

**ZARZĄDZENIE NR 113/2017**  
**WÓJTA GMINY ROGÓŹNO**

z dnia 29 grudnia 2017 r.

**w sprawie wyznaczenia Bezpiecznego Stanowiska Komputerowego do  
przetwarzania informacji niejawnych oznaczonych klauzul "zastrzeżone" w Urzędzie Gminy  
Rogóżno**

Na podstawie art. 14 ust. 1 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2016 r. poz. ) zarządza się, co następuje:

**§ 1.** Wyznaczam w Urzędzie Gminy Rogóżno Bezpieczne Stanowisko Komputerowe zlokalizowane w pomieszczeniu Nr 23, które ma na celu zapewnienie bezpieczeństwa teleinformatycznego i ochrony informacji niejawnych oznaczonych klauzul "zastrzeżone" przy ich przetwarzaniu. Wytwarzanie i przetwarzanie dokumentów papierowych oraz na nośnikach oznaczonych klauzul, "zastrzeżone" może się odbywać tylko na Bezpiecznym Stanowisku Komputerowym.

**§ 2.** Użytkownicy Bezpiecznego Stanowiska Komputerowego Urzędu Gminy Rogóżno powinni posiadać aktualne poświadczenie bezpieczeństwa, lub upoważnienie Wójta Gminy uprawniające do dostępu do informacji niejawnych oznaczonych klauzul "zastrzeżone".

**§ 3.** Użytkownicy systemu przed uzyskaniem faktycznego dostępu do Bezpiecznego Stanowiska Komputerowego Urzędu Gminy występują z wnioskiem o przydzielenie konta. Dopiero po wygenerowaniu początkowego hasła dostępu uzyskują formalne uprawnienia określone w "Dokumentacji bezpieczeństwa systemu teleinformatycznego dla stacji komputerowej przetwarzającej informacje niejawne o klauzuli "zastrzeżone" i mogą rozpocząć pracę na Bezpiecznym Stanowisku Komputerowym.

**§ 4.** Uprawnieni użytkownicy Bezpiecznego Stanowiska Komputerowego Urzędu Gminy przed rozpoczęciem pracy w systemie są zobowiązani odbyć szkolenie z zakresu bezpieczeństwa teleinformatycznego oraz zapoznać się z procedurami bezpiecznej eksploatacji. Szkolenia w tym zakresie prowadzone są przez Pełnomocnika do Spraw Ochrony Informacji Niejawnych.

**§ 5.** W czasie prac personelu technicznego lub sprząającego zabroniona jest praca na stanowisku komputerowym, a dokumenty niejawne należy zabezpieczyć.

**§ 6.** W związku z wyznaczeniem Bezpiecznego Stanowiska Komputerowego wprowadza się do stosowania następujące dokumenty:

1. "Dokumentacja bezpieczeństwa systemu teleinformatycznego dla stacji komputerowej przetwarzającej informacje niejawne o klauzuli "zastrzeżone" w Urzędzie stanowiąca załącznik Nr 1.

2. "Wniosek o przydzielenie konta w systemie do przetwarzania informacji niejawnych o klauzuli "zastrzeżone", stanowiący załącznik Nr 2.

3. Wykaz użytkowników Bezpiecznego Stanowiska Komputerowego, stanowiący załącznik Nr 3.

§ 7. Nadzór nad realizacją niniejszego zarządzenia powierza się Pełnomocnikowi do Spraw Ochrony Informacji Niejawnych.

§ 8. Zarządzenie wchodzi w życie z dniem 1 stycznia 2018 r.

**DOKUMENTACJA BEZPIECZENSTWA SYSTEMU TELEINFORMATYCZNEGO  
DLA STACJI KOMPUTEROWEJ PRZETWARZAJĄCEJ INFORMACJE NIEJAWNE  
O KLAUZULI "ZASTRZEŻONE"  
W URZĘDZIE GMINY ROGÓŻNO**

**SPIS TREŚCI**

**I. Wprowadzenie**

1. Informacje ogólne
2. Klauzula tajności bezpiecznej stacji komputerowej
3. Opis bezpiecznej stacji komputerowej

**II. Organizacja i administracja bezpieczeństwa**

1. Informacje ogólne
2. Inspektor Bezpieczeństwa Teleinformatycznego
3. Administrator Systemu Teleinformatycznego
4. Użytkownik Bezpiecznej Stacji Komputerowej
5. Informowanie o naruszeniu bezpieczeństwa Stacji Komputerowej
6. Informacje o wykryciu wirusa w Bezpiecznej Stacji Komputerowej

