

ZARZĄDZENIE NR 9/2013
Wójta Gminy Radomin
z dnia 6 lutego 2013 roku

w sprawie wprowadzenia Planu Ochrony Informacji Niejawnych w Urzędzie Gminy Radomin

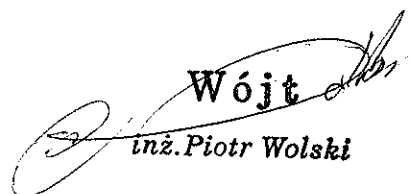
Na podstawie art. 15 ust. 1 pkt 5 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228), zarządzam, co następuje:

§ 1. Wprowadzam Plan Ochrony Informacji Niejawnych w Urzędzie Gminy Radomin, stanowiący załącznik do niniejszego zarządzenia.

§ 2. Uchylam Plan Ochrony Informacji Niejawnych zatwierdzony przez Wójta Gminy Radomin w 2006 r.

§ 3. Nadzór nad wykonaniem zarządzenia powierzam Pełnomocnikowi ds. ochrony informacji niejawnych.

§ 4. Zarządzenie wchodzi w życie z dniem podjęcia.


Wójt
inż. Piotr Wolski

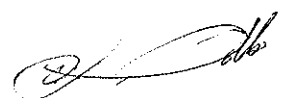
PLAN OCHRONY INFORMACJI NIEJAWNYCH

Rozdział 1 Postanowienia ogólne

- § 1.1. Przedmiotem ochrony w Urzędzie Gminy Radomin są informacje niejawne oznaczone klauzulą „poufne” i „zastrzeżone”. Plan ochrony informacji niejawnych jest dokumentem określającym sposób i tryb przetwarzania informacji niejawnych o klauzuli „poufne” i „zastrzeżone” w podległych komórkach organizacyjnych, a także sposoby zapewnienia fizycznego bezpieczeństwa informacji.
2. Środki i procedury określone w planie ochrony odnoszą się do informacji niejawnych oznaczonych klauzulą „poufne” i „zastrzeżone” w rozumieniu ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228).
3. Wprowadzone do stosowania środki i procedury w zakresie ochrony informacji niejawnych określa:
- 1) instrukcja sposobu i trybu przetwarzania informacji niejawnych o klauzuli „zastrzeżone” w Urzędzie Gminy Radomin;
 - 2) sposób i tryb przetwarzania informacji niejawnych o klauzuli „poufne” w Urzędzie Gminy Radomin.
4. W Urzędzie Gminy Radomin wyodrębniona jest komórka organizacyjna do spraw ochrony informacji niejawnych, w skład której wchodzi:
- 1) pełnomocnik ds. ochrony informacji niejawnych;
 - 2) osoba odpowiedzialna za rejestrację dokumentów niejawnych;
 - 3) inspektor bezpieczeństwa teleinformatycznego;
 - 4) administrator systemu.

Rozdział 2 Definicje używane w Planie ochrony informacji niejawnych

- § 2. Definicje użyte w Planie należy rozumieć następująco:
- 1) **informacje niejawne** - to informacje, których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne, niezależnie od formy i sposobu ich wyrażania, a także w trakcie ich opracowywania;
 - 2) **informacje niejawne o klauzuli „poufne”** – to informacje, których nieuprawnione ujawnienie spowoduje szkodę dla Rzeczypospolitej Polskiej w obszarze polityki międzynarodowej, obronności, porządku publicznego lub bezpieczeństwa obywateli, utrudniłoby wykonywanie ustawowych zadań przez organy, służby lub instytucje odpowiedzialne za ochronę bezpieczeństwa, osłabiłoby system finansowy Polski lub naraziłoby na szkodę interesy ekonomiczne lub funkcjonowanie gospodarki narodowej;
 - 3) **informacje niejawne o klauzuli „zastrzeżone”** – to informacje, których 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;

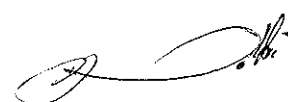
- 4) **rękojmia zachowania tajemnicy** - to zdolność osoby do spełnienia ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem, stwierdzona w wyniku przeprowadzenia postępowania sprawdzającego;
- 5) **dokument** – jest każda utrwalona informacja niejawna;
- 6) **material** – jest dokument lub przedmiot albo dowolna ich część, chronione jako informacja niejawna, a zwłaszcza urządzenie, wyposażenie lub broń wyprodukowane albo będące w trakcie produkcji, a także składnik użyty do ich wytworzenia;
- 7) **przetwarzanie informacji niejawnych** – to wszelkie operacje wykonywane w odniesieniu do informacji niejawnych i na tych informacjach, w szczególności ich wytwarzanie, modyfikowanie, kopiowanie, klasyfikowanie, gromadzenie, przechowywanie, przekazywanie lub udostępnianie;
- 8) **system teleinformatyczny** - zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie danych;
- 9) **sporządzający dokument** – pracownik, który przygotowuje i sporządza projekt dokumentu lub innego niż dokument materiału zawierającego informacje niejawne;
- 10) **wytwórca dokumentu** - pracownik upoważniony do podpisania dokumentu lub oznaczenia innego niż dokument materiału zawierającego informacje niejawne;
- 11) **śłużby ochrony państwa** – to Agencja Bezpieczeństwa Wewnętrznego;
- 12) **Urząd** – to Urząd Gminy Radomin;
- 13) **Wójt** – to Wójt Gminy Radomin ;
- 14) **Pełnomocnik ochrony** – to Pełnomocnik ds. Ochrony Informacji Niejawnych.

Rozdział 3

Ocena zagrożeń dla informacji niejawnych, w tym dla dokumentów o klauzuli „poufne”

§ 3. 1. Zagrożeniami zewnętrznymi dla Urzędu Gminy Radomin są:

- 1) możliwość napadu przez zorganizowane grupy przestępcze i terrorystyczne, działające w sposób profesjonalny, przemysłany i zorganizowany;
 - 2) możliwość napadu przez pojedynczych przestępców, przypadkowe osoby wykorzystujące nadarżającą się okazję z powodu nieprawidłowości w ochronie mienia Urzędu.
2. Symptomy mogące świadczyć o przygotowaniu napadu lub włamania do budynku:
- 1) wzmożone zainteresowanie osób postronnych obiektami, pomieszczeniami Urzędu objawiające się m. in. podejmowaniem prób uzyskania informacji o obiektach, pomieszczeniach od pracowników podczas rozmów;
 - 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 oraz sposobem wykonywania obowiązków służbowych;
 - 5) obserwacja sposobu działania ochrony budynku, sekretariatu, sprzątaczk i itp.;
 - 6) rozpoznawanie systemu technicznych zabezpieczeń;



- 7) celowe uszkodzanie urządzeń alarmowych, linii telefonicznych, oświetlenia itp.;
 - 8) próby pozyskania do grup przestępczych pracowników Urzędu.
3. Czynności uprzedzające ewentualne możliwości zaistnienia zagrożeń:
- 1) systematyczna, skrupulatna i wnikliwa kontrola systemu ochrony przez osoby odpowiedzialne za jego organizację;
 - 2) pracownicy pionu ochrony w czasie dnia pracy powinni zwracać szczególną uwagę na możliwość zaistnienia ewentualnych zagrożeń;
 - 3) stosowanie zasady niedopuszczania osób niepowołanych do penetracji strefy bezpieczeństwa, w której znajduje się rejestracja dokumentów niejawnych;
 - 4) wykonywanie prac porządkowych, remontowych itp. w strefie bezpieczeństwa wyłącznie pod nadzorem osób odpowiedzialnych.

