Zarządzenie Nr 75 /2015
Wójta Gminy Cielądz
z dnia 09.10.2015 r.
w sprawie wprowadzenia do stosowania dokumentów dotyczących ochrony informacji niejawnych w Urzędzie Gminy Cielądz

Na podstawie art. 15 ust. 1 pkt 5, art. 43 ust. 5 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2010 r. Nr 182 , poz. 1228 z póź. Zm.), art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U. z 2013 r., poz. 594 z póź. zm.),. zarządzam co następuje:

§ 1.

Zatwierdzam i wprowadzam do stosowania w Urzędzie Gminy Cielądz następujące dokumenty dotyczące ochrony informacji niejawnych:

1) plan ochrony informacji niejawnych, stanowiący załącznik nr 1 do zarządzenia,
2) dokumentację określającą poziom zagrożeń dla systemu ochrony informacji niejawnych, stanowiącą załącznik nr 2 do zarządzenia,
3) instrukcję określającą sposób i tryb przetwarzania informacji niejawnych o klauzuli „ZASTRZEŻONE", stanowiącą załącznik nr 3 zarządzenia.

§ 2

Zobowiązuję pracowników do zapoznania się z treścią niniejszego zarządzenia oraz przestrzegania zawartych w zarządzeniu postanowień.

§ 3

Wykonanie zarządzenia powierzam Pełnomocnikowi Ochrony do Spraw Informacji Niejawnych w Urzędzie Gminy Cielądz.

§ 4

Traci moc zarządzenie Nr 30/2006 Wójta Gminy Cielądz z dnia 06 grudnia 2006 r. w sprawie „wprowadzenia planu ochrony informacji niejawnych, szczegółowych wymagań w zakresie ochrony informacji niejawnych stanowiących tajemnicę służbową oznaczonych klauzulą „poufne", „zastrzeżone" oraz wykaz rodzajów informacji stanowiących tajemnicę służbową w Urzędzie Gminy w Cielądzu".

§ 5

Zarządzenie wchodzi w życie z dniem podpisania.

Załącznik Nr 1
do Zarządzenia Nr 75/2015
Wójta Gminy Cielądz
z dnia 09.10. 2015 r.

PLAN OCHRONY INFORMACJI NIEJAWNYCH W URZĘDZIE GMINY CIELĄDZ

opracowany na podstawie postanowień art. 15 ust. 1 pkt 5 ustawy
z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych
(Dz.U. z 2010 r. Nr 182, poz. 1228)

ZATWIERDZAM:

WÓJT
mgr Paweł Królak

.....
podpis i pieczęć imienna Wójta Gminy

OPRACOWAŁA: Ewelina Biernacka
Pełnomocnik ds. ochrony
informacji niejawnych

Cielądz – wrzesień 2015

SPIS TREŚCI

POSTANOWIENIA OGÓLNE

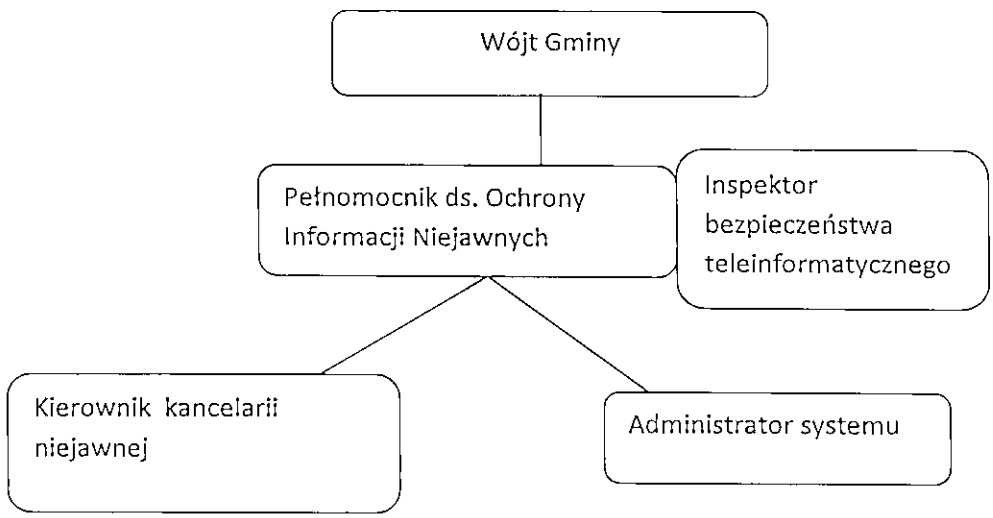
Przedmiotem ochrony w Urzędzie Gminy są informacje niejawne oznaczone klauzulą „zastrzeżone". Plan ochrony informacji niejawnych jest dokumentem określającym sposób i tryb przetwarzania informacji niejawnych o klauzuli „zastrzeżone", a także sposoby zapewnienia fizycznego bezpieczeństwa informacji.

Środki i procedury określone w planie ochrony odnoszą się do informacji niejawnych oznaczonych klauzulą „zastrzeżone" w rozumieniu ustawy z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych /Dz. U. z 2010 nr 182 poz.1228/.

Wprowadzone do stosowania środki i procedury w zakresie ochrony informacji niejawnych określa:

- „Instrukcja sposobu i trybu przetwarzania informacji niejawnych o klauzuli „zastrzeżone" w Urzędzie Gminy Cielądz",

W Urzędzie Gminy jest wyodrębniona komórka organizacyjna do spraw ochrony informacji niejawnych, zwana dalej „pionem ochrony" -rys. 1.



1. DEFINICJE W ROZUMIENIU PLANU OCHRONY INFORMACJI NIEJAWNYCH

W rozumieniu Planu ochrony informacji niejawnych:

1. służbami ochrony państwa - jest Agencja Bezpieczeństwa Wewnętrznego, Służby Kontrwywiadu Wojskowego
2. rękojmia zachowania tajemnicy - oznacza spełnienie przez osobę ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem, stwierdzona w wyniku przeprowadzenia postępowania sprawdzającego
3. dokumentem - jest każda utrwalona informacja niejawna, w szczególności na piśmie, mikrofilmach, negatywach i fotografiach, nośnikach do zapisów informacji w postaci cyfrowej i na taśmach elektromagnetycznych , także w formie mapy, wykresu, rysunku, obrazu, broszury, książki kopii, odpisu, wypisu, wyciągu i tłumaczenia dokumentu, zbędnego lub wadliwego wydruku, odbitki, kliszy, matrycy i dysku optycznego, kalki, taśmy atramentowej, oraz informacja niejawna utrwalona na elektronicznych nośnikach danych.
4. 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;
5. systemem teleinformatycznym - jest system teleinformatyczny służący do przetwarzania informacji niejawnych o klauzuli „zastrzeżone" w Urzędzie Gminy Cielądz. Tworzą go urządzenia, narzędzia, metody postępowania i procedury stosowane przez wyspecjalizowanych pracowników w sposób zapewniający odpowiednią ochronę.
6. akredytacja bezpieczeństwa teleinformatycznego - dopuszczenie systemu teleinformatycznego do wytwarzania, przetwarzania, przechowywania informacji niejawnych.
7. dokumentacja bezpieczeństwa systemu teleinformatycznego – dokument szczególnych wymagań bezpieczeństwa, oraz dokument procedur bezpiecznej eksploatacji systemu teleinformatycznego, opracowane zgodnie z zasadami określonymi w ustawie.
8. urzędem - jest Urząd Gminy Cielądz.
9. wójtem - jest Wójt Gminy Cielądz.
10. pełnomocnik ochrony - Pełnomocnik do spraw Ochrony Informacji Niejawnych w Urzędzie Gminy Cielądz.
11. pion ochrony – wyodrębniona komórka organizacyjna podległa pełnomocnikowi do spraw ochrony informacji niejawnych.

2. OCENA ZAGROŻEŃ

a) ZAGROŻENIA ZEWNĘTRZNE

1. Zagrożeniami zewnętrznymi dla Urzędu Gminy Cielądz są:

a) możliwość napadu przez zorganizowane grupy przestępcze i terrorystyczne, działające w sposób profesjonalny, przemyślany i zorganizowany,

b) możliwość napadu przez pojedynczych przestępców, przypadkowe osoby wykorzystujące nadarzającą się okazję z powodu nieprawidłowości w ochronie mienia Urzędu.

Symptomy mogące świadczyć o przygotowywaniu takich działań:

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, 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.

Wnioski

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

1) kontrolę 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) stosować zasadę niedopuszczania osób niepowołanych do penetracji stref bezpieczeństwa,

4) wykonywanie prac porządkowych, remontowych itp. w strefie bezpieczeństwa wyłącznie pod nadzorem osób odpowiedzialnych.

b) ZAGROŻENIA WEWNĘTRZNE

1. Zagrożeniami wewnętrznymi dla Urzędu Gminy Cielądz są:

a) próby zaboru dokumentów lub mienia przez pracowników Urzędu Gminy

b) próby powielania, kserowania dokumentów służbowych dla celów prywatnych przez byłych i obecnych pracowników Urzędu Gminy, a w szczególności przez byłych pracowników zwolnionych dyscyplinarnie,

Symptomy mogące świadczyć o przygotowywaniu takich działań:

1) rozpoznanie organizacji pracy Urzędu Gminy celem łatwiejszej pracy grup przestępczych na terenie Urzędu,

2) próby wglądu w dokumenty niejawne przez osoby nieuprawnione,

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 Wójta Gminy,

5) zwrócenie szczególnej uwagi na osoby, których zachowanie wskazuje na nadmierne spożywanie alkoholu i innych środków odurzających.