**III. Bezpieczeństwo personelu**

1. Informacje ogólne
2. Użytkownicy Bezpiecznej Stacji Komputerowej
3. Personel sprzątający
4. Osoby wizytujące

**IV. Bezpieczeństwo fizyczne**

1. Obszar przetwarzania danych
2. Ochrona Bezpiecznej Stacji Komputerowej oraz nośników w
3. Kontrola dostępu użytkowników do sprzętu
4. Zasady kontroli sprzętu

## **V. Bezpieczeństwo dokumentów**

1. Informacje ogólne
2. Wymiana informacji
3. Oznaczenie klasyfikacji dokumentów
4. Zmiana klasyfikacji dokumentów
5. Kontrola dokumentów
6. Niszczenie dokumentów
7. Biblioteka nośników
8. Dokumenty kontrolne

## **VI. Bezpieczeństwo sprzętu i oprogramowania**

1. Informacje ogólne
2. Bezpieczeństwo sprzętu
3. Bezpieczeństwo oprogramowania

## **VII. Bezpieczeństwo łączności**

1. Bezpieczeństwo kryptograficzne
2. Bezpieczeństwo elektromagnetyczne
3. Bezpieczeństwo transmisji

## **VIII Monitorowanie bezpieczeństwa i kontrole**

1. Informacje ogólne

## **IX Konserwacje i naprawy**

1. Konserwacje sprzętu i oprogramowania
2. Naprawa sprzętu

## **X. Plany awaryjne i zapobiegawcze**

1. Zasilanie
2. Kopie zapasowe
3. Klęski żywiołowe
4. Sytuacje specjalne

## **XI. Polityka antywirusowa**

1. Informacje ogólne
2. Świadomość użytkownika
3. Zasady higieny
4. Infekcja Stacji Komputerowej
5. Postępowanie w przypadku wykrycia wirusa

## **Rozdział 1. Wprowadzenie**

### **1. Informacje ogólne**

1. Niniejszy dokument zawiera procedury bezpieczeństwa teleinformatycznego dla Bezpiecznej Stacji Komputerowej w Urzędzie Gminy Rogóżno przetwarzającej informacje niejawne oznaczone klauzulą "Zastrzeżone". Opracowanie procedur bezpieczeństwa wynika z wymagań zawartych w ustawie o ochronie informacji niejawnych oraz w rozporządzeniu Prezesa Rady Ministrów w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych. Niniejsze procedury bezpieczeństwa są obowiązujące wszystkich użytkowników bezpiecznej stacji komputerowej.

### **2. Klauzula bezpiecznej stacji komputerowej**

Bezpieczna stacja komputerowa w Urzędzie Gminy Rogóżno opisana w Szczegółowych Wymaganiach Bezpieczeństwa jest autonomicznym stanowiskiem przetwarzającym informacje niejawne dla klauzuli „Zastrzeżone”. Wszystkie informacje przechowywane lub przetwarzane oraz wprowadzane do urządzenia są traktowane jako dokumenty „Zastrzeżone”.

### **3. Opis bezpiecznej stacji komputerowej**

Bezpieczna Stacja Komputerowa zlokalizowana jest w budynku Urzędu Gminy Rogóżno , Rogóżno 91 , pok. nr 23 Bezpieczna Stacja Komputerowa wyposażona jest w komputer spełniający wymogi przetwarzania danych do klauzuli "zastrzeżone".

## **Rozdział 2.**

### **Administracja i organizacja bezpieczeństwa**

### **1. Informacje ogólne**

Kierownik jednostki organizacyjnej zobowiązany jest zapewnić bezpieczeństwo teleinformatyczne przy przetwarzaniu informacji niejawnych za pośrednictwem Bezpiecznej Stacji Komputerowej. Wójt Gminy Rogóżno wyznaczył Inspektora Bezpieczeństwa Teleinformatycznego, odpowiedzialnych za funkcjonowanie i przestrzeganie zasad oraz wymagań bezpieczeństwa teleinformatycznego. Pełnomocnik ds. Ochrony Informacji Niejawnych Urzędu Gminy Rogóżno zwany dalej pełnomocnikiem ochrony, odpowiada za zapewnienie przestrzegania przepisów o ochronie informacji niejawnych. Pełnomocnik ochrony jest odpowiedzialny za funkcjonowanie bezpiecznej stacji komputerowej. Przed rozpoczęciem korzystania z bezpiecznej stacji komputerowej, każdy użytkownik zapoznaje się z procedurami bezpieczeństwa, co potwierdza podpisem.