§ 4.1. Zagrożeniami wewnętrznymi dla Urzędu Gminy Radomin są:

- 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) próby wglądu w dokumenty niejawne przez osoby nieuprawnione;
 - 5) nadmierne spożywanie alkoholu - przesłanka do wykroczeń dyscyplinarnych i przestępstw.
2. Czynności uprzedzające ewentualne możliwości zaistnienia zagrożeń:
- 1) zwracanie szczególnej uwagi na osoby, które mogą być zainteresowane zaborem dokumentów;
 - 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 wydane przez Wójta;
 - 5) zwrócenie szczególnej uwagi na osoby, których zachowanie wskazuje na nadmierne spożywanie alkoholu.

Rozdział 4

Postępowanie z informacjami niejawnymi w razie wprowadzenia stanu nadzwyczajnego

§ 5.1. Szczególny obowiązek zabezpieczenia materiałów zawierających informacje niejawne powstaje w przypadku wprowadzenia stanu nadzwyczajnego. Jako stany nadzwyczajne uważa się stany określone w art. 228 Konstytucji RP (Dz. U. z 1997 r. Nr 78, poz. 484 z późn. zm.), tj. stan wojenny, stan wyjątkowy lub stan klęski żywiołowej. Stan nadzwyczajny może być wprowadzony tylko na podstawie ustawy, w drodze rozporządzenia, które podlega dodatkowemu podaniu do publicznej wiadomości.

2. Działania podjęte w wyniku wprowadzenia stanu nadzwyczajnego muszą odpowiadać stopniowi zagrożenia i powinny zmierzać do jak najszybszego przywrócenia normalnego funkcjonowania państwa.



3. 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.
4. Ewakuacja materiałów zawierających informacje niejawne następuje na polecenie kierownika jednostki organizacyjnej. Koordynatorem ewakuacji jest pełnomocnik ochrony, który współpracuje w tym zakresie z kierownikami jednostek i komórek organizacyjnych. Dokumenty ewakuuje się w opłombowanych workach ewakuacyjnych.
5. Materiały niejawne po ewakuacji należy odpowiednio zabezpieczyć przez zamknięcie i opłombowanie pomieszczeń a także, jeżeli jest to możliwe, należy zapewnić całodobowy nadzór nad tymi pomieszczeniami.
6. W przypadku, gdy zabezpieczenie dokumentów w budynku Urzędu jest niemożliwe i niemożliwa jest ich ewakuacja, należy przystąpić do likwidacji dokumentów zawierających informacje niejawne.
7. Decyzję w sprawie likwidacji dokumentów niejawnych podejmuje kierownik jednostki organizacyjnej. W przypadku jego nieobecności decyzję podejmuje pełnomocnik ochrony.
- 8 W celu wykonywania zadań związanych z zabezpieczeniem materiałów będących przedmiotem zabezpieczenia konieczne jest:
 - 1) Wydanie stosownego polecenia pracownikom samodzielnych stanowisk;
 - 2) Zapewnienie niezbędnego środka transportu oraz pracowników w ilości niezbędnej do zapakowania i przeniesienia materiałów wymagających zabezpieczenia;
 - 3) Zabezpieczenie ewakuacji dokumentów dokonuje komisja wyznaczona przez osobę zarządzającą zabezpieczeniem materiałów;
 - 4) Komisja sporządza protokół, z którego musi wynikać:
 - określenie rodzaju i ilości dokumentów poddanych zabezpieczeniu lub ewakuacji,
 - określenie sposobu zabezpieczenia dokumentów w nowym miejscu ich przechowywania,
 - określenie sposobu zabezpieczenia dokumentów, które pozostały na stanowiskach pracy;
 - 5) W przypadku pozostawienia części materiałów, które nie podlegały zabezpieczeniu lub których nie zdołano zabezpieczyć, komisja zobowiązana jest zamknąć i zapłombować szafy w pomieszczeniach, gdzie były przechowywane. Spełnienie, lub nie spełnienie tej czynności komisja obowiązkowo uwzględnia w treści protokołu zabezpieczenia materiałów.

Rozdział 5

Przedmiot ochrony

§ 6. Przedmiotem ochrony w Urzędzie Gminy są:

- 1) Informacje niejawne oznaczone klauzulą „poufne” i „zastrzeżone”;
- 2) Pomieszczenia, w których są przechowywane i opracowywane materiały niejawne;
- 3) Autonomiczne stanowisko komputerowe przeznaczone do przetwarzania, wytwarzania i przechowywania informacji niejawnych o klauzuli „zastrzeżone”.



Rozdział 6

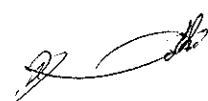
Zabezpieczenie materiałów niejawnych

- § 7.1. W celu zmniejszenia ryzyka zapoznania się z informacjami niejawnymi przez osoby do tego nieuprawnione utworzono specjalne pomieszczenie zwane kancelarią materiałów niejawnych. Pomieszczenie jest zabezpieczone przed podglądaniem z zewnątrz i wyposażone w szafę stalową klasy A, z zamkiem o skomplikowanym mechanizmie.
2. Informacje niejawne o klauzuli „poufne” są przechowywane w kancelarii materiałów niejawnych, w szafie metalowej. W uzasadnionych przypadkach podyktowanych względami dłuższego okresu czasu, niezbędnego do realizacji zadań związanych z dostępem do informacji niejawnych, dokumenty o klauzuli „poufne” mogą być wydawane poza kancelarię materiałów niejawnych, ale jedynie w sytuacji, gdy odbiorca dokumentu zapewnia warunki ochrony tych dokumentów, przechowując je w szafach metalowych z odpowiednim zamknięciem.
3. Szafa metalowa, w której przechowuje się dokumenty o klauzuli „poufne” podlega codziennemu zamykaniu po zakończeniu pracy.
4. Informacje niejawne oznaczone klauzulą „zastrzeżone” są przechowywane w pomieszczeniu kancelarii materiałów niejawnych lub na stanowiskach pracy, w meblach biurowych zamykanych na klucz.
5. Komputer wykorzystywany wyłącznie do przetwarzania i wytwarzania informacji niejawnych po zakończeniu pracy jest odłączany z sieci elektrycznej i przechowywany w szafie zamykanej na klucz.