3. PRZEDMIOT OCHRONY

Przedmiotem ochrony w Urzędzie Gminy Cielądz, są:

1. Informacje niejawne oznaczone klauzulą „zastrzeżone".

2. Pomieszczenia, w których są przechowywane i opracowane materiały niejawne.

3. Autonomiczne stanowisko komputerowe przeznaczone do przetwarzania informacji niejawnych oznaczonych klauzulą „zastrzeżone"

4. ZABEZPIECZENIE INFORMACJI NIEJAWNYCH

1. W celu zmniejszenia ryzyka zapoznania się z informacjami niejawnymi przez osoby do tego nieuprawnione utworzono specjalne pomieszczenie zwane kancelarią niejawną. Pomieszczenie jest zabezpieczone przed podglądaniem z zewnątrz i wyposażone w szafę stalową klasy A, z zamkami o skomplikowanym mechanizmie oraz szafy biurowe zamykane na klucz.
2. Informacje niejawne oznaczone klauzulą „zastrzeżone" są przechowywvane w pomieszczeniu kancelarii niejawnej, w meblach biurowych zamykanych na klucz.
3. Komputer wykorzystywany wyłącznie do przetwarzania i wytwarzania informacji niejawnych po zakończeniu pracy jest odłączany z sieci elektrycznej.

5. EWIDENCJA INFORMACJI NIEJAWNYCH PODLEGAJACYCH OCHRONIE

1. Dokumenty niejawne oznaczone klauzulą „zastrzeżone" mogą być wytwarzane i przetwarzane w pomieszczeniu kancelarii do spraw ochrony i przetwarzania informacji niejawnych.

2. Dokumenty niejawne wpływające do Urzędu i wychodzące z Urzędu podlegają ewidencjonowaniu w dzienniku ewidencyjnym.

3. Dokumenty niejawne wytworzone pozostające wyłącznie w Urzędzie rejestruje się w dzienniku ewidencyjnym.

4. Numer ewidencyjny każdego dokumentu niejawnego o klauzuli „zastrzeżone" powinien być poprzedzony skrótem literowym „Z".

5. Ewidencjonowaniu w kancelarii do spraw ochrony i przetwarzania informacji niejawnych podlegają wszystkie dokumenty zawierające informacje niejawne.

6. Osobą upoważnioną do przyjmowania niejawnej korespondencji wchodzącej w formie listów czy paczek jest Kierownik kancelarii ds. informacji niejawnych. Listy lub paczki zawierające korespondencję niejawną mogą wpływać z zewnątrz jako przesyłki „polecone" bezpośrednio do kancelarii niejawnej, poprzez sekretariat 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 Kierownika kancelarii

ds. informacji niejawnych o jej nadejściu.

7. Korespondencji niejawnej mylnie skierowanej nie ewidencjonuje się w kancelarii niejawnej, lecz przekazuje łącznie z poprzednim opakowaniem w nowej kopercie nadawcy za zwrotnym potwierdzeniem odbioru.

6. ZASADY DOSTĘPU DO INFORMACJI NIEJAWNYCH – POSTĘPOWANIE SPRAWDZAJĄCE

1.Informacje niejawne „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 do dostępu do informacji niejawnych o klauzuli „poufne" może nastąpić po:

a) uzyskaniu poświadczenia bezpieczeństwa, po przeprowadzonym zwykłym postępowaniu sprawdzającym,

b) odbyciu szkolenia z zakresu ochrony informacji niejawnych.

3. Uzyskanie uprawnień do dostępu do informacji niejawnych o klauzuli „zastrzeżone" może nastąpić po:

a) pisemnym upoważnieniu danej osoby przez Wójta Gminy oraz

b) odbyciu szkolenia w zakresie ochrony informacji niejawnych.

4. Zwykłe postępowanie sprawdzające związane z dostępem do informacji niejawnych przeprowadza Pełnomocnik Ochrony na pisemne polecenie Wójta Gminy.

5. Postępowanie sprawdzające ma na celu ustalenie, czy osoba sprawdzana daje rękojmię zachowania tajemnicy.

6. Każda osoba podlegająca procedurze postępowania sprawdzającego zobowiązana jest do:

a) wypełnienia określonej przepisami ankiety bezpieczeństwa osobowego,

b) wypełnienia ankiety w sposób dokładny i zgodny z prawdą.

7. Zwykłe postępowanie sprawdzające obejmuje:

a) 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;

b) 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.

c) 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, a w związku z tym nie uzyskanie poświadczenia bezpieczeństwa warunkującego dostęp do informacji podlegających ochronie skutkować może:

a) przeniesieniem danej osoby na stanowisko nie związane z informacjami niejawnymi,

b) rozwiązaniem umowy o pracę w przypadku niemożności zmiany stanowiska,

c) niemożnością zatrudnienia na danym stanowisku, w odniesieniu do osoby ubiegającej się o zatrudnienie w Urzędzie.

9. 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 Gminy.

7. KANCELARIA DO SPRAW OCHRONY INFORMACJI NIEJAWNYCH

W Urzędzie Gminy w Cielądzu nie przetwarza i nie przechowuje się: dokumentów zawierających informacje niejawne oznaczone klauzulą „poufne", „tajne", "ściśle tajne". W urzędzie Gminy nie funkcjonuje „kancelaria tajna" w rozumieniu ustawy o ochronie informacji niejawnych.

W Urzędzie funkcjonuje Kancelaria do Spraw Ochrony Informacji Niejawnych.

1. Kancelarię do Spraw Ochrony Informacji Niejawnych tworzy Wójt Gminy Cielądz.
2. Kancelarii Niejawnej są rejestrowane, przechowywane i wydawane uprawnionym osobom informacje niejawne o klauzuli „zastrzeżone". Kancelaria spełnia wszystkie wymagania prawne odnośnie ochrony fizycznej informacji niejawnych, co zabezpiecza materiały przed ich nieuprawnionym ujawnieniem, utratą, uszkodzeniem lub zniszczeniem.
3. Kancelarią kieruje Kierownik Kancelarii wyznaczony przez Wójta na wniosek Pełnomocnika do Spraw Ochrony Informacji Niejawnych.
4. Do obowiązków Kierownika Kancelarii do Spraw Ochrony Informacji Niejawnych należy:
   a) bezpośredni nadzór nad obiegiem materiałów niejawnych będących na stanie kancelarii
   b) udostępnianie materiałów osobom do tego uprawnionym,

c) wydawanie materiałów osobom do tego uprawnionym, które zapewniają odpowiednie warunki do ich przechowywania

d) egzekwowanie zwrotu materiałów,

e) kontrola przestrzegania właściwego oznaczania i rejestrowania materiałów niejawnych w Urzędzie,

f) prowadzenie bieżącej kontroli postępowania z dokumentami niejawnymi,

5. W przypadku zmiany na stanowisku Kierownika Kancelarii do Spraw Ochrony Informacji Niejawnych sporządza się protokół zdawczo-odbiorczy.

6. Protokół, o którym mowa w pkt 5 sporządza się w obecności Kierownika zdającego obowiązki, osoby przejmującej obowiązki Kierownika oraz Pełnomocnika do Spraw Ochrony Informacji Niejawnych. Protokół sporządza się w dwóch egzemplarzach, pierwszy egzemplarz przechowywany jest w Kancelarii do Spraw Ochrony Informacji Niejawnych, drugi u Pełnomocnika do Spraw Ochrony Informacji Niejawnych.

7. W przypadku czasowej nieobecności Kierownika Kancelarii jego obowiązki przejmuje Pełnomocnik do Spraw Ochrony Informacji Niejawnych lub pracownik pisemnie przez niego upoważniony.

8. Po zakończeniu pracy Kierownik Kancelarii do Spraw Ochrony Informacji Niejawnych jest obowiązany sprawdzić prawidłowość zamknięcia szaf i pomieszczeń Kancelarii.

9. Zasady przechowywania kluczy i pieczęci

a) Klucze do szafy metalowej oraz pieczęcie po zakończeniu pracy są złożone w pomieszczeniu kancelarii niejawnej w miejscu niewidocznym.

b) Kierownik kancelarii po zakończeniu pracy zamyka drzwi wejściowe do kancelarii niejawnej, klucze umieszcza w pojemniku, schowanym w biurku zamykanym na klucz.

10. Wszelkie nieprawidłowości związane z naruszeniem zasad określonych powyżej należy niezwłocznie zgłaszać Pełnomocnikowi do Spraw Ochrony Informacji Niejawnych.

11. Środki ochrony fizycznej informacji niejawnych w kancelarii niejawnej:

a) ściany i stropy wykonane są z materiałów niepalnych, spełniających wymagania w zakresie klasy odporności pożarowej oraz nośności granicznej odpowiadającej, co najmniej konstrukcji murowanej z pustaka Alfa cegły pełnej o grubości 380 m. Ściany działowe wykonane z cegły dziurkawki palonej o grubości 650 mm.

b) drzwi wewnętrzne wyposażone są w zamek drzwiowy wielopunktowy, które spełniają wymagania Polskiej Normy PN-90/B-92270,

c) szafy biurowe zamykane na klucz

d) szafa stalowa klasy A

➢ POSTĘPOWANIE Z PRZESYŁKAMI

1. Kierownik Kancelarii do Spraw Ochrony Informacji Niejawnych przyjmuje przesyłki lub dokumenty za pokwitowaniem i odciska na nich pieczęć oraz datę wpływu do Urzędu.
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 do Spraw Ochrony Informacji Niejawnych kwitujący odbiór przesyłki sporządza, wraz z doręczającym, protokół uszkodzenia. Jeden egzemplarz protokołu przekazuje się nadawcy, drugi Pełnomocnikowi do Spraw Ochrony Informacji Niejawnych w Urzędzie, a w przypadku gdy w obiegu przesyłek pośredniczył przewoźnik – kolejny egzemplarz protokołu przekazuje się także jemu.
4. Po otwarciu przesyłki Kierownik Kancelarii:
   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 sporządza w dwóch egzemplarzach protokół z otwarcia przesyłki zawierający opis nieprawidłowości, jeden egzemplarz przekazując do Kancelarii nadawcy, drugi egzemplarz zostaje w aktach kancelarii.
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, o której mowa w pkt 1, 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 5, 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 kolorem czarnym lub niebieskim. Zmian dokonuje się kolorem czerwonym, umieszczając datę i czytelny podpis dokonującego zmiany. Zabrania się wycierania i zamazywania adnotacji.

