami do ciągłej pracy;
   8) ustawienie monitorów stanowisk przetwarzania danych osobowych w sposób uniemożliwiający wgląd w dane osobom nieupoważnionym;
   9) automatyczne wygaszanie ekranu i blokowanie nieużywanego komputera po upływie określonego czasu;
   10) wymuszenie zmiany hasła do systemu informatycznego co 30 dni.
3. Formy zabezpieczeń przed nieautoryzowanym dostępem do baz danych Urzędu poprzez Internet:
   1) logiczne oddzielenie sieci wewnętrznej LAN od sieci zewnętrznej, uniemożliwiające uzyskanie połączenia z bazą danych spoza systemu informatycznego, jak również uzyskanie dostępu z systemu do sieci rozległej Internet;
   2) zastosowanie dwóch poziomów zabezpieczeń sieci:
      a) 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 blokującymi ruch o charakterze niepożądanym lub takim, który może zostać uznany za szkodliwy,
      b) drugi poziom zabezpieczeń stanowią listy dostępu do serwerów baz danych z określonych adresów i puli adresowej.

4. Formy zabezpieczeń przed utratą danych osobowych w wyniku awarii:
   1) ochrona serwerów przed zanikiem zasilania poprzez stosowanie zasilaczy zapasowych UPS;
   2) ochrona przed utratą zgromadzonych danych poprzez cykliczne wykonywanie kopii zapasowych, z których, w przypadku awarii, odtwarzane są dane i system operacyjny;
   3) ochrona przed awarią podsystemu dyskowego poprzez używanie macierzy dyskowych;
   4) zapewnienie właściwej temperatury i wilgotności powietrza dla pracy sprzętu komputerowego w serwerowni;
   5) zastosowanie ochrony przeciwpożarowej poprzez umieszczenie w serwerowni gaśnic, okresowo kontrolowanych przez specjalistę;
   6) zwiększenie niezawodności serwerów i urządzeń sieciowych poprzez logiczne rozmieszczenie ich w szafach.
5. Organizacyjną ochronę danych i ich przetwarzania realizuje się poprzez:
   1) zapoznanie każdej osoby z przepisami dotyczącymi ochrony danych osobowych, przed dopuszczeniem jej do pracy przy ich przetwarzaniu;
   2) przeszkolenie osób w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochroną danych osobowych oraz form zabezpieczenia pomieszczeń i budynku;
   3) kontrolowanie pomieszczeń i budynku;
   4) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;
   5) wyznaczenie administratora bezpieczeństwa informacji.

Załącznik nr 1
do Polityka bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy Zagnańsk

Wykaz zbiorów danych osobowych przetwarzanych w Urzędzie wraz z opisem struktury zbiorów danych wskazującym zawartość poszczególnych pól informacyjnych, ze wskazaniem programów zastosowanych do przetwarzania tych danych

Lp	Nazwa zbioru danych	Zakres przetwarzanych danych	Przepływ danych	System/Program
1	2	3	4	5
1	Skargi i wnioski obywateli	Imię i nazwisko, adres zamieszkania lub pobytu, nr telefonu	Nie dotyczy	Wersja papierowa
2	Stypendia szkolne	Imię i nazwisko, adres zamieszkania lub pobytu, nr telefonu, stan rodzinny		Dokument w MS Excel „stypendia szkolne rok...xls"
3	Zbiór danych kadrowych pracowników Urzędu (akta osobowe) Program Zbiór danych kadrowych pracowników Urzędu (akta osobowe) Program kadrowo - płacowy	Imię i Nazwisko, imiona rodziców, nazwisko rodowe,data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, PESEL, NIP, zawód wykonywany, obowiązek wojskowy, wykształcenie, stanowisko, historia pracy, kary, nagrody, seria i nr dowodu osobistego, nr telefonu, nr konta bankowego, historia pracy, termin badań okresowych, adres urzędu skarbowego, nieobecności w pracy, posiadana rodzina, ubezpieczenia ZUS,	Nie dotyczy 	Wersja papierowa Kadry/płace „Optivum" „Płatnik"
4	Ewidencja ludności i dowody osobiste	Imię i Nazwisko, imiona rodziców, nazwisko rodowe, dane o urodzeniu, adres zamieszkania lub pobytu, PESEL, płeć, stan cywilny, rysopis, dokument tożsamości, obywatelstwo, uprawnienia wyborcze, status mieszkańca	Nie dotyczy 	Wersja papierowa „Mikropesel"