## 2. Inspektor Bezpieczeństwa Teleinformatycznego

Sprawdza on zgodność stanu faktycznego ze Szczególnymi Wymaganiami Bezpieczeństwa oraz przestrzeganie Procedur Bezpieczeństwa. Inspektor Bezpieczeństwa Teleinformatycznego służy pomocą Administratorowi Systemu Teleinformatycznego i użytkownikom w zakresie bezpieczeństwa i przepisów dotyczących obiegu dokumentów wytwarzanych za pomocą stacji komputerowej. Pełnomocnik ds. Ochrony Informacji Niejawnych akceptuje listy osób upoważnionych do pracy z Bezpieczną Stacją Komputerową.

## 3. Administrator Systemu Teleinformatycznego

Administrator Systemu Teleinformatycznego wykonuje prace niezbędne do efektywnego oraz bezpiecznego zarządzania Bezpieczną Stacją Komputerową w Urzędzie Gminy Rogóżno. Zapewnienia dostęp wyłącznie autoryzowanym użytkownikom Bezpiecznej Stacji Komputerowej na podstawie listy osób uprawnionych do pracy według zarządzenia kierownika jednostki organizacyjnej w sprawie określenia stanowisk i osób mogących mieć dostęp w związku z wykonywaną pracą w Urzędzie Gminy Rogóżno do informacji niejawnych.

## 4. Użytkownik Bezpiecznej Stacji Komputerowej

Jest to osoba, posiadająca stosowny dokument bezpieczeństwa osobowego, dopuszczający do pracy z wykorzystaniem Bezpiecznego Stanowiska Komputerowego na podstawie listy uprawnionych osób zaakceptowanej przez Pełnomocnika ds. Ochrony Informacji Niejawnych.

## 5. Informowanie o naruszeniu bezpieczeństwa Stacji Komputerowej

Wszelkie zauważone przez użytkowników zjawiska mogące naruszyć bezpieczeństwo Stacji Komputerowej, osób, sprzętu, oprogramowania, dokumentów lub bezpieczeństwa fizycznego muszą być niezwłocznie zgłoszone do Pełnomocnika do spraw ochrony informacji niejawnych lub Inspektora Bezpieczeństwa Teleinformatycznego. Administrator Systemu Teleinformatycznego oraz Inspektor Bezpieczeństwa Teleinformatycznego mają obowiązek określenia skali naruszenia bezpieczeństwa, a w przypadku stwierdzenia rażących naruszeń bezpieczeństwa powiadomienia Agencji Bezpieczeństwa Wewnętrznego.

## 6. Informacje o wykryciu wirusa w Bezpiecznej Stacji Komputerowej

Przypadki wykrycia wirusa lub nieprawidłowości w pracy Bezpiecznej Stacji Komputerowej należy zgłosić do Pełnomocnika do spraw informacji niejawnych w celu przeprowadzenia analizy i badania przyczyn nieprawidłowego działania. Po stwierdzeniu obecności wirusa, Inspektor Systemu Teleinformatycznego przeprowadza działania zgodne z procedurą antywirusową.

### **Rozdział 3.**

#### **Bezpieczeństwo personelu**

##### **1. Informacje ogólne**

Każda osoba mająca dostęp do pomieszczenia, w którym znajduje się Bezpieczna Stacja Komputerowa może spowodować jej uszkodzenie lub uzyskać dostęp do informacji niejawnych wyświetlanych na monitorze lub wydrukowanych. Zagrożenia w stosunku do Bezpiecznej Stacji Komputerowej mogą pochodzić od każdej osoby (personelu sprząającego, technicznego, osób wizytujących), posiadającej wystarczające umiejętności i wiedzy pozwalające na uzyskanie dostępu do Bezpiecznej Stacji Komputerowej.