15. 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.

16. Dokumenty, materiały oraz zbiory dokumentów dotyczące spraw ostatecznie zakończonych przechowuje się w Kancelarii jako materiały archiwalne.

➢ ZAKRES UDOSTĘPNIANIA INFORMACJI NIEJAWNYCH

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.

8. ZASADY WYKONYWANIA DOKUMENTÓW ZAWIERAJĄCYCH INFORMACJE NIEJAWNE

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. Dokumenty niejawne powinny być opisane i oznaczone zgodnie z rozporządzeniem Prezesa Rady Ministrów z dnia 22 grudnia 2011 roku w sprawie sposobu oznaczania i umieszczania na nich klauzur tajności (Dz.U.2011.288.1692). Wzór opisania dokumentu stanowi załącznik nr 5 do Planu Ochrony.

9. WYKONYWANIE DOKUMENTÓW ZAWIERAJĄCYCH INFORMACJE NIEJAWNE ZA POMOCĄ SPRZĘTU KOMPUTEROWEGO

Pracownicy, którzy do opracowywania i wykonywania dokumentów zawierających informacje niejawne 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.

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 Gminy, który w szczególności:

a) zapewnia opracowanie dokumentacji bezpieczeństwa teleinformatycznego,

b) realizuje ochronę fizyczną, elektromagnetyczną i kryptograficzną systemu teleinformatycznego,

c) zapewnia niezawodność transmisji oraz kontrolę dostępu do urządzeń systemu teleinformatycznego,

d) dokonuje analizy stanu bezpieczeństwa teleinformatycznego oraz zapewnia usunięcie stwierdzonych nieprawidłowości,

e) zapewnia przeszkolenie z zakresu bezpieczeństwa teleinformatycznego dla osób uprawnionych do pracy w systemie lub sieci teleinformatycznej,

4. Ochrona fizyczna systemu lub sieci teleinformatycznej polega na:

1) umieszczeniu urządzeń systemu teleinformatycznego w strefie bezpieczeństwa, strefie administracyjnej lub specjalnej strefie bezpieczeństwa, zwanych dalej „strefą kontrolowanego dostępu" w zależności od:

a) klauzuli tajności,

b) ilości,

c) zagrożeń dla poufności, integralności lub dostępności informacji niejawnych,

2) zastosowaniu środków zapewniających ochronę fizyczną, w szczególności przed:

a) nieuprawnionym dostępem,

b) podglądem,

c) podsłuchem.

5. W celu zapewnienia kontroli dostępu do systemu teleinformatycznego:

a) Wójt Gminy lub osoba przez niego upoważniona ustala warunki i sposób przydzielania uprawnień osobom uprawnionym do pracy w systemie lub sieci teleinformatycznej,

b) administrator systemów określa warunki oraz sposób przydzielania tym osobom kont oraz mechanizmów kontroli dostępu, a także zapewnia ich właściwe wykorzystanie.

6. Systemy teleinformatyczne, w których mają być przetwarzane informacje niejawne podlegają akredytacji bezpieczeństwa teleinformatycznego.

7. Akredytacja następuje na podstawie dokumentów szczególnych wymagań bezpieczeństwa i procedur bezpiecznej eksploatacji.

8. Wójt Gminy wyznacza osobę odpowiedzialną za funkcjonowanie systemów teleinformatycznych oraz za przestrzeganie zasad i wymagań bezpieczeństwa systemów i sieci teleinformatycznych, zwaną administratorem systemu.

9. W przypadku wykonywania dokumentów przy wykorzystaniu komputera, gdy nie zachodzi potrzeba zachowania tekstu dokumentu niejawnego na elektronicznym nośniku magnetycznym, zaleca się nie wprowadzać zapisu do pamięci komputera, zarówno do pamięci stałej, na dysk twardy, jak też na dyskietkę, a więc doprowadzić do wykasowania tekstu z chwilą wykonania niezbędnej ilości egzemplarzy danego dokumentu.

KOPIE ZAPASOWE

1. W uzasadnionych przypadkach 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 opakowaniu.

10. ZMIANA I ZNOSZENIE KLAUZUL TAJNOŚCI

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

a) skreśla się wszystkie dotychczasowe oznaczenia znoszonej klauzuli tajności;

b) 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:

a) na każdej stronie skreśla się dotychczasowe klauzule tajności;

b) nad skreślonymi klauzulami tajności umieszcza się nowe klauzule tajności;

c) 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 odpowiednio Kierownik kancelarii niejawnej.

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:

a) w przypadku kopii - na pierwszej stronie sygnaturę literowo-cyfrową, na którą składają się: literowe oznaczenie jednostki lub komórki organizacyjnej, symbol oznaczenia klauzuli tajności, numer, pod którym ten dokument został zarejestrowany, rok, w którym dokonano

rejestracji, a także, w zależności od potrzeb, inne oznaczenia ułatwiające ustalenie miejsca wykonania dokumentu w jednostce lub komórce organizacyjnej lub też jego przynależność do określonej sprawy,

b) na wszystkich stronach: -w przypadku kopiowania napis "Wydruk", "Kopia", "Odpis", "Wyciąg" albo "Wypis", -w przypadku tłumaczenia napis "Tłumaczenie z języka (nazwa języka)" oraz podpis, imię i nazwisko lub inne oznaczenie wskazujące osobę dokonującą tłumaczenia;

d) na ostatniej stronie w przypadku kopiowania dodatkowo potwierdzenie zgodności z oryginałem zawierające: -napis "Za zgodność", -odcisk pieczęci z nazwą jednostki lub komórki organizacyjnej, w której wytworzono dokument, -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:

a) nazwie jednostki lub komórki organizacyjnej, w której wytworzono dokument;

b) liczbie egzemplarzy dokumentu wytworzonego;

c) dacie wytworzenia dokumentu;

d) numerze, pod jakim wytworzony dokument został zarejestrowany

11. GROMADZENIE DOKUMENTÓW ZAWIERAJĄCYCH INFORMACJE NIEJAWNE

Dokumenty zawierające informacje niejawne oznaczone odpowiednią klauzulą, podlegają gromadzeniu w teczkach akt oznaczonych właściwą klauzulą tajności.

12. NADZÓR W ZAKRESIE OCHRONY INFORMACJI NIEJAWNYCH

1. Za ochronę informacji niejawnych w Urzędzie Gminy Cielądz odpowiada Wójt Gminy.

2. Zadania określone ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych w imieniu Wójta wykonuje Pełnomocnik do Spraw Ochrony Informacji Niejawnych 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.

13. 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 niejawnych został określony przepisami Kodeksu Karnego (ustawa z dnia 06 czerwca 1997 r. Kodeks Karny, Dz. U. Nr 88, poz. 553 z późn. 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, dopuszczą 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.

14. 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, zasadami jej klasyfikowania i kwalifikowania oraz zasadami i trybem

przekazywania materiałów archiwalnych do archiwów państwowych (Dz.U.Nr 167, poz. 1375).

2. Dokumentacja wytwarzana i gromadzona dzieli się na:

a) materiały archiwalne - wchodzące do państwowego zasobu archiwalnego,

b) dokumentację niearchiwalną - inną dokumentację, niestanowiącą materiałów archiwalnych.

c) rzeczową klasyfikację oraz kwalifikację dokumentacji ze względu na okresy jej przechowywania, wytwarzania i gromadzenia zawierają jednolite rzeczowe wykazy akt.

3. Wykazy akt, o których mowa w pkt c stanowią podstawę gromadzenia dokumentacji w aktach spraw.

4. Dokumentacja niearchiwalna, podlega brakowaniu po upływie okresu przechowywania określonego we właściwym wykazie akt.

5. Brakowanie dokumentacji niearchiwalnej polega na ocenie jej przydatności do celów praktycznych, wydzieleniu dokumentacji nieprzydatnej i przekazaniu jej na makulaturę.

6. Brakowanie dokumentacji niearchiwalnej następuje na wniosek Wójta Gminy na podstawie zgody właściwego archiwum. Do wniosku o zgodę 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.

7. Protokół oraz spis dokumentacji niearchiwalnej sporządza komisja powołana przez Wójta Gminy.

8. W przypadku trudności w ocenie brakowanej dokumentacji niearchiwalnej, można zwrócić się do miejscowo właściwego archiwum państwowego o przeprowadzenie ekspertyzy.

9. W archiwum zakładowym przechowuje się dokumenty brakowania, wraz z dowodami przekazania nieprzydatnej dokumentacji niearchiwalnej na makulaturę bądź protokołami jej zniszczenia.

10. Uporządkowanie materiałów archiwalnych polega na podziale rzeczowym teczek i prawidłowym ułożeniu materiałów wewnątrz teczek, ich opisaniu, nadaniu właściwego układu, sporządzeniu ewidencji oraz technicznym zabezpieczeniu.

