

ZARZĄDZENIE NR 120/8//2017
WÓJTA GMINY WILCZYN
z dnia 14 lutego 2017 r.

w sprawie ochrony informacji niejawnych w Urzędzie Gminy w Wilczynie

Na podstawie art. 33 ust. 1 i ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2016r., poz. 446 z późn. zm.), art. 15 ust. 1 pkt 5, art. 43 ust. 5 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2016 r., poz. 1167 z późn. zm.)

zarządza się, co następuje:

§ 1. W celu zapewnienia ochrony informacji niejawnych oraz przestrzegania przepisów o ochronie informacji niejawnych, zatwierdza się:

- 1) Plan ochrony informacji niejawnych w Urzędzie Gminy w Wilczynie, stanowiący załącznik nr 1 do niniejszego zarządzenia.
- 2) Instrukcję dotyczącą sposobu i trybu przetwarzania informacji niejawnych oznaczonych klauzulą „zastrzeżone” oraz zakresu i warunków stosowania środków bezpieczeństwa fizycznego w celu ich ochrony w Urzędzie Gminy w Wilczynie, stanowiącą załącznik nr 2 do niniejszego zarządzenia.

§ 2. Wykonanie zarządzenia powierza się Pełnomocnikowi do spraw Ochrony Informacji Niejawnych w Urzędzie Gminy w Wilczynie.

§ 3. Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT GMINY
mjr Grzegorz Skowroński

Załącznik nr 1
do Zarządzenia Nr 120/8/2017
Wójta Gminy Wilczyn
z dnia 14 lutego 2017 r.

ZATWIERDZAM

mgr Grzegorz Skowronski
.....

PLAN OCHRONY INFORMACJI NIEJAWNYCH URZĘDU GMINY W WILCZYNIE

Opracowała:
Pełnomocnik Ochrony
Informacji Niejawnych
Renata Ćwiklińska

Wilczyn 2017 rok

URZĄD GMINY W WILCZYNIE

SPIS TREŚCI

I.	Podstawowe przepisy prawne z zakresu ochrony informacji niejawnych	3
II.	Charakterystyka Urzędu Gminy w Wilczynie	4
III.	Ocena zagrożeń dla informacji niejawnych	4
IV.	Organizacja ochrony informacji niejawnych	7
V.	Klasyfikowanie informacji niejawnych	13
VI.	Udostępnianie informacji niejawnych, postępowanie sprawdzające	14
VII.	Szkolenie w zakresie ochrony informacji niejawnych	17
VIII.	Organizacja kontroli przestrzegania zasad ochrony informacji niejawnych	17
IX.	Ochrona informacji niejawnych w systemach i sieciach informatycznych	18
X.	Stosowanie środków fizycznej ochrony informacji niejawnych	19
XI.	Postępowanie z materiałami zawierającymi informacje niejawne	20
XII.	Plany awaryjne uwzględniające potrzebę ochrony informacji niejawnych w razie wystąpienia sytuacji szczególnych	21
XIII.	Postanowienia końcowe	27
XIV.	Arkusz aktualizacyjny	28

Załączniki

1.	Tabela oceny istotności czynników zagrożeń	29
2.	Dobór środków bezpieczeństwa fizycznego	30
3.	Wykaz stanowisk, z którymi łączy się dostęp do informacji niejawnych o klauzuli „zastrzeżone”	32
4.	Wykaz informacji niejawnych stanowiących tajemnicę służbową o klauzuli „zastrzeżone	32
5.	Wzór protokołu oceny dokumentacji niearchiwalnej.	33
6.	Wzór protokołu przekazania dokumentów niejawnych	34
7.	Wzór protokołu otwarcia szafy, sejfu	35
8.	Wzór upoważnienia jednorazowego	36
9.	Wzór dokumentu potwierdzającego odbycie szkolenia z zakresu ochrony informacji niejawnych.	37
10.	Wzór oświadczenia osoby upoważnionej do przestrzegania przepisów dot. ochrony informacji niejawnych.	38

I. PODSTAWOWE PRZEPISY PRAWNE Z OCHRONY INFORMACJI NIEJAWNYCH:

- Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych – Dz.U. z 2016 r., poz.1167 z późn zm.
- Rozporządzenie Prezesa Rady Ministrów z dnia 27 kwietnia 2011 r. w sprawie przygotowania i przeprowadzania kontroli stanu zabezpieczenia informacji niejawnych – Dz.U. z 2011 r., Nr 93 poz. 541;
- Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie wzorów poświadczeń bezpieczeństwa - Dz.U. z 2015, poz. 220;
- Rozporządzenie Rady Ministrów z 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych – Dz.U. z 2012 r., poz. 683;
- Rozporządzenie Rady Ministrów z 7 grudnia 2011 r. w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych – Dz.U. z 2011 r. nr 276, poz. 1631;
- Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie wzorów zaświadczeń stwierdzających odbycie szkolenia w zakresie ochrony informacji niejawnych oraz sposobu rozliczania kosztów przeprowadzenia szkolenia przez Agencję Bezpieczeństwa Wewnętrznego lub Służbę Kontrwywiadu Wojskowego - Dz. U. 2015r. poz. 205;
- Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego – Dz.U. z 2011 r., Nr 159, poz. 948;
- Rozporządzenie Prezesa Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne – Dz.U. z 2011 r., Nr 271, poz. 1603;
- Rozporządzenie Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności – Dz.U. z 2011 r., Nr 288, poz. 1692;

NINIEJSZY PLAN OKREŚLA ZASADY OCHRONY INFORMACJI NIEJAWNYCH W URZĘDZIE GMINY W WILCZYNIE PRZED NIEUPRAWNIONYM UJAWNieniem, NIEZALEŻNIE OD FORMY I SPOSOBU ICH WYRAŻANIA.

Przedmiotem ochrony w Urzędzie Gminy w Wilczynie są informacje niejawne oznaczone klauzulą „zastrzeżone”.

II. CHARAKTERYSTYKA URZĘDU GMINY W WILCZYNIE

1. Charakterystyka obiektu

Budynek Urzędu jest obiektem dwukondygnacyjnym, usytuowanym u zbiegu ulicy Strzelińskiej 12D, oddzielony od ulicy chodnikiem. Ściany nośne i działowe murowane z pustaków, posadzka betonowa.

W pomieszczeniach biurowych: panele, wewnątrz schody betonowe. Brak okratowanych okien. W bezpośrednim otoczeniu budynku znajdują się parkingi, domy jednorodzinne i budynki użyteczności publicznej. W budynku nie ma zainstalowanego alarmu.

Urząd Gminy w Wilczynie jest właścicielem budynku. Pomieszczenia w obiekcie zajmowane są przez Urząd, Gminny Ośrodek Pomocy Społecznej oraz Centrum Usług Wspólnych.

2. Pomieszczenie do przetwarzania informacji niejawnych

Informacje niejawne o klauzuli „zastrzeżone” przetwarza się i przechowuje w pomieszczeniu stanowiska ds. ewidencji ludności, spraw wojskowych i obronnych nr 9. Pomieszczenie położone jest na parterze budynku. Dokumenty przechowywane są w szafie metalowej.

III. OCENA ZAGROŻEŃ DLA INFORMACJI NIEJAWNYCH

1. Zagrożenia zewnętrzne dla Urzędu to:

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

Symptomy mogące świadczyć o przygotowaniu napadu lub włamania do budynku

Urzędu:

- a) wzmożone zainteresowanie osób postronnych obiektem, pomieszczeniami urzędu objawiające się między innymi – podejmowaniem prób uzyskania informacji o danym obiekcie, pomieszczeniu od pracowników podczas luźnych rozmów po „przypadkowym” spotkaniu,
- b) nawiązywanie rozmów przez osoby postronne z pracownikami, podszywanie się pod byłych pracowników Urzędu i przejawianie zainteresowania tym, co się po latach zmieniło,
- c) interesowanie się osobami funkcyjnymi, w tym ich przywarami oraz sposobie wykonywania obowiązków służbowych,
- d) obserwacja sposobu działania systemu ochronnego, sekretariatu, sprzątaczek itd.,
- e) rozpoznawanie systemu technicznych zabezpieczeń,
- f) celowe uszkodzanie urządzeń alarmowych, zamków służących do zabezpieczeń, linii telefonicznych, oświetlenia itp.,
- g) próby pozyskania do grup przestępczych pracowników Urzędu (dotyczy głównie osób mających problemy finansowe, towarzyskie a także służbowe).

