ZARZĄDZENIE NR 149/14
WÓJTA GMINY GRÓDEK

z dnia 3 lipca 2014 r.

w sprawie zatwierdzenia „Planu ochrony informacji niejawnych w Urzędzie Gminy Gródek”

Na podstawie art. 15 ust. 1 pkt 5 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228 z późn. zm.) zarządzam, co następuje:

§ 1. W celu zapewnienia przestrzegania przepisów ustawy o ochronie informacji niejawnych w Urzędzie Gminy Gródek, zatwierdzam opracowany przez Pełnomocnika do spraw Ochrony Informacji Niejawnych „Plan ochrony informacji niejawnych w Urzędzie Gminy Gródek”, stanowiący załącznik do niniejszego zarządzenia.

§ 2. Nadzór nad realizacją niniejszego zarządzenia powierzam Pełnomocnikowi do spraw Ochrony Informacji Niejawnych.

§ 3. Zarządzenie wchodzi w życie z dniem podpisania.

Załącznik do Zarządzenia Nr 149/14
Wójta Gminy Gródek
z dnia 3 lipca 2014 r.

Urząd Gminy Gródek
ul. A. i G. Chodkiewiczów 2
16-040 Gródek

Zatwierdzam:

PLAN
OCHRONY INFORMACJI NIEJAWNYCH
W URZĘDZIE GMINY GRÓDEK

OPRACOWAŁ:
Pełnomocnik ds. ochrony
informacji niejawnych
Dorota Bójko

Gródek, lipiec 2014 r.

SPIS TREŚCI

I. Podstawy prawne ochrony informacji niejawnych ***(str. – 3)***

II. Definicje w rozumieniu Planu ochrony informacji niejawnych ***(str. – 4)***

III. Przedmiot ochrony ***(str. – 5)***

IV. Charakterystyka budynku i stref ochronnych ***(str. – 6)***

V. Klasyfikacja informacji niejawnych ***(str. – 8)***

VI. Ewidencja informacji niejawnych ***(str. – 8)***

VII. Dostęp do informacji niejawnych oznaczonych klauzulą „zastrzeżone"***(str. – 9)***

VIII. Kancelaria materiałów niejawnych ***(str. – 10)***

IX. Zasady wykonywania dokumentów niejawnych ***(str. – 14)***

X. Wykonywanie dokumentów zawierających informacje niejawne sprzętu komputerowego ***(str. – 15)***

XI. Gromadzenie dokumentów zawierających informacje niejawne ***(str. – 17)***

XII. Oznaczanie, nadawanie, zmiana i znoszenie klauzuli niejawności materiałom niejawnym ***(str. – 18)***

XIII. Ocena zagrożeń zewnętrznych i wewnętrznych ***(str. – 19)***

XIV. Nadzór w zakresie ochrony informacji niejawnych ***(str. – 22)***

XV. Odpowiedzialność karna, dyscyplinarna i służbowa za naruszenie przepisów o ochronie informacji niejawnych ***(str. – 23)***

XVI. Archiwizowanie, gromadzenie i niszczenie materiałów niejawnych ***(str. – 23)***

XVII. Ustalenia końcowe ***(str. – 26)***

Załączniki do Planu:

1. **Załącznik Nr 1** – Instrukcja przechowywania kluczy i pieczęci ***(str. – 27)***
2. **Załącznik nr 2** - Instrukcja postępowania w sytuacjach kryzysowych i stanach nadzwyczajnych ***(str. – 28)***
3. **Załącznik nr 3** - Instrukcja alarmowa w przypadku zgłoszenia o podłożeniu lub znalezieniu ładunku wybuchowego w budynkach Urzędu ***(str. – 30)***
4. **Załącznik nr 4** - Instrukcja postępowania w przypadku otrzymania przesyłki niewiadomego pochodzenia ***(str. – 33)***

ROZDZIAŁ I
PODSTAWY PRAWNE OCHRONY INFORMACJI NIEJAWNYCH

Plan ochrony informacji niejawnych w Urzędzie Gminy Gródek określa zasady i tryb postępowania z informacjami niejawnymi oraz zapewnia jednolity sposób postępowania z tymi informacjami w Urzędzie Gminy Gródek.

Akty prawne regulujące ochronę informacji niejawnych:

- ✓ **Ustawa** z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2010, Nr 182, poz. 1228);
- ✓ **Rozporządzenie Prezesa Rady Ministrów** z dnia 28 grudnia 2010 r. w sprawie przekazywania informacji, udostępniania dokumentów oraz udzielania pomocy służbom i instytucjom uprawnionym do prowadzenia poszerzonych postępowań sprawdzających, kontrolnych postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego (Dz. U. z 2010, Nr 258, poz. 1750);
- ✓ **Rozporządzenie Prezesa Rady Ministrów** z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności (Dz. U. z 2011 r., Nr 288, poz. 1692);
- ✓ **Rozporządzenie Prezesa Rady Ministrów** z dnia 20 lipca 2011 r. w sprawie wzoru świadectwa akredytacji bezpieczeństwa systemu teleinformatycznego (Dz. U. z 2011 r., Nr 156, poz. 926);
- ✓ **Rozporządzenie Prezesa Rady Ministrów** z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. z 2011 r., Nr 159, poz. 948);
- ✓ **Rozporządzenie Prezesa Rady Ministrów** z dnia 27 kwietnia 2011 r. w sprawie przygotowania i przeprowadzania kontroli stanu zabezpieczenia informacji niejawnych (Dz. U. z 2011 r., Nr 93 poz. 541);
- ✓ **Rozporządzenie Prezesa Rady Ministrów** z dnia 28 grudnia 2010 r. w sprawie wzorów zaświadczeń stwierdzających odbycie szkolenia w zakresie ochrony informacji niejawnych oraz sposobu rozliczania kosztów przeprowadzenia szkolenia przez Agencję Bezpieczeństwa Wewnętrznego lub Służbę Kontrwywiadu Wojskowego (Dz. U. z 2010, Nr 258, poz. 1751);
- ✓ **Rozporządzenie Prezesa Rady Ministrów** z dnia 28 grudnia 2010 r. w sprawie wzorów poświadczeń bezpieczeństwa (Dz. U. z 2010, Nr 258, poz. 1752);
- ✓ **Rozporządzenie Prezesa Rady Ministrów** z dnia 28 grudnia 2010 r. w sprawie wzoru decyzji o odmowie wydania poświadczenia bezpieczeństwa (Dz. U. z 2010, Nr 258, poz. 1753);

- ✓ **Rozporządzenie Prezesa Rady Ministrów** z dnia 28 grudnia 2010 r. w sprawie wzoru decyzji o cofnięciu poświadczenia bezpieczeństwa (Dz. U. z 2010, Nr 258, poz. 1754);
- ✓ **Rozporządzenie Prezesa Rady Ministrów** z dnia 7 grudnia 2011 r. w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych (Dz. U. z 2011 r., Nr 276, poz. 1631);
- ✓ **Rozporządzenie Prezesa Rady Ministrów** z dnia 7 grudnia 2011 r. w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne (Dz. U. z 2011 r., Nr 271, poz. 1603);
- ✓ **Rozporządzenie Ministra Sprawiedliwości** z dnia 20 lutego 2012 r. w sprawie sposobu postępowania z protokołami przesłuchań i innymi dokumentami lub przedmiotami, na które rozciąga się obowiązek zachowania w tajemnicy informacji niejawnych albo zachowania tajemnicy związanej z wykonywaniem zawodu lub funkcji (Dz. U. z 2012 r. poz. 219);
- ✓ **Rozporządzenie Rady Ministrów** z dnia 19 czerwca 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych (Dz. U. z 2012 r., Nr 271, poz. 1603).

ROZDZIAŁ II
DEFINICJE W ROZUMIENIU PLANU OCHRONY INFORMACJI NIEJAWNYCH

W rozumieniu planu ochrony informacji niejawnych:

- ✓ **ustawą** jest ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2010, Nr 182, poz. 1228);
- ✓ **rękojmia zachowania tajemnicy** oznacza spełnienie przez osobę ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem, stwierdzona w wyniku przeprowadzenia postępowania sprawdzającego;
- ✓ **dokumentem** jest każda utrwalona informacja niejawna;
- ✓ **materiałem** jest dokument lub przedmiot, albo dowolna ich część, chronione jako informacja niejawna a zwłaszcza urządzenie, wyposażenie lub broń wyprodukowana albo będąca w trakcie produkcji, a także składnik użyty do ich wytworzenia;
- ✓ **przetwarzaniem informacji niejawnych** są wszelkie operacje wykonywane w odniesieniu do informacji niejawnych i na tych informacjach, w szczególności ich wytwarzanie, modyfikowanie, kopiowanie, klasyfikowanie, gromadzenie, przechowywanie, przekazywanie lub udostępnianie;

- ✓ **systemem teleinformatycznym** jest zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie danych;
- ✓ **akredytacją bezpieczeństwa teleinformatycznego** jest dopuszczenie systemu teleinformatycznego do przetwarzania informacji niejawnych;
- ✓ **dokumentacją bezpieczeństwa systemu teleinformatycznego** jest dokument szczególnych wymagań bezpieczeństwa oraz dokument procedur bezpiecznej eksploatacji systemu teleinformatycznego, opracowane zgodnie z zasadami określonymi w ustawie;
- ✓ **dokumentem elektronicznym** jest dokument przetwarzany w systemie teleinformatycznym podlegający rejestracji w odpowiedniej ewidencji przed przekazaniem go drogą elektroniczną;
- ✓ **dokumentem nieelektronicznym** jest dokument utrwalony na nośniku innym, niż informatyczny nośnik danych, podlegający rejestracji w odpowiedniej ewidencji;
- ✓ **Kancelarią** jest Kancelaria Materiałów Niejawnych w Urzędzie Gminy Gródek;
- ✓ **Urzędem** jest Urząd Gminy Gródek;
- ✓ **Wójtem** jest Wójt Gminy Gródek;
- ✓ **Pełnomocnikiem Ochrony** jest Pełnomocnik do spraw Ochrony Informacji Niejawnych w Urzędzie Gminy Gródek.