Rozdział 7

Ewidencja informacji niejawnych podlegających ochronie.

- § 8.1. Informacje niejawne oznaczone klauzulą „poufne” i „zastrzeżone” są rejestrowane w dzienniku ewidencji dokumentów niejawnych w kancelarii materiałów niejawnych Urzędu.
2. Dziennik ewidencji – jest urządzeniem ewidencyjnym służącym do ewidencjonowania dokumentów niejawnych wytworzonych w Urzędzie, korespondencji niejawnej otrzymanej (wchodzącej) i wysyłanej (wychodzącej). Wzór dziennika ewidencji dokumentów niejawnych stanowi załącznik nr 1 do Planu ochrony.
3. Dokumenty niejawne wpływające do Urzędu i wytworzone – wychodzące z Urzędu rejestruje się w dzienniku ewidencji. Każdy dokument niejawny przychodzący lub wychodzący z Urzędu rejestruje się w odrębnej pozycji dziennika ewidencji.
4. Osobą upoważnioną do przyjmowania niejawnej korespondencji wchodzącej w formie listów czy paczek jest Pełnomocnik ochrony lub osoba odpowiedzialna za rejestrację dokumentów niejawnych. Listy lub paczki zawierające korespondencję niejawną mogą wpływać z zewnątrz jako przesyłki „polecone” bezpośrednio do kancelarii materiałów niejawnych, sekretariatu Urzędu. Pracownik sekretariatu, po stwierdzeniu, że wewnątrz znajduje się druga koperta oznaczona klauzulą tajności, nie otwiera jej i nie rejestruje w swojej ewidencji, informując niezwłocznie Pełnomocnika ochrony, a w przypadku jego nieobecności osobą odpowiedzialną za rejestrację dokumentów niejawnych o jej nadejściu.
5. Korespondencji niejawnej mylnie skierowanej nie ewidencjonuje się w kancelarii materiałów niejawnych, lecz przekazuje łącznie z poprzednim opakowaniem w nowej kopercie właściwemu adresatowi za zwrotnym potwierdzeniem odbioru.
6. Nr ewidencyjny każdego dokumentu niejawnego powinien być poprzedzony skrótem literowym:
- 1) „Pf” – poufny,
 - 2) „Z” – zastrzeżony.



Rozdział 8

Zasady dostępu do informacji niejawnych – postępowanie sprawdzające

- § 9.1. Informacje niejawne oznaczone klauzulą „poufne” lub „zastrzeżone” mogą być udostępniane wyłącznie osobie uprawnionej do dostępu do informacji niejawnych o określonej klauzuli niejawności.
2. Uzyskanie uprawnień do dostępu do informacji niejawnych o klauzuli „poufne” może nastąpić po:
- 1) uzyskaniu przez daną osobę poświadczenia bezpieczeństwa, po przeprowadzonym zwykłym postępowaniu sprawdzającym oraz
 - 2) odbyciu szkolenia w zakresie ochrony informacji niejawnych.
3. Uzyskanie uprawnień do dostępu do informacji niejawnych o klauzuli „zastrzeżone” może nastąpić po:
- 1) pisemnym upoważnieniu danej osoby przez Wójta Gminy oraz
 - 2) odbyciu szkolenia w zakresie ochrony informacji niejawnych.
4. Zwykłe postępowanie sprawdzające w związku z dostępem do informacji niejawnych oznaczonych klauzulą „poufne” przeprowadza Pełnomocnik ochrony na pisemne polecenie Wójta.
5. Postępowanie sprawdzające ma na celu ustalenie, czy osoba sprawdzana daje rękojmię zachowania tajemnicy.
6. Każda osoba podlegająca procedurze postępowania sprawdzającego zobowiązana jest do:
- 1) wypełnienia określonej przepisami ankiety bezpieczeństwa osobowego;
 - 2) wypełnienia ankiety w sposób dokładny i zgodny z prawdą.
7. Zwykłe postępowanie sprawdzające obejmuje:
- 1) sprawdzenie, w niezbędnym zakresie, w ewidencjach, rejestrach i kartotekach, w szczególności w Krajowym Rejestrze Karnym, danych zawartych w wypełnionej i podpisanej przez osobę sprawdzaną ankiecie, a także sprawdzenie innych informacji uzyskanych w toku postępowania sprawdzającego, w zakresie niezbędnym do ustalenia, czy osoba sprawdzana daje rękojmię zachowania tajemnicy;
 - 2) sprawdzenie w ewidencjach i kartotekach niedostępnych powszechnie danych zawartych w ankiecie oraz innych informacji uzyskanych w toku postępowania sprawdzającego, w zakresie niezbędnym do ustalenia, czy osoba sprawdzana daje rękojmię zachowania tajemnicy;
 - 3) rozmowę z osobą sprawdzaną, jeżeli jest to konieczne w wyniku uzyskanych informacji.
8. Odmowa poddania się postępowaniu sprawdzającemu, ze strony osoby, która jest lub będzie zatrudniona na stanowisku związanym z dostępem do informacji niejawnych o klauzuli „poufne”, a w związku z tym nie uzyskanie poświadczenia bezpieczeństwa warunkującego dostęp do informacji podlegających ochronie skutkować może:
- 1) przeniesieniem danej osoby na stanowisko nie związane z informacjami niejawnymi;
 - 2) rozwiązaniem umowy o pracę w przypadku niemożności zmiany stanowiska;
 - 3) niemożnością zatrudnienia na danym stanowisku, w odniesieniu do osoby ubiegającej się o zatrudnienie w Urzędzie.
9. Ankieta bezpieczeństwa osobowego po wypełnieniu stanowi tajemnicę prawnie chronioną i podlega ochronie przewidzianej dla informacji niejawnych o klauzuli tajności „zastrzeżone”.

10. Po zakończeniu zwykłego postępowania sprawdzającego z wynikiem pozytywnym Pełnomocnik wydaje poświadczenie bezpieczeństwa (ważne przez okres 10 lat od daty wydania) i przekazuje osobie sprawdzanej, zawiadamiając o tym Wójta.

Rozdział 9

Kancelaria materiałów niejawnych Urzędu.

§ 10.1. W Urzędzie funkcjonuje kancelaria materiałów niejawnych, która jest wyodrębnioną komórką organizacyjną w zakresie ochrony informacji niejawnych, podległą Pełnomocnikowi ochrony, która znajduje się w strefie bezpieczeństwa.

2. W kancelarii materiałów niejawnych są rejestrowane, przechowywane i wydawane uprawnionym osobom informacje niejawne o klauzuli „poufne” i „zastrzeżone”. Kancelaria spełnia wszystkie wymagania prawne odnośnie ochrony fizycznej informacji niejawnych, co zabezpiecza materiały przed ich nieuprawnionym ujawnieniem, utratą, uszkodzeniem lub zniszczeniem.