6	Urząd Stanu Cywilnego	Akta urodzenia, akta małżeństwa, akta zgonu – dane wynikające z przepisów prawa w tym zakresie	Nie dotyczy 	Wersja papierowa
7	Ewidencja osobowa: Rady Gminy, Sołtysów, Przewodniczących Rad Sołeckich	Imię i Nazwisko, adres zamieszkania, nr telefonu	Nie dotyczy 	Wersja papierowa Dokument w MS Excel „Rada Gminy rok...xls" „Sołtysi rok...xxls" „Przewodniczący rady sołeckiej rok...xls"
8	Ewidencja działalności gospodarczej	Imię i Nazwisko, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, PESEL, NIP, adres urzędu skarbowego,	Nie dotyczy 	Wersja papierowa
9	Podatki i opłaty Gminne	Imię i Nazwisko, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, PESEL, NIP, adres urzędu skarbowego,	Nie dotyczy 	Wersja papierowa Podatki i opłaty gminne -wersja: 1.52f
10	Ewidencja gospodarowania odpadami stałymi i ciekłymi	Imię i Nazwisko, adres zamieszkania, PESEL	Nie dotyczy 	Wersja papierowa Dokument w MS Excel „Odpady stałe i ciekłe"
11	Oświadczenia o stanie majątkowym osób zobowiązanych do ich składania	Imię i Nazwisko, data urodzenia, miejsce zamieszkania, pełnione funkcje, posiadany majątek i uzyskiwane dochody, członkowstwo w spółkach itp,	Nie dotyczy	Wersja papierowa
12	Ewidencja osób, którym udzielono zezwolenia na wycinkę drzew	Imię i nazwisko, adres, nr działki	Nie dotyczy	Wersja papierowa

13	Ewidencja osób, którym wydano zawiadomienia o nadaniu numeru porządkowego nieruchomości	Imię i Nazwisko, adres, nr nieruchomości	Nie dotyczy	Wersja papierowa
14	Wypis i wyrys z planu zagospodarowania terenu	Imię i Nazwisko, adres, nr ewidencyjny działki	Nie dotyczy	Wersja papierowa
15	Rejestr gruntów: dzierżawy, najmu, użytkowania, nabytych, sprzedanych	Imię i Nazwisko, adres, nr działki, daty ważności umów	Nie dotyczy	Wersja papierowa
16	Rejestr umów najmu lokali	Imię i Nazwisko, adres lokalu, nr działki rodzaj umowy, daty ważności umów	Nie dotyczy	Wersja papierowa
17	Rejestr akcyzy	Imię i nazwisko, adres, PESEL, dowód tożsamości, posiadane użytki rolne	Nie dotyczy	Wersja papierowa
18	Rejestr przedpoborowych	Imię i nazwisko, data urodzenia, adres zameldowania i pobytu, dane dokumentu tożsamości,	Nie dotyczy	Wersja papierowa
19	Wykaz poborowych	Imię i nazwisko, data urodzenia, adres zameldowania i pobytu, dane dokumentu tożsamości, kategoria przydatności do służby wojskowej, nr książeczki wojskowej	Nie dotyczy	Wersja papierowa

Załącznik nr 2
do Polityka bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy Zagnańsk

Wykaz pomieszczeń tworzących obszary, w których przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego

Lp	Nazwa zbioru danych	Referat	Lokalizacja bazy
1	2	3	4
1	Skargi i wnioski obywateli	Organizacyjny i Spraw Obywatelskich	Pokój nr 5
2	Stypendia szkolne	Organizacyjny i Spraw Obywatelskich	Pokój nr 5 i 9
3	Zbiór danych kadrowych pracowników Urzędu (akta osobowe).Program kadrowy	Organizacyjny i Spraw Obywatelskich	Pokój nr 1
4	Zbiór danych kadrowych pracowników Urzędu (akta osobowe).Program płacowy	Finanse	Pokój 28B
5	Ewidencja ludności i dowody osobiste	Organizacyjny i Spraw Obywatelskich	Pokój nr 6
6	Urząd stanu Cywilnego	Urząd Stanu Cywilnego	Pokój nr 6 i 7
7	Ewidencja osobowa: Rady Gminy, Sołtysów, Przewodniczących Rad Sołeckich	Organizacyjny i Spraw Obywatelskich	Pokój nr 1
8	Ewidencja działalności gospodarczej	Organizacyjny i Spraw Obywatelskich	Pokój nr 19 i Holl na parterze obsługi klienta
9	Podatki i opłaty Gminne	Finanse	Pokój nr 11, 12, 27, 28A-C
10	Ewidencja gospodarowania odpadami stałymi i ciekłymi	Gospodarczy i Gospodarki Komunalnej	Pokój nr 13, 23
11	Oświadczenia o stanie majątkowym osób zobowiązanych do ich składania	Organizacyjny i Spraw Obywatelskich	Pokój nr 1
12	Ewidencja osób, którym udzielono zezwolenia na wycinkę drzew	Nieruchomości, Planowania Przestrzennego, Ochrony Środowiska i Rolnictwa	Pokój nr 10
13	Ewidencja osób, którym wydano zawiadomienia o nadaniu numeru porządkowego nieruchomości	Nieruchomości, Planowania Przestrzennego, Ochrony Środowiska i Rolnictwa	Pokój nr 10