Wnioski:

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

- 1. Przeprowadzać systematyczną, skrupulatną i wnikliwą kontrolę systemu ochrony przez osoby odpowiedzialne za jego organizację,
- 2. Stosować zasadę niedopuszczenia osób niepowołanych do penetracji miejsc przechowywania dokumentów niejawnych,
- 3. Wykonywać prace porządkowe, remontowe itp. wyłącznie pod nadzorem osób odpowiedzialnych.

2. Zagrożenia wewnętrzne dla Urzędu to:

- 1. Próby zaboru dokumentów lub mienia przez pracowników Urzędu,
- 2. Próby powielania, kserowania dokumentów służbowych dla celów prywatnych,
- 3. Byli pracownicy Urzędu zwolnieni dyscyplinarnie,

4. Rozpoznanie organizacji pracy Urzędu celem łatwiejszej pracy grup przestępczych na terenie Urzędu,
5. Próby wglądu w dokumenty niejawne przez osoby nieuprawnione,
6. Pozyskiwanie informatorów spośród zatrudnionych pracowników;
7. Umieszczenie informatora wśród nowo zatrudnionych,
8. Instytucję przykrycia np. firmę wykonującą jakiekolwiek prace w obiekcie,
9. Spożywanie alkoholu – przesłanka do wykroczeń dyscyplinarnych i przestępstw.

Wnioski:

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

1. Zwracać szczególną uwagę na osoby, które mogą być zainteresowane zaborem dokumentów,
2. Prowadzić szczególny nadzór, by nie dokonywano prób kserowania, kopiowania bez zgody przełożonego,
3. Uwrażliwić pracowników w trakcie prowadzonych szkoleń na możliwość prób kontaktu grup przestępczych z pracownikami, którzy mają dostęp do dokumentów szczególnie ważnych,
4. Stosować zasadę, że do informacji niejawnych mogą mieć dostęp tylko pracownicy posiadający poświadczenie bezpieczeństwa lub właściwe upoważnienie wydane przez Wójta,
5. Zwracać uwagę na osoby, których zachowanie wskazuje na nadmierne spożycie alkoholu.

3. Postępowanie w sytuacjach kryzysowych

W przypadku wystąpienia sytuacji kryzysowych np. pożar, powódź, należy w pierwszej kolejności powiadomić Wójta, Pełnomocnika ochrony oraz osoby odpowiedzialne za pomieszczenia, w których przechowuje się dokumenty niejawne.

W pierwszej kolejności należy zabezpieczyć:

- pieczęcie,
- dokumenty o klauzuli „zastrzeżone”,

- kopie zapasowe, jeżeli są przechowywane,
- inne dokumenty i materiały według sporządzonego planu ewakuacji.

Dokumenty ewakuuje się w opłombowanych, workach ewakuacyjnych. Za ewakuację odpowiedzialny jest Pełnomocnik ochrony. Miejscem ewakuacji są pomieszczenia Archiwum Zakładowego. Z uwzględnieniem zapewnienia odpowiedniej ochrony w miejscu ewakuacji. W sytuacji, gdy ewakuacja jest niemożliwa, w pierwszej kolejności należy zniszczyć dokumenty o klauzuli „zastrzeżone”, pieczęcie i w miarę możliwości pozostałe dokumenty i materiały. W przypadku zaistnienia stanów nadzwyczajnych (stan wojny, stan wyjątkowy, stan klęski żywiołowej), powiadamia się Wójta Gminy i inne osoby odpowiedzialne, przy pomocy dostępnych środków teletechnicznych, lub gdy jest to możliwe, za pomocą gońca. Sposób i kolejność powiadamiania zamieszczono w Planie stałego dyżuru, który przechowywany jest w szafie zamykanej na klucz w pokoju nr 9. Powiadamia się także Policję, Straż Pożarną i inne służby oraz instytucje, w zależności od zaistniałej sytuacji.

IV. ORGANIZACJA OCHRONY INFORMACJI NIEJAWNYCH

1. Organizacja.

Za ochronę informacji niejawnych w Urzędzie Gminy w Wilczynie odpowiada kierownik jednostki organizacyjnej, którym jest Wójt Gminy.

Wójtowi podlega bezpośrednio pełnomocnik ochrony informacji niejawnych, który odpowiada przede wszystkim za zapewnienie przestrzegania przepisów o ochronie informacji niejawnych oraz za postępowania sprawdzające osób, dopuszczonych do prac związanych z dostępem do informacji niejawnych.

Do szczegółowych zadań pełnomocnika ochrony w zakresie ochrony informacji niejawnych należy:

- 1) zapewnienie ochrony informacji niejawnych, w tym stosowanie środków bezpieczeństwa fizycznego;
- 2) zapewnienie ochrony Bezpiecznego Stanowiska Komputerowego, w których są przetwarzane informacje niejawne;
- 3) zarządzanie ryzykiem bezpieczeństwa informacji niejawnych, w szczególności szacowanie ryzyka;

- 4) kontrola ochrony informacji niejawnych oraz przestrzegania przepisów o ochronie tych informacji, w szczególności okresowa (co najmniej raz na trzy lata) kontrola ewidencji, materiałów i obiegu dokumentów;
- 5) opracowywanie i aktualizowanie, wymagającego akceptacji Wójta, planu ochrony informacji niejawnych w Urzędzie;
- 6) prowadzenie szkoleń w zakresie ochrony informacji niejawnych;
- 7) prowadzenie zwykłych postępowań sprawdzających oraz kontrolnych postępowań sprawdzających;
- 8) prowadzenie aktualnego wykazu osób zatrudnionych w Urzędzie, albo wykonujących czynności zlecone, które posiadają uprawnienia do dostępu do informacji niejawnych, oraz osób, którym odmówiono wydania poświadczenia bezpieczeństwa lub je cofnięto, obejmującego wyłącznie:
 - Imię i nazwisko,
 - numer PESEL,
 - imię ojca,
 - datę i miejsce urodzenia,
 - adres miejsca zamieszkania lub pobytu,
- 9) określenie dokumentu kończącego procedurę, datę jego wydania oraz numer;
- 10) przekazywanie do ABW ewidencji, danych osób uprawnionych do dostępu do informacji niejawnych, a także osób, którym odmówiono wydania poświadczenia bezpieczeństwa lub wobec których podjęto decyzję o cofnięciu poświadczenia bezpieczeństwa;
- 11) zapewnienie ochrony fizycznej Urzędu w tym:
 - nadzór nad funkcjonowaniem systemu ochrony;
 - zapewnienie ochrony informacji niejawnych.
 - opracowywanie i organizowanie szkolenia.
- 12) szkolenie w zakresie ochrony informacji niejawnych przeprowadza się w celu zapoznania z:
 - przepisami dotyczącymi ochrony informacji niejawnych oraz odpowiedzialności karnej, dyscyplinarnej i służbowej za ich naruszenie, w szczególności za nieuprawnione ujawnienie informacji niejawnych;

- zasadami ochrony informacji niejawnych w zakresie niezbędnym do wykonywania pracy lub pełnienia służby, z uwzględnieniem zasad zarządzania ryzykiem bezpieczeństwa informacji niejawnych, w szczególności szacowania ryzyka
 - sposobami ochrony informacji niejawnych oraz postępowania w sytuacjach zagrożenia dla takich informacji lub w przypadku ich ujawnienia.
- 13) opracowanie instrukcji dotyczącej sposobu i trybu przetwarzania informacji niejawnych o klauzuli "zastrzeżone" w podległych komórkach organizacyjnych oraz zakres i warunki stosowania środków bezpieczeństwa fizycznego w celu ich ochrony.
- 14) zapewnienie ochrony systemów i sieci teleinformatycznych.
- 15) wykonywanie zadań inspektora bezpieczeństwa teleinformatycznego.