ROZDZIAŁ III
PRZEDMIOT OCHRONY

Przedmiotem ochrony w Urzędzie Gminy Gródek, są:

- ➢ informacje niejawne oznaczone klauzulą „zastrzeżone”,
- ➢ pomieszczenia, w których są przechowywane i opracowane materiały niejawne,
- ➢ autonomiczne stanowisko komputerowe przeznaczone do przetwarzania, wytwarzania i przechowywania informacji niejawnych o klauzuli „zastrzeżone”.

ROZDZIAŁ IV
CHARAKTERYSTYKA BUDYNKU I STREF OCHRONNYCH

1. Charakterystyka budynku

1) Pomieszczenia, w których przetwarzane są materiały niejawne oznaczone klauzulą „zastrzeżone”, usytuowane są na parterze dwukondygnacyjnego budynku murowanego zlokalizowanego w Gródku, przy ul. Fabrycznej 8. Budynek jest siedzibą: Urzędu Stanu Cywilnego, Gminnego Ośrodka Pomocy Społecznej oraz Przedszkola Samorządowego. Poza tym, w budynku swoje siedziby mają: gabinet stomatologiczny oraz biuro usług księgowych.
2) Ściany budynku są murowane, a strop i podłoga stanowi konstrukcję żelbetową.
3) Teren wokół budynku ogrodzony jest metalowym ogrodzeniem wysokości ok. 1,6 m.
4) Do pomieszczeń Urzędu Stanu Cywilnego w Gródku, w którym przetwarzane są informacje niejawne, prowadzi odrębne wejście, zamykane na dwa zamki.
5) Ogólnodostępny parking usytuowany jest za ogrodzeniem po południowej stronie budynku. Od północnej strony na bezpośrednio sąsiadującej działce w odległości ok. 100 m od budynku, płynie rzeka Supraśl, zaś od zachodu umiejscowiony jest plac zabaw dostępny jedynie dla dzieci z miejscowego przedszkola.
6) Budynek jest wyposażony w system alarmowy i okratowanie stalowe w każdym oknie.

2. Ochrona fizyczna budynku i pomieszczeń

1) Budynek i znajdujące się w nim pomieszczenia stanowiące siedzibę Urzędu, podlegają ochronie. Ochrona fizyczna polega na stałym monitoringu budynku i znajdujących się w nim pomieszczeń poprzez system alarmowy.
2) Kody do instalacji alarmowej do budynku Urzędu, w którym są przetwarzane informacje niejawne, posiadają: Wójt, Pełnomocnik Ochrony oraz Kierownik Kancelarii Materiałów Niejawnych. Kody zmienia się co najmniej raz w roku, a także w przypadku:
   - każdej zmiany składu osób znających kod;
   - zaistnienia podejrzenia, że osoba nieuprawniona mogła poznać kod;
   - gdy zamek poddano konserwacji lub naprawie.

3) Klucze do Kancelarii Materiałów Niejawnych oraz szaf, mogą być udostępnione tylko tym osobom, którym posiadanie kluczy jest niezbędne do wykonywania obowiązków służbowych.
4) Klucze od szaf metalowych Kancelarii Materiałów Niejawnych po zakończeniu pracy są składane w pomieszczeniu Kancelarii w miejscu niewidocznym.
5) Pomieszczenia, w których znajdują się informacje niejawne z klauzulą „zastrzeżone” po godzinach pracy są zamykane, a klucze zabierane i umieszczane w miejscu niewidocznym w wyznaczonym pomieszczeniu.
6) Tworzy się zapasowy komplet kluczy od pomieszczeń Kancelarii Materiałów Niejawnych, który jest zdeponowany w szafie metalowej u Wójta.
7) Sprzątanie pomieszczeń, w których są przechowywane informacje niejawne odbywa się w obecności upoważnionego pracownika przed zakończeniem pracy.

3. Opis strefy ochronnej

1) Informacje niejawne o klauzuli „zastrzeżone” przetwarza się w pomieszczeniu lub obszarze wyposażonych w system kontroli dostępu i przechowuje się w szafie metalowej, pomieszczeniu wzmocnionym lub zamkniętym na klucz meblu biurowym.
2) W celu zapewnienia skutecznej ochrony informacji niejawnych, w Urzędzie zastosowano środki bezpieczeństwa fizycznego oraz wydzielono strefę ochronną, w której wprowadzono system kontroli wejść i wyjść oraz określono uprawnienia do przebywania strefie.
3) Strefa ochronna obejmuje pomieszczenie Kancelarii Materiałów Niejawnej, w której przetwarzane są informacje niejawne o klauzuli „zastrzeżone”. Dostęp do strefy skutkuje uzyskaniem bezpośredniego dostępu do tych informacji.
4) W strefie mogą pracować lub pełnić służbę osoby posiadające poświadczenia bezpieczeństwa, upoważniające do dostępu do informacji niejawnych o klauzuli odpowiadającej co najmniej klauzuli najwyżej sklasyfikowanej informacji przetwarzanej w tej strefie i zaświadczenie o szkoleniu na temat ochrony informacji niejawnych oraz kontrolerzy badający funkcjonowanie systemu ochrony informacji niejawnych.
5) Wstęp osób bez wymaganych uprawnień do strefy może nastąpić po uzyskaniu zgody Wójta lub uprawnionej przez niego osoby i pod nadzorem upoważnionego pracownika, pod warunkiem zabezpieczenia informacji niejawnych w sposób uniemożliwiający ich przypadkowe ujawnienie.
6) Granice strefy ochronnej stanowią ściany zewnętrzne i wewnętrzne budynku, które zabezpieczają cały obwód strefy.

7) Drzwi do strefy ochronnej są stale zamknięte. Otwarte mogą być wyłącznie przez Wójta, Pełnomocnika Ochrony bądź Kierownika Kancelarii Materiałów Niejawnych.
8) Wprowadzony system kontroli dostępu do strefy pozwala na wstęp osób, które posiadają odpowiednie uprawnienie do dostępu do informacji niejawnych, w zakresie niezbędnym do wykonywania pracy lub pełnienia służby albo wykonywania czynności zleconych.
9) W strefie ochronnej zlokalizowane są:
   - Kancelaria Materiałów Niejawnych,
   - Bezpieczne Stanowisko Komputerowe.

ROZDZIAŁ V
KLASYFIKACJA INFORMACJI NIEJAWNYCH

Informacjom niejawnym nadaje się klauzulę **„zastrzeżone”** jeżeli nie nadano im wyższej klauzuli tajności, a ich nieuprawnione ujawnienie może mieć szkodliwy wpływ na wykonywanie przez organy władzy publicznej lub inne jednostki organizacyjne zadań w zakresie obrony narodowej, polityki zagranicznej, bezpieczeństwa publicznego, przestrzegania praw i wolności obywateli, wymiaru sprawiedliwości albo interesów ekonomicznych Rzeczypospolitej Polskiej.

ROZDZIAŁ VI
EWIDENCJA INFORMACJI NIEJAWNYCH

1. Ewidencjonowanie oraz wszelkie zasady postępowania z dokumentami zawierającymi informacje niejawne oznaczone klauzulą „zastrzeżone”, określa opracowana przez Pełnomocnika Ochrony *„Instrukcja dotycząca sposobu i trybu przetwarzania informacji niejawnych o klauzuli "zastrzeżone" oraz zakresu i warunków stosowania środków bezpieczeństwa fizycznego w celu ich ochrony w Urzędzie Gminy Gródek"*, zatwierdzona odrębnym zarządzeniem Wójta.

2. Ewidencją objęte są dokumenty zastrzeżone zarówno otrzymane jak i wytworzone w Urzędzie. Dokumenty te ewidencjonowane są we właściwym dzienniku ewidencji dokumentów, który prowadzi Kierownik Kancelarii Materiałów Niejawnych, a w razie jego nieobecności upoważniony pracownik.