14	Wypis i wyrys z planu zagospodarowania terenu	Nieruchomości, Planowania Przestrzennego, Ochrony Środowiska i Rolnictwa	Pokój nr 22
15	Rejestr gruntów; dzierżawy, najmu, użytkowania, nabytych, sprzedanych	Nieruchomości, Planowania Przestrzennego, Ochrony Środowiska i Rolnictwa	Pokój nr 21
16	Rejestr umów najmu lokali	Gospodarczy i Gospodarki Komunalnej	Pokój nr 23
17	Rejestr akcyzy	Finansowy	Pokój nr 27
18	Rejestr przedpoborowych	Organizacyjny i Spraw Obywatelskich	Pokój nr 9
19	Rejestr poborowych	Organizacyjny i Spraw Obywatelskich	Pokój nr 9

Załącznik nr 3
do Polityka bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy Zagnańsk

Lp	Forma zabezpieczenia	Osoba odpowiedzialna za zabezpieczenie
1	2	3
1	**Zabezpieczenie pomieszczeń:**	
	1) wszystkie pomieszczenia, w których przetwarza się dane osobowe są zamykane na klucz w przypadku opuszczenia pomieszczenia przez ostatniego pracownika upoważnionego do przetwarzania danych osobowych – także po godzinach pracy;	Osoba przetwarzająca dane osobowe
	2) dane osobowe przechowywane w wersji tradycyjnej (papierowej) lub elektronicznej (pamięć flash, płyta CD, DVD, dyskietka) po zakończeniu pracy są przechowywane w zamykanych na klucz w meblach biurowych, a tam gdzie jest to możliwe – w szafach metalowych lub pancernych; klucze od szafek należy zabezpieczyć przed dostępem osób nieupoważnionych do przetwarzania danych osobowych;	Osoba przetwarzająca dane osobowe
	3) nieaktualne lub błędne wydruki zawierające dane osobowe niszczone w niszczarkach	Osoba przetwarzająca dane osobowe
2	**Zabezpieczenie przed nieautoryzowanym dostępem:**	
	1) udostępnianie użytkownikowi zasobów sieci zawierających dane osobowe (programów i baz danych) przez administratora serwera lub administratora bazy następuje na podstawie upoważnienia do przetwarzania danych osobowych;	Administrator sieci
	2) identyfikacja użytkownika w systemie poprzez zastosowanie podwójnego uwierzytelnienia;	Administrator sieci
	3) Przydzielenie indywidualnego identyfikatora każdemu użytkownikowi systemu informatycznego i rejestrowanie przez system czasu logowania użytkownika i rodzaju wprowadzonych przez niego danych;	Administrator sieci
	4) udostępnianie kluczy i uprawnień do wejścia centrum przetwarzania danych (serwerowni) tylko pracownikom do tego upoważnionym;	Administrator bezpieczeństwa informacji
	5) stosowanie programu antywirusowego z zaporą antywłamaniową na komputerach ze środowiskiem operacyjnym MS Windows;	Administrator sieci
	6) zabezpieczenie hasłami kont na komputerach, używanie kont z ograniczonymi uprawnieniami do ciągłej pracy;	Administrator sieci
	7) ustawienie monitorów stanowisk przetwarzania danych osobowych w sposób uniemożliwiający wgląd w dane osobom nieupoważnionym;	Osoba przetwarzająca dane osobowe