2. Ochrona fizyczna

Aby informacje niejawne mogły być prawidłowo przetwarzane należy stosować środki bezpieczeństwa fizycznego odpowiednie do poziomu zagrożeń w celu uniemożliwienia osobom nieuprawnionym dostępu do tych informacji lub ich utraty.

Środki bezpieczeństwa fizycznego:

- bariery fizyczne – środki chroniące granice miejsca, w którym przetwarzane są informacje niejawne, w szczególności są to ogrodzenia, ściany, drzwi, kraty i okna;
- kontrola dostępu – stosowana jest w celu zagwarantowania, że dostęp do pomieszczenia uzyskują wyłącznie osoby posiadające odpowiednie uprawnienia. Osoby przebywające w wyodrębnionym pomieszczeniu do przetwarzania informacji niejawnych o klauzuli „zastrzeżone” (personel autoryzowany) muszą posiadać odpowiednie poświadczenie bezpieczeństwa lub upoważnienie Wójta. Personel autoryzowany przebywający w tym pomieszczeniu musi posiadać rzeczywistą potrzebę uzyskania dostępu do informacji. Przebywanie ich w wyodrębnionym pomieszczeniu każdorazowo odnotowywane jest w rejestrze kontroli wejść i wyjść z podaniem godziny wejścia i wyjścia, a także celu wizyty.
- szafa i zamki – szafa metalowa, w której przechowuje się dokumenty o klauzuli „zastrzeżone” po zakończeniu pracy należy dokładnie zamknąć.

W uzasadnionych przypadkach podyktowanych względami dłuższego okresu czasu, niezbędnego do wykonania zadań związanych z dostępem do informacji niejawnych, dokumenty o klauzuli „zastrzeżone” mogą być wydawane poza pomieszczenie służące do przechowywania lecz pod warunkiem, że odbiorca dokumentu zapewni warunki ochrony tych dokumentów przechowując je w szafach metalowych z odpowiednimi zamknięciami.

3. Procedury zarządzania uprawnieniami do wejścia, wyjścia i przebywania w strefie ochronnej.

Prawo wstępu i przebywania w pomieszczeniu pełnomocnika ochrony w jego obecności mają:

- osoby upoważnione do wykonywania dokumentów niejawnych na bezpiecznym systemie komputerowym;
- osoby posiadające dopuszczenie do pracy na stanowiskach związanych z dostępem do informacji niejawnych o klauzuli „zastrzeżone”;
- osoby mające uprawnienia do kontroli;
- osoby wykonujące prace porządkowe, konserwacyjne i remontowe.

W związku z tym, że pomieszczenie pełnomocnika jest zarówno pomieszczeniem, gdzie znajduje się bezpieczny system komputerowy, opis wszystkich procedur znajduje się w „Procedurach bezpiecznej eksploatacji”.

4. Opis zastosowanych środków bezpieczeństwa fizycznego.

W celu przeprowadzenia doboru właściwych środków bezpieczeństwa przeprowadzono analizę wszystkich istotnych czynników mogących mieć wpływ na bezpieczeństwo informacji niejawnych przetwarzanych w Urzędzie. Szczegółowa analiza stanowi odrębny dokument pn. „Ocena istotności czynników zagrożeń mających lub mogących mieć wpływ na bezpieczeństwo informacji niejawnych w Urzędzie Gminy Wilczyn”. Określony został poziom zagrożeń o wartości **NISKI**.

Aby uzyskać wymagana minimalną liczbę punktów dla niskiego poziomu zagrożeń i najwyższej klauzuli tajności informacji niejawnych „zastrzeżone” zastosowano niżej wymienione środki bezpieczeństwa fizycznego (szczegółowy dobór środków bezpieczeństwa

fizycznego wraz z tabelą punktacji zastosowanych środków bezpieczeństwa fizycznego stanowi odrębny dokument):

- 1) dokumenty niejawne przechowywane są w szafie metalowej – typ 1,
- 2) konstrukcję pomieszczenia ze względu na grubość ścianek działowych zakwalifikować można do typu 1;
- 3) drzwi do pomieszczenia - typ-1
- 4) budynek w którym zlokalizowany jest KMN spełnia wymagania typu 3;
- 5) kontrola osób nieposiadających stałego upoważnienia do wejścia na obszar Urzędu (interesantów) - brak kontroli osób;
- 6) otoczenie budynku jest oświetlone w celu skutecznej kontroli budynku przez personel bezpieczeństwa.

5. Procedury zarządzania kluczami do szaf, pomieszczeń, w których są przetwarzane informacje niejawne

Klucze do pomieszczenia nr 9 przechowywane są w sekretariacie. Prowadzona jest ewidencja pobranych kluczy. Zabrania się wynoszenia kluczy do pomieszczenia poza budynek Urzędu. Klucze od szaf przechowywane są przez pełnomocnika w zamkniętej szafce w pomieszczeniu biurowym zajmowanym przez pełnomocnika.

6. Plany awaryjne uwzględniające potrzebę ochrony informacji niejawnych w razie wystąpienia sytuacji szczególnych, w tym wprowadzenia stanów nadzwyczajnych, w celu zapobieżenia utracie poufności, integralności lub dostępności informacji niejawnych.

W sytuacjach szczególnych zagrożeń, jeżeli zwykłe środki konstytucyjne są niewystarczające, może zostać wprowadzony odpowiedni stan nadzwyczajny: stan wojenny, stan wyjątkowy lub stan klęski żywiołowej. Działania podjęte w celu ochrony materiałów niejawnych będących w posiadaniu jednostki organizacyjnej muszą odpowiadać stopniowi zagrożenia podstawowych interesów Rzeczypospolitej Polskiej w zakresie obronności, bezpieczeństwa, stosunków gospodarczych i międzynarodowych państwa. W przypadku wprowadzenia stanu wojennego lub stanu wyjątkowego wzmacnia się ochronę budynku Urzędu, w tym pomieszczenia RZK. Wzmocnienie ochrony w przypadku stanu wojennego ma na celu zabezpieczenie budynku przed grupami dywersyjnymi i sabotażowymi oraz przed

ewentualnymi demonstrantami czy też uczestnikami starć z siłami porządkowymi w przypadku wprowadzenia stanu wyjątkowego. W analogiczny sposób postępuje się w przypadku wystąpienia zdarzeń kryzysowych, gdy jest to konieczne.

Działania jakie zostaną podjęte obejmują m.in.:

- 1) wprowadzenie kontroli interesantów w oparciu o imienne przepustki,
- 2) wzmocnienie ochrony obiektu funkcjonariuszami Komisariatu Policji.

W przypadku bezpośredniego zagrożenia przeprowadza się ewakuację materiałów niejawnych. W przypadku nagłego zagrożenia, decyzję o zniszczeniu materiałów niejawnych podejmuje Prezydent, a w przypadku jego nieobecności Pełnomocnik Ochrony. Bezpośrednie zagrożenie może wynikać z działań wojennych, w wyniku których materiały niejawne mogą dostać się w ręce agresora.

Ewakuacja akt powinna obejmować: zapakowanie materiałów do worków ewakuacyjnych, przemieszczenie worków na środek transportu i przewiezienie do wyznaczonego przez Prezydenta miejsca ewakuacji.

W sytuacji kiedy ewakuacja staje się konieczna, ewakuacji podlegają wszystkie dokumenty niejawne przechowywane w Urzędzie. Niszczenie materiałów dokonywane jest za pomocą odpowiedniej niszczarki dokumentów lub ich spalanie.