##### **2. Użytkownicy Bezpiecznej Stacji Komputerowej**

Użytkownicy Bezpiecznej Stacji Komputerowej muszą zastosować się do niniejszych procedur bezpieczeństwa. Zapoznanie z Procedurami Bezpieczeństwa użytkownik potwierdza podpisem na liście użytkowników. Użytkownicy Bezpiecznej Stacji Komputerowej Urzędu Gminy Rogóżno posiadają odpowiednie dokumenty uprawniające dostępu do informacji co najmniej o klauzuli "zastrzeżone", oraz korzystają z informacji przechowywanej i przetwarzanej za pośrednictwem Bezpiecznej Stacji Komputerowej na zasadach wiedzy koniecznej.

W przypadku przetwarzania informacji o klauzuli "zastrzeżone" zabrania się przechowywania informacji w Bezpiecznej Stacji Komputerowej. Należy ją zarchiwizować na nośniku, oraz przechowywać w kancelarii do spraw ochrony informacji niejawnych. Użytkownik Bezpiecznej Stacji Komputerowej korzysta z jej zasobów w zakresie niezbędnym do wykonywania czynności służbowych.

##### **3. Personel sprząający**

Praca personelu sprząającego może odbywać się pod nadzorem wyznaczonej osoby jedynie wtedy, gdy nie prowadzi się pracy na stanowisku komputerowym, a dokumenty niejawne schowane.

##### **4. Osoby wizytujące**

Osoby wizytujące pomieszczenie, w którym znajduje się Bezpieczne Stanowisko Komputerowe mogą w nim przebywać w towarzystwie pracownika uprawnionego do korzystania z Bezpiecznej Stacji Komputerowej oraz gdy posiadają uzasadniony powód wizyty lub zezwolenie kierownika jednostki organizacyjnej. Drukarka oraz monitor są umiejscowione w sposób uniemożliwiający łatwe odczytywanie informacji przez osoby postronne. Bez zezwolenia Pełnomocnika do Spraw Ochrony Informacji Niejawnych w trakcie przebywania osób wizytujących nie może odbywać się przetwarzanie informacji niejawnych, a dokumenty i wydruki zawierające informacje niejawne muszą być schowane.



## **Rozdział 4.**

### **Bezpieczeństwo fizyczne**

#### **1. Obszar przetwarzania danych**

Urząd Gminy Rogóźno, Rogóźno 91 b jest to budynek wolnostojący, dwukondygnacyjny, murowany ze stropami żelbetowymi. Ciągi komunikacyjne od części biurowej oddzielone są ścianami z cegły palonej. Poszczególne pomieszczenia biurowe oddzielają ścianki działowe wykonane z cegły pełnej. Gmina Rogóźno jest właścicielem budynku. Pomieszczenia w obiekcie zajmowane są przez Urząd Gminy, a w części parterowej również przez Gminny Ośrodek Pomocy Społecznej w Rogóźnie i punkt kasowy Banku Spółdzielczego w Łasinie. Pomieszczenie do przetwarzania informacji niejawnych o klauzuli „zastrzeżone” przetwarza się w pomieszczeniach nr 12, a przechowuje w szafie metalowej w Kancelarii Dokumentów Niejawnych, (pomieszczenie nr 23). Pomieszczenia te położone są na piętrze budynku. W pokoju nr 12 otwierana jest jedynie korespondencja niejawna oraz podpisywane są dokumenty niejawne.

#### **2. Ochrona Bezpiecznej Stacji Komputerowej oraz nośników**

Ochrona Bezpiecznej Stacji Komputerowej oraz nośników jest wykonywana przez Pełnomocnika do spraw ochrony informacji niejawnych oraz przez Inspektora Bezpieczeństwa Teleinformatycznego

#### **4. Kontrola dostępu użytkowników do sprzętu**

Kontrola dostępu użytkowników do sprzętu wykonywana jest przez pracownika na stanowisku do spraw wojskowych i o.co.

#### **5. Zasady kontroli sprzętu**

Pełnomocnik do spraw informacji niejawnych odpowiedzialny jest za okresową kontrolę zgodności stanu faktycznego zainstalowanego sprzętu i oprogramowania z zapisami w Szczególnych Wymaganiach Bezpieczeństwa. Wyniki kontroli zapisuje w stosownej ewidencji kontroli.