11. 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.

12. 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, to jest symbolu literowego komórki organizacyjnej oraz symbolu klasyfikacyjnego według wykazu akt, obowiązującego w jednostce organizacyjnej,

c) tytułu teczki, to jest 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, to jest dat najwcześniejszego i najpóźniejszego materiału archiwalnego w teczce,

e) sygnatury teczki, to jest numeru spisu zdawczo-odbiorczego i numeru pozycji teczki w spisie zdawczoodbiorczym,

f) symbolu kwalifikacyjnego materiałów archiwalnych (kategoria A),

g) liczby stron w teczce.

13. Czynności związane z brakowaniem materiałów niearchiwalnych, wobec których archiwum państwowe wyraziło zgodę są dokumentowanie przez sporządzenie protokołu komisyjnego zniszczenia dokumentów niearchiwalnych.

14. Protokół komisyjnego zniszczenia materiałów niearchiwalnych sporządzany jest w dwóch egzemplarzach, z czego jeden egzemplarz należy przesłać do właściwego archiwum państwowego.

15. USTALENIA KOŃCOWE

1. Wójt, Sekretarz, Pełnomocnik do Spraw Ochrony Informacji Niejawnych:

a) zapoznają podległych pracowników z ustaleniami Planu Ochrony Informacji Niejawnych w Urzędzie.

b) zapewnią bieżące przestrzeganie postanowień Planu Ochrony na stanowiskach, gdzie występują informacje niejawne.

2. Osoby wymienione w pkt 1, wprowadzą jako obowiązującą zasadę, zapoznawania z Planem Ochrony wszystkie osoby, które podejmują pracę na stanowiskach związanych z przetwarzaniem 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 w każdym czasie zwracać się o wyjaśnienia czy też instruktaż do Pełnomocnika Ochrony, w razie potrzeby pełnomocnik organizuje szkolenie w zakresie przepisów zawiązanych z ochroną informacji niejawnych.

4. Integralną część Planu ochrony stanowią załączniki w ilości 6, wyspecyfikowane poniżej.

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 Gminy.

16. ZAŁĄCZNIKI DO PLANU OCHRONY INFORMACJI NIEJAWNYCH W URZĘDZIE GMINY CIELĄDZ

1. Załącznik nr 1 – Instrukcja alarmowa w przypadku zgłoszenia o podłożeniu lub znalezieniu ładunku wybuchowego w budynkach Urzędu

2. Załącznik nr 2 – Instrukcja postępowania w przypadku otrzymania przesyłki niewiadomego pochodzenia

3. Załącznik nr 3 – Wykaz informacji niejawnych oznaczonych klauzulą „zastrzeżone" w zadaniach realizowanych przez Urząd Gminy Cielądz.

4. Załącznik nr 4 – Wykaz stanowisk i funkcji z którymi może wiązać się dostęp do informacji niejawnych oznaczonych klauzulą zastrzeżone.

5. Załącznik nr 5 - Sposób oznaczania dokumentów niejawnych oraz umieszczania klauzul na tych dokumentach.

6. Załącznik nr 6 – Plan postępowania z materiałami zawierającymi informacje niejawne w razie wprowadzenia stanu nadzwyczajnego.

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.

3. 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 Gminy.

4. 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 Gminy powinien na bieżąco organizować szkolenie pracowników w zakresie sposobu zachowania się w sytuacjach wymienionych w tej części Planu oraz winien znać rozmieszczenie newralgicznych punktów - węzły energetyczne i wodne, które udostępnia się na żądanie policjanta kierującego akcją.

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

INSTRUKCJA POSTĘPOWANIA W PRZYPADKU OTRZYMANIA PRZESYŁKI NIEWIADOMEGO POCHODZENIA

W przypadku otrzymania jakiejkolwiek przesyłki niewiadomego pochodzenia 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.

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 Wójta Gminy, oraz

Komendę Powiatową Policji tel. 997
Komendę Powiatową Straży Pożarnej tel. 998
Służby te podejmą wszelkie niezbędne kroki w celu bezpiecznego przejęcia przesyłki.

W przypadku gdy podejrzana przesyłka została otwarta i zawiera jakąkolwiek podejrzaną zawartość w formie stałej (galaretę, pianę, pył lub inną).
Ważne:
1. **NIE NARUSZAĆ ZAWARTOŚCI** - 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 Wójta Gminy, oraz Komendę Powiatową Policji, Komendę Powiatową Państwowej Straży Pożarnej.

PO PRZYBYCIU WŁASCIWYCH SŁUŻB
NALEŻY BEZWZGLĘDNIE STOSOWAĆ SIĘ DO ICH ZALECEŃ

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

WYKAZ INFORMACJI NIEJAWNYCH OZNACZONYCH KLAUZULĄ „ZASTRZEŻONE" W ZADANIACH REALIZOWANYCH PRZEZ URZĄD GMINY CIELĄDZ

L.p.	Nazwa zadania	Uwagi
1.	Plan Akcji Kurierskiej	
2.	Sprawozdanie roczne z realizacji Akcji Kurierskiej	
3.	Karty realizacji zadań w zakresie uruchomienia akcji kurierskiej	
4.	Plan Operacyjny Funkcjonowania Gminy w warunkach zewnętrznego zagrożenia bezpieczeństwa państwa w czasie wojny	
5.	Bilans personelu medycznego na potrzeby obronne państwa na terenie Gminy Cielądz	
6.	Regulamin Organizacyjny Urzędu na czas wojny	
7.	Zestawienie świadczeń rzeczowych i osobistych	
8.	Organizacja głównego stanowiska kierowania w stałej siedzibie Urzędu Gminy na czas bezpośredniego zagrożenia państwa i wojny	

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

WYKAZ STANOWISK I FUNKCJI Z KTÓRYMI MOŻE ŁĄCZYĆ SIĘ DOSTĘP DO INFORMACJI NIEJAWNYCH OZNACZONYCH KLAUZULĄ „ZASTRZEŻONE"

L.p.	Stanowisko – Funkcja	Uwagi
1.	Wójt Gminy Cielądz	
2.	Sekretarz	
3.	Skarbnik	
4.	Kierownik Referatu Organizacyjnego i Spraw Obywatelskich	
5.	Z-ca Kierownika USC	
6.	Pełnomocnik ds. ochrony informacji niejawnych	
7.	Kierownik Gminnego Ośrodka Pomocy Społecznej	
8.	Kierownik Gminnego Zespołu Administracyjno – Ekonomicznego Szkół	
9.	Inspektor ds. ewidencji ludności	
10.	Osoby Funkcyjne Akcji Kurierskiej/kurierzy wykonawcy/	

Załącznik nr 5
do Planu Ochrony Informacji Niejawnych
w Urzędzie Gminy Cielądz

Sposób oznaczania dokumentów niejawnych oznaczonych klauzulą „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 .....

CD. TREŚCI DOKUMENTU

Nr strony/ilość stron dokumentu

KLAUZULA TAJNOŚCI

Ostatnia strona dokumentu zawierającego informacje niejawne

KLAUZULA TAJNOŚCI

Sygnatura literowo-cyfrowa Egz. Nr .....

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

-dyspozycję „ad acta" w przypadku egzemplarza pozostawionego w aktach nadawcy

-nazwisko osoby, która wykonała dokument

Nr strony/ilość stron dokumentu

KLAUZULA TAJNOŚCI

Załącznik nr 6
do Planu Ochrony Informacji Niejawnych
w Urzędzie Gminy Cielądz

PLAN

POSTĘPOWANIA Z MATERIAŁAMI ZAWIERAJĄCYMI INFORMACJE NIEJAWNE W RAZIE WPROWADZENIA STANU NADZWYCZAJNEGO

Rozdział 1

Postanowienia ogólne

§1

Plan postępowania z materiałami zawierającymi informacje niejawne w razie wprowadzenia stanu nadzwyczajnego – zwany dalej „planem" jest dokumentem określającym:

1. Zadania i przedsięwzięcia techniczno – organizacyjne, przewidywane do realizacji dla zapewnienia skutecznej ochrony, przechowywanych materiałów zawierających informacje niejawne, na wypadek wystąpienia lub wprowadzenia stanu nadzwyczajnego;
2. Sposoby zapewnienia fizycznego bezpieczeństwa ochrony dokumentów zawierających informacje niejawne.

§2

Za stan nadzwyczajny uważa się wymienione w art. 288 Konstytucji RP, stany takie jak: stan wojenny, stan wyjątkowy lub stan klęski żywiołowej oraz każdą sytuację, w której zaistnieje groźba lub stan bezpośredniego zagrożenia bezpieczeństwa osób przebywających w budynku urzędu, a także mienia tam zgromadzonego, wywołaną czynnikami zewnętrznymi, np. pożar, włamanie, zamach, atak terrorystyczny, powódź, katastrofa budowlana itp. sytuacje kryzysowe.

§3

1. W przypadku wystąpienia lub wprowadzenia w urzędzie stanu nadzwyczajnego, kierowanie realizacją zadań i przedsięwzięć określonych w planie dla ochrony obiektu i pracowników przejmuje Wójt, w przypadku nieobecności Wójta Sekretarz, o ile posiada on odpowiednie poświadczenie bezpieczeństwa osobowego lub upoważnienie wydane przez kierownika jednostki upoważniające do dostępu do informacji niejawnych.
2. Jeżeli Sekretarz nie posiada poświadczenia bezpieczeństwa lub upoważnienia, o którym mowa w ust. 1, kierowanie realizacją zadań i przedsięwzięć określonych w planie dla ochrony obiektu i pracowników przejmuje pełnomocnik ochrony.

