ZARZĄDZENIE Nr 9/2013
Wójta Gminy Karniewo
z dnia 05.04. 2013 r.

w sprawie wprowadzenia do użytku służbowego „Polityki bezpieczeństwa informacji" oraz „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych" w Urzędzie Gminy Karniewo.

Na podstawie art. 31 oraz art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U. z 2001 r. Nr 142, poz. 1591 ze zm.) i art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r. Nr 101, poz. 926 ze zm.) oraz § 1 pkt 1 w związku z § 3 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. z 2004 r. Nr 100, poz. 1024.) zarządza się co następuje:

§ 1.

Wprowadza się do użytku służbowego „Politykę bezpieczeństwa informacji Urzędu Gminy Karniewo", w brzmieniu stanowiącym załącznik nr 1 do zarządzenia.

§ 2.

Wprowadza się do użytku służbowego „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Karniewo" w brzmieniu stanowiącym załącznik nr 2 do zarządzenia.

§ 3.

Wykonanie zarządzenia powierza się Zastępcy Wójta Gminy Karniewo.

§ 4.

Zarządzenie wchodzi w życie z dniem podjęcia.

WÓJT
mgr Michał Wojciech Jasiński

Kancelaria Radców Prawnych
J. Niećcior i Z. Wołłański s.c. w Pułtusku
Dominik Pogorzelski
prawnik

Załącznik nr 1
do Zarządzenia Nr 9/2013
Wójta Gminy Karniewo
z dnia 05.04.2013 r.

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH WRAZ Z INSTRUKCJĄ ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI W URZĘDZIE GMINY KARNIEWO

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH W URZĘDZIE GMINY KARNIEWO

W celu zabezpieczenia danych gromadzonych i przetwarzanych w Urzędzie Gminy Karniewo oraz jego systemie informatycznym, a w szczególności w celu ochrony danych osobowych, wprowadza się określone w niniejszym dokumencie zasady bezpieczeństwa.
Mając świadomość, że żadne zabezpieczenie techniczne nie gwarantuje 100% -towej szczelności systemu, konieczne jest, aby każdy pracownik pełen świadomej odpowiedzialności, postępował zgodnie z przyjętymi zasadami i minimalizował zagrożenia wynikające z ludzkich błędów.

Podstawa prawna.

1. Ustawa z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz.U. z 2002 r. Nr 101, poz. 926 z późn. zm.)

2. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r. Nr 100, poz. 1024).

Definicje

Ilekroć w niniejszym dokumencie jest mowa o:

1. **Urzędzie** – należy przez to rozumieć Urząd Gminy Karniewo.

2. **Administratorze Danych** – należy przez to rozumieć Wójta Gminy Karniewo.

3. **Administratorze Systemu Informatycznego** – należy przez to rozumieć osobę odpowiedzialną za funkcjonowanie systemu informatycznego urzędu oraz stosowanie technicznych i organizacyjnych środków ochrony.

4. **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji narzędzi programowych zastosowanych w celu przetwarzania danych.

5. **Użytkownik systemu** – należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym urzędu. Użytkownikiem może być pracownik urzędu, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno prawnej, osoba odbywająca staż w urzędzie posiadająca stosowne upoważnienie.

6. **Sieci lokalnej** – należy przez to rozumieć połączenie systemów informatycznych urzędu wyłącznie dla własnych jej potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych.

7. **Sieci rozległej** – należy przez to rozumieć sieć publiczną w rozumieniu ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz.U. z 2004 r. Nr 171, poz. 1800, ze. zm.).

8. **Zbiorze danych** – należy przez to rozumieć każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

9. **Przetwarzanie danych** – należy przez to rozumieć 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.

10. **Zabezpieczenie danych w systemie informatycznym** – należy przez to rozumieć wdrożenie i eksploatacja stosowanych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.

11. **Identyfikator użytkownika** – należy przez to rozumieć ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.

12. **Hasło** – należy przez to rozumieć ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

13. **Uwierzytelnianie** – należy przez to rozumieć działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

14. **Rozliczalność** – należy przez to rozumieć właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

15. **Integralność danych** – należy przez to rozumieć właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.

16. **Poufność danych** – należy przez to rozumieć właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom.