3. Środki ochrony fizycznej informacji niejawnych w kancelarii materiałów niejawnych:

- 1) ściany i stropy wykonane są z materiałów niepalnych, spełniających wymagania w zakresie klasy odporności pożarowej oraz nośności granicznej odpowiadającej, co najmniej konstrukcji murowanej z cegły pełnej o grubości 250 mm;
- 2) drzwi wewnętrzne wyposażone są w zamki drzwiowe wielopunktowy, które spełniają wymagania Polskiej Normy PN-90/B-92270;
- 3) okno jest zabezpieczone przed obserwacją z zewnątrz;
- 4) szafa stalowa.

4. Szafa stalowa posiada:

- 1) korpus szafy, drzwi, skrytka i inne elementy konstrukcyjne są wykonane z blachy ze stali konstrukcyjnej, zabezpieczonej przed korozją. Połączenia korpusu szafy zapewniają mu dostateczną sztywność;
- 2) drzwi szafy są jednoskrzydłowe, wyposażone w mechanizm dźwigowy;
- 3) podstawa szafy posiada te same rozmiary co wierzch.

5. Dokumenty i materiały oznaczone różnymi klauzulami tajności mogą być przechowywane w jednej szafie pod warunkiem ich fizycznego oddzielenia.

6. Po zakończeniu pracy Pełnomocnik ochrony jest obowiązany sprawdzić prawidłowość zamknięcia szafy w kancelarii materiałów niejawnych.

§ 11.1. Klucze do szafy metalowej oraz pieczęcie po zakończeniu pracy są złożone w pomieszczeniu kancelarii materiałów niejawnych w miejscu niewidocznym.

2. Pełnomocnik ochrony po zakończeniu pracy zamyka drzwi wejściowe do kancelarii materiałów niejawnych, klucze umieszcza w woreczku, następnie umieszcza je w szafce zamykanej na klucz.

3. Zapasowy komplet kluczy do pomieszczenia kancelarii materiałów niejawnych jest umieszczony w opieczętowanym woreczku i zdeponowany w pomieszczeniu biurowym w szafce zamykanej na klucz osoby odpowiedzialnej za rejestrację dokumentów niejawnych.

§ 12.1 Osobą upoważnioną do przyjmowania niejawnej korespondencji wchodzącej do Urzędu w formie listów czy paczek jest Pełnomocnik ochrony oraz osoba odpowiedzialna za rejestrację dokumentów niejawnych.

2. Listy lub paczki zawierające korespondencję niejawną mogą wpływać z zewnątrz jako przesyłki „polecone” bezpośrednio do kancelarii materiałów niejawnych bądź poprzez sekretariat.



3. Pracownik sekretariatu, po stwierdzeniu, że wewnątrz znajduje się druga koperta oznaczona klauzulą tajności, nie otwiera jej i nie rejestruje w swojej ewidencji, informując niezwłocznie Pełnomocnika ochrony o jej nadejściu.
4. Pełnomocnik ochrony przyjmuje przesyłki lub dokumenty za pokwitowaniem i odciska na nich pieczęć oraz datę wpływu do kancelarii materiałów niejawnych.
5. Przyjmując przesyłkę sprawdza się :
 - 1) prawidłowość adresu;
 - 2) całość pieczęci i opakowania;
 - 3) zgodność odcisku pieczęci na opakowaniu z nazwą jednostki nadawcy;
 - 4) zgodność numeru na przesyłce z numerem tej przesyłki w wykazie lub w książce doręczeń.
6. W razie stwierdzenia uszkodzenia opakowania przesyłki niejawnej lub śladów jej otwierania, osoba przyjmująca przesyłkę sporządza wraz z doręczycielem protokół uszkodzenia w trzech egzemplarzach, z których pierwszy otrzymuje Pełnomocnik ochrony, drugi wysyła się nadawcy, a trzeci pozostawia się w aktach doręczyciela.
7. Po otwarciu przesyłki Pełnomocnik ochrony:
 - 1) sprawdza, czy zawartość przesyłki odpowiada wyszczególnionym na niej numerom ewidencyjnym;
 - 2) ustala, czy liczba załączników i stron jest zgodna z liczbą oznaczoną na poszczególnych dokumentach.
8. W przypadku stwierdzenia nieprawidłowości Pełnomocnik ochrony sporządza w dwóch egzemplarzach protokół z otwarcia przesyłki zawierający opis nieprawidłowości, jeden egzemplarz przekazuje do kancelarii nadawcy. Fakt sporządzenia protokołu odnotowuje się w dzienniku ewidencji w rubryce „Informacje uzupełniające/Uwagi”.
9. Przekazywanie przesyłek niejawnych bezpośrednio adresatowi z pominięciem kancelarii materiałów niejawnych jest zabronione, nawet gdy są oznaczone napisem „Do rąk własnych”.
10. W kancelarii materiałów niejawnych nie otwiera się przesyłek oznaczonych „do rąk własnych”. Rejestruje się je w dzienniku ewidencji z adnotacją o ich oznaczeniu, opisuje na opakowaniu datę wpływu, pozycję i numer w dzienniku, a następnie przekazuje bezpośrednio adresatowi – za pokwitowaniem. W razie nieobecności adresata przesyłkę przekazuje się osobie posiadającej pisemne upoważnienie do odbioru korespondencji niejawnej - za pokwitowaniem w dzienniku ewidencji.
11. Przesyłki oznaczone „Do rąk własnych”, po wykorzystaniu zwraca się do kancelarii w stanie otwartym bądź zamkniętym. Jeśli zwrot nastąpi w stanie otwartym, uzupełnia się pozostałe kolumny w dzienniku ewidencji i odciska pieczęć wpływu na dokumencie, natomiast jeśli zwrot nastąpi w stanie zamkniętym, osoba zwracająca dokument zobowiązana jest udzielić osobie odpowiedzialnej za rejestrację dokumentów niejawnych informacji, czego dokument dotyczy, ile zawiera stron, ilość załączników oraz osobiście odciska pieczęć wpływu wpisując numer z dziennika ewidencji. Dokument jest przechowywany w kancelarii materiałów niejawnych lub wraca do pracownika, który go otrzymał.
12. Dokumenty niejawne, wpływające do Urzędu przed zarejestrowaniem wymagają decyzji Wójta Gminy lub Sekretarza Gminy, w formie pisemnej dekretacji dokonanej w sposób trwały na dokumencie, kierującej ten dokument do konkretnego pracownika do załatwienia.
13. Następnie Pełnomocnik ochrony przekazuje dokument osobie odpowiedzialnej za rejestrację dokumentów niejawnych, który rejestruje pismo w dzienniku ewidencji dokumentów niejawnych. Pismo wchodzące po rejestracji w kancelarii materiałów niejawnych trafia do wskazanego w dekretacji uprawnionego pracownika, który kwituje



odbiór dokumentu w dzienniku ewidencji. Dokumenty są tematycznie upinane w teczkach i przechowywane w kancelarii materiałów niejawnych lub innych pomieszczeniach, jeżeli będą umieszczane w meblach biurowych zamykanych na klucz, zgodnie z ustawowymi wymogami.