## **Rozdział 5.**

### **Bezpieczeństwo dokumentów**

#### **1. Informacje ogólne**

Dokumentem jest każda forma nośnika informacji niejawnej, która została wytworzona lub przetworzona za pośrednictwem Bezpiecznej Stacji Komputerowej. Pojęcie dokumentu obejmuje nośniki papierowe, nośniki magnetyczne i optyczne, dyski twarde oraz pamięci stałe.

## 2. Wymiana informacji

W przypadku zaistnienia konieczności wymiany informacji, z wykorzystaniem dyskietek lub innych wymiennych nośników magnetycznych, z systemem lub sieci teleinformatycznej. funkcjonuje - w trybie innym niż "zastrzeżone", użytkownik musi postępować dokładnie wg poniższych zasad:

informacje niejawne mogą być importowane do Bezpiecznej Stacji Komputerowej z systemów teleinformatycznych o niższych klauzulach tajności. W tym celu użytkownik zabezpiecza przed zapisem wkładany do napędu nośnik oraz sprawdza dyskietka na obecność wirusa programem

antywirusowym. Użyty nośnik zachowuje swoją klasyfikację (etykiety) tajności. Przekazywanie informacji niejawnych z Bezpiecznej Stacji Komputerowej do systemów lub sieci teleinformatycznych o niższej klauzuli tajności jest zabronione. Zapisywanie informacji o niższych klauzulach tajności na dyskietki może być wykonane z wykorzystaniem licencjonowanych programów, którymi dokument utworzono lub modyfikowano.

## 3. Oznaczenie klasyfikacji dokumentów

Wszystkie dokumenty zawierające informacje niejawne oznaczane stosownie do klauzuli tajności informacji, które zawierają.

Oznaczenie dokumentu powinno być zgodne z wymogami zawartymi w:

- a) ustawie o ochronie informacji niejawnych z dnia 22 stycznia 1999 r.
- b) rozporządzeniu Ministrów Spraw Wewnętrznych i Administracji oraz Obrony Narodowej z dnia 26 lutego 1999 r. w sprawie sposobu oznaczania materiałów, w tym klauzulami tajności, oraz sposobu umieszczania klauzul na tych materiałach.

Wszystkie dokumenty (wydruki, dyskietki i dyski twarde) są zakwalifikowane jako informacje niejawne zgodnie z nadaną przez wykonawcę klauzulę tajności. Wydruki niejawne wprowadzane na drukarkę wykonawca ewidencjonuje i rejestruje w kancelarii tajnej.

## 4. Zmiana klasyfikacji dokumentów

Magnetyczne nośniki danych zawierające informacje niejawne stanowiące tajemnicy państwowej nie podlegają deklasyfikacji, są niszczone poprzez pocięcie lub spalanie, natomiast nośniki danych zawierające informacje niejawne stanowiące tajemnicy służbową mogą być deklasyfikowane.

## 5. Kontrola dokumentów

Wszystkie dokumenty niejawne muszą być zarejestrowane przez kancelarię do spraw ochrony informacji niejawnych. Inspektor Bezpieczeństwa Teleinformatycznego przeprowadza okresowe kontrole użytkowania Bezpiecznej Stacji Komputerowej.

Kontrola okresowa obejmuje w szczególności sprawdzenie przestrzegania przepisów o ochronie informacji niejawnych w zakresie ewidencji i obiegu dokumentów.

## 6. Niszczenie dokumentów

Niszczenie dokumentu niejawnego wykonuje się zgodnie z obowiązującymi przepisami w tym zakresie, wykorzystując do tego celu maszyny tnące na skrawki (niszczarka odpowiedniej klasy). Płyty CD-R1RW oraz uszkodzone nośniki me podlegają deklasyfikacji należy je zniszczyć fizycznie.

## 7. Biblioteka nośników

Kancelaria do Spraw Ochrony Informacji Niejawnych odpowiada za oznakowanie i ewidencję magnetycznych nośników danych użytkowników Bezpiecznej Stacji Komputerowej. Każdorazowe pobranie nośnika informacji przez użytkownika z kancelarii jest odnotowywane w rejestrze dokumentów użytkownika.

## 8. Dokumenty kontrolne

Administrator Systemu Teleinformatycznego zobowiązany jest posiadać listy użytkowników Bezpiecznej Stacji Komputerowej oraz według potrzeb inne dokumenty.