3. Dokumenty niejawne oznaczone klauzulą „zastrzeżone” wpływające pocztą lub dostarczone kurierem na adres Urzędu Gminy w zaklejonych dwóch kopertach (zewnętrznej i wewnętrznej) odbierane są za pokwitowaniem w Sekretariacie Urzędu Gminy, rejestrowane są w dzienniku korespondencji bez otwierania koperty wewnętrznej, a następnie niezwłocznie przekazywane Kierownikowi Kancelarii Materiałów Niejawnych.
4. Kierownik Kancelarii Materiałów Niejawnych, ewidencjonuje zastrzeżony dokument w dzienniku ewidencji, a następnie przekazuje go, po uzyskaniu potwierdzenia przyjęcia dokumentu do konkretnego pracownika odpowiedzialnego za załatwienie sprawy.
5. Numer ewidencyjny każdego dokumentu niejawnego stanowiącego o klauzuli „zastrzeżone” powinien być poprzedzony skrótem literowym „Z”.
6. Ewidencjonowaniu podlegają wszystkie dokumenty niejawne, oznaczone klauzulą „zastrzeżone”.

ROZDZIAŁ VII
DOSTĘP DO INFORMACJI NIEJAWNYCH OZNACZONYCH KLAUZULĄ „ZASTRZEŻONE”

1. Informacje niejawne oznaczone klauzulą „zastrzeżone” mogą być udostępniane wyłącznie osobie uprawnionej do dostępu do informacji niejawnych o określonej klauzuli niejawności, wyłącznie w zakresie niezbędnym do wykonywania przez nią pracy na zajmowanym stanowisku.
2. Uzyskanie uprawnień dostępu do informacji niejawnych o klauzuli „zastrzeżone” może nastąpić:
   - po uzyskaniu przez pracownika upoważnienia do dostępu do informacji niejawnych oznaczonych klauzulą „zastrzeżone” wydanego przez Wójta,
   - po przeszkoleniu danej osoby w zakresie przepisów ustawy o ochronie informacji niejawnych i uzyskaniu odpowiedniego zaświadczenia.

ROZDZIAŁ VIII
KANCELARIA MATERIAŁÓW NIEJAWNYCH

1. W Urzędzie funkcjonuje Kancelaria Materiałów Niejawnych, która została utworzona dla potrzeb Urzędu, dla właściwego przechowywania, ewidencjonowania materiałów niejawnych.
2. Organizacja pracy Kancelarii Materiałów Niejawnych zapewnia możliwość ustalenia w każdych okolicznościach, gdzie znajduje się materiał niejawny pozostający w dyspozycji jednostki organizacyjnej oraz kto z tym materiałem się zapoznał.
3. Kancelaria Materiałów Niejawnych odmawia udostępnienia lub wydania materiału osobie nieuprawnionej.
4. Kancelarię Materiałów Niejawnych tworzy Wójt.
5. Kancelarią kieruje Kierownik Kancelarii Materiałów Niejawnych, wyznaczany przez Wójta na wniosek Pełnomocnika Ochrony.
6. Do podstawowych zadań Kierownika Kancelarii Materiałów Niejawnych należy:
    a) bezpośredni nadzór nad obiegiem dokumentów,
    b) udostępnianie lub wydawanie dokumentów osobom do tego uprawnionym, które zapewniają odpowiednie warunki do ich przechowywania,
    c) egzekwowanie zwrotu udostępnionych lub wydanych materiałów niejawnych,
    d) prowadzenie bieżącej kontroli postępowania z dokumentami,
    e) niezwłoczne powiadamianie Pełnomocnika Ochrony w przypadku naruszenia przepisów o postępowaniu z materiałami niejawnymi,
    f) zapewnienie ochrony przechowywanym materiałom niejawnych, przewidzianej w obowiązujących przepisach,
    g) dokonywanie na bieżąco i w sposób czytelny wpisów w dzienniku ewidencji,
    h) przygotowywanie i pakowanie zgodnie z obowiązującymi przepisami dokumentów przeznaczonych do wysyłki,
    i) prowadzenie Kancelarii Materiałów Niejawnych,
    j) wykonywanie poleceń Pełnomocnika Ochrony.
7. W przypadku zmiany na stanowisku Kierownika Kancelarii Materiałów Niejawnych sporządza się protokół zdawczo-odbiorczy. Protokół, sporządza się w obecności pracownika zdającego obowiązki, osoby przejmującej obowiązki oraz Pełnomocnika Ochrony. Protokół sporządza się w dwóch egzemplarzach

- pierwszy egzemplarz przechowywany jest w Kancelarii Materiałów Niejawnych, drugi - u Pełnomocnika Ochrony.

8. W przypadku czasowej nieobecności Kierownika Kancelarii jego obowiązki przejmuje protokolarnie inny pracownik wyznaczony przez Wójta.
9. W pomieszczeniach Kancelarii można wydzielić miejsce, w którym osoby upoważnione mogą zapoznawać się z dokumentami – czytelnię.
    a) czytelnia powinna być zorganizowana w sposób umożliwiający stały nadzór ze strony pracownika kancelarii,
    b) w czytelni zabrania się instalowania systemu nadzoru wizyjnego.
10. Dokumenty i materiały oznaczone różnymi klauzulami tajności są przechowywane w odrębnych szafach lub pomieszczeniach, chyba że wchodzą one w skład zbioru dokumentów.
11. Po zakończeniu pracy Kierownik Kancelarii Materiałów Niejawnych lub upoważniony pracownik Kancelarii Materiałów Niejawnych jest obowiązany sprawdzić prawidłowość zamknięcia szaf i pomieszczeń Kancelarii.
12. Zasady i sposób zdawania, przechowywania i wydawania kluczy oraz ich duplikatów do pomieszczeń oraz szaf Kancelarii Materiałów Niejawnych, a także zasady ustalania, zmiany i deponowania haseł lub szyfrów, w przypadku stosowania zamków szyfrowych, określa Plan Ochrony Informacji Niejawnych.
13. Wszelkie nieprawidłowości związane z naruszeniem zasad, określonych powyżej należy niezwłocznie zgłaszać Pełnomocnikowi Ochrony.
14. Zasady określone obowiązują odpowiednio w stosunku do innych pomieszczeń, w których są przechowywane dokumenty lub materiały, oraz osób za te pomieszczenia odpowiedzialnych.
15. W Kancelarii Materiałów Niejawnych przyjmuje się, rejestruje, przechowuje, przekazuje i wysyła dokumenty niejawne oraz prowadzi:
    a) rejestr dzienników, książek ewidencyjnych i teczek,
    b) dziennik ewidencji,
    c) książkę doręczeń przesyłek miejscowych.
16. W przypadkach uzasadnionych organizacją ochrony informacji niejawnych, Kancelaria może prowadzić także inne rejestry niż wyżej wymienione, w tym odrębne rejestry dla dokumentów oznaczonych różnymi klauzulami tajności – np. kartę zapoznania się z dokumentem niejawnym oznaczonym klauzulą „poufne”.

POSTĘPOWANIE Z PRZESYŁKAMI PRZYCHODZĄCYMI:

1. Kierownik Kancelarii Materiałów Niejawnych przyjmuje przesyłki lub dokumenty za pokwitowaniem i odciska na nich pieczęć oraz datę wpływu do Kancelarii.
2. Przyjmując przesyłkę, sprawdza:
   a) prawidłowość adresu,
   b) całość pieczęci i opakowania,
   c) zgodność odcisku pieczęci na opakowaniu z nazwą jednostki nadawcy,
   d) zgodność numeru na przesyłce z numerem tej przesyłki w wykazie lub w książce doręczeń.
3. W przypadku stwierdzenia uszkodzenia przesyłki lub śladów jej otwierania, Kierownik Kancelarii Materiałów Niejawnych kwitujący odbiór przesyłki sporządza, wraz z doręczającym, protokół uszkodzenia. Jeden egzemplarz protokołu przekazuje się nadawcy, drugi Pełnomocnikowi Ochrony w Urzędzie, a w przypadku gdy w obiegu przesyłek pośredniczył przewoźnik - kolejny egzemplarz protokołu przekazuje się także jemu.
4. Po otwarciu przesyłki Kierownik Kancelarii Materiałów Niejawnych:
   a) sprawdza, czy zawartość przesyłki odpowiada wyszczególnionym na niej numerom ewidencyjnym,
   b) ustala, czy liczba załączników i stron jest zgodna z liczbą oznaczoną na poszczególnych dokumentach.
5. W przypadku stwierdzenia nieprawidłowości Kierownik Kancelarii Materiałów Niejawnych sporządza w dwóch egzemplarzach protokół z otwarcia przesyłki zawierający opis nieprawidłowości, jeden egzemplarz przekazując do Kancelarii nadawcy.
6. Kierownik Kancelarii odnotowuje fakt sporządzenia protokołu, o którym mowa w pkt. 3 i 5, w odpowiednim dzienniku w rubryce „Informacje uzupełniające/Uwagi”.
7. W Kancelarii nie otwiera się przesyłek oznaczonych „do rąk własnych”. W odpowiednim dzienniku wpisuje się nadawcę, numer i datę wpływu dokumentu. W rubryce „Informacje uzupełniające/Uwagi” odnotowuje się, że przesyłka była oznaczona „do rąk własnych”.
8. Na opakowaniu przesyłek wpisuje się datę wpływu, pozycję i numer, pod którym zarejestrowano przesyłkę. Przesyłkę przekazuje się - za pokwitowaniem - bezpośrednio adresatowi, a w razie jego nieobecności - osobie przez niego upoważnionej do odbioru.
9. Zatrzymanie przez adresata dokumentu, adresowanego "do rąk własnych", odnotowuje się w rubryce „Informacje uzupełniające/Uwagi”.