Polityka bezpieczeństwa określa:

1. Wykaz budynków oraz pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe.

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

3. Opis struktury zbiorów danych wskazujących zawartości poszczególnych pól informacyjnych i powiązań miedzy nimi.

4. Sposób przepływu danych pomiędzy systemami. Systemy, w których przetwarza się dane osobowe są rozproszone i nie są ze sobą połączone, co uniemożliwia przepływ danych pomiędzy nimi.

5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności i rozliczalności przetwarzanych danych.

Ad. 1.
Obszar przetwarzania danych osobowych
Miejscem przetwarzania danych osobowych są pomieszczenia pracy komórek organizacyjnych i samodzielnych stanowisk Urzędu Gminy Karniewo, adres: ul. Pułtuska 3, 06 - 425 Karniewo.

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

Za zbiór danych osobowych przetwarzanych w Urzędzie Gminy Karniewo uważa się:

1. dokumentację papierową (korespondencja, wnioski, deklaracje, itd.),

2. systemy informatyczne przetwarzania danych oraz oprogramowanie komputerowe służące do przetwarzania informacji,

3. wydruki komputerowe.

Wykaz zbiorów oraz programów służących do ich przetwarzania:

Lp.	Nazwa zbioru	Sposób gromadzenia	Nazwa programu
1.	Ewidencja ludności	Forma papierowa Forma elektroniczna	SELWIN
2.	Urząd Stanu Cywilnego	Forma papierowa Forma elektroniczna	USC WIN 2
3.	Dowody osobiste	Forma papierowa Forma elektroniczna	System Wydawania Dowodów Osobistych
4.	Podatki i opłaty lokalne (rejestr wymiarowy podatków	Forma papierowa Forma elektroniczna	INFO SYSTEM

5.	Rejestr ewidencji gospodarowania odpadami	Forma papierowa Forma elektroniczna	GOMIC firmy ARISCO
6.	Rejestr numeracji porządkowej nieruchomości	Forma papierowa	
7.	Umowy najmu lokali mieszkalnych i dzierżawy lokali użytkowych	Forma papierowa	
8.	Rejestr wniosków o zmianę przeznaczenia w Studium Uwarunkowań i Zagospodarowania Przestrzennego i Miejscowym Planie Zagospodarowania Przestrzennego.	Forma elektroniczna	
9.	Dokumentacja dot. przyznania dodatków mieszkaniowych	Forma papierowa	
10.	Rejestr zezwoleń na sprzedaż napojów alkoholowych	Forma papierowa	
11.	Rejestr skarg i wniosków	Forma papierowa	
12.	Rejestry zaświadczeń	Forma papierowa	

Ad. 3

Opis struktury zbiorów danych osobowych oraz sposób przepływu danych pomiędzy systemami informatycznymi.

Opis struktury przetwarzanych danych osobowych oraz realizacji pomiędzy danymi, procesy przetwarzania oraz struktura danych zostały zawarte w dokumentacji technicznej systemów informatycznych dostępnej u dostawców oprogramowania informatycznego. Licencje oprogramowania nie obejmują listingu danych źródłowych lecz jedynie prawo korzystania z rozwiązań.

Struktura zbiorów danych osobowych i powiązań między nimi:

Lp.	Nazwa zbioru	Opis zbioru
1.	Ewidencja ludności	Nazwisko, imiona, nazwisko rodowe, nazwiska poprzednie, PESEL, data i miejsce urodzenia, imiona i nazwiska rodowe rodziców, seria i numer dowodu osobistego, nr książeczki wojskowej, stan cywilny, nr aktu urodzenia, płeć, adres zamieszkania.
2.	Urząd Stanu Cywilnego	Nazwisko, imiona, nazwisko rodowe, nazwiska poprzednie, PESEL, data i miejsce urodzenia, imiona i nazwiska rodowe rodziców, seria i numer dowodu osobistego, nr książeczki wojskowej, stan cywilny, nr aktu urodzenia, płeć, adres zamieszkania, wykształcenie, nazwisko panieńskie, rodowe, z poprzedniego małżeństwa, data i numer aktu zgonu.
3.	Dowody osobiste	Nazwisko, imiona, nazwisko rodowe, nazwiska poprzednie, PESEL, data i miejsce urodzenia, imiona i nazwiska rodowe rodziców, płeć,