# **Rozdział 6.**

## **Bezpieczeństwo sprzętu i oprogramowania**

### 1. Informacje ogólne

Wykorzystywanie Bezpiecznej Stacji Komputerowej Urzędu do przetwarzania, składowania, wyświetlania, wykorzystywania nieautoryzowanych, prywatnie wytwarzanych lub pozyskanych danych lub programów jest zabronione.

### 2. Bezpieczeństwo sprzętu

Stanowisko komputerowe jest organizacyjnym i technicznym połączeniem elementów komputera, którego skład jest określony w dokumentacji urządzenia. Niedopuszczalne jest przemieszczanie lub zmiana jego konfiguracji. Zmiany lub modyfikacje konfiguracji i oprogramowania i sprzętu może dokonać Inspektor Systemu Teleinformatycznego. Inspektor Systemu Teleinformatycznego ma obowiązek codziennego sprawdzania czy nie ma żadnych zauważalnych oznak manipulowania przy sprzęcie. Wszelkie nieprawidłowości muszą być

niezwłocznie zgłoszone Inspektorowi Bezpieczeństwa Teleinformatycznego. Inspektor Systemu Teleinformatycznego ma obowiązek zablokowania dostępu do niewykorzystywanych portów Bezpiecznej Stacji Komputerowej. Bezpieczna Stacja Komputerowa podlega rutynowym czynnościom konserwacyjnym oraz przeglądom wykonywanym przez Inspektora Systemu Teleinformatycznego.

Należy odnotować uszkodzenia zestawu komputerowego oraz wykonane naprawy (np. przez autoryzowany serwis). Przekazanie urządzenia do zewnętrznego serwisu wymaga spełnienia następujących warunków:

- a) uzyskanie zgody pełnomocnika ochrony;
- b) sprzęt przekazuje się bez elementów (dyski, pamięci stale) zawierających informacje niejawne.

Każdorazowo, w wyniku przeprowadzonych przeglądów i napraw przeprowadza się diagnostykę urządzenia. Każdy przegląd jest odnotowywany w dokumentacji Inspektora Systemu Teleinformatycznego.

### 3. Bezpieczeństwo oprogramowania

Oprogramowanie instaluje wyłącznie Inspektor Systemu Teleinformatycznego. Dla ułatwienia kontroli nad konfiguracją oprogramowania, oprogramowanie Bezpiecznej Stacji Komputerowej jest identyfikowane poprzez nazwy, numer wersji i numer licencji. Oprogramowanie systemowe i użytkowe przechowuje Inspektor Systemu Teleinformatycznego. Używanie oprogramowania nie licencjonowanego oraz nie ujętego w wykazie Bezpiecznej Stacji Komputerowej jest kategorycznie zabronione. Wykaz aktualnie zainstalowanego oprogramowania znajduje się u Inspektora Systemu Teleinformatycznego.

Inspektor Systemu Teleinformatycznego jest zobowiązany do aktualizacji oprogramowania systemowego oraz użytkowego ujętego w Szczególnych Wymaganiach Bezpieczeństwa. Bezpieczeństwo Stacji Komputerowej jest realizowane programowo poprzez wykorzystanie mechanizmów bezpieczeństwa oferowanych przez system operacyjny:

- a) kontrola dostępu (umożliwienie dostępu osobom posiadającym odpowiedni identyfikator oraz znającym odpowiednie hasło dostępu);
- b) uwierzytelnienie (proces ustanawiania wiarygodności użytkownika);
- c) monitorowanie (kontrola zdarzeń, które mogą zagrozić bezpieczeństwu Stacji Komputerowej, m.in. kontrola kopiowania plików);

d) integralność (funkcje pozwalające określić i utrzymać dokładność oraz pewność powiązań pomiędzy danymi);

e) dostępność (zapewnienie dostępu do zasobów oraz umożliwienie ich użytkowania na żądanie uprawnionych osób w określonym czasie i miejscu);

Wniosek o uzyskanie dostępu do Bezpiecznej Stacji Komputerowej akceptuje pełnomocnik ochrony informacji niejawnych. Oprogramowanie antywirusowe (bazy danych o wirusach) jest aktualizowane przez Inspektora Systemu Teleinformatycznego w miarę pojawiania się nowych wersji biblioteki wirusów.