Protokół zniszczenia materiałów niejawnych winien zawierać opis okoliczności, w jakich dokonano zniszczenia, gdzie, kiedy, na czyje polecenie i w jaki sposób oraz spis zniszczonych materiałów. Za zapewnienie przestrzegania przepisów dotyczących ochrony informacji niejawnych odpowiada Pełnomocnik Ochrony. Osoby, które stwierdziły jakiegokolwiek naruszenie przepisów zagrożenie dla bezpieczeństwa informacji niejawnych, zobowiązane są niezwłocznie powiadomić Pełnomocnika Ochrony, jak również zobowiązane są do:

- 1) zabezpieczenia miejsca zdarzenia, śladów, dowodów,
- 2) zabezpieczenia informacji niejawnych przed ewentualnym dalszym ujawnieniem,
- 3) złożenia szczegółowych wyjaśnień dotyczących zdarzenia osobom prowadzącym postępowanie wyjaśniające.

W przypadku stwierdzenia naruszenia w Urzędzie przepisów o ochronie informacji niejawnych Pełnomocnik Ochrony zawiadamia o tym Wójta i podejmuje niezwłocznie działania zmierzające do wyjaśnienia okoliczności tego naruszenia oraz ograniczenia jego

negatywnych skutków. Pełnomocnik Ochrony ustala czyli jakie informacje zostały ujawnione lub zniszczone czy też była to jedynie próba zdobycia informacji przez osobę nieuprawnioną. W przypadku stwierdzenia zaistnienia uzasadnionego podejrzenia popełnienia przestępstwa ujawnienia informacji niejawnych (art. 266 k.k.) istnieje obowiązek niezwłocznego zawiadomienia właściwego organu ścigania (prokuratura lub Agencja Bezpieczeństwa Wewnętrznego). Naruszenie przepisów o ochronie informacji niejawnych przez pracownika posiadającego poświadczenie bezpieczeństwa może stanowić podstawę do wdrożenia postępowania kontrolnego niezależnie od odpowiedzialności dyscyplinarnej lub karnej.

V. KLASYFIKOWANIE INFORMACJI NIEJAWNYCH

Klasyfikowanie informacji niejawnych oznacza przyznanie tej informacji, w sposób wyraźny jednej z klauzul tajności, zgodnie z ustawą o ochronie informacji niejawnych. Informacjom niejawnym, materiałom, a zwłaszcza dokumentom lub ich zbiorom, przyznaje się klauzule tajności co najmniej równą najwyższej zaklasyfikowanej informacji lub najwyższej klauzuli w zbiorze.

Klauzulę tajności przyznaje osoba, która jest upoważniona do podpisania dokumentu lub oznaczenia innego niż dokument materiału.

Informacje niejawne podlegają ochronie w sposób określony w ustawie do czasu zniesienia lub zmiany klauzuli tajności.

Osoba upoważniona do podpisywania dokumentów może określić datę lub wydarzenie, po których nastąpi zniesienie lub zmiana klauzuli tajności.

Zniesienie lub zmiana klauzuli tajności są możliwe wyłącznie po wyrażeniu pisemnej zgody przez w/w osobę, albo jej przełożonego.

Wójt przeprowadza nie rzadziej niż raz na 3 lata przegląd materiałów w celu weryfikacji posiadanych materiałów. Informacjom niejawnym nadaje się klauzulę "zastrzeżone", jeżeli nie nadano im wyższej klauzuli tajności, a ich nieuprawnione ujawnienie może mieć szkodliwy wpływ na wykonywanie przez organy władzy publicznej lub inne jednostki organizacyjne zadań w zakresie obrony narodowej, polityki zagranicznej, bezpieczeństwa publicznego, przestrzegania praw i wolności obywateli, wymiaru sprawiedliwości albo interesów ekonomicznych Rzeczypospolitej Polskiej.

Informacjom niejawnym, materiałom, a zwłaszcza dokumentom lub ich zbiorom, przyznaje się klauzulę tajności co najmniej równą najwyższej zaklasyfikowanej informacji lub najwyższej klauzuli w zbiorze.

Dopuszczalne jest przyznawanie różnych klauzul tajności częściom dokumentu (rozdziałom, załącznikom, aneksom) lub poszczególnym dokumentom w zbiorze dokumentów, pod warunkiem wyraźnego ich oznaczenia i wskazania klauzuli tajności po odłączeniu dokumentu bądź jego części.

Informacje niejawne mogą występować w dwóch formach :

- **dokumentu** - dokumentem jest każda utrwalona informacja niejawna;
- **materiału** - to 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.

VI. UDOSTĘPNIANIE INFORMACJI NIEJAWNYCH, POSTĘPOWANIA SPRAWDZAJĄCE

Informacje niejawne mogą być udostępnione wyłącznie osobie dającej rękojmię zachowania tajemnicy i tylko w zakresie niezbędnym do wykonywania przez nią pracy lub pełnienia służby na zajmowanym stanowisku albo wykonywania czynności zleconych. Zasady zwalniania od obowiązku zachowania w tajemnicy informacji niejawnych oraz sposób postępowania z aktami spraw zawierającymi informacje niejawne w postępowaniu przed sądami i innymi organami określają przepisy odrębnych ustaw. Jeżeli przepisy odrębnych ustaw uprawniają organy, służby lub instytucje albo ich upoważnionych pracowników do dokonywania kontroli, w szczególności do swobodnego dostępu do pomieszczeń i materiałów, a jej zakres dotyczy informacji niejawnych, uprawnienia te są realizowane z zachowaniem przepisów ustawy.

Dopuszczenie do pracy lub pełnienia służby na stanowiskach albo zlecenie prac, związanych z dostępem danej osoby do informacji niejawnych o klauzuli "zastrzeżone" może nastąpić po:

- a) pisemnym upoważnieniu przez Wójta, jeżeli nie posiada ona poświadczenia bezpieczeństwa;
- b) odbyciu szkolenia w zakresie ochrony informacji niejawnych przez Pełnomocnika ochrony.

Upoważnienie do dostępu do informacji niejawnych o klauzuli „zastrzeżone” udzielone przez Wójta Gminy w Wilczynie może być:

- a) bezterminowe – ważne do odwołania, może być cofnięte w każdym czasie,
- b) terminowe – udzielone na określony czas lub uprawniające do dostępu do informacji zawartych w dokumencie wskazanym w upoważnieniu,
- c) okresowe – udzielone na czas realizacji czynności zleconych.

W zależności od stanowiska lub wykonywania czynności zleconych, o które ubiega się osoba, zwana dalej "osobą sprawdzaną", przeprowadza się:

- a) zwykle postępowanie sprawdzające - przy stanowiskach i pracach związanych z dostępem do informacji niejawnych o klauzuli "poufne";
- b) poszerzone postępowanie sprawdzające - wobec pełnomocników ochrony, zastępców pełnomocników ochrony oraz kandydatów na te stanowiska

Osobom w/w wydaje się poświadczenia bezpieczeństwa upoważniające do dostępu do informacji niejawnych o takiej klauzuli, jaka została wskazana w poleceniu. Pełnomocnik ochrony informacji niejawnych przeprowadza zwykle postępowanie sprawdzające na pisemne polecenie Wójta. ABW przeprowadza poszerzone postępowania sprawdzające na pisemny wniosek Wójta lub osoby uprawnionej do obsady stanowiska lub zlecenia prac;

Zwykle 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. Powyższe sprawdzenie, jest prowadzone na pisemny wniosek pełnomocnika ochrony przez ABW. W toku sprawdzenia ABW ma prawo przeprowadzić rozmowę z osobą sprawdzaną w celu usunięcia nieścisłości lub sprzeczności zawartych w uzyskanych informacjach. ABW przekazuje pełnomocnikowi ochrony informacji niejawnych pisemną informację o wynikach z przeprowadzonych czynności;

- c) jeżeli jest to konieczne w wyniku uzyskanych informacji, zwykłe postępowanie sprawdzające obejmuje ponadto rozmowę z osobą sprawdzaną.
- d) jeżeli w toku zwykłego postępowania sprawdzającego wystąpią wątpliwości niepozwalające na ustalenie, czy osoba sprawdzana daje rękojmię zachowania tajemnicy, organ prowadzący postępowanie sprawdzające zapewnia osobie sprawdzanej w trakcie wysłuchania możliwość osobistego ustosunkowania się do informacji wywołujących te wątpliwości. Osoba ta może stawić się na wysłuchanie ze swoim pełnomocnikiem. Z przebiegu wysłuchania sporządza się protokół, który podpisują osoba prowadząca wysłuchanie, osoba wysłuchana oraz pełnomocnik, jeżeli w nim uczestniczył.