10. W przypadku zwrotu do Kancelarii przesyłki, adresowanej „do rąk własnych”, Kierownik Kancelarii uzupełnia dane dotyczące przesyłki w odpowiednim dzienniku.
11. Jeżeli adresat podjął decyzję o przechowywaniu przesyłki „do rąk własnych” w Kancelarii w stanie zamkniętym, Kierownik Kancelarii dokonuje czynności, o których mowa w pkt. 10, przy udziale adresata. Przesyłka jest w takim przypadku przechowywana w formie zapieczętowanego pakietu, a fakt ten odnotowuje się w rubryce „Informacje uzupełniające/Uwagi”.
12. Przesyłki pilne, telegramy i szyfrogramy doręcza się adresatom bezzwłocznie. Przy kwitowaniu odbioru tych przesyłek odnotowuje się godzinę doręczenia.
13. Otrzymaną i wysyłaną przesyłkę bądź wytworzony dokument rejestruje się odpowiednio w kolejności wytworzenia lub otrzymania.
14. Wszelkich adnotacji w dziennikach ewidencyjnych dokonuje się atramentem lub tuszem w kolorze niebieskim lub czarnym. Zmian dokonuje się kolorem czerwonym, umieszczając datę i czytelny podpis dokonującego zmiany.
15. Zabrania się wycierania, zamazywania lub nadpisywania zapisów dokonanych w dziennikach ewidencyjnych.
16. Dokumenty, materiały oraz zbiory dokumentów dotyczące spraw ostatecznie zakończonych przechowuje się w Kancelarii jako materiały archiwalne.

POSTĘPOWANIE Z PRZESYŁKAMI WYCHODZACYMI:

1. Kierownik Kancelarii Materiałów Niejawnych po otrzymaniu dokumentu niejawnego do wysłania, przed jego zarejestrowaniem, sprawdza, jaką posiada klauzulę tajności oraz czy dokument:
    a) odpowiada wymogom formalnym;
    b) wytworzono go w takiej ilości egzemplarzy jak podano w rozdzielniku (dotyczy również załączników);
    c) zawiera dane określające faktyczną ilość załączników i ich arkuszy;
    d) podpisała go osoba upoważniona.
2. W razie niedopełnienia jednego z warunków opisanych wyżej, Kierownik Kancelarii zwraca dokument wykonawcy celem uzupełnienia lub poprawienia.
3. W przypadku wykonania dokumentu w dwóch egzemplarzach, Kierownik Kancelarii wysyła pierwszy egzemplarz do adresata, drugi pozostawia w aktach Urzędu.

4. Dokumenty wykonane w trzech lub więcej egzemplarzach, Kierownik Kancelarii wysyła wg zamieszczonego rozdzielnika na każdym egzemplarzu pisma lub wg rozdzielnika stałego, przy czym egzemplarz Nr 1, pozostaje w aktach nadawcy.
5. Dokument wykonany w egzemplarzu pojedynczym, Kierownik Kancelarii wysyła do adresata, czyniąc adnotację w kolumnie „Uwagi" dziennika korespondencji - „Adresat".
6. Po zaewidencjonowaniu dokument jest pakowany do drugiej koperty i kierowany wraz z wykazem przesyłek nadanych do Sekretariatu Urzędu Gminy celem zarejestrowania w dzienniku korespondencji wychodzącej i wysłania do adresata.
7. Fakt wysłania dokumentu wykonanego w Urzędzie Gminy odnotowywany jest w dzienniku ewidencji.

OBOWIĄZKI OSÓB FUNKCYJNYCH:

1. Przed otwarciem drzwi sprawdzić stan zamków i zabezpieczenie drzwi.
2. Sprawdzić stan zabezpieczeń szaf i sprzętu komputerowego.
3. Przestrzegać zasad zakazu wstępu osobom nieuprawnionym do Kancelarii Materiałów Niejawnych.
4. W miarę możliwości niezbędne sprawy załatwiać w strefie bezpieczeństwa.
5. Stosować zasadę, że do Kancelarii wstęp mogą mieć tylko osoby upoważnione lub posiadające poświadczenie bezpieczeństwa.

ROZDZIAŁ IX
ZASADY WYKONYWANIA DOKUMENTÓW NIEJAWNYCH

1. Propozycje przyznania klauzuli niejawności na wykonywanym dokumencie przedstawia osoba sporządzająca dokument.
2. Klauzulę niejawności na danym dokumencie przyznaje osoba, która jest upoważniona do podpisania dokumentu.
3. Rękopisy sporządzanych dokumentów niejawnych powinny być opracowywane w brulionach (zeszytach pracy) uprzednio zarejestrowanych w Kancelarii Materiałów Niejawnych.
4. Dokumenty niejawne powinny być opisane i oznaczone zgodnie Rozporządzeniem Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności (Dz. U. z 2011 r., Nr 288, poz. 1692).

ROZDZIAŁ X

WYKONYWANIE DOKUMENTÓW ZAWIERAJĄCYCH INFORMACJE NIEJAWNE Z WYKORZYSTANIEM SPRZĘTU KOMPUTEROWEGO

1. Do wytwarzania i przetwarzania dokumentów zawierających informacje niejawne o klauzuli „zastrzeżone" w Urzędzie, może być wykorzystywany wyłącznie System Teleinformatyczny posiadający akredytację bezpieczeństwa teleinformatycznego nadaną przez Wójta.
2. Pracownicy, którzy do opracowywania i wykonywania dokumentów zawierających informacje oznaczone klauzulą „zastrzeżone", wykorzystują urządzenia komputerowe, obowiązani są zabezpieczać informacje podlegające ochronie przed ich nieuprawnionym ujawnieniem, a także przed dotarciem do tych informacji przez osoby, które nie powinny zapoznać się z ich treścią.
3. Bezpieczeństwo teleinformatyczne zapewnia się, chroniąc informacje przetwarzane w systemach teleinformatycznych przed utratą właściwości gwarantujących to bezpieczeństwo, w szczególności przed utratą poufności, dostępności i integralności.
4. Bezpieczeństwo teleinformatyczne zapewnia się przed rozpoczęciem oraz w trakcie przetwarzania informacji niejawnych w systemie teleinformatycznym.
5. Za właściwą organizację bezpieczeństwa teleinformatycznego odpowiada Wójt, który w szczególności:
   - zapewnia opracowanie dokumentacji bezpieczeństwa teleinformatycznego,
   - realizuje ochronę fizyczną, elektromagnetyczną i kryptograficzną systemu teleinformatycznego,
   - zapewnia niezawodność transmisji oraz kontrolę dostępu do urządzeń systemu teleinformatycznego,
   - dokonuje analizy stanu bezpieczeństwa teleinformatycznego oraz zapewnia usunięcie stwierdzonych nieprawidłowości,
   - zapewnia przeszkolenie z zakresu bezpieczeństwa teleinformatycznego dla osób uprawnionych do pracy w systemie lub sieci teleinformatycznej.
6. Ochrona fizyczna systemu lub sieci teleinformatycznej polega na:
   - umieszczeniu urządzeń systemu teleinformatycznego w strefie bezpieczeństwa, strefie administracyjnej lub specjalnej strefie bezpieczeństwa, zwanych dalej „strefą kontrolowanego dostępu” w zależności od:

- ✓ klauzuli tajności,
- ✓ ilości,
- ✓ zagrożeń dla poufności, integralności lub dostępności informacji niejawnych,

➢ zastosowaniu środków zapewniających ochronę fizyczną, w szczególności przed:

- ✓ nieuprawnionym dostępem,
- ✓ podglądem,
- ✓ podsłuchem.