14. Każdy pracownik, który zapoznał się z treścią dokumentów niejawnego, dokonuje stosowanej adnotacji stwierdzającej ten fakt w karcie zapoznania się z dokumentem. Wzór karty zapoznania się z dokumentem stanowi *załącznik nr 2*.

15. Korespondencji niejawnej mylnie skierowanej nie ewidencjonuje się w kancelarii materiałów niejawnych, lecz przekazuje łącznie z poprzednim opakowaniem w nowej kopercie właściwemu adresatowi za zwrotnym potwierdzeniem odbioru.

16. Przesyłki pilne, telegramy i szyfrogramy doręcza się adresatom bezzwłocznie. Przy kwitowaniu tych przesyłek odnotowuje się godzinę doręczenia.

17. W przypadku otrzymania przesyłki niewiadomego pochodzenia lub budzącej podejrzenia z jakiegokolwiek powodu należy postępować zgodnie z instrukcją - *załącznik nr 3*.

18. Wytworzony dokument niejawny w Urzędzie oraz wysyłaną przesyłkę niejawną osoba odpowiedzialna za rejestrację dokumentów niejawnych rejestruje w dzienniku ewidencji odpowiednio w kolejności wytworzenia.

19. Zapisów w dzienniku ewidencji dokonuje się kolorem czarnym lub niebieskim, a zmiany tych zapisów kolorem czerwonym z datą, powodem dokonania zmiany i czytelnym podpisem dokonującego zmiany. Zabrania się wycierania i zamazywania zapisów w dzienniku ewidencji.

20. Korespondencja niejawna wysyłana jest pocztą, lisem poleconym za zwrotnym potwierdzeniem odbioru w podwójnej kopercie. Przygotowaną przesyłkę należy wpisać do „pocztowej książki nadawczej” wypełniając poszczególne kolumny, a następnie dostarczyć do wysłania jako przesyłkę poleconą do sekretariatu Urzędu.

Rozdział 10

Zakres udostępniania informacji niejawnych

§ 13.1. Udostępnianie pracownikowi informacji niejawnych uwarunkowane jest posiadaniem właściwego i ważnego poświadczenia bezpieczeństwa lub upoważnienia Wójta, tylko w zakresie niezbędnym do załatwienia konkretnej sprawy.

2. Pełnomocnik ochrony współdziała ze służbami ochrony państwa za wiedzą i zgodą Wójta, w przypadku naruszenia przepisów o ochronie informacji niejawnych.

3. Służby ochrony państwa mogą zwracać się do Wójta z pisemnym wnioskiem o przekazanie informacji oraz udostępnienie niezbędnych dokumentów, w celu potwierdzenia danych o osobach sprawdzanych.

Rozdział 11

Zasady wytwarzania dokumentów zawierających informacje niejawne

§ 14.1. Propozycję 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 sporządzonych dokumentów zawierające informacje niejawne muszą być wykonane w brulionach (zeszytach) uprzednio zarejestrowanych w dzienniku ewidencji dokumentów niejawnych.

Dokumenty niejawne powinny być opisane i oznaczone zgodnie z rozporządzeniem Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów, umieszczania na nich klauzul tajności, a także zmiany nadanej klauzuli tajności (Dz. U. Nr 288, poz. 1692).

4. Sposób właściwego opisanie dokumentu niejawnego został przedstawiony w załączniku nr 4 do Planu ochrony.

Rozdział 12

Wytwarzanie dokumentów niejawnych z wykorzystaniem sprzętu komputerowego

§ 15.1. Bezpieczeństwo teleinformatyczne zapewnia się chroniąc informacje przetwarzane w systemach teleinformatycznych przed utratą właściwości gwarantujących to bezpieczeństwo, w szczególności przed utratą poufności, dostępności i integralności.

2. Bezpieczeństwo teleinformatyczne zapewnia się przed rozpoczęciem oraz w trakcie przetwarzania informacji niejawnych w systemie teleinformatycznym.

3. Za właściwą organizację bezpieczeństwa teleinformatycznego odpowiada Wójt, który w szczególności:

- 1) zapewnia opracowanie dokumentacji bezpieczeństwa systemu teleinformatycznego;
- 2) realizuje ochronę fizyczną systemu teleinformatycznego;
- 3) zapewnia niezawodność transmisji oraz kontrolę dostępu do urządzeń systemu teleinformatycznego;
- 4) dokonuje analizy stanu bezpieczeństwa teleinformatycznego oraz zapewnia usunięcie stwierdzonych nieprawidłowości;
- 5) zapewnia przeszkolenie z zakresu bezpieczeństwa teleinformatycznego dla osób uprawnionych do pracy w systemie teleinformatycznym.

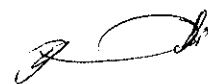
4. Wójt wyznacza:

- 1) Inspektora bezpieczeństwa teleinformatycznego – pracownik pionu ochrony odpowiedzialny za:
 - a) weryfikację i bieżącą kontrolę zgodności funkcjonowania systemu teleinformatycznego, ze szczególnymi wymaganiami bezpieczeństwa oraz przestrzegania procedur bezpiecznej eksploatacji.
- 2) Administratora systemu – pracownik odpowiedzialny za:
 - a) funkcjonowanie systemu teleinformatycznego,
 - b) przestrzeganie zasad i wymagań bezpieczeństwa przewidzianych dla systemu teleinformatycznego.

Wyżej wymienione osoby powinny posiadać poświadczenie bezpieczeństwa odpowiednie do klauzuli informacji wytwarzanych, przetwarzanych, przechowywanych lub przekazywanych w systemie teleinformatycznym oraz odbyć specjalistyczne szkolenia z zakresu bezpieczeństwa teleinformatycznego prowadzone przez służby ochrony państwa. Zaświadczenie o odbytym szkoleniu jest przechowywane w aktach osobowych oraz dokumentacji Pełnomocnika ochrony.

5. Systemy teleinformatyczne, w których mają być przetwarzane informacje niejawne o klauzuli:

- 1) „poufne” – podlegają akredytacji bezpieczeństwa teleinformatycznego, które udziela Agencja Bezpieczeństwa Wewnętrznego wydając świadectwo akredytacji bezpieczeństwa teleinformatycznego;
 - 2) „zastrzeżone” – Wójt udziela akredytacji bezpieczeństwa teleinformatycznego przez zatwierdzenie dokumentacji bezpieczeństwa systemu teleinformatycznego.
6. Ochrona fizyczna systemu teleinformatycznego polega na zastosowaniu środków zapewniających ochronę przed nieuprawnionym dostępem, podglądem czy podsłuchem.