Organ prowadzący zwykłe postępowanie sprawdzające odstępuje od przeprowadzenia w/w czynności, jeżeli:

- a) jej przeprowadzenie wiązałoby się z ujawnieniem informacji niejawnych;
- b) postępowanie sprawdzające doprowadziło do nie budzącego wątpliwości ustalenia, że osoba sprawdzana nie daje rękojmi zachowania tajemnicy.

Poświadczenie bezpieczeństwa wydaje się na okres:

- a. 10 lat w przypadku dostępu do informacji niejawnych oznaczonych klauzulą „poufne”;
- b. 7 lat w przypadku dostępu do informacji niejawnych oznaczonych klauzulą „tajne”;
- c. 5 lat w przypadku dostępu do informacji niejawnych oznaczonych klauzulą „ściśle tajne”.

Poświadczenie bezpieczeństwa upoważniające do dostępu do informacji niejawnych o wyższej klauzuli tajności uprawnia do dostępu do informacji niejawnych o niższej klauzuli tajności, odpowiednio przez te okresy. W przypadku, gdy o osobie, której wydano poświadczenie bezpieczeństwa, zostaną ujawnione nowe informacje wskazujące, że nie daje ona rękojmi zachowania tajemnicy, przeprowadza się kontrolne postępowanie sprawdzające. Osoba sprawdzana nie wypełnia nowej ankiety dla celów tego postępowania.

O wszczęciu kontrolnego postępowania sprawdzającego zawiadamia się:

- a) osobę uprawnioną do obsady stanowiska;
- b) pełnomocnika ochrony informacji niejawnych w Urzędzie;
- c) osobę sprawdzaną.

Po otrzymaniu zawiadomienia, Wójt lub osoba uprawniona do obsady stanowiska uniemożliwia osobie sprawdzanej dostęp do informacji niejawnych.

VII. SZKOLENIE W ZAKRESIE OCHRONY INFORMACJI NIEJAWNYCH

Szkolenie w zakresie ochrony informacji niejawnych przeprowadza się w celu zapoznania z:

- 1) przepisami dotyczącymi ochrony informacji niejawnych oraz odpowiedzialności karnej, dyscyplinarnej i służbowej za ich naruszenie, w szczególności za nieuprawnione ujawnienie informacji niejawnych;
- 2) zasadami ochrony informacji niejawnych w zakresie niezbędnym do wykonywania pracy lub pełnienia służby, z uwzględnieniem zasad zarządzania ryzykiem bezpieczeństwa informacji niejawnych, w szczególności szacowania ryzyka;
- 3) sposobami ochrony informacji niejawnych oraz postępowania w sytuacjach zagrożenia dla takich informacji lub w przypadku ich ujawnienia.
- 4) Szkolenie, o którym mowa:
 - przeprowadza ABW - dla pełnomocników ochrony oraz osób przewidzianych na te stanowiska;
 - organizuje pełnomocnik lub zastępca pełnomocnika ochrony informacji niejawnych - dla pozostałych osób zatrudnionych, lub wykonujących czynności zlecone w Urzędzie.

Szkolenie przeprowadza się nie rzadziej niż raz na 5 lat. Można odstąpić od przeprowadzenia szkolenia, jeżeli osoba podejmująca pracę lub rozpoczynająca pełnienie służby albo wykonywanie czynności zleconych przedstawi pełnomocnikowi ochrony aktualne zaświadczenie o odbyciu szkolenia. Szkolenie kończy się wydaniem zaświadczenia. Odbierając zaświadczenie, osoba przeszkolona składa pisemne oświadczenie o zapoznaniu się z przepisami o ochronie informacji niejawnych.

VIII. ORGANIZACJA KONTROLI PRZESTRZEGANIA ZASAD OCHRONY INFORMACJI NIEJAWNYCH

Pełnomocnik ochrony przeprowadza kontrolę ochrony informacji niejawnych oraz przestrzegania przepisów o ochronie tych informacji, co najmniej raz na trzy lata – dotyczy w szczególności: kontroli ewidencji, materiałów i obiegu dokumentów.

Kontrole stanu ochrony informacji niejawnych przeprowadza się w celu:

- a) ustalenia stanu faktycznego realizacji zadań w zakresie ochrony informacji niejawnych oraz oceny przestrzegania przepisów w tym zakresie;
- b) określenie przyczyn i skutków ewentualnych naruszeń obowiązujących przepisów;
- c) sformułowanie wniosków oraz zaleceń dotyczących doskonalenia systemu ochrony informacji niejawnych.

IX. OCHRONA INFORMACJI NIEJAWNYCH W SYSTEMACH I SIECIACH TELEINFORMATYCZNYCH

Urządzenia komputerowe, w których są wytwarzane, przetwarzane, przechowywane lub przekazywane informacje niejawne podlegają zatwierdzeniu przez kierownika jednostki organizacyjnej i akceptacji bezpieczeństwa teleinformatycznego przez Agencję Bezpieczeństwa Wewnętrznego. Akceptacja, o której mowa następuje na podstawie szczególnych wymagań bezpieczeństwa zwanych dalej SWB i procedur bezpiecznej eksploatacji zwanych dalej PBE. Dokumenty SWB są kompletnym i wyczerpującym opisem ich budowy, zasad działania i eksploatacji. PBE opracowuje się w celu prawidłowego, bezpiecznego posługiwania się sprzętem teleinformatycznym jakim jest Bezpieczne Stanowisko Komputerowe zwane dalej BSK.

Wójt udziela akredytacji bezpieczeństwa teleinformatycznego dla systemu teleinformatycznego przeznaczonego do przetwarzania informacji niejawnych o klauzuli "zastrzeżone" przez zatwierdzenie dokumentacji bezpieczeństwa systemu teleinformatycznego. Następnie dokumentacja jest opiniowana przez Agencję Bezpieczeństwa Wewnętrznego.

Za organizację, eksploatację i bezpieczeństwo BSK w Urzędzie odpowiada Wójt.

Za zapewnienie ochrony stanowiska informatycznego funkcjonującego w Urzędzie odpowiada pełnomocnik ochrony informacji niejawnych, który:

- opracowuje dokumentację bezpieczeństwa systemu (wspólnie z inspektorem bezpieczeństwa teleinformatycznego)
- zapewnia przestrzeganie zasad ochrony informacji, w tym właściwego i bezpiecznego obiegu dokumentów oraz elektronicznych nośników Informacji;
- zapewnia bezpieczeństwo fizyczne obszaru w którym znajduje się BSK;
- zapewnia dostęp do systemu tylko osobom upoważnionym;

- kontroluje znajomość i przestrzeganie PBE przez użytkowników;
- prowadzi nadzór nad bezpieczną eksploatacją BSK.

Za realizację zadań w zakresie zapewnienia funkcjonowania oraz przestrzegania zasad bezpieczeństwa BSK odpowiada administrator systemu informatycznego który:

- wdraża procedury bezpiecznej eksploatacji;
- systematycznie kontroluje funkcjonowanie mechanizmów zabezpieczeń systemu;
- utrzymuje zgodność konfiguracji i parametrów systemu;
- prowadzi na bieżąco wykaz osób mających dostęp do BSK.