3. Wójt lub Sekretarz kierujący realizacją zadań i przedsięwzięć, o których mowa w ust. 1:
    a) współdziała z pełnomocnikiem ochrony, który wypracowuje propozycje wszystkich decyzji związanych z realizacją planu oraz bezpośrednio koordynuje ich realizację;
    b) może podjąć decyzję o wprowadzeniu na terenie gminy:
        - ograniczonego wstępu;
        - zakazu wstępu;
        - wprowadzenia systemu przepustek;
4. Przepisu ust. 3 pkt 1 nie stosuje się w przypadku, o którym mowa w ust. 2.
5. Pełnomocnik ochrony koordynuje realizację decyzji, o których mowa w ust. 3 pkt 1, może prowadzić konsultacje z właściwymi służbami ochrony państwa.

Rozdział 2

Szczegółowy tryb postępowania

§4

1. W zakresie przedsięwzięć techniczno – organizacyjnych, podejmowanych w ramach profilaktyki na wypadek wystąpienia lub wprowadzenia stanu nadzwyczajnego, dla zapewnienia skutecznej ochrony przechowywanych w urzędzie materiałów zawierających informacje niejawne, Kierownik Kancelarii do spraw informacji niejawnych wyposaży pomieszczenie z wyznaczoną strefą ochronną w niezbędny sprzęt ppoż., a także dodatkowo pojemniki lub worki wykonane z materiałów niepalnych, przeznaczone do ochrony i ewentualnej ewakuacji materiałów niejawnych z tej strefy, w asortymencie i ilościach odpowiadających faktycznym potrzebom zgłoszonym przez pełnomocnika ochrony.
2. Kierownik Kancelarii, o którym mowa w ust. 1 ponosi odpowiedzialność za utrzymanie w należytym stanie technicznym i jakościowym wyposażenia, o którym mowa w ust. 1, w tym również za przestrzeganie terminów dokonywania przeglądów sprzętu ppoż.

§5

1. W przypadku wystąpienia lub wprowadzenia stanu nadzwyczajnego, niezależnie od przyczyny jego wywołania, pełnomocnik ochrony, po otrzymaniu odpowiednich dyspozycji podjętych w trybie§4 ust. 1.
2. Wstępnego zabezpieczenia materiałów dokonuje się poprzez właściwe oznakowanie następującymi symbolami: E – ewakuować, Z – zniszczyć, zgodnie z symbolami umieszczonymi pod kategorią archiwalną.
3. Za prawidłową selekcję i właściwe oznaczenie materiałów w sposób, o którym mowa w ust. 2, odpowiedzialny jest pracownik ochrony po uzgodnieniu z wytwórcą materiału.
4. Symbole określające sposób postępowania z materiałami, nadaje się na bieżąco lub nanosi na już istniejące teczki aktowe i obowiązujące formularze ewidencyjne.
5. Ewakuację materiałów zawierających informacje niejawne przeprowadza pracownik pionu ochrony informacji niejawnych, niezwłocznie po otrzymaniu odpowiedniej decyzji podjętej w trybie §3 ust.1. Decyzja ta powinna wskazać miejsce wyznaczone do ewakuacji, z zastrz. ust. 6.
6. Miejsce ewakuacji powinno gwarantować bezpieczeństwo ewakuowanym materiałom. W przypadku braku takiego miejsca w urzędzie, materiały ewaluowane mogą być przetransportowane poza urząd.
7. Kierownik Kancelarii zapewnia odpowiedni środek transportowy w celu przeprowadzenia ewakuacji.
8. W sytuacjach nagłych, gdy stan nadzwyczajny wywołany został w godzinach pracy urzędu, np. zdarzeniami skierowanymi na kradzież materiałów zawierających informacje niejawne, wtargnięciem itp., pracownik pionu ochrony może samodzielnie podjąć decyzję o fizycznym zniszczeniu tych materiałów, o ile w jego ocenie ich bezpieczeństwo jest zagrożone.
9. O zniszczeniu dokumentów, o których mowa w ust. 8, pracownik ten niezwłocznie powiadamia Wójta Gminy lub Sekretarza oraz pełnomocnika ochrony. Wójt lub sekretarz o fakcie tym powiadamia właściwą służbę ochrony państwa i nadawcę dokumentów.

Rozdział 3

Postanowienia końcowe

§6

1. Z chwilą ustania przyczyn wystąpienia stanu nadzwyczajnego lub jego odwołania, co następuje w trybie jego wprowadzenia, pracownik pionu ochrony, pod nadzorem pełnomocnika ochrony, przystępuje do przewiezienia do pomieszczenia w której, wyznaczono strefę ochronną wcześniej ewakuowanych materiałów zawierających informacje niejawne. Przepis §4 ust. 1 stosuje się odpowiednio.
2. Po zakończeniu prac, o których mowa w ust. 1, pracownik pionu ochrony przeprowadza inwentaryzację całego zasobu materiałów zawierających informacje niejawne w Urzędzie. Wynik inwentaryzacji pracownik przekłada wójtowi i pełnomocnikowi ochrony.

Plan opracowała:
Ewelina Biernacka
Pełnomocnik ds. Ochrony
Informacji Niejawnych

Załącznik nr 2
do Zarządzenia Nr 75/2015
Wójta Gminy Cielądz
z dnia 09.10.2015r.

Dokumentacja określająca poziom zagrożeń dla systemu ochrony informacji niejawnych w Urzędzie Gminy Cielądz

ZATWIERDZAM:

WÓJT
mgr Paweł Królak

.....
Podpis Wójta

Opracowała Ewelina Biernacka
Pełnomocnik ds. ochrony
informacji niejawnych

Podstawowe kryteria i sposób określania poziomu zagrożeń

I. Wstęp

W celu prawidłowego zabezpieczenia informacji niejawnych, w tym doboru odpowiednich środków bezpieczeństwa fizycznego należy określić poziom zagrożeń nieuprawnionym ujawnieniem lub utratą informacji niejawnych. Określenie poziomu zagrożeń jest indywidualną oceną znaczenia czynników, o których mowa w przepisie § 3 ust. 6 rozporządzenia, mogących mieć wpływ na bezpieczeństwo informacji niejawnych w Urzędzie Gminy.

Z uwagi na specyfikę, zakres i różnorodność zadań realizowanych przez podmioty podlegające przepisom ustawy, ocena przedstawionych czynników leży w sferze odpowiedzialności kierownika jednostki organizacyjnej, w której informacje niejawne są przetwarzane.

Każdy z wymienionych czynników powinien zostać poddany wnikliwej analizie pod kątem jego znaczenia dla zagrożenia ujawnieniem lub utratą informacji niejawnych. Ocena poziomu zagrożeń uwzględniająca klauzule tajności przetwarzanych informacji będzie determinowała stosowanie odpowiednich środków bezpieczeństwa fizycznego.

II. Charakterystyka obiektu

1.1.Położenie obiektu

Budynek Urzędu zlokalizowany jest przy drodze wojewódzkiej nr 707. Tutaj też znajduje się kancelaria niejawna usytuowana na pierwszym piętrze budynku.

1.2. Dostępność komunikacyjna

Odległość budynku Urzędu od poszczególnych jednostek ratowniczych:

- Policja- 9,9 km
- Straż Pożarna – 10,9 km
- Pogotowie Ratunkowe – 8,8 km

W pobliżu budynku (max. 30 m) znajdują się przystanki autobusowe komunikacji dziennej.

1.3. Otoczenie budynku

Budynek Urzędu Gminy połączony jest korytarzem z innym budynkiem w którym znajduje się Ośrodek Zdrowia, USC oraz pomieszczenie biurowe.

W otoczeniu budynku Urzędu znajdują się inne obiekty na sąsiedniej działce – budynki mieszkalne, handlowo-usługowe.

1.4. Charakterystyka budynku

Jest to budynek o konstrukcji tradycyjnej wykonany z pustaka Alfa (kramzyt), spełniających wymagania w zakresie klasy odporności pożarowej. Posiada 3 kondygnacje. Ciągi

komunikacyjne od części biurowej i poszczególne pomieszczenia oddzielone są ścianami z pustaka.

III. Ocena istotności czynników zagrożeń

W ramach systemu bezpieczeństwa fizycznego informacji niejawnych stosuje się środki bezpieczeństwa fizycznego w celu zapewnienia poufności, integralności i dostępności tych informacji.

W celu doboru adekwatnych środków bezpieczeństwa fizycznego określa się poziom zagrożeń związanych z utratą poufności, integralności lub dostępności informacji niejawnych, zwany dalej „poziomem zagrożeń".

Poziom zagrożeń określa się dla pomieszczenia lub obszaru, w którym są przetwarzane informacje niejawne jako wysoki, średni albo niski.

Przy określaniu poziomu zagrożeń uwzględnia się:

a) Zagrożenia naturalne, wynikające z działania sił przyrody lub awarii urządzeń;
b) Zagrożenia związane zarówno z umyślnym, jak i nieumyślnym zachowaniem człowieka.

W celu określenia poziomu zagrożeń przeprowadza się analizę, w której uwzględnia się wszystkie istotne czynniki mogące mieć wpływ na bezpieczeństwo informacji niejawnych.

Cel zapewnienia bezpieczeństwa fizycznego informacji niejawnych osiąga się poprzez:

a) Zapewnienie właściwego przetwarzania informacji niejawnych
b) Umożliwienie zróżnicowania dostępu do informacji niejawnych dla pracowników zgodnie z posiadanymi przez nich uprawnieniami oraz uzasadnioną potrzebą dostępu do informacji niejawnych;
c) Wykrywanie, udaremnianie lub powstrzymywanie działań nieuprawnionych;
d) Uniemożliwienie lub opóźnianie wtargnięcia osób nieuprawnionych w sposób niezauważony lub z użyciem siły do pomieszczenia lub obszaru, w którym są przetwarzane informacje niejawne.