7. Ochrona elektromagnetyczna systemu teleinformatycznego polega na niedopuszczeniu do utraty poufności i dostępności informacji niejawnych przetwarzanych w urządzeniach teleinformatycznych:

- 1) utrata poufności następuje w szczególności na skutek wykorzystania elektromagnetycznej emisji ujawniającej, pochodzącej z tych urządzeń;
 - 2) utrata dostępności następuje w szczególności na skutek zakłócania pracy urządzeń teleinformatycznych za pomocą impulsów elektromagnetycznych o dużej mocy.
8. W celu zapewnienia kontroli dostępu do systemu teleinformatycznego:
- 1) Wójt lub osoba przez niego upoważniona ustala warunki i sposób przydzielania uprawnień osobom uprawnionym do pracy w systemie teleinformatycznym;
 - 2) Administrator systemu określa warunki oraz sposób przydzielania tym osobom kont oraz mechanizmów kontroli dostępu, a także zapewnia ich właściwe wykorzystanie.
9. W sytuacjach wymagających konsultacji lub uzgodnień Wójt może zwrócić się do Agencji Bezpieczeństwa Wewnętrznego o wydanie opinii lub zleceń w zakresie bezpieczeństwa teleinformatycznego.

Rozdział 13 **Klauzule tajności**

§ 16.1. Oznaczenie materiału klauzulą tajności polega na umieszczeniu na nim klauzuli tajności. Przyznaną klauzulę tajności nanosi się w sposób wyraźny i w pełnym jej brzmieniu.

2. Wprowadza się następujące oznaczenia klauzul tajności dla dokumentów niejawnych stanowiących tajemnicę służbową:

- 1) „Pf” - dla klauzuli „poufne”;
- 2) „Z” - dla klauzuli „zastrzeżone”.

3. Materiały zawierające informacje niejawne utrwalone na piśmie oznaczają się w następujący sposób:

- 1) na każdej stronie pisma umieszcza się:
 - a) na środku, jako pierwszy element w nagłówku strony, klauzulę tajności,
 - b) numer egzemplarza pisma, a w przypadku gdy dokument wykonano w jednym egzemplarzu - napis "egz. pojedynczy",
 - c) sygnaturę literowo-cyfrową, na którą składają się: literowe oznaczenie jednostki lub komórki organizacyjnej, symbol oznaczenia klauzuli tajności, numer, pod którym dokument został zarejestrowany i rok, w którym dokonano rejestracji,
 - d) numer strony łamany przez liczbę stron całego pisma,
 - e) w środku, jako ostatni element w stopce strony, klauzulę tajności;
- 2) na pierwszej stronie pisma umieszcza się również:
 - a) nazwę jednostki lub komórki organizacyjnej,
 - b) nazwę miejscowości i datę podpisania dokumentu,
 - c) w przypadku pisma, któremu nadano bieg korespondencyjny, imię i nazwisko lub nazwę stanowiska adresata, a w przypadku wielu adresatów dopuszcza się możliwość umieszczenia jedynie adnotacji „adresaci według rozdzielnika”;
- 3) na ostatniej stronie pisma umieszcza się również:
 - a) liczbę załączników,
 - b) liczbę stron lub innych jednostek miary wszystkich załączników lub informację określającą rodzaj załączonego materiału i jego odpowiednią jednostkę miary,

- c) klauzule tajności załączników wraz z numerami, pod jakimi zostały zarejestrowane oraz liczbę stron każdego załącznika lub informację określającą rodzaj załączonego materiału i jego odpowiednią jednostkę miary,
- d) w przypadku, gdy adresatowi wysyła się inną liczbę załączników niż pozostawia w aktach, dodatkowo umieszcza się napis "tylko adresat" – jeżeli załączniki mają być przekazane adresatowi bez pozostawiania ich w aktach, napis "do zwrotu" - jeżeli załączniki mają zostać zwrócone nadawcy,
- e) stanowisko oraz imię i nazwisko lub inne oznaczenie wskazujące osobę uprawnioną do jego podpisania,
- f) liczbę wykonanych egzemplarzy,
- g) adresatów poszczególnych egzemplarzy pisma lub adnotację "adresaci według rozdzielnika",
- h) dyspozycję „ad acta” w przypadku egzemplarza pozostającego w aktach nadawcy,
- i) imię i nazwisko lub inne dane identyfikujące wykonawcę.

4. Na pismach stanowiących załączniki, na pierwszej stronie umieszcza się dodatkowo napis: „Załącznik nr ... do pisma nr ... z dnia ...”.

5. Jeżeli przy piśmie przewodnim przesyła się załączniki oznaczone klauzulami tajności, to:

- 1) klauzula pisma przewodniego lub dokumentu nie może być niższa niż klauzula załącznika o najwyższym stopniu tajności;
- 2) na piśmie przewodnim, jeżeli jego klauzula jest inna po odłączeniu załączników, zamieszcza się dyspozycję co do klauzuli tajności pisma po trwałym ich odłączeniu;
- 3) na każdej stronie pod numerem egzemplarza zamieszcza się napis: "... (nazwa klauzuli tajności) po odłączeniu załączników" lub "Jawne po odłączeniu załączników".

6. Na materiałach innych niż pismo klauzulę tajności i sygnaturę literowo-cyfrową umieszcza się przez ostemplowanie, nadrukowanie, wpisanie odręczne, trwałe dołączenie metek, nalepek, kalkomanii lub w inny widoczny sposób, bezpośrednio, a jeżeli to nie jest możliwe - na ich obudowie lub opakowaniu.

§ 17.1. Na pismach zawierających informacje niejawne, wobec których minął okres ochrony lub okres ustanowiony przez wytwórcę dokumentu:

- 1) skreśla się wszystkie dotychczasowe oznaczenia znoszonej klauzuli tajności;
 - 2) na pierwszej stronie nad skreśloną klauzulą tajności umieszcza się napis „zniesiono klauzulę tajności” oraz datę, imię, nazwisko i podpis imię i nazwisko osoby dokonującej tych adnotacji oraz wskazuje się podstawę dokonania czynności.
2. Na pismach zawierających informacje niejawne, wobec których zniesiono lub zmieniono przyznaną klauzulę tajności:
- 1) na każdej stronie skreśla się dotychczasowe klauzule tajności;
 - 2) nad skreślonymi klauzulami tajności umieszcza się nowe klauzule tajności;
 - 3) nad pierwszym w kolejności skreślonym oznaczeniem klauzuli tajności umieszcza się datę, podpis, imię i nazwisko lub inne oznaczenie wskazujące osobę dokonującą tych adnotacji oraz wskazuje się podstawę dokonania czynności.
3. Skreśleń i adnotacji dokonuje osoba odpowiedzialna za rejestrację dokumentów niejawnych, albo upoważnione przez Wójta inne osoby.
4. Skreśleń i adnotacji dokonuje się kolorem czerwonym w sposób czytelny. Wycieranie, wywabianie lub zamazywanie klauzuli tajności i dokonanych zmian jest niedozwolone.