7. Ochrona elektromagnetyczna systemu lub sieci teleinformatycznej polega na niedopuszczeniu do utraty poufności i dostępności informacji niejawnych przetwarzanych w urządzeniach teleinformatycznych:
   - ➢ utrata poufności następuje w szczególności na skutek wykorzystania elektromagnetycznej emisji ujawniającej pochodzącej z tych urządzeń,
   - ➢ utrata dostępności następuje w szczególności na skutek zakłócania pracy urządzeń teleinformatycznych za pomocą impulsów elektromagnetycznych o dużej mocy.
8. Ochronę elektromagnetyczną systemu teleinformatycznego zapewnia się w szczególności przez umieszczenie urządzeń teleinformatycznych, połączeń i linii w strefach kontrolowanego dostępu spełniających wymagania w zakresie tłumienności elektromagnetycznej odpowiednio do wyników szacowania ryzyka dla informacji niejawnych lub zastosowanie odpowiednich urządzeń teleinformatycznych, połączeń i linii o obniżonym poziomie emisji lub ich ekranowanie z jednoczesnym filtrowaniem zewnętrznych linii zasilających i sygnałowych.
9. W celu zapewnienia kontroli dostępu do systemu teleinformatycznego:
   - ➢ Wójt lub osoba przez niego upoważniona ustala warunki i sposób przydzielania uprawnień osobom uprawnionym do pracy w systemie lub sieci teleinformatycznej,
   - ➢ administrator systemów określa warunki oraz sposób przydzielania tym osobom kont oraz mechanizmów kontroli dostępu, a także zapewnia ich właściwe wykorzystanie.
10. System teleinformatyczny wyposaża się w mechanizmy kontroli dostępu odpowiednie do klauzuli tajności informacji niejawnych w nich przetwarzanych.
11. Systemy teleinformatyczne, w których maja być przetwarzane informacje niejawne podlegają akredytacji bezpieczeństwa teleinformatycznego.

12. Akredytacji bezpieczeństwa teleinformatycznego dla systemu teleinformatycznego przeznaczonego do przetwarzania informacji niejawnych o klauzuli „zastrzeżone” udziela Wójt.
13. Akredytacja, o której mowa w pkt. 12, następuje na podstawie dokumentów szczególnych wymagań bezpieczeństwa i procedur bezpiecznej eksploatacji.
14. Wójt wyznacza osobę odpowiedzialną za funkcjonowanie systemów teleinformatycznych oraz za przestrzeganie zasad i wymagań bezpieczeństwa systemów i sieci teleinformatycznych zwaną administratorem systemu.

KOPIE ZAPASOWE

1. Zaleca się wykonywanie kopii zapasowych wykonanych dokumentów niejawnych.
2. Sposób przechowywania zapasowych kopii jest identyczny jak przechowywanie dokumentów wykonanych w formie tradycyjnej (pismo), w przypadku gdy nośnikiem informacji jest materiał inny niż pismo klauzule tajności i sygnaturę literowo-cyfrową umieszcza się przez ostemplowanie, nadrukowanie, wpisanie odręczne, trwałe dołączenie metek, nalepek, kalkomanii lub w inny sposób, bezpośrednio, a jeżeli nie jest to możliwe - na ich obudowie lub opakowani.

ROZDZIAŁ XI
GROMADZENIE DOKUMENTÓW ZAWIERAJĄCYCH INFORMACJE NIEJAWNE

1. Dokumenty zawierające informacje niejawne powinny być przechowywane zgodnie z rzeczowym wykazem akt.
2. Dokumenty ostatecznie załatwione wymagają wszycia w teczkę pism, po zakończeniu roku kalendarzowego, klauzule niejawności teczek określa się według dokumentu o najwyższej klauzuli tajności.
3. Dokumenty niejawne o klauzuli „poufne” (o ile występują), muszą być przechowywane w Kancelarii Materiałów Niejawnych. W szczególnie uzasadnionych przypadkach dokumenty te mogą, za zgodą Wójta lub innej upoważnionej przez niego osoby, być przechowywane poza Kancelarią, pod warunkiem spełnienia wymogów bezpieczeństwa odpowiednich do tej klauzuli, na czas niezbędny do realizacji zadań związanych z dostępem do tych dokumentów.

4. Dokumenty niejawne o klauzuli „zastrzeżone” są przechowywane w Kancelarii Materiałów Niejawnych lub na stanowiskach pracy w meblach biurowych zamykanych na klucz.

ROZDZIAŁ XII
OZNACZANIE, NADAWANIE, ZMIANA I ZNOSZENIE KLAUZULI TAJNOŚCI MATERIAŁOM NIEJAWNYM

1. Klauzulę tajności nadaje osoba, która jest uprawniona do podpisania dokumentu lub oznaczenia innego niż dokument materiału.
2. Informacje niejawne podlegają ochronie w sposób określony w ustawie o ochronie informacji niejawnych do czasu zniesienia lub zmiany klauzuli tajności.
3. Osoba wymieniona w pkt.1 może określić datę lub wydarzenie, po którym nastąpi zniesienie lub zmiana klauzuli tajności.
4. Zniesienie lub zmiana klauzuli tajności jest możliwe wyłącznie po wyrażeniu pisemnej zgody przez osobę, o której mowa w pkt.1, albo jej przełożonego w przypadku ustania lub zmiany ustawowych przesłanek ochrony.
5. Należy nie rzadziej niż raz na 5 lat dokonać przeglądu materiałów celem ustalenia, czy spełniają ustawowe przesłanki ochrony.
6. Po zniesieniu lub zmianie klauzuli tajności podejmuje się czynności polegające na naniesieniu odpowiednich zmian w oznaczeniu materiału i poinformowaniu o nich odbiorców. Odbiorcy materiału, którzy przekazali go kolejnym odbiorcom, są odpowiedzialni za poinformowanie ich o zniesieniu lub zmianie klauzul tajności.
7. Poszczególne części materiału mogą być oznaczone różnymi klauzulami tajności.
8. Oznaczenie materiału klauzulą tajności polega na umieszczeniu na nim klauzuli tajności. Przyznaną klauzulę tajności nanosi się w sposób wyraźny i w pełnym jej brzmieniu.
9. Wprowadza się następujące oznaczenia klauzul tajności:

   „Z” – dla klauzuli „zastrzeżone”.
10. Szczegółowe zasady oznaczania materiałów zawierające informacje niejawne określa Rozporządzenie Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności (Dz. U. z 2011 r., Nr 288, poz. 1692).

ROZDZIAŁ XIII
OCENA ZAGROŻEŃ DLA INFORMACJI NIEJAWNYCH

1. OCENA ZAGROŻEŃ ZEWNĘTRZNYCH

1.1. Zagrożeniami zewnętrznymi dla Urzędu Gminy Gródek mogą być:

1) możliwość napadu przez zorganizowane grupy przestępcze i terrorystyczne, działające w sposób profesjonalny, przemyślany i zorganizowany,
2) możliwość napadu przez pojedynczych przestępców, przypadkowe osoby wykorzystujące nadarzającą się okazję z powodu nieprawidłowości w ochronie mienia Urzędu.

1.2. Symptomy mogące świadczyć o przygotowaniu napadu lub włamania do budynku:

1) wzmożone zainteresowanie osób postronnych obiektem, pomieszczeniami Urzędu objawiające się m.in. podejmowaniem prób uzyskania informacji o obiekcie, pomieszczeniach od pracowników podczas luźnych rozmów po „przypadkowym” spotkaniu,
2) nawiązanie rozmów przez osoby postronne z pracownikami,
3) podszywanie się pod byłych pracowników Urzędu i przejawianie zainteresowania tym, co się po latach zmieniło,
4) interesowanie się osobami funkcyjnymi, w tym także ich przywarami oraz sposobem wykonywania obowiązków służbowych,
5) obserwacja sposobu działania systemu ochronnego, sekretariatu, sprzątaczek, itp.,
6) rozpoznawanie systemu technicznych zabezpieczeń, w tym stosowanych urządzeń alarmowych,
7) celowe uszkadzanie urządzeń alarmowych, linii telefonicznych, oświetlenia, itp.,
8) próby pozyskania do grup przestępczych pracowników Urzędu (dotyczy głównie osób mających problemy finansowe, towarzyskie, a także służbowe).

1.3. Wnioski

W związku z przedstawionymi kierunkami zagrożeń należy wykonywać następujące czynności uprzedzające ewentualne możliwości zaistnienia zagrożeń:

1) stosować systematyczną, skrupulatną i wnikliwą kontrolę systemu ochrony przez osoby odpowiedzialne za jego organizację,
2) zwracać szczególną uwagę przez wszystkich pracowników Urzędu na możliwość zaistnienia ewentualnych zagrożeń,
3) stosować zasadę niedopuszczania osób niepowołanych do penetracji stref bezpieczeństwa,
4) wykonywanie prac porządkowych, remontowych, itp. w strefie bezpieczeństwa wyłącznie pod nadzorem osób odpowiedzialnych.

2. OCENA ZAGROŻEŃ WEWNĘTRZNYCH

2.1. Zagrożeniami wewnętrznymi dla Urzędu Gminy Gródek mogą być:

1) próby zaboru dokumentów lub mienia przez pracowników Urzędu,
2) próby powielania, kserowania dokumentów służbowych dla celów prywatnych,
3) byli pracownicy Urzędu zwolnieni dyscyplinarnie,
4) rozpoznanie organizacji pracy Urzędu celem łatwiejszej pracy grup przestępczych na terenie Urzędu,
5) próby wglądu w dokumenty niejawne przez osoby nieuprawnione,
6) nadmierne spożywanie alkoholu i innych środków odurzających - przesłanka do wykroczeń dyscyplinarnych i przestępstw.