System środków bezpieczeństwa fizycznego obejmuje stosowanie rozwiązań organizacyjnych, wyposażenia i urządzeń służących ochronie informacji niejawnych oraz elektronicznych systemów pomocniczych wspomagających ochronę informacji niejawnych.

W zależności od poziomu zagrożeń określonego w wyniku przeprowadzonej analizy, stosuje się odpowiednią kombinację następujących środków bezpieczeństwa fizycznego:

a) Personel bezpieczeństwa – osoby przeszkolone, nadzorowane a w razie konieczności posiadające odpowiednie uprawnienie do dostępu do informacji niejawnych, wykonujące czynności związane z fizyczną ochroną informacji niejawnych, w tym kontrolę dostępu do

pomieszczeń lub obszarów, w których są przetwarzane informacje niejawne, a także reagowanie na alarmy lub sygnały awaryjne z możliwością zwrócenia się o dobrowolne poddanie się kontroli lub udostępnienie do kontroli rzeczy osobistych, a także przedmiotów wnoszonych lub wynoszonych – stosowany w celu zapobiegania próbom nieuprawnionego wnoszenia na chroniony obszar rzeczy zagrażających bezpieczeństwu informacji niejawnych lub nieuprawnionego wynoszenia informacji niejawnych z budynków lub obiektów;

b) Bariery fizyczne – środki chroniące granice miejsca, w których są przetwarzane informacje niejawne, w szczególności ogrodzenia, ściany, bramy, drzwi i okna;

c) Szafy i zamki – stosowane do przechowywania informacji niejawnych lub zabezpieczające te informacje przed nieuprawnionym dostępem;

d) System kontroli dostępu – obejmujący elektroniczny system pomocniczy lub rozwiązanie organizacyjne, stosowany w celu zagwarantowania uzyskiwania dostępu do pomieszczenia lub obszaru, w którym są przetwarzane informacje niejawne, wyłącznie przez osoby posiadające odpowiednie uprawnienia;

e) System organizacji włamania i napadu – elektroniczny system pomocniczy stosowany w celu realizacji procedur ochrony informacji niejawnych oraz podwyższenia poziomu bezpieczeństwa, który zapewnia bariery fizyczne, a w pomieszczeniach i budynkach zastępujący lub wspierający personel bezpieczeństwa;

TABELA OCENY ISTOTNOŚCI CZYNNIKÓW ZAGROŻEŃ

Lp.	CZYNNIK	OCENA ISTOTNOŚCI CZYNNIKA			UZASADNIENIE
		BARDZO ISTOTNY (8 pkt)	ISTOTNY (4 pkt)	MAŁO ISTOTNY (1 pkt)	
1	2	3	4	5	6
1.	Klauzula tajności przetwarzanych informacji niejawnych			1	Mała ilość dokumentów oznaczonych klauzulą tajności
2.	Liczba materiałów niejawnych			1	Mała liczba dokumentów zawierających informacje niejawne
3.	Postać informacji niejawnych			1	Mała ilość dokumentów. Te które są wytwarzane mają klauzulę nadawaną ręcznie
4.	Liczba osób			1	Niewielka ilość osób upoważnionych do dostępu do informacji niejawnych w stosunku do wszystkich zatrudnionych
5.	Lokalizacja		4		Budynek UG użytkowany jest również na działalność gospodarczą, sąsiedztwo parkingu.
6.	Dostęp osób do budynku		4		Obiekty UG w nocy są zamknięte i strzeżone. W godzinach urzędowania są powszechnie dostępne. Możliwość swobodnego poruszania się po budynku interesantów. Brak wyraźnych granic oddzielających dostęp do pomieszczeń biurowych urzędu.
7.	Inne czynniki*)			1	Brak zdefiniowanych zagrożeń
Suma punktów		13			

*) Jeśli kierownik jednostki organizacyjnej uzna, że w jego jednostce występują inne niż wymienione w wierszach 1–6 tabeli czynniki mające wpływ na zagrożenie ujawnieniem lub utratą informacji niejawnych, powinien je określić, stanowisko uzasadnić (informacje zamieszcza się w rubryce „Uzasadnienie"), a następnie dokonać oceny istotności tych czynników. Ocenie podlegają wszystkie inne czynniki łącznie. Oznacza to, że jeśli w jednostce występuje tylko jeden z wymienionych czynników, należy go ocenić jako „bardzo istotny", „istotny" lub „mało istotny" dla zagrożenia ujawnieniem lub utratą informacji niejawnych. Jeśli w jednostce występują dwa lub więcej czynników z tej grupy, należy oszacować je łącznie i ocenić wpływ tych czynników na ocenę zagrożenia ujawnieniem lub utratą informacji niejawnych. W sytuacji gdy np. jeden z „innych" czynników został oceniony jako „bardzo istotny", a drugi jako „mało istotny", należy wskazać ocenę o najwyższym znaczeniu (w tym przypadku ocena istotności „Innych czynników" zostałaby wskazana na poziomie „bardzo istotnym"). W sytuacji gdy kierownik jednostki organizacyjnej uzna, że w jego jednostce czynniki wymienione w tabeli są nieistotne lub ich występowanie jest mało realne (np. zagrożenie ze strony obcych służb specjalnych) czynnik 7. powinien zostać oceniony jako „mało istotny".

TABELA DO OKREŚLANIA POZIOMU ZAGROŻEŃ

POZIOM ZAGROŻEŃ		
NISKI	ŚREDNI	WYSOKI
7 pkt - 16 pkt	17 pkt - 32 pkt	powyżej 32 pkt

Na podstawie oceny czynników poziom zagrożeń wynosi 13 punktów, co klasyfikuje poziom zagrożeń obiektu na poziomie niskim (przedział 7-16 pkt.

TABELA ŚRODKÓW BEZPIECZEŃSTWA FIZYCZNEGO

PUNKTACJA ZASTOSOWANYCH ŚRODKÓW BEZPIECZEŃSTWA

ŚRODEK BEZPIECZEŃSTWA	PKT
KATEGORIA K1: Szafy do przechowywania informacji niejawnych	
Środek bezpieczeństwa K1S1 – Konstrukcja szafy	
Liczba punktów za środek bezpieczeństwa (K1S1=4,3,2 lub 1 pkt)	2
Środek bezpieczeństwa K1S2 – Zamek do szafy	
Liczba punktów za środek bezpieczeństwa (K1S2=4,3,2 lub 1 pkt)	2
Liczba punktów za kategorię K1 stanowiąca iloczyn liczby punktów za oba powyższe środki bezpieczeństwa (K1=K1S1×K1S2)	4
KATEGORIA K2: Pomieszczenia	
Środek bezpieczeństwa K2S1 – Konstrukcja pomieszczenia	
Liczba punktów za środek bezpieczeństwa (K2S1=4,3,2 lub 1 pkt)	1
Środek bezpieczeństwa K2S2 – Zamek do drzwi pomieszczenia	
Liczba punktów za środek bezpieczeństwa (K2S2=4,3,2 lub 1 pkt)	1
Liczba punktów za kategorię K2 stanowiąca iloczyn liczby punktów za oba powyższe środki bezpieczeństwa (K2=K2S1×K2S2)	2
KATEGORIA K3: Budynki	
Liczba punktów za kategorię (K3=5,3,2 lub 1 pkt)	3
KATEGORIA K4: Kontrola dostępu	
Środek bezpieczeństwa K4S1 – Systemy kontroli dostępu	
Liczba punktów za środek bezpieczeństwa (K4S1=4,3,2 lub 1 pkt)	
Środek bezpieczeństwa K4S2 – Kontrola osób nieposiadających stałego upoważnienia do wejścia na obszar jednostki organizacyjnej (interesantów)	
Liczba punktów za środek bezpieczeństwa (K4S2=3 lub 1 pkt)	
Liczba punktów za kategorię K4 stanowiąca sumę liczby punktów za oba powyższe środki bezpieczeństwa (K4=K4S1+K4S2)	

KATEGORIA K5: Personel bezpieczeństwa i systemy sygnalizacji napadu i włamania	
Środek bezpieczeństwa K5S1 – Personel bezpieczeństwa	
Liczba punktów za środek bezpieczeństwa (K5S1=5,4,3,2 lub 1 pkt)	
Środek bezpieczeństwa K5S2 – Systemy sygnalizacji napadu i włamania	
Liczba punktów za środek bezpieczeństwa (K5S2=4,3,2 lub 1 pkt)	
Liczba punktów za kategorię K5 stanowiąca sumę liczby punktów za oba powyższe środki bezpieczeństwa (K5=K5S1+K5S2)	
KATEGORIA K6: Granice	
Środek bezpieczeństwa K6S1 – Ogrodzenie	
Liczba punktów za środek bezpieczeństwa (K6S1=4,3,2 lub 1 pkt)	
Środek bezpieczeństwa K6S2 – Kontrola w punktach dostępu	
Liczba punktów za środek bezpieczeństwa (K6S2=1 lub 0 pkt)	
Środek bezpieczeństwa K6S3 – System kontroli osób i przedmiotów przy wejściu/wyjściu	
Liczba punktów za środek bezpieczeństwa (K6S3=1 lub 0 pkt)	
Środek bezpieczeństwa K6S4 – System wykrywania naruszenia ogrodzenia	
Liczba punktów za środek bezpieczeństwa (K6S4=1 lub 0 pkt)	
Środek bezpieczeństwa K6S5 – Oświetlenie chronionego obszaru	
Liczba punktów za środek bezpieczeństwa (K6S5=1 lub 0 pkt)	
Środek bezpieczeństwa K6S6 – System dozoru wizyjnego granic	
Liczba punktów za środek bezpieczeństwa (K6S6=1 lub 0 pkt)	
Liczba punktów za kategorię K6 stanowiąca sumę liczby punktów za oba powyższe środki bezpieczeństwa (K6=K6S1+K6S2+K6S3+K6S4+K6S5+K6S6)	
Ogólna liczba punktów stanowiąca sumę punktów za wszystkie kategorie PUNKTY = K1+K2+K3+K4+K5+K6	19

Podsumowanie

Poziom zagrożeń przy doborze środków bezpieczeństwa fizycznego biorąc pod uwagę czynniki oceny istotności zagrożeń, które są ważne dla Urzędu Gminy w Cielądzu do zapewnienia bezpieczeństwa fizycznego takich jak lokalizacja oraz liczbę osób posiadających dostęp do dokumentów niejawnych, kształtuje się na poziomie niskim.