## **Rozdział 7.**

### **Bezpieczeństwo łączności**

#### **1. Bezpieczeństwo kryptograficzne**

Bezpieczeństwo łączności obejmuje sposób lokalizacji elementów łączności, takich jak np. telefony w wymaganej odległości od Bezpiecznej Stacji Komputerowej oraz zakaz włączania telefonów komórkowych w pomieszczeniu Bezpiecznej Stacji Komputerowej.

#### **2. Bezpieczeństwo elektromagnetyczne**

Przy korzystaniu z Bezpiecznego Stanowiska Komputerowego w Urzędzie Gminy Rogóźno przetwarzającym informacje o klauzuli "zastrzeżone" nie stosuje się zabezpieczenia kryptograficznego.

#### **3. Bezpieczeństwo transmisji**

Bezpieczne Stanowisko Komputerowe nie ma żadnych połączeń z innymi systemami lub sieciami teleinformatycznymi.

## **Rozdział 8.**

### **Monitorowanie bezpieczeństwa i kontrole**

Pełnomocnik ochrony do spraw informacji niejawnych oraz Inspektor Bezpieczeństwa Teleinformatycznego zobowiązani są do przeprowadzania okresowych kontroli systemu bezpieczeństwa podległej im Stacji Komputerowej. Nieprawidłowości lub rozbieżności wykryte podczas kontroli poddane są szczegółowym badaniom. Jeżeli naruszone zostały warunki bezpieczeństwa natychmiast muszą być zgłoszone do Pełnomocnika do Spraw

Ochrony Informacji Niejawnych. W przypadku naruszenia bezpieczeństwa Stacji Komputerowej należy o tym fakcie poinformować Inspektora Bezpieczeństwa Teleinformatycznego oraz Pełnomocnika do spraw informacji niejawnych Użytkownicy i osoby funkcyjne Bezpiecznej Stacji

Komputerowej zobowiązane są do udzielania pomocy organom śledczym podczas wyjaśniania naruszeń.

## **Rozdział 9.**

### **Plany awaryjne i zapobiegawcze**

#### **1. Konserwacje sprzętu i oprogramowania**

Bezpieczne Stanowisko Komputerowe podlega okresowym czynnościom konserwacyjnym oraz przeglądom sprzętu.

#### **2. Naprawa sprzętu**

Naprawa urządzenia Bezpiecznej Stacji Komputerowej wykonywana jest przez uprawniony personel techniczny. Naprawy gwarancyjne realizowane są przez serwis dostawcy sprzętu w miejscu zainstalowania sprzętu lub punkcie serwisowym dostawcy (producenta). Przekazanie urządzenia do naprawy wymaga uzyskania zgody pełnomocnika ochrony. Decyzja o potrzebie wykonania naprawy podejmuje Inspektor Systemu Teleinformatycznego po przeprowadzeniu testów diagnostycznych.

Przed rozpoczęciem naprawy Inspektor Systemu Teleinformatycznego sprawdza czy wszystkie niejawne wydruki oraz nośniki magnetyczne zostały usunięte oraz wyzerowane pamięci ulotne. Wszystkie czynności naprawcze muszą być odnotowane w karcie urządzenia(gwarancyjnej) przez osoby dokonujące naprawy. Wpis powinien zawierać daty naprawy, nazwisko osoby przeprowadzającej naprawy oraz podjęte przez tą osoby działania.

## **Rozdział 10.**

### **Plany awaryjne i zapobiegawcze**

#### **1. Zasilanie**

Bezpieczne Stanowisko Komputerowe jest zabezpieczone urządzeniem podtrzymującym zasilanie (zasilacz awaryjny UPS), które jest w stanie utrzymać pracę przez okres do 30 min.

#### **2. Kopie zapasowe**

Kopie archiwalne programów wykonuje i przechowuje Inspektor System Teleinformatycznego.

Kopie plików użytkowników wykonują użytkownicy i przechowują w przeznaczonym do tego sejfie.

#### **3. Klęski żywiołowe**

W przypadku wystąpienia klęski żywiołowej (pożaru, powodzi, itp.) należy zastosować się do aktualnie obowiązujących instrukcji przeciwpożarowych i ewakuacyjnych jednostki organizacyjnej zawartych w Planie Ochrony Informacji Niejawnych . Podstawową czynnością użytkowników

po zakończeniu pracy jest zabezpieczenie nośników informacji i wyłączenie Bezpiecznej Stacji Komputerowej.