	8) automatyczne wygaszanie ekranu i blokowanie nieużywanego komputera po upływie określonego czasu; 9) wymuszenie zmiany hasła do systemu informatycznego co 90 dni	Administrator sieci Administrator sieci
3	**Zabezpieczenie przed nieautoryzowanym dostępem poprzez Internet:** 1) logiczne oddzielenie sieci wewnętrznej LAN od sieci zewnętrznej, uniemożliwiające uzyskanie połączenia z bazą danych spoza systemu informatycznego, jak również uzyskanie dostępu z systemu do sieci rozległej Internet; 2) zastosowanie dwóch poziomów zabezpieczenia sieci	 Administrator sieci Administrator sieci
4	**Zabezpieczenie przed utratą danych:** 1) odrębne zasilanie sprzętu komputerowego 2) ochrona serwerów przed zanikiem zasilania poprzez stosowanie zasilaczy zapasowych UPS 3) ochrona przed utratą zgromadzonych danych poprzez cykliczne wykonywanie kopii zapasowych, z których, w przypadku awarii, odtwarzane są dane i system operacyjny; 4) ochrona przed awarią podsystemu dyskowego poprzez używanie macierzy dyskowych; 5) zapewnienie właściwej temperatury i wilgotności powietrza dla pracy sprzętu komputerowego, poprzez zastosowanie redundantnych klimatyzatorów 6) Zastosowanie ochrony przeciwpożarowej poprzez umieszczenie w serwerowni gaśnic, okresowo kontrolowanych przez specjalistę 7) zwiększenie niezawodności serwerów i urządzeń sieciowych poprzez logiczne rozmieszczenie ich w szafie serwerowej	Kierownik Referatu Organizacyjnego Administrator sieci Administrator sieci Administrator sieci Kierownik Referatu Organizacyjnego – zapewnienie możliwości stosowania; Administrator sieci – właściwe stosowanie systemu klimatyzatorów Kierownik Referatu Organizacyjnego Administrator sieci
5	**Środki organizacyjne ochrony danych osobowych i ich przetwarzania:** 1) zapoznanie każdej osoby z przepisami dotyczącymi ochrony danych osobowych, przed dopuszczeniem jej do pracy przy ich przetwarzaniu; 2) przeszkolenie osób w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochroną danych osobowych oraz zabezpieczenia pomieszczeń i budynku; 3) kontrolowanie pomieszczeń i budynku 4) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych 5) wyznaczenie administratora bezpieczeństwa informacji	Kierownik Referatu Organizacyjnego Administrator bezpieczeństwa informacji Administrator bezpieczeństwa informacji Kierownik Referatu Organizacyjnego Administrator bezpieczeństwa informacji Wójt Gminy

Załącznik Nr 2
do Zarządzenia Nr 178/2011
Wójta Gminy Zagnańsk
z dnia 02 grudnia 2011r.

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

Rozdział 1

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 przez niego wyznaczonych i użytkowników przetwarzających dane osobowe w Urzędzie Gminy w Zagnańsku, zwanym dalej „Urzędem".
2. Instrukcja została opracowana zgodnie z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r. 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 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).
3. Wyjaśnienia używanych pojęć:
   1) Administrator Danych Osobowych – należy rozumieć przez to Wójta Gminy Zagnańsk,
   2) Administrator Bezpieczeństwa Informacji – osoba wyznaczona przez Administratora Danych Osobowych do pełnienia funkcji,
   3) Administrator Sieci – osoba odpowiedzialna za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych, służących do przetwarzania danych osobowych w Urzędzie;
   4) 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;
   5) Nośniki danych osobowych – dyskietki, płyty CD lub DVD, pamięć flash, dyski twarde, taśmy magnetyczne lub inne urządzenia/materiały służące do przechowywania plików z danymi;
   6) Użytkownik– osoba posiadająca upoważnienie wydane przez administratora Danych Osobowych lub przez osobę przez niego wyznaczoną i dopuszczoną, w zakresie wskazanym w tym upoważnieniu do przetwarzania danych osobowych w systemie informatycznym danej komórki organizacyjnej Urzędu;

Rozdział 2

Nadawanie uprawnień do przetwarzania danych osobowych oraz ich rejestrowanie w systemie informatycznym

1. Przed dopuszczeniem do pracy przy przetwarzaniu danych osobowych, każdy użytkownik powinien zostać zapoznany przez przełożonego lub administratora bezpieczeństwa informacji z przepisami dotyczącymi ochrony danych osobowych oraz obowiązującymi w Urzędzie wewnętrznymi regulacjami w tym zakresie.
2. Do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych , mogą zostać dopuszczone , z zastrzeżeniem ust. 3, wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych wydane przez Administratora Bezpieczeństwa Informacji osobowych. Wzór upoważnienia stanowi załącznik nr 1 do Instrukcji.