2.2. Wnioski

W związku z przedstawionymi kierunkami zagrożeń należy wykonywać następujące czynności uprzedzające ewentualne możliwości zaistnienia zagrożeń:

1) zwracanie szczególnej uwagi na osoby, które mogą być zainteresowane zaborem dokumentu,
2) prowadzenie szczególnego nadzoru by nie dokonywano prób kserowania, kopiowania bez zgody przełożonego,
3) uwrażliwienie pracowników w trakcie prowadzonych szkoleń na możliwość prób kontaktu grup przestępczych z pracownikami, którzy mają dostęp do dokumentów szczególnie ważnych,

4) zastosowanie zasady, że do informacji niejawnych mogą mieć dostęp tylko pracownicy posiadający poświadczenie bezpieczeństwa lub właściwe upoważnienie jednorazowe wydane przez Prezydenta,
5) zwrócenie szczególnej uwagi na osoby, których zachowanie wskazuje na nadmierne spożywanie alkoholu i innych środków odurzających.

W celu prawidłowego zabezpieczenia informacji niejawnych, w tym doboru odpowiednich środków bezpieczeństwa fizycznego, należało przeprowadzić analizę i określić poziom zagrożeń związanych z utratą poufności, dostępności lub integralności, z ujawnieniem lub utratą informacji niejawnych.

Powyższa analiza została przeprowadzona w opracowanym przez Pełnomocnika Ochrony dokumencie „Szacowanie ryzyka i analiza poziomu zagrożeń dla systemu ochrony informacji niejawnych Urzędu Gminy Gródek” i obejmowała czynniki mogące mieć wpływ na bezpieczeństwo informacji niejawnych, a w szczególności:

- klauzule tajności przetwarzanych informacji niejawnych;
- postać i ilość informacji niejawnych;
- sposób przechowywania informacji niejawnych;
- otoczenie i strukturę budynków lub obszarów, w których przetwarzane są informacje niejawne;
- ilość osób mających lub mogących mieć dostęp do informacji niejawnych, a także posiadane przez nich uprawnienia oraz uzyskaną potrzebę dostępu do informacji niejawnych;
- inne czynniki wynikające ze specyfiki jednostki organizacyjnej, nie wykazane powyżej, a mogące mieć wpływ na ochronę informacji niejawnych, np.: działalnie obcych służb specjalnych, sabotaż, zamach terrorystyczny, kradzież lub inna działalność przestępcza, pożar, działalnie sił przyrody (np. obszar zagrożony powodzią) lub szkody górnicze.

Zgodnie z wyżej wymienionym dokumentem, zatwierdzonym odrębnym zarządzeniem, określono poziom zagrożeń w Urzędzie Gminy Gródek jako: **N I S K I**.

ROZDZIAŁ XIV
NADZÓR W ZAKRESIE OCHRONY INFORMACJI NIEJAWNYCH

1. Za ochronę informacji niejawnych w Urzędzie Gminy Gródek odpowiada Wójt.
2. Zadania określone ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2010, Nr 182, poz. 1228), w imieniu Wójta wykonuje Pełnomocnik Ochrony, poprzez:
   a) sprawowanie nadzoru nad realizacją zadań i przestrzeganiem przepisów określonych w Planie Ochrony Informacji Niejawnych,
   b) sprawowanie kontroli w zakresie ochrony informacji niejawnych oraz przestrzegania związanych z upoważnianiem do dostępu do tych informacji, w odniesieniu do wszystkich komórek organizacyjnych Urzędu.
3. Zadania określone w pkt. 2 mogą być realizowane przez innego upoważnionego pracownika pionu ochrony.
4. W przypadku ujawnienia informacji niejawnych przez podległych pracowników, Wójt lub upoważniony przez niego pracownik, zawiadamia na piśmie Pełnomocnika Ochrony podając jaka informacja niejawna została ujawniona lub jakie naruszenie przepisów zostało stwierdzone.
5. Pełnomocnik Ochrony przeprowadza okresowe kontrole przestrzegania ustawy w Urzędzie.
6. Pełnomocnik Ochrony, w przypadku stwierdzenia naruszenia przepisów o ochronie informacji niejawnych przez pracowników Urzędu, przedkłada Wójtowi pisemną informację o naruszeniu przepisów i wnioski do podjęcia odpowiednich decyzji.
7. W przypadku stwierdzenia naruszenia przepisów o ochronie informacji niejawnych oznaczonych klauzulą „poufne” lub wyższą Pełnomocnik Ochrony powiadamia Wójta oraz właściwe Służby Ochrony Państwa.

ROZDZIAŁ XV
ODPOWIEDZIALNOŚĆ KARNA, DYSCYPLINARNA I SŁUŻBOWA ZA NARUSZENIE PRZEPISÓW O OCHRONIE INFORMACJI NIEJAWNYCH

1. Zakres odpowiedzialności karnej osób, które dopuściły się przestępstwa lub czynu zabronionego przeciwko ochronie informacji, został określony przepisami ustawy z dnia 6 czerwca 1997 r. Kodeks Karny (Dz. U. z 1997 r. Nr 88, poz. 553 z późń. zm.), w art. 266:

   § 1. Kto, wbrew przepisom ustawy lub przyjętemu na siebie zobowiązaniu, ujawnia lub wykorzystuje informację, z którą zapoznał się w związku z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną, gospodarczą lub naukową, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

   § 2. Funkcjonariusz publiczny, który ujawnia osobie nieuprawnionej informację niejawną o klauzuli „zastrzeżone" lub „poufne" lub informację, którą uzyskał w związku z wykonywaniem czynności służbowych, a której ujawnienie może narazić na szkodę prawnie chroniony interes, podlega karze pozbawienia wolności do lat 3.".

2. Wobec pracowników, którzy nie przestrzegają wymagań związanych z ochroną informacji niejawnych, dopuszczają się uchybień w zakresie niewłaściwego zabezpieczania dokumentów, stwarzając warunki do ujawnienia tajemnicy osobom nieuprawnionym, mogą być zastosowane sankcje służbowe i dyscyplinarne.

ROZDZIAŁ XVI
ARCHIWIZOWANIE, GROMADZENIE I NISZCZENIE MATERIAŁÓW NIEJAWNYCH

1. Archiwizowanie materiałów niejawnych odbywa się z zachowaniem zasad określonych w Rozporządzeniu Ministra Kultury z dnia 16 września 2002 r. w sprawie postępowania z dokumentacją, zasad jej klasyfikowania i kwalifikowania oraz zasad i trybu przekazywania materiałów archiwalnych do archiwów państwowych (Dz. U. z 2002 r. Nr 167, poz. 1375).
2. Zasady postępowania z dokumentacją w komórkach organizacyjnych wykonujących zadania w zakresie obronności i bezpieczeństwa państwa zostały określone w rozporządzeniu Prezesa Rady Ministrów z dnia 26 lutego 2010 r. (Dz. U. z 2010 r. Nr 34 poz. 181).

3. Dokumentacja wytwarzana i gromadzona w Urzędzie dzieli się na:
    a) materiały archiwalne - wchodzące do państwowego zasobu archiwalnego;
    b) dokumentację niearchiwalną - inną dokumentację, niestanowiącą materiałów archiwalnych.
4. Rzeczową klasyfikację oraz kwalifikację dokumentacji ze względu na okresy jej przechowywania, wytwarzanej i gromadzonej, zawierają jednolite rzeczowe wykazy akt.
5. Wykazy akt, o których mowa w pkt. 4 stanowią podstawę gromadzenia dokumentacji w aktach spraw.
6. Dokumentacja niearchiwalna, podlega brakowaniu po upływie okresu przechowywania określonego we właściwym wykazie akt.
7. Brakowanie dokumentacji niearchiwalnej polega na ocenie jej przydatności do celów praktycznych, wydzieleniu dokumentacji nieprzydatnej i przekazaniu jej na makulaturę.
8. Brakowanie dokumentacji niearchiwalnej następuje na podstawie zgody.
9. Zgodę, na brakowanie dokumentacji niearchiwalnej, wyraża dyrektor miejscowo właściwego archiwum państwowego bądź archiwum wojskowego.
10. Wniosek o wyrażenie zgody na brakowanie dokumentacji niearchiwalnej należy złożyć dyrektorowi miejscowo właściwego archiwum państwowego bądź archiwum wojskowego.
11. Do wniosku o zgodę jednorazową dołącza się:
    a) protokół oceny dokumentacji niearchiwalnej,
    b) spis dokumentacji niearchiwalnej przeznaczonej do przekazania na makulaturę lub zniszczenie, albo spis dokumentacji technicznej, niearchiwalnej przeznaczonej na makulaturę lub zniszczenie.
12. Protokół oraz spis dokumentacji niearchiwalnej, sporządza komisja powołana przez Wójta, w której skład wchodzą: osoba kierująca lub prowadząca archiwum zakładowe albo składnicę akt oraz przedstawiciele komórek organizacyjnych, których dokumentacja niearchiwalna podlega brakowaniu oraz Kierownik Kancelarii.
13. W przypadku trudności w ocenie brakowanej dokumentacji niearchiwalnej można zwrócić się do miejscowo właściwego archiwum państwowego lub archiwum wojskowego o przeprowadzenie ekspertyzy.
14. Urząd przechowuje w archiwum zakładowym dokumenty brakowania wraz z dowodami przekazania nieprzydatnej dokumentacji niearchiwalnej na makulaturę bądź protokółami jej zniszczenia.