Z uwagi na osiągnięcie przy analizie ryzyka jego granicznej maksymalnej wartości, klasyfikującej poziom zagrożeń jako niski, przy ocenie punktacji zastosowanych środków zabezpieczeń dokonano założeń oceny jak dla zagrożeń na poziomie średnim. Pomimo tego uzyskano wyższą liczbę punktów od wymaganej, odpowiadającą warunkom przechowywania dokumentów niejawnych o wyższych klauzulach tajności.

Załącznik Nr 3
do Zarządzenia Nr 75/2015
Wójta Gminy Cielądz
z dnia 09.10.2015 r.

ZATWIERDZAM

Wójt Gminy Cielądz

WÓJT
mgr Paweł Królak

Instrukcja

dotycząca sposobu i trybu przetwarzania informacji niejawnych oznaczonych klauzulą „zastrzeżone" oraz zakresu i warunków stosowania środków bezpieczeństwa fizycznego w celu ich ochrony

w Urzędzie Gminy Cielądz

§1

Instrukcja dotycząca sposobu i trybu przetwarzania informacji niejawnych oznaczonych klauzulą **„zastrzeżone"** oraz zakresu i warunków stosowania środków bezpieczeństwa fizycznego w celu ich ochrony zwana dalej instrukcją stanowi wewnętrzne uregulowanie w Urzędzie Gminy Cielądz dotyczące całokształtu zagadnień związanych z ochroną informacji niejawnych oznaczonych klauzulą „zastrzeżone", zwanych dalej informacjami zastrzeżonymi i określa:

1) warunki dostępu do informacji zastrzeżonych,
2) zasady udostępniania informacji zastrzeżonych,
3) zasady ewidencjonowania dokumentów zastrzeżonych,
4) zasady przechowywania i zabezpieczania dokumentów zastrzeżonych,
5) zasady opracowania dokumentów zastrzeżonych,
6) zasady wysyłania przesyłek zawierających informacje zastrzeżone,
7) zasady gromadzenia dokumentów zastrzeżonych,
8) zasady nadzoru w zakresie przestrzegania warunków ochrony informacji zastrzeżonych.

§2

1) Informacjami niejawnymi o klauzuli „zastrzeżone" są informacje, którym nie nadano wyższej klauzuli tajności, a ich nieuprawnione ujawnienie może mieć szkodliwy wpływ na wykonywanie przez organy władzy publicznej lub inne jednostki organizacyjne zadań z zakresu obrony narodowej, polityki zagranicznej, bezpieczeństwa publicznego, przestrzegania praw i wolności obywateli, wymiaru sprawiedliwości albo interesów ekonomicznych Rzeczypospolitej Polskiej.
2) Informacjami niejawnymi o klauzuli „zastrzeżone" w Urzędzie Gminy są informacje dotyczące m.in.:

1) Załączników do „Planu operacyjnego funkcjonowania Gminy Cielądz w warunkach zewnętrznego zagrożenia bezpieczeństwa państwa i w czasie wojny".
2) Dokumentacji Akcji Kurierskiej Gminy Cielądz.
3) Instrukcji działania „Stałego dyżuru" Wójta Gminy Cielądz.
4) Inne wg decyzji osób uprawnionych do podpisania dokumentów zastrzeżonych.

§3

Uprawnienia do dostępu do określonych informacji zastrzeżonych mogą posiadać osoby, które spełniają warunki:

1) posiadają poświadczenie bezpieczeństwa upoważniające do dostępu do informacji niejawnych o klauzuli „zastrzeżone" lub upoważnienie Wójta Gminy zgodnie z art. 21 ust. 4 ustawy o ochronie informacji niejawnych,
2) odbyli przeszkolenie w zakresie ochrony informacji niejawnych i posiadają zaświadczenie stwierdzające odbycie tego szkolenia;
3) realizują zadanie, które wymaga dostępu do określonej informacji zastrzeżonej.

§4

1. Osobą upoważnioną do przyjmowania niejawnej korespondencji wchodzącej w formie listów, czy paczek jest Kierownik kancelarii niejawnej.
2. Listy lub paczki zawierające korespondencję niejawną mogą wpływać z zewnątrz jako przesyłki „polecone" bezpośrednio do sekretariatu Urzędu Gminy.
3. Pracownik sekretariatu, po stwierdzeniu, że wewnątrz znajduje się druga koperta oznaczona klauzulą „zastrzeżone", nie otwiera jej i nie rejestruje w swojej ewidencji, informując niezwłocznie Kierownika Kancelarii ds. informacji niejawnych o jej nadejściu.
4. Przekazywanie przesyłek niejawnych bezpośrednio adresatowi z pominięciem Kancelarii Niejawnej oraz ich otwieranie jest zabronione, nawet gdy są oznaczone napisem „Do rąk własnych". Adresat nie może wynieść otrzymanego dokumentu poza teren kancelarii.
5. Korespondencji niejawnej mylnie skierowanej nie ewidencjonuje się w kancelarii niejawnej, lecz przekazuje łącznie z poprzednim opakowaniem w nowej kopercie nadawcy za zwrotnym potwierdzeniem odbioru.
6. Korespondencja niejawna może być prowadzona tylko w języku polskim. Dokumenty obcojęzyczne otrzymane, powinny być przetłumaczone na język polski przez tłumacza przysięgłego.
7. 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.
8. Zabrania się wykonywania jakichkolwiek trwałych kopii udostępnionych dokumentów z klauzulą tajności, ze względu na konieczność zachowania pełnej informacji o miejscu lokalizacji każdego zarejestrowanego egzemplarza.

9. Kancelaria niejawna przyjmuje, rejestruje, przechowuje, przekazuje i wysyła dokumenty zawierające informacje niejawne oznaczone klauzulą „zastrzeżone" oraz prowadzi rejestr tych dokumentów.

10. Rejestracja pism przychodzących o klauzuli „zastrzeżone" odbywa się poprzez odbiór takiej korespondencji w sekretariacie Urzędu, a następnie pracownik sekretariatu odnotowuje w Dzienniku Korespondencyjnym wpływ przesyłki. Kierownika Kancelarii, który przyjmuje przesyłkę potwierdza odbiór w Dzienniku Korespondencyjnym.

11. W przypadku stwierdzenia uszkodzenia przesyłki lub śladów jej otwarcia osoba kwitująca odbiór przesyłki sporządza, wraz z doręczycielem, protokół uszkodzenia. Jeden egzemplarz protokołu przekazuje się nadawcy, drugi -pełnomocnikowi ochrony informacji niejawnych w jednostce organizacyjnej odbiorcy, w przypadku gdy w obiegu przesyłek pośredniczył przewoźnik -kolejny egzemplarz protokołu przekazuje się także jemu.

12. Po otwarciu przesyłki Kierownik Kancelarii ds. informacji niejawnych sprawdza, czy zawartość przesyłki odpowiada wyszczególnionym na niej numerom ewidencyjnym, ustala, czy liczba załączników jest zgodna z liczbą oznaczoną na poszczególnych dokumentach i odciska pieczęć wpływu na której kolejno są informacje: data wpływu korespondencji do kancelarii niejawnej, oraz podpis Kierownika Kancelarii ds. informacji niejawnych.

13. Dokumenty zastrzeżone, wpływające do Urzędu przed zarejestrowaniem wymagają decyzji Wójta Gminy Cielądz, w formie pisemnej dekretacji dokonanej w sposób trwały na dokumencie, kierującej ten dokument do konkretnego pracownika do załatwienia.

14. Następnie Kierownik Kancelarii ds. informacji niejawnych rejestruje pismo w dzienniku ewidencyjnym. Pismo wchodzące po rejestracji w kancelarii niejawnej trafia do wskazanego w dekretacji uprawnionego pracownika, który kwituje odbiór dokumentu w dzienniku ewidencyjnym. Dokumenty są tematycznie upinane w teczkach i przechowywane w kancelarii niejawnej lub innych pomieszczeniach, jeżeli będą umieszczane w meblach biurowych zamykanych na klucz, zgodnie z ustawowymi wymogami.

15. W kancelarii nie otwiera się przesyłek oznaczonych „do rąk własnych", rejestruje się je w dzienniku ewidencyjnym z numerem i datą wpływu i przekazuje za pokwitowaniem - bezpośrednio adresatowi.