3. Do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych, mogą zostać dopuszczone również osoby, którym udzielono upoważnień do przetwarzania danych osobowych na podstawie porozumień zawartych w sprawie powierzenia Urzędowi przetwarzania danych osobowych.
4. Wydanie upoważnienia oraz rejestracja użytkownika w systemie informatycznym przetwarzającym dane osobowe następuje na wniosek przełożonego użytkownika.
5. Procedury wydawania i odwoływania upoważnień użytkowników do przetwarzania danych osobowych realizowane są według następujących zasad:
   1) przełożony użytkownika składa do administratora danych osobowych pisemny wniosek o wydanie upoważnienia, który zawiera:
      a) imię i nazwisko użytkownika,
      b) stanowisko zajmowane przez użytkownika,
      c) nazwę zbioru danych osobowych oraz nazwę systemu informatycznego, do którego użytkownik będzie miał dostęp,
      d) zakres upoważnienia do przetwarzania danych osobowych,
      e) datę, z jaką upoważnienie ma być wydane,
      f) okres ważności upoważnienia;
   2) oryginał upoważnienia zostaje przekazany użytkownikowi z potwierdzeniem odbioru, kopia zostaje włączona do akt osobowych użytkownika oraz przekazana do wiadomości przełożonego;
   3) wyrejestrowania użytkownika z systemu informatycznego dokonuje na wniosek administratora danych osobowych lub przełożonego użytkownika administrator sieci po uzgodnieniu z administratorem bezpieczeństwa informacji.
6. Osobie niebędącej pracownikiem Urzędu danych udziela upoważnienia na wniosek kierownika referatu danej komórki organizacyjnej przetwarzającej dane osobowe lub zapewniającej obsługę administracyjną podmiotu, który przetwarza w zakresie swojej właściwości dane osobowe w systemach informatycznych Urzędu.
7. Użytkownik niebędący pracownikiem Urzędu otrzymuje oryginał upoważnienia za potwierdzeniem odbioru. Kopia upoważnienia przechowywana jest u administratora bezpieczeństwa informacji.
8. 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.
9. Za przydzielenie i wygenerowanie identyfikatora i hasła użytkownikowi, który po raz pierwszy korzysta z systemu informatycznego, odpowiada administrator sieci.
10. Identyfikator użytkownika nie może być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego nie może być przydzielany innej osobie.
11. Przełożeni użytkowników i dla osób o których mowa w ust. 6 , zobowiązani są pisemnie informować administratora danych osobowych lub administratora bezpieczeństwa informacji o każdej zmianie dotyczącej użytkowników mającej wpływ na zakres posiadanych uprawnień do przetwarzania danych osobowych.
12. Administrator bezpieczeństwa informacji jest zobowiązany do prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych. Wzór wykazu osób upoważnionych do przetwarzania danych osobowych stanowi załącznik nr 2 do Instrukcji.

Rozdział 3

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

1. Użytkownik uzyskuje dostęp do danych osobowych przetwarzanych w systemie informatycznym wyłącznie po podaniu identyfikatora i hasła.
2. Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi. Użytkownik jest odpowiedzialny za wszystkie czynności wykonane przy użyciu swojego identyfikatora.

3. Identyfikator składa się minimalnie z 4 znaków, które nie są rozdzielone spacjami ani znakami interpunkcyjnymi. Identyfikator jest tworzony przy użyciu małych liter, z wyłączeniem polskich znaków.
4. Użytkownik otrzymuje hasło początkowe z chwilą przystąpienia do pracy w systemie informatycznymi jest zobowiązany zmienić je natychmiast po rozpoczęciu na sobie tylk znany ciąg znaków.
5. Hasło składa się z co najmniej 8 znaków.
6. Hasło powinno zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.
7. Hasło nie może być zapisane w miejscu dostępnym dla osób nieuprawnionych i należy je zachować w tajemnicy, również po upływie jego ważności.
8. Użytkownik nie może udostępniać osobom nieuprawnionym swojego identyfikatora oraz hasła. Po uwierzytelnieniu w systemie użytkownik nie może udostępniać osobom nieuprawnionym swojego stanowiska pracy.
9. 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.
10. Osoby uprawnione do wykonywania prac administracyjnych w systemie informatycznym posiadają własne konta administracyjne oraz hasła.