15. Uporządkowanie materiałów archiwalnych polega na podziale rzeczowym teczek i prawidłowym ułożeniu materiałów wewnątrz teczek, ich opisaniu, nadaniu właściwego układu, sporządzeniu ewidencji oraz technicznym zabezpieczeniu.
16. Materiały archiwalne powinny być ułożone wewnątrz teczek w kolejności spraw, a w ramach sprawy - chronologicznie, poczynając od pierwszego pisma wszczynającego sprawę. Poszczególne strony akt znajdujących się w teczce powinny być opatrzone kolejną numeracją.
17. Opisanie materiałów archiwalnych polega na umieszczeniu na wierzchniej stronie każdej teczki:
    a) nazwy jednostki organizacyjnej i komórki organizacyjnej, w której materiały powstały,
    b) znaku akt, tj. symbolu literowego komórki organizacyjnej oraz symbolu klasyfikacyjnego według wykazu akt, obowiązującego w jednostce organizacyjnej,
    c) tytułu teczki, tj. nazwy hasła klasyfikacyjnego według wykazu akt, obowiązującego w danej jednostce organizacyjnej, i informacji o rodzaju materiałów archiwalnych, znajdujących się w teczce,
    d) rocznych dat krańcowych, tj. dat najwcześniejszego i najpóźniejszego materiału archiwalnego w teczce,
    e) sygnatury teczki, tj. numeru spisu zdawczo-odbiorczego i numeru pozycji teczki w spisie zdawczo-odbiorczym,
    f) symbolu kwalifikacyjnego materiałów archiwalnych (kategoria A),
    g) liczby stron w teczce.
18. Czynności związane z brakowaniem materiałów niearchiwalnych, wobec których archiwum państwowe wyraziło zgodę na brakowanie, są dokumentowane przez sporządzenie protokołu komisyjnego zniszczenia dokumentów niearchiwalnych.
19. Protokół komisyjnego zniszczenia materiałów niearchiwalnych sporządzany jest w dwóch egzemplarzach, z czego jeden egzemplarz należy przesłać do właściwego archiwum państwowego.

ROZDZIAŁ XVII
USTALENIA KOŃCOWE

1. Wójt, Sekretarz oraz Skarbnik Gminy:
   - zapoznają podległych pracowników z ustaleniami Planu Ochrony Informacji Niejawnych w Urzędzie,
   - zapewnią bieżące przestrzeganie postanowień Planu Ochrony w zakresie ochrony informacji niejawnych, mogących występować w działalności kierowanej komórki organizacyjnej.
2. Osoby wymienione w pkt.1, wprowadzą jako obowiązującą zasadę, zapoznawania z Planem Ochrony wszystkie osoby, które podejmują pracę w komórkach organizacyjnych, z którą może się łączyć dostęp do informacji niejawnych.
3. W przypadku wystąpienia wątpliwości, a także potrzeby przybliżenia zasad dotyczących realizacji zadań związanych z ochroną informacji niejawnych, sporządzania i wykonania dokumentów zawierających informacje niejawne, pracownicy Urzędu mogą zwracać się o wyjaśnienia czy też instruktaż do:
   - Pełnomocnika Ochrony,
   - Kierownika Kancelarii Materiałów Niejawnych.
4. Integralną część Planu ochrony stanowią załączniki, wyspecyfikowane poniżej.

ZAŁĄCZNIKI
DO PLANU OCHRONY INFORMACJI NIEJAWNYCH W URZĘDZIE GMINY GRÓDEK

1. Załącznik Nr 1 – Instrukcja przechowywania kluczy i pieczęci,
2. Załącznik nr 2 - Instrukcja postępowania w sytuacjach kryzysowych i stanach nadzwyczajnych,
3. Załącznik nr 3 - Instrukcja alarmowa w przypadku zgłoszenia o podłożeniu lub znalezieniu ładunku wybuchowego w budynkach Urzędu,
4. Załącznik nr 4 - Instrukcja postępowania w przypadku otrzymania przesyłki niewiadomego pochodzenia.

Załącznik nr 1
do Planu Ochrony Informacji Niejawnych w Urzędzie Gminy Gródek

INSTRUKCJA
PRZECHOWYWANIA KLUCZY I PIECZĘCI

Ustala się zasady gospodarki kluczami i pieczęciami:

1. Klucze od szaf metalowych kancelarii materiałów niejawnych oraz pieczęcie, po zakończeniu pracy należy złożyć w pomieszczeniu kancelarii w miejscu niewidocznym.
2. Szafy metalowe kancelarii po zamknięciu mogą być dodatkowo plombowane pieczęcią do plasteliny.
3. Po zakończeniu pracy, pracownik kancelarii materiałów niejawnych zamyka na klucz drzwi wejściowe kancelarii.
4. Klucz od drzwi wejściowych należy umieścić w pojemniku lub woreczku, a następnie tak przygotowany pojemnik lub woreczek należy umieścić w miejscu niewidocznym w wyznaczonym pomieszczeniu.
5. Pieczęć do plasteliny pracownik kancelarii materiałów niejawnych powinien zabezpieczać tak, by osoby nieuprawnione nie mogły z niej korzystać.
6. Tworzy się zapasowy komplet kluczy od pomieszczeń kancelarii materiałów niejawnych, który należy złożyć do zdeponowania w szafie metalowej u Wójta Gminy.
7. Pracownik kancelarii materiałów niejawnych po przybyciu do urzędu, przed otwarciem kancelarii powinien sprawdzić, czy nie zostały naruszone pieczęcie zabezpieczające klucze oraz zabezpieczające drzwi wejściowe do kancelarii. W dalszej kolejności sprawdza czy nie zostały naruszone pieczęcie na szafach znajdujących się w kancelarii.

Załącznik nr 2
do Planu Ochrony Informacji Niejawnych w Urzędzie Gminy Gródek

INSTRUKCJA
POSTĘPOWANIA W SYTUACJACH KRYZYSOWYCH I STANACH NADZWYCZAJNYCH

1. W przypadku wystąpienia sytuacji kryzysowych, np. pożar, powódź, należy w pierwszej kolejności powiadomić Wójta, Pełnomocnika Ochrony oraz osoby odpowiedzialne za pomieszczenia, w których przechowuje się dokumentu niejawne.
2. Należy zabezpieczyć:
   - pieczęcie,
   - dokumenty o klauzuli „zastrzeżone”,
   - kopie zapasowe, jeżeli są przechowywane,
   - inne dokumenty i materiały według sporządzonego planu ewakuacji.
3. Dokumenty ewakuuje się w oplombowanych, brezentowych workach ewakuacyjnych.
4. Miejscem ewakuacji są pomieszczenia Archiwum Zakładowego bądź inne miejsce ustalone przez Wójta z uwzględnieniem zapewnienia odpowiedniej ochrony w miejscu ewakuacji.
5. W sytuacji, gdy ewakuacja jest niemożliwa, należy zniszczyć dokumenty o klauzuli „zastrzeżone”, pieczęcie i w miarę możliwości pozostałe dokumenty i materiały.
6. Szczególny obowiązek zabezpieczenia materiałów zawierających informacje niejawne oznaczonych klauzulą „zastrzeżone” powstaje w przypadku wprowadzenia stanu nadzwyczajnego.
7. Za stan nadzwyczajny uważa się stan określone w art. 228 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. Nr 78, poz. 483 z późn. zm.), tj. stan wojenny, stan wyjątkowy lub stan klęski żywiołowej.
8. Stan nadzwyczajny może być wprowadzony tylko na podstawie ustawy, w drodze rozporządzenia, które podlega dodatkowemu podaniu do publicznej wiadomości.
9. W związku z wprowadzeniem stanu nadzwyczajnego działania podjęte w celu ochrony dokumentów niejawnych będących w posiadaniu Urzędu muszą odpowiadać stopniowi zagrożenia podstawowych interesów RP w zakresie

obronności, bezpieczeństwa, stosunków gospodarczych i międzynarodowych państwa.