Za realizację zadań w zakresie bieżącej kontroli zgodności funkcjonowania BSK z dokumentacją bezpieczeństwa teleinformatycznego odpowiada inspektor bezpieczeństwa teleinformatycznego, który:

- opracowuje dokumentację bezpieczeństwa systemu (wspólnie z pełnomocnikiem ochrony informacji niejawnych);
- przechowuje SWB i PBE
- kontroluje zasady ochrony informacji niejawnych w BSK;
- kontroluje stan zabezpieczeń fizycznych pomieszczeń komputerowych;
- sprawdza znajomość przestrzegania zasad przez użytkowników PBE;
- analizuje rejestr zdarzeń w systemie;
- prowadzi szkolenia z użytkownikami w zakresie ochrony informacji niejawnych oraz zasad bezpieczeństwa.

X. STOSOWANIE ŚRODKÓW FIZYCZNEJ OCHRONY INFORMACJI NIEJAWNYCH

Urząd Gminy w Wilczynie jest jednostką organizacyjną w której są wytwarzane, przetwarzane, przekazywane, przechowywane materiały niejawne, w związku z powyższym mamy obowiązek stosowania środków ochrony fizycznej w celu uniemożliwienia osobom nieupoważnionym dostępu do tych informacji, a w szczególności przed:

- a) działaniem obcych służb specjalnych;
- b) zamachem terrorystycznym lub sabotażem;

- c) kradieżą lub zniszczeniem materiału;
- d) próbą wejścia osób nieuprawnionych;
- e) nieuprawnionym dostępem pracowników do materiałów oznaczonych wyższą klauzulą tajności

W celu uniemożliwienia osobom nieuprawnionym dostępu do informacji niejawnych w Urzędzie:

- a) wydzielono i wyposażono w zabezpieczenia kancelarię dokumentów niejawnych.
- b) do wydzielonego pomieszczenia klucze użytku bieżącego pobierane są i zdawane w sekretariacie.

Ochrona fizyczna Urzędu jest wspomagana środkami technicznymi, które stanowią:

- a. łączność:
 - przewodowa;
 - telefonia komórkowa
- b. oświetlenie obiektu – zewnętrzne i wewnętrzne,
- c. zabezpieczenia mechaniczne:
 - ściany i stropy o odpowiedniej konstrukcji;
 - dokumenty niejawne przechowywane są w metalowej szafie;

Pełnomocnik ochrony informacji niejawnych Urzędu jest zobowiązany do bieżącego nadzoru nad stosowaniem środków ochrony fizycznej.

XI. POSTĘPOWANIE Z MATERIAŁAMI ZAWIERAJĄCYMI INFORMACJE NIEJAWNE

Do obiegu dokumentów zawierających informacje niejawne stanowiące tajemnicę służbową oznaczone klauzulą „zastrzeżone” mają zastosowanie:

- przepisy instrukcji kancelaryjnej obowiązującej w Urzędzie,
- uregulowania i zasady wynikające z „Instrukcji w zakresie ochrony informacji niejawnych oznaczonych klauzulą „zastrzeżone”;
- uregulowania zawarte w niniejszym planie ochrony informacji niejawnych.

Dostęp do informacji oznaczonych klauzulą „zastrzeżone” mają:

- osoby, które posiadają poświadczenie bezpieczeństwa uprawniające do dostępu do informacji niejawnych stanowiących tajemnicę służbową oznaczonych klauzulą „poufne”,
- osoby, w odniesieniu do których przeprowadzone zostało postępowanie sprawdzające i które uzyskały poświadczenie bezpieczeństwa lub dopuszczenie upoważniające do dostępu do informacji stanowiących tajemnicę służbową oznaczonych klauzulą „zastrzeżone”,
- osoby, które uzyskały upoważnienie kierownika jednostki organizacyjnej.

Dokumenty zawierające informacje niejawne stanowiące tajemnicę służbową oznaczone klauzulą „poufne” i „zastrzeżone” podlegają gromadzeniu w teczkach akt oznaczonych właściwą klauzulą tajności. Dokumenty ostatecznie załatwionych spraw, po zakończeniu roku, wymagają wszywania do teczek akt, zgodnie z rzeczowym podziałem akt. Całość zawartościteczki kwalifikuje się według dokumentu o najwyższej klauzuli tajności.

XII. PLANY AWARYJNE UWZGLĘDNIAJĄCE POTRZEBĘ OCHRONY INFORMACJI NIEJAWNYCH W RAZIE WYSTĄPIENIA SYTUACJI SZCZEGÓLNYCH

1. Postępowanie z informacjami niejawnymi oznaczonymi klauzulą „zastrzeżone” w stanach nadzwyczajnych

Rozróżniane są następujące stany nadzwyczajne:

- stan klęski żywiołowej;
- stan wyjątkowy;
- stan kryzysu;
- stan wojny.

W sytuacjach nadzwyczajnych, gdy wzrasta zagrożenie dla przechowywanych dokumentów i materiałów niejawnych wzmacnia się ochronę III strefy ochronnej. Wzmocnienie ochrony informacji niejawnych i aktualizacja dokumentacji (związanej z przygotowaniem pomieszczenia pełnomocnika ochrony do ewakuacji) wprowadzane jest na zarządzenie wójta gminy zgodnie z „Kartami realizacji zadań operacyjnych” umieszczonych w „Planie operacyjnym funkcjonowania Gminy Wilczyn w warunkach zewnętrznego zagrożenia bezpieczeństwa państwa i w czasie wojny”. Karty realizacji zadań operacyjnych

obejmują osoby odpowiedzialne za przetwarzanie i ochronę informacji niejawnych oraz wszystkie dokumenty niejawne.

Postępowanie w stanach nadzwyczajnych:

- wprowadza się dodatkowe obostrzenia i regulacje w zakresie fizycznej ochrony pomieszczenia pełnomocnika ochrony;
- zastrza się kontrolę osób wchodzących do budynku;
- sprawdza się funkcjonowanie systemu alarmowego;
- archiwizuje się i zabezpiecza zawartość systemów (sieci) teleinformatycznych;
- przeprowadza się odprawę z osobami związanymi z dostępem do informacji niejawnych i udziela im się stosownego instruktażu w zakresie postępowania z dokumentami niejawnymi po wprowadzeniu stanu nadzwyczajnego;
- gromadzi się wszystkie dokumenty niejawne w pomieszczeniu pełnomocnika ochrony;
- przygotowuje się worki ewakuacyjne i protokoły przekazania zgromadzonych dokumentów i materiałów niejawnych;
- osiąga się gotowość do ewakuacji pomieszczenia pełnomocnika ochrony.

Interesanci mogą wejść na teren budynku po okazaniu dowodów tożsamości, spisaniu danych osobowych oraz sprawdzeniu zawartości toreb (teczek).

W sytuacjach, gdy Państwo Polskie znajduje się w stanie wojny, wprowadzono stan wojenny, występuje realne zagrożenie ze strony grup terrorystycznych czy przestępczych albo też służb specjalnych państw obcych; oprócz wyżej opisanej wzmocnionej ochrony obiektu, osoby odpowiedzialne bezpośrednio za ochronę strefy bezpieczeństwa realizują swoje zadania poprzez:

- wzmoczenie czujności w ochronie strefy bezpieczeństwa, a zwłaszcza podczas wchodzenia do tej strefy interesantów;
- utrzymywanie stałego kontaktu pełnomocnika ochrony ze służbą ochrony i wójtem gminy;
- systematyczne (codzienne) sprawdzanie kompletów kluczy do pomieszczenia pełnomocnika ochrony przez osoby odpowiedzialne za ich przechowywanie;
- utrzymywanie stałej gotowości do ewakuacji dokumentów z pomieszczenia pełnomocnika ochrony.

Warianty ewakuacji pomieszczenia pełnomocnika ochrony

wariant zasadniczy

W zależności od charakteru i rozmiaru zagrożenia stosować się będzie różne warianty ewakuacji. Decyzję o ewakuowaniu pomieszczenia pełnomocnika ochrony podejmuje Wójt Gminy Wilczyn. Do ewakuacji wykorzystywać się będzie worki, plombowane po wypełnieniu dokumentami.