Rozdział 4

Rozpoczęcie, zawieszenie i zakończenie przez użytkowników systemu

1. Użytkownik rozpoczynając pracę na komputerze loguje się do systemu informatycznego.
2. Dostęp do danych osobowych możliwy jest jedynie po dokonaniu uwierzytelnienia użytkownika .
3. Maksymalna liczba prób wprowadzenia hasła przy logowaniu się do systemu informatycznego wynosi 3. Po przekroczeniu tej liczby prób logowania system blokuje dostęp do zbioru danych na poziomie danego użytkownika. Odblokowanie dostępu do zbioru danych może dokonać administrator sieci w porozumieniu z administratorem bezpieczeństwa informacji.
4. W przypadku braku aktywności użytkownika na komputerze przez okres dłuższy niż 10 minut następuje automatyczne włączenie wygaszacza ekranu.
5. Monitory stanowisk komputerowych, na których przetwarzane SA dane osobowe, znajdujące się w pomieszczeniach, gdzie przebywają osoby, które nie posiadają upoważnień do przetwarzania danych osobowych, należy ustawić w taki sposób, aby uniemożliwić tym osobom wgląd w dane.
6. Przebywanie osób nieuprawnionych w pomieszczeniach znajdujących się na obszarze, w którym są przetwarzane dane osobowe, jest dopuszczalne tylko w obecności osoby upoważnionej do ich przetwarzania.
7. Pomieszczenia, w których przetwarzane są dane osobowe, należy zamykać na czas nieobecności osób upoważnionych, w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym.
8. Przed opuszczeniem stanowiska pracy użytkownik obowiązany jest:
   1) wylogować się z systemu informatycznego albo
   2) wywołać blokowany hasłem wygaszacz ekranu.
9. Kończąc pracę użytkownik obowiązany jest:
   1) wylogować się z systemu informatycznego, następnie wyłączyć sprzęt komputerowy;
   2) zabezpieczyć stanowisko pracy.

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

Rozdział 5

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 sieci lub inna osoba przez niego wyznaczona.
3. W przypadku lokalnego przetwarzania danych osobowych na służbowych komputerach użytkownicy systemu informatycznego zobowiązani są do centralnego przechowywania kopii danych, tak aby możliwe było zabezpieczenie ich dostępności poprzez wykonanie kopii zapasowych.
4. Przez centralne przechowywanie kopii danych rozumie się cotygodniowe przegrywanie zbioru danych na specjalnie wydzielony do tego celu obszar dysku na serwerze. W przypadku, gdy z przyczyn technicznych nie jest możliwe, użytkownicy systemu są zobowiązani do sporządzania kopii zapasowych zbiorów danych na nośniku danych i przechowywania w szafie zamykanej na klucz.
5. Kopie zapasowe zbiorów danych należy okresowo sprawdzać pod kątem ich przydatności do odtworzenia w przypadku awarii systemu informatycznego. Za przeprowadzenie tej procedury odpowiedzialny jest administrator sieci.
6. Kopie zapasowe wykonywane są zgodnie z następującym harmonogramem:
   1) kopia zapasowa aplikacji przetwarzającej dane osobowe – pełna kopia wykonywana jest po wprowadzeniu zmian aplikacji i zapisywana na nośnikach danych;
   2) kopia zapasowa danych osobowych przetwarzanych przez aplikację – pełna kopia wykonywana jest raz w tygodniu, a w przypadku wprowadzenia znacznych zmian danych osobowych, może być wykonywana częściej;
   3) kopia zapasowa danych konfiguracyjnych systemu informatycznego przetwarzającego dane osobowe, w tym uprawnień użytkowników systemu – pełna kopia wykonywana jest raz w miesiącu.
7. Kopie zapasowe przechowywane są w szafie zamykanej na klucz.

Rozdział 6

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

1. Użytkownicy nie mogą wynosić z budynku Urzędu nośników danych z zapisami danymi osobowymi bez zgody administratora danych osobowych lub administratora bezpieczeństwa informacji.
2. Okresowe kopie zapasowe wykonywane są na dyskietkach, płytach CD, DVD, taśmach lub innych nośnikach danych. Kopie przechowuje się w innych pomieszczeniach, niż te, których przechowywane są zbiory dany wykorzystane na bieżąco. Kopie zapasowe przechowuje się w sposób uniemożliwiający nieuprawnione przejęcie, modyfikacje, uszkodzenie lub zniszczenie.
3. Dostęp do nośników danych z kopiami zapasowymi, ma wyłącznie administrator bezpieczeństwa informacji oraz administrator sieci.
4. Usunięcie danych z systemu powinno zostać zrealizowane przy pomocy oprogramowania przeznaczonego do bezpiecznego usuwania danych z nośnika danych.
5. Za zniszczenie kopii zapasowych sporządzanych indywidualnie przez użytkownika odpowiada użytkownik.
6. Dane osobowe w postaci elektronicznej należy usuwać z nośnika danych w sposób uniemożliwiający ich ponowne odtworzenie, nie później niż po upływie 5 dni po wykorzystaniu tych danych, chyba że z odrębnych przepisów wynika obowiązek ich przechowywania.
7. Nośniki danych podlegają komisyjnemu zniszczeniu w przypadku wycofania z eksploatacji sprzętu komputerowego, na którym przetwarzane były dane osobowe, oraz po przeniesieniu danych osobowych do zbiorów w systemie informatycznym z nośników, których ponownie wykorzystanie nie jest możliwe. Członków komisji wyznacza Wójt. Z przeprowadzonych czynności komisja sporządza protokół.
8. Przez zniszczenie nośników danych należy rozumieć ich trwałe i nieodwracalne zniszczenie fizyczne do stanu uniemożliwiającego ich rekonstrukcję i odzyskanie danych.