10. Ewakuacja materiałów zawierających informacje niejawne następuje na polecenie Wójta.
11. Koordynatorem ewakuacji jest Wójt bądź Pełnomocnik Ochrony, który współpracuje z wyznaczonymi pracownikami Urzędu.
12. Pracownicy Urzędu zobowiązani są, na żądanie Wójta bądź Pełnomocnika Ochrony do udzielenia natychmiastowej pomocy.
13. Materiały niejawne przechowywane w Urzędzie, Kierownik Kancelarii Materiałów Niejawnych oznakowuje symbolami **„Z”** i **„E”** (Zniszczyć, Ewakuować), który dokonuje tej czynności w uzgodnieniu z wytwórcami merytorycznymi.
14. Zabezpieczeniu podlegają:
    - wszystkie materiały zawierające informacje niejawne – jeśli ilość tych materiałów jest niewielka,
    - w przypadku przechowywania w Urzędzie większej ilości dokumentów zawierających informacje niejawne w pierwszej kolejności zabezpieczeniu podlegają materiały niezbędne do wykonywania przez Urząd zadań obronnych w stanach nadzwyczajnych oraz zapewniające ciągłość jego funkcjonowania – oznakowane symbolem „E”, w drugiej kolejności – gdy czas i warunki na to pozwolą– pozostałe materiały niejawne;

14. Materiały niejawne oznakowane symbolem „Z” należy zniszczyć np. poprzez pocięcie w niszczarce.
15. Przed ewakuacją sporządza się, w miarę możliwości, w dwóch egzemplarzach spis dokumentów przeznaczonych do ewakuacji oraz do zniszczenia - jeden egzemplarz przekazuje się Wójtowi, drugi zabiera wraz z ewakuowaną dokumentacją.
16. Decyzję w sprawie zabezpieczenia – ewakuacji materiałów podejmuje Wójt.
17. Ewakuacja powinna obejmować:
    - zapakowanie materiałów do worków ewakuacyjnych lub skrzyń pakowych,
    - przemieszczenie worków na środek transportu,
    - przewiezienie do wyznaczonego przez Wójta miejsca ewakuacji.

Załącznik nr 3
do Planu Ochrony Informacji Niejawnych w Urzędzie Gminy Gródek

INSTRUKCJA ALARMOWA W PRZYPADKU ZGŁOSZENIA O PODŁOŻENIU LUB ZNALEZIENIU ŁADUNKU WYBUCHOWEGO W BUDYNKACH URZĘDU

I. ALARMOWANIE

1. Osoba, która przyjęła zgłoszenie o podłożeniu ładunku wybuchowego, albo zauważyła w obiekcie przedmiot niewiadomego pochodzenia mogący być ładunkiem wybuchowym jest obowiązana o tym powiadomić:
   - Wójta,
   - Policję.
2. Zawiadamiając Policję należy podać: treść rozmowy ze zgłaszającym o podłożeniu ładunku wybuchowego, która należy prowadzić wg poniższych wskazówek:
   - miejsce i opis zlokalizowanego przedmiotu, który może być ładunkiem wybuchowym,
   - numer telefonu, z którego prowadzona jest rozmowa i swoje stanowisko,
   - uzyskać od Policji potwierdzenie przyjętego zawiadomienia.

II. AKCJA POSZUKIWAWCZA ŁADUNKU WYBUCHOWEGO PO UZYSKANIU INFORMACJI O JEGO PODŁOŻENIU

1. Do czasu przybycia Policji akcją kieruje Wójt, a w czasie jego nieobecności Zastępca Wójta lub inna osoba przez niego upoważniona.
2. Kierujący akcją zarządza, aby użytkownicy pomieszczeń dokonali sprawdzenia czy w tych pomieszczeniach znajdują się:
   - przedmioty, rzeczy lub urządzenia, paczki itp., których wcześniej nie było i nie wnieśli ich użytkownicy pomieszczeń,
   - ślady przemieszczania elementów wyposażenia pomieszczeń,
   - zmiany w wyglądzie zewnętrznym przedmiotów, rzeczy, urządzeń, które przedtem w pomieszczeniu były oraz emitowane z nich sygnały (np. dźwięki mechanizmów zegarowych, świecące elementy elektroniczne, itp.).

3. Pomieszczenia ogólnodostępne takie jak: korytarze, klatki schodowe, hale, windy, toalety, piwnice, strychy itp. oraz najbliższe otoczenie zewnętrzne obiektu powinny być sprawdzone przez wyznaczonych do tego pracowników.
4. Zlokalizowanych przedmiotów, rzeczy, urządzeń, których w ocenie użytkowników obiektu przedtem nie było, a zachodzi podejrzenie, iż mogą to być ładunki wybuchowe nie wolno dotykać. O ich umiejscowieniu należy natychmiast powiadomić Wójta i Policję.
5. W przypadku, gdy użytkownicy pomieszczeń faktycznie stwierdzą obecność przedmiotów (rzeczy, urządzeń), których wcześniej nie było lub zmiany w wyglądzie i usytuowaniu przedmiotów stale znajdujących się w tych pomieszczeniach, należy domniemywać, że pojawienie się tych przedmiotów lub zmiany w ich wyglądzie i usytuowaniu mogły nastąpić na skutek działania sprawcy podłożenia ładunku wybuchowego. W takiej sytuacji kierujący akcją może wydać decyzje ewakuacji osób z zagrożonego obiektu przed przybyciem Policji.
6. Należy zachować spokój i opanowanie aby nie dopuścić do przejawów paniki.

III. WSPÓŁPRACA Z POLICJĄ W CZASIE AKCJI

1. Po przybyciu do obiektu policjanta bądź policyjnej grupy interwencyjnej kierujący akcją powinien przekazać im wszelkie informacje dotyczące zdarzenia oraz wskazać miejsce zlokalizowanych przedmiotów, rzeczy, urządzeń obcego pochodzenia i punkty newralgiczne w obiekcie.
2. Policjant lub dowódca grupy interwencyjnej przejmuje kierowanie akcją, a kierujący akcją winien udzielić mu wszechstronnej pomocy.
3. Na wniosek policjanta kierującego akcją Wójt podejmuje decyzję o ewakuacji użytkowników i innych osób z obiektu, o ile wcześniej to nie nastąpiło.
4. Identyfikacją i rozpoznaniem zlokalizowanych przedmiotów, rzeczy, urządzeń obcych oraz neutralizowaniem ewentualnie podłożonych ładunków wybuchowych zajmują się uprawnione i wyspecjalizowane ogniwa organizacyjne policji, przy wykorzystaniu specjalistycznych środków technicznych.
5. Policjant kierujący akcją po zakończeniu działań przekazuje protokolarnie obiekt Wójtowi.

IV. POSTANOWIENIA KOŃCOWE DOTYCZĄCE DZIAŁAŃ W PRZYPADKU ZGŁOSZENIA O PODŁOŻENIU ŁADUNKU WYBUCHOWEGO

1. Osobom przyjmującym zgłoszenie o podłożeniu ładunku wybuchowego oraz Wójtowi nie wolno lekceważyć żadnej informacji na ten temat. Każdorazowo osoby te winny zawiadamiać o tym Policję, która z urzędu dokona sprawdzenia wiarygodności każdego zgłoszenia.
2. Wójt powinien na bieżąco organizować szkolenie pracowników w zakresie sposobu zachowania się w sytuacjach wymienionych w tej części Planu Ochrony oraz winien znać rozmieszczenie newralgicznych punktów - węzły energetyczne i wodne, które udostępnia się na żądanie policjanta kierującego akcją.

Załącznik nr 4
do Planu Ochrony Informacji Niejawnych w Urzędzie Gminy Gródek

INSTRUKCJA POSTĘPOWANIA W PRZYPADKU OTRZYMANIA PRZESYŁKI NIEWIADOMEGO POCHODZENIA

I. W przypadku **<u>otrzymania</u>** jakiejkolwiek **<u>przesyłki niewiadomego pochodzenia</u>** lub budzącej podejrzenia z jakiegokolwiek innego powodu:

- brak nadawcy,
- brak adresu nadawcy,
- przesyłka pochodzi od nadawcy lub z miejsca, z którego nie spodziewamy się,
- inne podejrzenia.

<u>Nie należy otwierać tej przesyłki.</u>

Należy:

1. Umieścić przesyłkę w grubym worku plastikowym, szczelnie zamknąć.
2. Worek należy umieścić w drugim plastikowym worku, szczelnie zamknąć, zakleić taśmą lub plastrem.
3. Paczki nie należy przemieszczać, należy pozostawić ją na miejscu.
4. Powiadomić:
   - Komendę Powiatową Policji **tel. 997**
   - Komendę Powiatową Państwowej Straży Pożarnej **tel. 998**

<u>Służby te podejmą wszelkie niezbędne kroki w celu bezpiecznego przejęcia przesyłki.</u>

II. W przypadku gdy **<u>podejrzana przesyłka została otwarta</u>** i zawiera jakąkolwiek podejrzaną zawartość w formie stałej (galaretę, pianę, pył lub inną).

Należy:

1. **<u>Nie naruszyć zawartości</u>** - nie rozsypywać, nie przenosić, nie dotykać, nie wąchać, nie powodować ruchu powietrza w pomieszczeniu (wyłączyć systemy wentylacyjne, zamknąć okna).
2. Całą zawartość umieścić w worku plastikowym, zamknąć go i zakleić taśmą lub plastrem.
3. Dokładnie umyć ręce.
4. Zaklejony worek umieścić w drugim worku, zamknąć go i zakleić.
5. Ponownie umyć ręce.
6. Powiadomić:
   - Komendę Powiatową Policji **tel. 997**
   - Komendę Powiatową Państwowej Straży Pożarnej **tel. 998**
   - Pogotowie Ratunkowe **tel. 999**
   - Powiatową Stację Sanitarno-Epidemiologiczną **tel. (85) 73-25-236**

<u>Po przybyciu właściwej służby należy bezwzględnie stosować się do jej zaleceń.</u>