5. Na dokumencie nieelektronicznym wytworzonym w wyniku kopiowania lub tłumaczenia umieszcza się:

- 1) w przypadku kopii - na pierwszej stronie sygnaturę literowo-cyfrową, o której mowa w § 16 ust.3 pkt 1 lit. „c”;
- 2) na wszystkich stronach:
 - a) w przypadku kopiowania napis "Wydruk", "Kopia", "Odpis", "Wyciąg" albo "Wypis",
 - b) w przypadku tłumaczenia napis "Tłumaczenie z języka (nazwa języka)" oraz podpis, imię i nazwisko lub inne oznaczenie wskazujące osobę dokonującą tłumaczenia;
- 3) na ostatniej stronie w przypadku kopiowania dodatkowo potwierdzenie zgodności z oryginałem zawierające:
 - a) napis "Za zgodność",
 - b) odcisk pieczęci z nazwą jednostki lub komórki organizacyjnej, w której wytworzono dokument,
 - c) podpis, imię i nazwisko lub inne oznaczenie wskazujące kierownika jednostki lub komórki organizacyjnej, w której dokonano kopiowania, albo osobę przez niego upoważnioną.

6. Wytworzenie dokumentu w wyniku kopiowania lub tłumaczenia dokumentu nieelektronicznego odnotowuje się na ostatniej stronie dokumentu kopiowanego lub tłumaczonego przez umieszczenie informacji o:

- 1) nazwie jednostki lub komórki organizacyjnej, w której wytworzono dokument;
- 2) liczbie egzemplarzy dokumentu wytworzonego;
- 3) dacie wytworzenia dokumentu;
- 4) numerze, pod jakim wytworzony dokument został zarejestrowany.

Rozdział 14

Nadzór w zakresie ochrony informacji niejawnych

§ 18.1. Za ochronę informacji niejawnych w Urzędzie odpowiada Wójt.

2. Wójt przeprowadza nie rzadziej niż raz na 5 lat przegląd materiałów w celu ustalenia czy spełniają ustawowe przesłanki ochrony.

3. Zadania określone ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych w imieniu Wójta wykonuje Pełnomocnik ochrony poprzez:

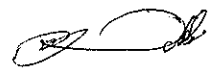
- 1) sprawowanie nadzoru nad realizacją zadań i przestrzeganiem przepisów określonych w Planie ochrony;
- 2) sprawowanie kontroli w zakresie ochrony informacji niejawnych oraz przestrzegania procedur związanych z upoważnianiem do dostępu do tych informacji, w odniesieniu do wszystkich komórek organizacyjnych Urzędu.

Rozdział 15

Odpowiedzialność karna, dyscyplinarna i służbowa za naruszenie przepisów o ochronie informacji niejawnych

§ 19.1. Zakres odpowiedzialności karnej osób, które dopuściły się przestępstwa lub czynu zabronionego przeciwko ochronie informacji niejawnych został określony przepisami Kodeksu Karnego (ustawa z dnia 6 czerwca 1997 r. Kodeks Karny, Dz. U. Nr 88, poz. 553 ze 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. W stosunku do pracowników, którzy nie przestrzegają wymagań związanych z ochroną informacji niejawnych i nierzetelnie wykonują swoje obowiązki, dopuszczają się uchybień w zakresie niewłaściwego zabezpieczenia dokumentów i informacji podlegających ochronie stwarzając warunki do ujawnienia tajemnicy osobom nieuprawnionym, zastosowane być mogą przewidziane prawem sankcje dyscyplinarne i służbowe.

Rozdział 16

Archiwizowanie, gromadzenie i niszczenie materiałów niejawnych

§ 20.1. Archiwizowanie materiałów niejawnych odbywa się z zachowaniem zasad określonych:

- 1) 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. Nr 167, poz. 1375);
- 2) w rozporządzeniu Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz. U. Nr 14, poz. 67).
2. Dokumentacja wytwarzana i gromadzona dzieli się na:
 - 1) materiały archiwalne - wchodzące do państwowego zasobu archiwalnego;
 - 2) dokumentację niearchiwalną - inną dokumentację, niestanowiącą materiałów archiwalnych;
3. Rzeczową klasyfikację oraz kwalifikację dokumentacji ze względu na okresy jej przechowywania wytwarzania i gromadzenia zawierają jednolite rzeczowe wykazy akt (załącznik nr 2 - Dz. U. z 2011 r. Nr 14, poz. 67).
4. Wykazy akt, o których mowa w pkt 3 stanowią podstawę gromadzenia dokumentacji w aktach spraw.
5. Dokumentacja niearchiwalna podlega brakowaniu po upływie okresu przechowywania określonego we właściwym wykazie akt.
6. Brakowanie dokumentacji niearchiwalnej polega na ocenie jej przydatności do celów praktycznych, wydzieleniu dokumentacji nieprzydatnej i przekazaniu jej na makulaturę.
7. Brakowanie dokumentacji niearchiwalnej następuje na wniosek Wójta na podstawie zgody właściwego archiwum. Do wniosku o zgodę dołącza się:
 - 1) protokół oceny dokumentacji niearchiwalnej;
 - 2) spis dokumentacji niearchiwalnej przeznaczonej do przekazania na makulaturę lub zniszczenie albo spis dokumentacji technicznej niearchiwalnej przeznaczonej na makulaturę lub zniszczenie (wzór stanowi załącznik nr 5 - Dz. U. z 2002 r. Nr 167, poz. 1375).
8. Protokół oraz spis dokumentacji niearchiwalnej sporządza komisja powołana przez Wójta, w której skład wchodzi: osoba prowadząca archiwum zakładowe, przedstawiciel komórki organizacyjnej, której dokumentacja niearchiwalna podlega brakowaniu oraz Pełnomocnik ochrony.

9. W przypadku trudności w ocenie brakowanej dokumentacji niearchiwalnej można zwrócić się do miejscowo właściwego archiwum państwowego o przeprowadzenie ekspertyzy.
10. W archiwum zakładowym Urzędu przechowuje się dokumenty brakowania wraz z dowodami przekazania nieprzydatnej dokumentacji niearchiwalnej na makulaturę bądź protokołami jej zniszczenia.
11. Uporządkowanie materiałów archiwalnych polega na podziale rzeczowym teczek i prawidłowym ułożeniu materiałów wewnątrz teczek, ich opisaniu, nadaniu właściwego układu, sporządzeniu ewidencji oraz technicznym zabezpieczeniu.
12. 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 teście powinny być opatrzone kolejną numeracją.
13. Akta spraw niejawnych ostatecznie załatwionych Urząd przechowuje w swoim archiwum zakładowym, po wcześniejszym zniesieniu klauzuli tajności.
14. Przekazywanie akt odbywa się na podstawie spisu zdawczo-odbiorczego przez komórkę, w której dokument niejawny był przechowywany, pod nadzorem Pełnomocnika ochrony.