Rozdział 7

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

1. Za ochronę antywirusową systemu informatycznego odpowiada administrator sieci.
2. System antywirusowy zainstalowany jest w każdym komputerze z dostępem do danych osobowych. Ustawienie poziomu bezpieczeństwa i wysyłanie aktualizacji bazy sygnatur wirusów zarządzane jest centralnie.
3. Programy antywirusowe SA uaktywnione przez cały czas pracy każdego komputera w systemie informatycznym.
4. Wszystkie pliki otrzymywane z zewnątrz, jak również wysyłane na zewnątrz, podlegają automatycznemu sprawdzeniu przez system antywirusowy pod kątem występowania wirusów, z zastosowaniem najnowszej dostępnej wersji programu antywirusowego.
5. W przypadku pojawienia się wirusa, użytkownik obowiązany jest zaprzestać wykonywania jakichkolwiek czynności w systemie i niezwłocznie powiadomić administratora sieci, administratora bezpieczeństwa informacji.
6. Niedozwolone jest otwieranie wiadomości poczty elektronicznej i załączników od „niezaufanych" nadawców.
7. Niedozwolone jest wyłączanie, blokowanie i odinstalowywanie programów zabezpieczających komputer przed oprogramowaniem złośliwym oraz nieautoryzowanym dostępem (skaner antywirusowy, firewall).
8. Administrator sieci jest odpowiedzialny za aktywowanie i poprawne konfigurowanie specjalistycznego oprogramowania monitorującego wymianę danych na styku:
   1) sieci lokalnej i rozległej;
   2) stanowiska komputerowego użytkownika systemu i pozostałych urządzeń wchodzących w skład sieci lokalnej.

Rozdział 8

Udostępnianie danych osobowych i sposób odnotowywania informacji o udostępnianiu danych

1. Dane osobowe przetwarzane w Urzędzie mogą być udostępniane osobom lub podmiotom 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 przez inny podmiot można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
4. Administrator bezpieczeństwa informacji prowadzi ewidencję udostępnionych danych, która zawiera:
   1) numer ewidencyjny wydruku;
   2) zakres udostępnianych danych;
   3) adresata udostępnionych danych;
   4) datę udostępnienia.
5. Odnotowanie informacji powinno nastąpić niezwłocznie po udostępnieniu danych.

Rozdział 9

Wykonywanie przeglądów i konserwacji systemu oraz nośników danych służących do przetwarzania danych

1. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe mogą być wykonywane przez administratora sieci.
2. Administrator sieci okresowo sprawdza możliwość odtworzenia danych z kopii zapasowej. Częstotliwość wykonywania procedury odtwarzania danych jest uzgadniana z administratorem bezpieczeństwa informacji.

3. Aktualizacja oprogramowania powinna 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 sieci.
5. Nieprawidłowości w działaniu systemu informatycznego oraz oprogramowania są niezwłocznie usuwane przez administratora sieci, a ich przyczyny analizowane.
6. Zmiana konfiguracji sprzętu komputerowego, na którym znajdują się dane osobowe lub zmiana jej lokalizacji, może być dokonana tylko za wiedzą i zgodą administratora bezpieczeństwa informacji.