Niezależnie od wariantu, ewakuację prowadzi się w określonej kolejności:

- dokumenty i materiały o najwyższych klauzulach tajności, urządzenia ewidencyjne i pieczęcie;
- dokumenty i materiały o klauzuli „zastrzeżone”;
- pozostałe dokumenty i materiały.

wariant awaryjny

W razie konieczności ewakuacji dokumentów i materiałów niejawnych (np. napadu i zniszczenia drzwi wejściowych do pomieszczenia – na czas ich naprawy) – miejscem ewakuacji będzie pomieszczenie wyznaczone przez Wójta Gminy Wilczyn (przebieg ewakuacji pełnomocnik ochrony uzgadnia z Wójtem).

2. Instrukcja alarmowa w przypadku zgłoszenia o podłożeniu lub znalezieniu ładunku wybuchowego w budynku Urzędu

Osoba, która podjęła zgłoszenie o podłożeniu ładunku wybuchowego albo zauważyła w obiekcie przedmiot niewiadomego pochodzenia, mogący być ładunkiem wybuchowym zobowiązana jest powiadomić o tym Wójta oraz Komisariat Policji w Kleczewie.

Zawiadamiając Policję, należy podać:

- treść rozmowy ze zgłaszającym o podłożeniu ładunku wybuchowego;
- miejsce i opis zlokalizowanego przedmiotu, który może być ładunkiem wybuchowym,
- numer telefonu, z którego prowadzona jest rozmowa i swoje stanowisko służbowe.

Należy uzyskać od Policji potwierdzenie przyjętego zawiadomienia.

Akcja poszukiwawcza ładunku wybuchowego po uzyskaniu informacji o jego podłożeniu.

Do czasu przybycia Policji akcją kieruje Wójt lub osoba go zastępująca.

Kierujący akcją zarządza, aby użytkownicy pomieszczeń dokonali sprawdzenia, czy w tych pomieszczeniach znajdują się:

- przedmioty, rzeczy, urządzenia, paczki itp., których wcześniej nie było i nie wniesli ich użytkownicy pomieszczeń ;
- ślady przemieszczania elementów wyposażenia pomieszczeń;
- zmiany w wyglądzie zewnętrznym przedmiotów, rzeczy, urządzeń, które przedtem w pomieszczeniu były oraz emitowane z nich sygnały.

Pomieszczenia ogólnodostępne takie jak: korytarze, klatki schodowe, toalety, piwnice oraz najbliższe otoczenie zewnętrzne obiektu powinno być sprawdzone przez wyznaczone osoby funkcyjne.

Zlokalizowanych przedmiotów, rzeczy, urządzeń, których – w ocenie użytkowników – przedtem nie było, a zachodzi podejrzenie, iż mogą to być ładunki wybuchowe – nie wolno dotykać. O ich umiejscowieniu należy natychmiast powiadomić Policję.

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, iż pojawienie się tych przedmiotów lub zmiany w ich wyglądzie i usytuowaniu mogły nastąpić na skutek działania sprawcy podłożenia ładunku wybuchowego. W tej sytuacji kierujący akcją może wydać decyzję ewakuacji osób z zagrożonego obiektu przed przybyciem Policji.

Akcja rozpoznawczo - neutralizująca zlokalizowanych ładunków wybuchowych .

- po przybyciu do Urzędu grupy interwencyjnej Policji, kierujący akcją powinien przekazać im wszystkie informacje dotyczące zdarzenia i wskazać miejsca zlokalizowanych przedmiotów, rzeczy, urządzeń pochodzenia oraz punkty newralgiczne w obiekcie.
- policjant lub dowódca grupy policjantów przejmuje kierowanie akcją, a Wójt lub osoba go zastępująca winna udzielić mu wszechstronnej pomocy podczas jej prowadzenia.
- na wniosek policjanta kierującego akcją, Wójt podejmuje decyzję o ewakuacji użytkowników i innych osób z obiektu – o ile to nie nastąpiło wcześniej.
- identyfikacją i rozpoznawaniem zlokalizowanych przedmiotów, rzeczy, urządzeń obcych oraz neutralizowaniem ewentualnie podłożonych ładunków wybuchowych

zajmują się uprawnione i wyspecjalizowane ogniwa organizacyjne Policji, przy wykorzystaniu specjalistycznych środków technicznych.

- policjant kierujący akcją, po zakończeniu działań, przekazuje protokolarnie obiekt.

3. Instrukcja postępowania w przypadku otrzymania przesyłki niewiadomego pochodzenia bądź stwierdzenia obecności substancji niewiadomego pochodzenia w obiekcie

W przypadku dostarczenia do Urzędu jakiegokolwiek przesyłki niewiadomego pochodzenia lub budzącej podejrzenia z jakiegokolwiek innego powodu, gdy stwierdza się np.:

- brak nadawcy;
- brak adresu nadawcy;
- przesyłka pochodzi od nadawcy lub z miejsca z którego się nie spodziewamy, bądź budzącej jakiejkolwiek podejrzenia z innego powodu;
- obecności proszku (pudru, innej substancji) na powierzchni koperty, opakowania;
- zaadresowana do osoby niepracującej;
- jest nadmiernie oklejona taśmą
- charakteryzuje się nienaturalnym zapachem lub przebarwieniami;
- znak stempla pocztowego nie odpowiada adresowi zwrotnemu

NALEŻY:

- nie otwierać tej przesyłki;
- umieścić tę przesyłkę w grubym worku plastikowym na śmieci, szczelnie zamknąć;
- worek ten należy umieścić w drugim grubym worku na śmieci, szczelnie zamknąć, zawiązać supeł i zakleić taśmą klejącą;
- paczki nie należy przenosić – należy pozostawić ją na miejscu;
- należy dokładnie umyć ręce;
- powiadomić właściwą jednostkę Państwowej Straży Pożarnej oraz Powiatową Stację Sanitarno – Epidemiologiczną;
- sporządzić listę osób mających kontakt z podejrzaną przesyłką – przekazać ją przełożonym;
- powiadomić Policję w celu zabezpieczenia przesyłki do czasu przejęcia jej przez Powiatową Stację Sanitarno – Epidemiologiczną oraz rozpoczęcia czynności dochodzeniowo – śledczych;

W przypadku gdyby jednak podejrzana przesyłka została otwarta i zawierała jakąkolwiek podejrzaną zawartość w formie stałej (pył, blok, galaretę, pianę, itp.) lub płynnej.

NALEŻY:

- możliwie nie naruszać tej zawartości, nie rozsypywać, nie przenosić, nie dotykać, nie wachać, nie próbować smakowo, nie robić przeciągów pomieszczeń;
- całą zawartość umieścić w worku plastikowym, zamknąć go i zakleić taśmą klejącą;
- zaklejony worek umieścić w drugim worku, zamknąć go i zakleić;
- dokładnie umyć ręce;
- zamknąć okna, wyłączyć urządzenia wentylacyjne, opuścić pomieszczenie i zamknąć drzwi;
- zmienić i usunąć zanieczyszczoną odzież, umieścić ją w plastikowym worku lub innym szczelnym pojemniku;
- ponownie dokładnie umyć ręce;
- sporządzić listę personelu mającego kontakt z podejrzaną przesyłką i przekazać ją przełożonym;
- powiadomić właściwą jednostkę Państwowej Straży Pożarnej oraz Powiatową Stację Sanitarno – Epidemiologiczną;
- bezzwłocznie powiadomić Policję.

W przypadku stwierdzenia na terenie obiektu Urzędu podejrzanych i nieznanych substancji stałych (kawałki materiału, blok, galaretę, pianę, lub inne)

NALEŻY:

- zabezpieczyć teren zagrożony;
- ile to możliwe przykryć nieznaną substancję folią w sposób uniemożliwiający jej rozprzestrzenianie się bądź roznoszenie np. przez wiatr lub inne czynniki;
- postępować zgodnie z w/w wytycznymi.