		adres zamieszkania.
4.	Podatki i opłaty lokalne	Nazwisko i imiona, adres zamieszkania, NIP, PESEL.
5.	Rejestr ewidencji gospodarowania odpadami	Nazwisko i imiona, adres zamieszkania, nr telefonu, PESEL, NIP, e-mail.
6.	Rejestr numeracji porządkowej nieruchomości	Nazwisko i imiona, adres.
7.	Umowy najmu lokali mieszkalnych i użytkowych	Nazwisko i imiona, adres zamieszkania, numer i seria dowodu osobistego.
8.	Rejestr wniosków o zmianę przeznaczenia w Studium Uwarunkowań i Zagospodarowania Przestrzennego i Miejscowym Planie Zagospodarowania Przestrzennego.	Nazwisko i imiona, adres zamieszkania, nr działki i miejscowość.
9.	Dokumentacja dot. przyznania dodatków mieszkaniowych	Nazwisko i imiona, adres zamieszkania, ilość osób zamieszkujących, miejsce zatrudnienia.
10.	Rejestr zezwoleń na sprzedaż napojów alkoholowych	Nazwisko i imiona, adres.
11.	Rejestr skarg i wniosków	Nazwisko i imiona, adres.
12.	Rejestry zaświadczeń	Nazwisko i imiona, adres.

Ad. 5
Środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

A. Dane w postaci elektronicznej.

Dane przetwarzane są przy użyciu komputerów pracujących wyłącznie w wewnętrznej sieci komputerowej oddzielonej fizycznie od sieci publicznej przy pomocy bramy internetowej wyposażonej w firewall oraz programowe firewalle na stacjach roboczych, dodatkowo zabezpieczonych oprogramowaniem antywirusowym.
Dostęp do danych następuje po autoryzacji. Autoryzacja polega na podaniu identyfikatora oraz hasła przydzielonego przez Administratora danych.

Uwzględniając kategorie przetwarzanych danych wprowadza się podstawowy poziom bezpieczeństwa.
Środki bezpieczeństwa na poziomie podstawowym określa instrukcja zarządzania systemem informatycznym.

B. Dane w rejestrach papierowych.
Dane przetwarzane przy użyciu tradycyjnych środków pisarskich gromadzone są w rejestrach, księgach, zeszytach papierowych oraz segregatorach i przechowywane w zamykanych szafach oraz kasach pancernych.

C. Środki organizacyjne.

Administrator systemu informatycznego jest osobę odpowiedzialną za funkcjonowanie systemu informatycznego urzędu oraz stosowanie technicznych i organizacyjnych środków ochrony określonych w instrukcji zarządzania systemem informatycznym a sprawy dotyczące ochrony danych osobowych przetwarzanych w tradycyjnych rejestrach nadzoruje bezpośrednio Administrator danych.

D. Środki organizacyjne oraz środki ochrony fizycznej.

1. Wejście do budynku Urzędu Gminy zabezpieczone jest zamkami drzwiowymi, alarmem oraz monitoringiem widokowym. Poszczególne pokoje, w których odbywa się przetwarzanie danych osobowych i ich składowanie muszą być wyposażone w niezależne zamki i muszą być zamykane podczas nieobecności pracownika. Odpowiedzialność za właściwą ochronę pomieszczeń ponosi właściwy pracownik .

2. Przebywanie osób nieuprawnionych w pomieszczeniach tworzących obszar przetwarzania danych osobowych dopuszczalne jest tylko w obecności osoby zatrudnionej przy przetwarzaniu danych.

3. Pomieszczenia, o których mowa wyżej, zamykane są na czas nieobecności pracownika zatrudnionego przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich. Klucze do pomieszczeń służbowych znajdują się w budynku Urzędu – sekretariat. Pozostawienie kluczy w zamkach pomieszczeń gdzie przetwarzane są dane osobowe jest niedopuszczalne (także podczas pobytu pracownika w pokoju).

4. W pomieszczeniach, w których przewiduje się przyjmowanie interesantów monitory stanowisk komputerowych ustawione są w sposób uniemożliwiający wgląd w przetwarzane dane.

5. Pracownicy przetwarzający dane osobowe obowiązani są do prawidłowego ich zabezpieczenia na swoich stanowiskach pracy.

E. Środki sprzętowe, informatyczne i telekomunikacyjne.

1. Urządzenia wchodzące w skład systemu informatycznego podłączone są do obwodu elektrycznego, zabezpieczonego na wypadek zaniku napięcia albo awarii w sieci zasilającej listwą filtrującą oraz urządzeniem UPS.