Rozdział 10

Postępowanie w przypadku naruszenia ochrony danych osobowych

1. Każdy użytkownik, który stwierdzi lub podejrzewa naruszenie ochrony danych w systemie informatycznym, zobowiązany jest niezwłocznie poinformować o tym administratora bezpieczeństwa informacji lub administratora sieci.
2. Do czasu przybycia administratora bezpieczeństwa informacji lub administratora sieci na miejsce naruszenia lub ujawnienia ochrony danych osobowych, należy:
   1) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile występuje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców naruszenia;
   2) rozważyć wstrzymanie bieżącej pracy na komputerze w celu zabezpieczenia miejsca zdarzenia;
   3) zaniechać, o ile to możliwe, dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić jego udokumentowanie i analizę;
   4) udokumentować wstępnie zaistniałe naruszenie;
   5) nie opuszczać, bez uzasadnionej potrzeby, miejsca zdarzenia do czasu przybycia administratora sieci lub administratora bezpieczeństwa informacji.
3. Po przybyciu na miejsce naruszenia lub ujawnienia naruszenia ochrony danych osobowych, administrator bezpieczeństwa informacji we współpracy z administratorem sieci:
   1) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania, mając na uwadze ewentualne zagrożenia dla prawidłowości pracy Urzędu;
   2) może zażądać wyjaśnień dotyczących zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej osoby, która może posiadać informacje związane z zaistniałym naruszeniem;
      dokonuje zabezpieczenia systemu informatycznego przed dalszym rozprzestrzenianiem się skutków naruszenia;
   3) dokonuje zabezpieczenia systemu informatycznego przed dalszym rozprzestrzenianiem się skutków naruszenia;
   4) podejmuje odpowiednie kroki w celu powstrzymania lub ograniczenia dostępu osoby niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów naruszenia;
   5) rozważa celowość i potrzebę powiadomienia o zaistniałym naruszeniu administratora danych osobowych.
4. Po wyczerpaniu niezbędnych środków doraźnych, administrator bezpieczeństwa informacji we współpracy z administratorem sieci zasięga niezbędnych opinii i proponuje działania mające na celu usunięcie naruszenia i jego skutków oraz ustosunkowanie się do kwestii ewentualnego odtworzenia danych z kopii zapasowej i terminu wznowienia przetwarzanych danych.
5. Administrator bezpieczeństwa informacji dokumentuje zaistniały przypadek naruszenia oraz sporządza raport, który zawiera w szczególności:
   1) wskazanie osoby powiadamiającej o naruszeniu oraz innych osób, które złożyły wyjaśnienia w związku z naruszeniem;
   2) określenie czasu i miejsca naruszenia oraz powiadomieniu o naruszeniu;
   3) określenie okoliczności towarzyszących i rodzaju naruszenia;

4) wyszczególnienie uwzględnionych przesłanek wyboru metody postępowania i opis podjętego działania;
5) wstępną ocenę przyczyn wystąpienia naruszenia;
6) ocenę przeprowadzonego postępowania wyjaśniającego i działań podjętych w celu usunięcia naruszenia i jego skutków

6. Raport, o którym mowa w ust. 6, administrator bezpieczeństwa informacji przekazuje administratorowi danych osobowych w terminie 14 dni od daty zdarzenia.
7. Po przywróceniu prawidłowego funkcjonowania systemu informatycznego, administrator bezpieczeństwa informacji we współpracy z administratorem sieci przeprowadza szczegółowa analizę w celu określenia przyczyn naruszenia ochrony danych osobowych lub podejrzenia takiego naruszenia oraz podejmuje kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.

Załącznik Nr 1
do Instrukcji
Zarządzania systemem informatycznym
służącym do przetwarzania danych osobowych

Zagnańsk, ...

Urząd Gminy Zagnańsk
Administrator Bezpieczeństwa Informacji

S.1334. .201....

UPOWAŻNIENIE
DO PRZETWARZANIA DANYCH OSOBOWYCH NR .....

Na podstawie art.37. ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz.U. z 2002r., Nr 101, poz 926, z późn. zm.) nadaję

Pani/Panu.....
(imię i nazwisko osoby upoważnionej)

uprawnienia do przetwarzania danych osobowych gromadzonych w

.....
(nazwa zbioru danych osobowych)

w zakresie.....
(zakres uprawnień)

Niniejsze upoważnienie nadaje się na czas zatrudnienia na stanowisku.....

.....
(podpis Administratora Bezpieczeństwa Informacji)

Oświadczam, że zapoznałam/em się z przepisami dotyczącymi ochrony danych osobowych, w tym z ustawą z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz.U. z 2002 r., Nr 101, poz. 926, z późn. zm.) i Zarządzeniem Nr178/2011 Wójta Gminy Zagnańsk z dnia 02.12.2011 w sprawie zasad ochrony danych osobowych przetwarzanych w Urzędzie Gminy w sprawie środków technicznych i organizacyjnych zapewniających ochronę danych osobowych przetwarzanych w Urzędzie Gminy Zagnańsk oraz zobowiązuje się zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia.

.....
(data i podpis osoby upoważnionej)

Do wiadomości:

Referat Organizacyjny
i Spraw Obywatelskich - Kadry

Załącznik Nr 2
do Instrukcji
Zarządzania systemem informatycznym
służącym do przetwarzania danych osobowych

Wykaz osób upoważnionych do przetwarzania danych osobowych w Urzędzie Gminy Zagnańsk

Nr upoważnienia	Referat/stanowisko	Upoważnienie od:	Upoważnienie do:	Imię i Nazwisko	Nazwa zbioru	Zakres upoważnienia	Identyfikator