Rozdział 17

Ustalenia końcowe

§ 21.1. Kierownicy Referatów Urzędu, przełożeni pracowników, a także Pełnomocnik ochrony:

- 1) zapoznają podległych pracowników z ustaleniami Planu ochrony informacji niejawnych w Urzędzie;
- 2) zapewnią bieżące przestrzeganie postanowień Planu ochrony w zakresie ochrony informacji niejawnych, mogących występować w działalności kierowanej komórki organizacyjnej.
2. Osoby wymienione w ust. 1, wprowadzą jako obowiązującą zasadę zapoznawania z Planem ochrony wszystkie osoby, które podejmują pracę w komórkach organizacyjnych.
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 w każdym czasie zwracać się o wyjaśnienia czy też instruktaż do Pełnomocnika ochrony.
4. O wszelkich nieprawidłowościach, będących następstwem naruszenia zasad określonych w Planie ochrony, każdy pracownik jest zobowiązany niezwłocznie poinformować o tym swojego przełożonego, a ten Pełnomocnika ochrony, który podejmie stosowne działania zmierzające do wyjaśnienia okoliczności powstałej sytuacji, informując o tym Wójta.
5. W sprawach nieuregulowanych w planie ochrony mają zastosowanie odpowiednie przepisy ustawy o ochronie informacji niejawnych, aktów wykonawczych wydanych na jej podstawie oraz odpowiednich zarządzeń Wójta.

Wójt
inż. Piotr Wolski

Dziennik ewidencji dokumentów niejawnych

Strona lewa

Oznaczenie klauzuli tajności	Numer kolejny zapisu	Adnotacje dotyczące obowiązywania klauzuli tajności lub jej zniesienia albo zmiany	Data rejestracji dokumentu	Nazwa nadawcy/a dresata	Numer i data dokumentu otrzymanego	Nazwa dokumentu lub czego dotyczy	Liczba egzemplarzy	Liczba wychodzących/przychodzących		
								Stron dokumentu	Załączników	Stron wszystkich załączników
1	2	3	4	5	6	7	8	9	10	11

Strona/.....

Strona prawa

Nr dokumentu, z którego wykonano wydruk, kopię, wyciąg, wypis, odpis, tłumaczenie lub numer nośnika	Imię i nazwisko osoby sporządzającej dokument	Imię i nazwisko osoby otrzymującej dokument, data i podpis	Potwierdzenie zwrotu dokumentu (data i podpis)	Adnotacje		Informacje uzupełniające/Uwagi
				O wystaniu dokumentu lub załącznika (pozycja w książce wychodzącej Urzędu/załącznik do pisma nr...)	O wybrakowaniu lub archiwizacji	
12	13	14	15	16	17	18

Strona/.....

Karta zapoznania się z dokumentem nr ...

Lp.	UDOSTĘPNIENIE DOKUMENTU			Uwagi
	Imię i nazwisko osoby, której dokument udostępniono	data	podpis	

Strona/.....



**Instrukcja postępowania w przypadku otrzymania
przesyłki niewiadomego pochodzenia**

I. W przypadku otrzymania jakiegokolwiek **przesyłki niewiadomego pochodzenia** lub budzącej podejrzenia z jakiegokolwiek innego powodu:

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

NIE NALEŻY OTWIERAĆ TEJ PRZESYŁKI

Należy:

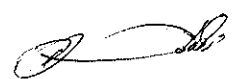
1. Umieścić przesyłkę w grubym worku plastikowym, szczelnie zamknąć.
 2. Worek należy umieścić w drugim plastikowym worku, szczelnie zamknąć, zakleić taśmą lub plastrem.
 3. Paczki nie należy przemieszczać, należy pozostawić ją na miejscu.
 4. Powiadomić:
 - Komendę Powiatową Policji tel. 997; 56 6823200; kom. 112,
 - Komendę Powiatową Państwowej Straży Pożarnej tel. 998; 56 6835389.
- Służby te podejmą wszelkie niezbędne kroki w celu bezpiecznego przejęcia przesyłki.

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

Należy:

1. **NIE NARUSZYĆ ZAWARTOŚCI** - nie rozsypywać, nie przenosić, nie dotykać, nie wachać, nie powodować ruchu powietrza w pomieszczeniu (wylączyć 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; 56 6823200; kom. 112,
 - Komendę Powiatową Państwowej Straży Pożarnej tel. 998; 56 6835389;
 - Powiatową Stację Sanitarno- Epidemiologiczną 56 6832442;
 - Pogotowie Ratunkowe tel. 999; 56 6832291.

**PO PRZYBYCIU WŁAŚCIWEJ SŁUŻBY NALEŻY
BEZWZGLĘDNIE STOSOWAĆ SIĘ DO JEJ ZALECEŃ**



**Sposób oznaczania dokumentów niejawnych oznaczonych klauzulą „poufne” lub
„zastrzeżone” oraz umieszczania klauzuli na tych dokumentach**

Pierwsza strona dokumentu zawierającego informacje niejawne

KLAUZULA TAJNOŚCI

.....
.....
Nazwa jednostki organizacyjnej

.....
Miejscowość, data

Sygnatura literowo-cyfrowa

Egz. Nr/Egzemplarz pojedynczy

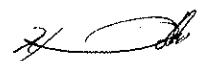
ADRESAT

.....
.....

TREŚĆ DOKUMENTU

Nr strony/ilość stron dokumentu

KLAUZULA TAJNOŚCI



Druga i kolejne strony dokumentu zawierającego informacje niejawne

KLAUZULA TAJNOŚCI

Sygnatura literowo-cyfrowa

Egz. Nr/Egzemplarz pojedynczy

CD. TREŚCI DOKUMENTU

Nr strony/ilość stron dokumentu

KLAUZULA TAJNOŚCI



Ostatnia strona dokumentu zawierającego informacje niejawne

KLAUZULA TAJNOŚCI

Sygnatura literowo-cyfrowa

Egz. Nr/Egzemplarz pojedynczy

CD. TREŚCI DOKUMENTU

- liczba załączników
- liczba stron lub innych jednostek miary wszystkich załączników lub informację określającą rodzaj załączonego materiału i jego odpowiednią jednostkę miary,
- klauzule tajności załączników wraz z numerami, pod jakim zostały zarejestrowane - liczba stron każdego załącznika, liczbę stron każdego załącznika,
- w przypadku gdy adresatowi wysyła się inną liczbę załączników niż pozostawia w aktach, dodatkowo: napis „tylko adresat” - jeżeli załączniki mają być przekazane adresatowi bez pozostawiania ich w aktach, napis "do zwrotu" - jeżeli załączniki mają zostać zwrócone nadawcy

.....
Nazwa stanowiska oraz imię i nazwisko
osoby uprawnionej do jego podpisania

- liczba wykonanych egzemplarzy
- adresaci poszczególnych egzemplarzy
- dyspozycja „ad acta” w przypadku egzemplarza pozostawionego w aktach nadawcy
- nazwisko osoby, która wykonała dokument

Nr strony/ilosc stron dokumentu

KLAUZULA TAJNOŚCI