2. Dostęp fizyczny do sieci lokalnej jest ograniczony, koncentrator umieszczony jest w specjalnie przygotowanej zamykanej szafie.

3. Dostęp do sieci WAN zabezpieczony jest Firewall–em wraz z oprogramowaniem antywirusowym.

4. Kopie awaryjne wykonywane są w cyklach:
tygodniowa na dysku twardym,
miesięcznie nośnikach zewnętrznych (na pendraive, na płycie CD-R.)

5. Każdy dokument papierowy zawierający dane osobowe przeznaczony do wyrzucenia zostaje zniszczony w sposób uniemożliwiający jego odczytanie przy pomocy niszczarki.

6. Inne środki przetwarzania: drukarki, skanery, modemy, niszczarki dokumentów.

F. Środki ochrony w ramach oprogramowania.

1. Każda jednostka komputerowa zabezpieczona została:
- hasłem uruchomieniowym (BIOS),
- hasłem wejściowym do systemu operacyjnego lub do profilu użytkownika oraz hasłem do każdej aplikacji przy pomocy której przetwarzane są dane osobowe.

2. Zastosowano wygaszanie ekranu w przypadku dłuższej nieaktywności użytkownika.

3. Zastosowano identyfikator i hasło dostępu do danych na poziomie aplikacji.

4. Dla każdego użytkownika systemu jest ustalony odrębny identyfikator.

5. Zdefiniowano użytkowników i ich prawa dostępu do danych osobowych na poziomie aplikacji (unikalny identyfikator i hasło).

6. Hasła do aplikacji zmieniane są co 30 dni.

Do zapoznania się z niniejszym dokumentem oraz stosowania zawartych w nim zasad zobowiązani są wszyscy pracownicy urzędu upoważnieni do przetwarzania danych osobowych.

WÓJT

mgr Michał Wojciech Jasiński

Załącznik nr 2 do Zarządzenia Nr
9/2013 Wójta Gminy Karniewo
z dnia 05.04.2013 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI W URZĘDZIE GMINY KARNIEWO

Procedury nadawania i zmiany uprawnień do przetwarzania danych.

1. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych jest zobowiązany do zapoznania się z :

- przepisami ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych/(Dz.U. z 2002 r. Nr 101, poz. 926 z późn. zm.)

- polityką bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy,
- instrukcją zarządzania systemami informatycznymi w Urzędzie Gminy.

2. Administrator systemu informatycznego przyznaje uprawnienia w zakresie dostępu do systemu informatycznego.

3. Przyznanie uprawnień w zakresie dostępu do systemu informatycznego polega na wprowadzeniu do systemu dla każdego użytkownika unikalnego identyfikatora, hasła oraz zakresu dostępnych danych i operacji.

4. Pracownik ma prawo do wykonywania tylko tych czynności, do których został upoważniony.

5. Pracownik ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu.

6. Wszelkie przekroczenia lub próby przekroczenia przyznanych uprawnień traktowane będą jako naruszenie podstawowych obowiązków pracowniczych.

7. Pracownik zatrudniony przy przetwarzaniu danych osobowych zobowiązany jest do zachowania ich w tajemnicy. Tajemnica obowiązuje go również po ustaniu zatrudnienia.

8. Identyfikator osoby, która utraciła uprawnienia dostępu do danych osobowych należy niezwłocznie wyrejestrować z systemu informatycznego oraz unieważnić jej hasło.

9. Administrator Bezpieczeństwa Informacji zobowiązany jest do prowadzenia rejestru użytkowników i ich uprawnień w systemie informatycznym.

Zasady posługiwania się hasłami.

1. Bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.

2. Hasło użytkownika powinno być zmieniane co najmniej raz w miesiącu.

3. Identyfikator użytkownika nie powinien być zmieniany bez wyraźnej przyczyny, a po wyrejestrowaniu użytkownika z systemu informatycznego nie powinien być przydzielany innej osobie.

4. Pracownicy są odpowiedzialni za zachowanie poufności swoich haseł.

5. Hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności.

6. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie.

7. W sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, pracownik zobowiązany jest do natychmiastowej zmiany hasła.

Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie.