16. Rejestracja pism wytworzonych, którym nadaje się bieg korespondencyjny odbywa się w następujący sposób: na piśmie nanosi się sygnaturę literowo-cyfrową, składającą się z symbolu komórki organizacyjnej urzędu oddzielonej myślnikiem od „Z", kolejnym myślnikiem od numeru z rzeczowego wykazu akt, następnie od numeru z dziennika ewidencyjnego, łamany przez dwie ostanie dwie cyfry roku, na załącznikach oznaczonych

klauzulą "zastrzeżone" do pisma wychodzącego sygnaturę nadaje się również w powyższy sposób. Jeden egzemplarz pisma przewodniego i załączników pozostaje w dokumentacji a/a w teczkach tematycznych przechowywanych w szafach zamykanych na klucz.

§5

1) Dokumenty zawierające informacje niejawne o klauzuli „zastrzeżone" są przechowywane w kancelarii niejawnej, w sposób uniemożliwiający ich zabór przez osoby postronne poprzez umieszczenie ich w zamykanych szafach meblowych.
2) Zabezpieczenie przechowywanych materiałów, dokumentów w pomieszczeniu kancelarii lub innym pomieszczeniu, polega na przestrzeganiu zasady, że po każdorazowym opuszczeniem kancelarii przez użytkownika pomieszczenia, w którym te dokumenty się znajdują, drzwi muszą być zamknięte w sposób uniemożliwiający wejście lub wtargnięcie osób postronnych i ewentualną kradzież.
3) Podczas przewożenia lub przenoszenia materiałów niejawnych oznaczonych klauzulą „zastrzeżone" poza kancelarią niejawną, należy zachować wszelkie środki ostrożności, aby nie doprowadzić do kradzieży materiału.
4) Sprzątanie kancelarii niejawnej odbywa się w obecności osoby za nie odpowiedzialnej.
5) Zabrania się:
   – pozostawiać materiału bez nadzoru,
   – przekazywać materiał osobom postronnym,
   – wyjmować materiał z teczki (lub innego opakowania) w środkach komunikacji publicznej),
   – wynosić materiał do miejsca zamieszkania (internatu, hotelu, itp.)
6) Dokumenty zastrzeżone przechowuje się zamknięte w meblach biurowych, szafach metalowych lub sejfach zamykanych co najmniej na jeden zamek patentowy.
7) Teczki spraw zawierające dokumenty zastrzeżone nie mogą być przechowywane z dokumentami jawnymi.
8) Dokumenty zastrzeżone w postaci cyfrowej mogą być przechowywane w systemach i sieciach teleinformatycznych posiadających akredytację służby ochrony państwa zgodnie z zapisami ustawy o ochronie informacji niejawnych.
9) Nadzór nad prawidłowym przechowywaniem dokumentów zastrzeżonych sprawuje kierownik kancelarii niejawnej.

§6

1) Dokumenty o klauzuli „zastrzeżone" są sporządzane i wykonywane przez pracownika merytorycznie odpowiedzialnego za jego opracowanie.
2) Praca z dokumentem zastrzeżonym, w tym sporządzanie i wykonanie może odbywać się w jednostce organizacyjnej urzędu, jeśli warunki pracy umożliwiają zapewnienie warunków ochrony przed jego nieuprawnionym ujawnieniem i nieuprawnionym do niego dostępem i zapoznaniem się przez osoby do tego nieuprawnionych.
3) Jeżeli w jednostce organizacyjnej urzędu nie ma wymaganych warunków wówczas dokument zastrzeżony musi być sporządzony i wykonany na terenie kancelarii niejawnej.
4) Jeżeli dokument zastrzeżony w danej chwili nie jest wykorzystywany do realizacji zadania przez uprawnionego pracownika musi być on zabezpieczony zgodnie z §6 instrukcji.
5) Dokumenty zastrzeżone mogą być przetwarzane w systemach i sieciach teleinformatycznych posiadających akredytację służby ochrony państwa zgodnie z zapisami ustawy o ochronie informacji niejawnych.
6) Wykonany dokument jest rejestrowany w odpowiedniej ewidencji dokumentów w kancelarii niejawnej, następnie zostaje podpisany przez uprawnioną do tego osobę.

§7

1) Przekazywanie dokumentu o klauzuli „zastrzeżone" poza kancelarię niejawną odbiorca (wykonawca) kwituje w odpowiednim urządzeniu ewidencyjnym kancelarii.
2) Po pobraniu materiału niejawnego oznaczonego klauzulą „zastrzeżone" z kancelarii, odbiorca (wykonawca) ponosi pełną odpowiedzialność za bezpieczeństwo materiału i informacji niejawnych w nim zawartych.
3) Odbiorca (wykonawca) dokumentu niejawnego o klauzuli „zastrzeżone" w postaci pliku elektronicznego odpowiada za bezpieczeństwo wydruków dokumentów w tym za ich ewentualną ewidencję w zależności od potrzeb.
4) Odbiorca (wykonawca) przekazujący materiały niejawne o klauzuli „zastrzeżone" innej osobie może żądać pokwitowania przyjęcia dokumentu (materiału) w odpowiednim urządzeniu ewidencyjnym lub na innym egzemplarzu dokumentu.

§ 8

1) Osobą upoważnioną do wysyłania na zewnątrz Urzędu Gminy Cielądz niejawnej korespondencji w formie listów lub paczek jest pracownik ds. prowadzenia kancelarii

niejawnej i Pełnomocnik ochrony. Rejestruje on korespondencję niejawną w dzienniku ewidencji, opisuje i wysyła.

2) Korespondencja niejawna o klauzuli „zastrzeżone" wysyłana jest za pośrednictwem „Poczty Polskiej", lisem poleconym za zwrotnym potwierdzeniem odbioru w podwójnej kopercie, z których wewnętrzna zawierająca właściwy dokument jest opatrzona pieczęcią nagłówkową i ma wpisany nr pozycji z dziennika ewidencji (taki sam jak na dokumencie), klauzulą tajności, a poniżej imieniem i nazwiskiem kopertującego oraz datą i podpisem. W środkowej części koperty wewnętrznej umieszcza się pełną nazwę adresata i ewentualnie napis „Do rąk własnych". W miejscach sklejenia odciśnięta jest pieczęć „Do pakietów" i zaklejone są one przezroczystą taśmą samoprzylepną. Koperta zewnętrzna jest zwyczajnie zaadresowana, bez pieczęci do pakietów i oklejania taśmą.

3) Przygotowaną przesyłkę należy wpisać do „pocztowej książki nadawczej" wypełniając poszczególne kolumny, a następnie dostarczyć do wysłania jako przesyłkę poleconą do sekretariatu Urzędu.

§9

1) Kopie, odpisy, wyciągi, tłumaczenia lub wypisy z dokumentu oznaczonego klauzulą „zastrzeżone" wykonuje się o ile nie naniesiono zastrzeżeń na dokumencie o wykonywaniu kopii, wyciągu, wypisu, odpisu lub tłumaczenia.
2) Kopie, odpisy, wyciągi, tłumaczenia lub wypisy z dokumentu wykonuje się za pisemną zgodą wykonawcy naniesioną na ostatniej stronie (odwrocie) oryginału dokumentu.
3) Wykonanie kopii, odpisu, wypisu, wyciągu lub tłumaczenia z dokumentu ewidencjonuje się w Dzienniku Ewidencyjnym i oznacza zgodnie z rozporządzeniem Prezesa Rady Ministrów w sprawie sposobu oznaczania materiałów, umieszczania na nich klauzul tajności, a także zmiany nadanej klauzuli tajności.
4) Dokumenty oznaczone klauzulą „zastrzeżone" kopiuje się i skanuje w urządzeniach posiadających akredytację bezpieczeństwa teleinformatycznego w rozumieniu ustawy OIN.
5) Zabrania się wykonywania kopii (skanów) dokumentów niejawnych o klauzuli „zastrzeżone" na urządzeniach włączonych do jawnej sieci teleinformatycznej – np. faxach lub jawnych systemach teleinformatycznych.

§10

1) Dokumenty zastrzeżone są gromadzone przez pracowników upoważnionych do dostępu do tych informacji w teczkach akt z klauzulą „zastrzeżone".
2) Informacje zastrzeżone podlegają ochronie do czasu zniesienia klauzuli tajności.
3) W przypadku spraw ostatecznie zakończonych, gdy dokument jest nadal chroniony, teczki akt o klauzuli „zastrzeżone" mogą być przechowywane do kancelarii niejawnej do chwili zniesienia klauzuli tajności.
4) W przypadku zniesienia klauzuli tajności, kancelaria niejawna przekazuje teczki akt do archiwum zakładowego.

§11

1) Pracownik samorządowy jest zobowiązany do dochowania tajemnicy ustawowo chronionej zgodnie z ustawą o pracownikach samorządowych oraz Regulaminem Organizacyjnym Urzędu Gminy.
2) Odpowiedzialność karną za przestępstwa przeciwko ochronie informacji w tym informacji zastrzeżonych określa ustawa kodeks karny.
3) Odpowiedzialność służbową za nieprzestrzeganie zasad ochrony informacji zastrzeżonych są regulowane przez Regulamin Pracy Urzędu Gminy Cielądz.
4) W przypadku nieuprawnionego ujawnienia informacji niejawnych o klauzuli „zastrzeżone" należy o tym powiadomić bezpośredniego przełożonego oraz pełnomocnika ds. ochrony informacji niejawnych.
5) Nadzór nad obiegiem i ewidencją materiałów niejawnych w Urzędzie Gminy Cielądz sprawuje Pełnomocnik ds. Ochrony Informacji Niejawnych.
6) Kierownik Kancelarii ds. prowadzenia kancelarii niejawnej odpowiada za obieg, przechowywanie i ewidencję materiałów niejawnych oznaczonych klauzula „zastrzeżone".