#### 4. Sytuacje specjalne

W przypadku wystąpienia sytuacji nadzwyczajnych (atak terrorystyczny, zagrożenie ładunkiem wybuchowym, sabotaż itp.) należy zastosować się( do aktualnie obowiązujących procedur postępowania zawartych w Planie Ochrony Informacji Niejawnych Urzędu Gminy Rogóżno.

### **Rozdział 11.**

#### **Polityka antywirusowa**

##### 1. Informacje ogólne

Potrzeba wprowadzenia danych z zewnętrznego nośnika do Bezpiecznej Stacji Komputerowej jest zawsze związana z możliwością, wprowadzenia wirusa do środowiska, w którym przetwarzane są informacje niejawne. W związku z tym faktem zakupuje się lub aktualizuje oprogramowanie antywirusowe. W celu możliwie najskuteczniejszego zabezpieczenia się przed wprowadzeniem wirusa do Bezpiecznej Stacji Komputerowej definiuje się następujące środki zapobiegawcze:

- a) świadomość użytkownika,
- b) zasady higieny,
- c) kontrola dostępu.

##### 2. Świadomość użytkownika

Zabrania się użytkownikom używania lub uruchamiania nieautoryzowanego oprogramowania oraz danych z nośników niewiadomego pochodzenia. Może to doprowadzić do utraty danych lub ograniczenia funkcjonalności stacji poprzez infekcję stanowiska komputerowego wirusem.

##### 3. Zasady higieny

W celu ograniczenia możliwości infekcji oprogramowaniem złośliwym użytkownicy są zobowiązani do:

- użytkowania wyłącznie oprogramowania zainstalowanego przez Inspektora Systemu Teleinformatycznego;
- nie używania oprogramowania i danych niewiadomego pochodzenia np. pozyskanych z czasopism komputerowych;
- zgłaszania do Inspektora Systemu Teleinformatycznego potrzeb w zakresie instalacji dodatkowego oprogramowania;

- sprawdzania zewnętrznych nośników danych programem antywirusowym.

#### 4. Infekcja Stacji Komputerowej

Istnieją dwie zasadnicze drogi infekcji Bezpiecznej Stacji Komputerowej:

- a) używanie zainfekowanej dyskietki;
- b) uruchamianie zainfekowanego oprogramowania.

Dla uniknięcia ww. przypadków infekcji, uruchamianie nieautoryzowanego oprogramowania jest zabronione. W przypadku konieczności skorzystania z dyskietek, zawsze muszą one przed użyciem być przetestowane na obecność wirusa.

#### 5. Postępowanie w przypadku wykrycia wirusa

W przypadku wykrycia wirusa, na ekranie wyświetlony zostanie komunikat programu antywirusowego. Użytkownik Bezpiecznego Stanowiska Komputerowego ma obowiązek niezwłocznie powiadomić osoby funkcyjne systemu teleinformatycznego i wykonać czynności zgodnie z skróconą instrukcją programu antywirusowego: zapoznać się treścią komunikatu programu antywirusowego o wykrytym wirusie, nie kasowanie, nie kopiowanie, nie przenoszenie plików danych i nie niszczenie nośników danych (zachowane dowody), jeżeli wirus nie został usunięty przez program antywirusowy zaprzestanie dalszego przetwarzania informacji.



**Wniosek**  
**o przydzielenie konta w systemie informatycznym do przetwarzania informacji**  
**niejawnych o klauzuli "zastrzeżone"**

Imię i nazwisko	
Lokalizacja BSK(bezpiecznego stanowiska komputerowego)	
Stanowiska służbowe	
Komórka organizacyjna	
Nr pomieszczenia i Nr telefonu	
Poświadczenie bezpieczeństwa/zaświadczenie kierownika jednostki o dostępie do informacji niejawnych (numer , data ważności, klauzula tajności)	
Zaświadczenie o odbyciu szkolenia podstawowego z zakresu Ochrony Informacji Niejawnych	
Pełnomocnik ds Ochrony Informacji Niejawnych	
Nazwa użytkownika	
Okres ważności konta (dokładna data)	
Hasło	

**WYKAZ UZYTEKOWNIKOW  
BEZPIECZNEGO STANOWISKA KOMPUTEROWEGO**

Lp.	Nazwisko i Imię	Stanowisko	Data przydzielenia uprawnień	Data wygaśnięcia uprawnień	podpis