1. Przed rozpoczęciem pracy w systemie komputerowym należy zalogować się do systemu przy użyciu indywidualnego identyfikatora oraz hasła.

2. Po opuszczeniu stanowiska pracy na odległość uniemożliwiającą jego obserwację należy wylogować się z systemu (zablokować dostęp), lub jeżeli taka możliwość nie istnieje wyjść z programu.

3. Przed wyłączeniem komputera należy bezwzględnie zakończyć pracę uruchomionych programów oraz wykonać zamknięcie.

4. Niedopuszczalne jest zamknięcie komputera przed zamknięciem oprogramowania.

Zasady instalacji oprogramowania.

1. Dopuszcza się instalację na serwerze nowego oprogramowania do przetwarzania danych osobowych lub aktualizacji istniejących pod warunkiem spełnienia określonych wymagań.

2. Instalacji oprogramowania lub aktualizacji dokonuje Administrator systemu informatycznego lub osoba przez niego upoważniona.

3. Na wszystkich komputerach Urzędu Gminy Karniewo dopuszcza się instalację tylko legalnego, licencjonowanego oprogramowania.

Procedury tworzenia zabezpieczeń.

1. Za systematyczne przygotowanie kopii bezpieczeństwa odpowiada pracownik wraz z Administratorem systemu informatycznego.
2. Kopie bezpieczeństwa wykonywane są w systemie tygodniowo na dysk twardy oraz raz na miesiąc na nośnik zewnętrzny.
3. Nośniki z kopiami bezpieczeństwa przechowywane są w szafie pancernej urzędu gminy.
4. Na każdym stanowisku komputerowym oraz serwerze zainstalowane jest oprogramowanie antywirusowe pracujące w trybie monitora.
5. Zabrania się używania nośników niewiadomego pochodzenia bez wcześniejszego sprawdzenia ich programem antywirusowym.

6. Zabrania się pobierania plików z Internetu niewiadomego pochodzenia.
7. Administrator Systemu Informatycznego przeprowadza cyklicznie kontrole antywirusowe na wszystkich komputerach – minimum raz na miesiąc.

Zasady dokonywania napraw.
1.Dokonywanie napraw, przeglądów i konserwacji systemu przez pracowników serwisu mogą odbywać się jedynie w obecności pracownika i Administratora Systemu Informatycznego.

2. Przeglądów należy dokonywać nie rzadziej niż raz na kwartał.

3. Uszkodzone nośniki magnetyczne lub inne zawierające dane osobowe nie mogą być użytkowane. Muszą być odpowiednio zabezpieczone przed nieuprawnionym udostępnieniem, a następnie zniszczone lub naprawione pod nadzorem osoby upoważnionej przez Administratora Danych.

Nośniki papierowe danych – wydruki.
1. W przypadku konieczności przechowywania wydruków zawierających dane osobowe należy je przechowywać w miejscu uniemożliwiającym bezpośredni dostęp osobom niepowołanym.

2. Pomieszczenie, w którym przechowywane są wydruki robocze musi być należycie zabezpieczone po godzinach pracy.

3. Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

Profilaktyka antywirusowa.

1. Każdy użytkownik komputera w urzędzie gminy zobowiązany jest do używania w pracy dyskietek i płyt CD zakupionych przez urząd (nie prywatnych).

2. Informacje i dane przechowywane na dyskietkach i płytach CD mogą mieć wyłącznie charakter związany z pracą.

3. Każdy komputer minimum raz w tygodniu powinien zostać sprawdzony aktualną wersją programu antywirusowego.

Zasady korzystania z internetu.

Przy korzystaniu z Internetu w Urzędzie Gminy Karniewo należy stosować następujące zasady:
1. O potrzebie wyposażenia stanowiska pracy w oprogramowanie i urządzenia techniczne umożliwiające korzystanie z zasobów internetu decyzję podejmuje Wójt Gminy.
2. Wykorzystanie z internetu powinno ograniczać się tylko do celów służbowych. Po zakończeniu sesji należy sprawdzić komputer programem antywirusowym.

Dyskietki lub płyty CD przekazywane urzędowi gminy mogą być odczytywane na komputerach, TYLKO I WYŁĄCZNIE PO WCZEŚNIEJSZYM SPRAWDZENIU PROGRAMEM ANTYWIRUSOWYM.

WÓJT
mgr Michał Wojciech Jasiński