Po wykonaniu tych czynności należy w sposób rygorystyczny przestrzegać dalszych zaleceń kompetentnych służb ratowniczych lub sanitarno – epidemiologicznych wydanych na miejscu w trakcie dochodzenia.

XIII. POSTANOWIENIA KOŃCOWE

1. Zachowanie tajemnicy służbowej obowiązuje każdego pracownika bez względu na zajmowane stanowisko, rodzaj i miejsce wykonywanej pracy oraz charakter stosunku pracy.
2. Zachowanie tajemnicy obowiązuje zarówno w czasie trwania stosunku pracy, jak i po jego ustaniu.
3. O wszelkich nieprawidłowościach, będących następstwem naruszenia zasad określonych w planie ochrony, każdy pracownik jest zobowiązany niezwłocznie poinformować pełnomocnika ochrony informacji niejawnych, który podejmie stosowne działania, zmierzające do wyjaśnienia okoliczności powstałej sytuacji, informując o tym Wójta.
4. O każdym fakcie ujawnienia informacji niejawnej wytworzonej, otrzymywanej lub przechowywanej w urzędzie, utracie dokumentu zawierającego takie informacje jego zaginięciu bądź powstania sytuacji, w której zagrożona byłaby jej ochrona, należy niezwłocznie informować pełnomocnika ochrony informacji .
5. W sprawach nieuregulowanych w planie ochrony mają zastosowanie odpowiednie przepisy ustawy, aktów wykonawczych wydanych na jej podstawie oraz odpowiednich zarządzeń Wójta.
6. Interpretacji i wyjaśnień dotyczących zasad i zakresu ochrony informacji zastrzeżonych określonych w szczegółowych wymaganiach dokonuje pełnomocnik ochrony informacji niejawnych.

XIV. ARKUSZ AKTUALIZACYJNY

Lp.	Data	Wprowadzona aktualizacja	Podpis

ZAŁĄCZNIKI:

1. Tabela oceny istotności czynników zagrożeń

L.P.	CZYNNIK	OCENA ISTOTNOŚCI CZYNNIKA			UZASADNIENIE
		BARDZO ISTOTNY (8 pkt.)	ISTOTNY (4 pkt.)	MAŁO ISTOTNY (1 pkt.)	
1.	Klauzula tajności przetwarzanych informacji niejawnych			1	Z uwagi na fakt, iż w Urzędzie Gminy Wilczyn występują wyłącznie materiały niejawne o klauzuli „zastrzeżone” czynnik jest mało istotny – przyznano 1 pkt.
2.	Liczba materiałów niejawnych			1	Materiały niejawne przetwarzane w Urzędzie Gminy Wilczyn opatrzone klauzulą „zastrzeżone” są to głównie dokumenty wytwarzane w celach obronnych. Dokumenty przechowywane są w pomieszczeniu do tego wyznaczonym.
3.	Postać informacji niejawnych			1	Przetwarzane informacje niejawne nie są przesyłane w formie email, ani przekazywane poza Urząd Gminy w postaci elektronicznej, tylko drukowane i przesyłane oraz przechowywane w formie papierowej po wydrukowaniu. Wersje elektroniczne dokumentów tworzone są w celu możliwości ich odtwarzania i ewentualnej korekty czy aktualizacji. Dokumenty wytwarzane są osobiście przez upoważnionych pracowników. Z uwagi na ilość występujących materiałów niejawnych o klauzuli „zastrzeżone” określa się czynnik jako mało istotny – przyznano 1 pkt
4.	Liczba osób		4		Z uwagi na dużą ilość osób mających lub mogących mieć dostęp do informacji niejawnych określono czynnik jako istotny – przyznano 4 pkt.
5.	Lokalizacja		4		Dokumenty „zastrzeżone” przechowywane są w wyznaczonym pomieszczeniu w metalowej szafie. Drzwi wejściowe do Urzędu Gminy oraz okna nie są okratowane. Brak alarmu.
6.	Dostęp osób do budynku		4		Dostęp do budynku Urzędu Gminy jest swobodny dla osób z zewnątrz. Urząd nie posiada odrębnej strefy obsługi interesantów, a dostęp w godzinach pracy do poszczególnych biur jest nieograniczony. Dostęp do pomieszczenia, w którym są przechowywane informacje niejawne jest możliwy jedynie pod kontrolą pracowników, którzy posiadają do niego wyłączny dostęp.
7.	Inne czynniki			1	Stały dostęp do informacji niejawnych jest ograniczony, a klauzula chronionych dokumentów jest najniższa, zatem działanie obcych służb specjalnych, sabotaż, zamach terrorystyczny, kradzież lub inna działalność przestępcza, pożar, działanie sił przyrody ocenia się na poziomie mało istotnym z uwagi na specyfikę działalności Urzędu oraz charakterystykę klimatu panującego na terenie Gminy. Istnieje jedynie możliwość awarii wewnętrznej sieci wodnokanalizacyjnej i zalanie dokumentów lub instalacji elektrycznej ze skutkiem spalenia w wyniku powstałego pożaru.
SUMA PUNKTÓW			12	4	
RAZEM – wszystkie punkty			16		

TABELA DO OKREŚLENIA POZIOMU ZAGROŻEŃ

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

W wyniku przeprowadzonej analizy poszczególnych czynników ostateczny poziom zagrożeń mających lub mogących mieć wpływ na bezpieczeństwo informacji niejawnych w Urzędzie Gminy Wilczyn określono jako **NISKI**.

2. Dobór środków bezpieczeństwa fizycznego**KATEGORIA K1: Szafy do przechowywania informacji niejawnych,**

Środek bezpieczeństwa K1S1 - Konstrukcja szafy: typ 1

K1S1= 1 pkt.

Środek bezpieczeństwa K1S2- Zamek do szafy: typ 1

K1S2=1 pkt.

Liczba punktów za kategorię stanowiącą iloczyn liczby punktów za powyższe środki bezpieczeństwa ($K1 = K1S1 \times K1S2$) = 1 pkt.

KATEGORIA K2 - pomieszczenia

Środek bezpieczeństwa K2S1 – konstrukcja pomieszczenia: typ 1

K2S1= 1 pkt.

Środek bezpieczeństwa K2S2 - zamek do drzwi pomieszczenia: typ 1

K2S2= 1 pkt.

Liczba punktów za kategorię stanowiącą iloczyn liczby punktów za powyższe środki bezpieczeństwa ($K2 = K2S1 \times K2S2$) = 1 pkt.

KATEGORIA K3- budynki: typ 3

Liczba punktów za kategorię K3=3 pkt.

**OSTATECZNA TABELA WYZNACZONEJ PUNKTACJI ZA ZASTOSOWANE
ŚRODKI BEZPIECZEŃSTWA FIZYCZNEGO
W URZĘDZIE GMINY WILCZYN**

ŚRODEK BEZPIECZEŃSTWA	PUNKTACJA
<u>KATEGORIA K1: SZAFY DO PRZECHOWYWANIA INFORMACJI NIEJAWNYCH</u>	
<i>ŚRODEK BEZPIECZEŃSTWA K1S1 - Konstrukcja szafy – TYP 1</i>	
<i>Liczba punktów za środek bezpieczeństwa K1S1</i>	1
<i>ŚRODEK BEZPIECZEŃSTWA K1S2 – Zamek do szafy</i>	
<i>Liczba punktów za środek bezpieczeństwa K1S2</i>	1
<i>Liczba punktów za kategorię K1 stanowiącą iloczyn punktów za oba powyższe środki bezpieczeństwa ($K1=K1S1 \times K1S2$)</i>	1
<u>KATEGORIA K2: POMIESZCZENIA</u>	
<i>ŚRODEK BEZPIECZEŃSTWA K2S1 – Konstrukcja pomieszczenia</i>	
<i>Liczba punktów za środek bezpieczeństwa K2S1</i>	1
<i>ŚRODEK BEZPIECZEŃSTWA K2S2 - Zamek do drzwi pomieszczenia</i>	
<i>Liczba punktów za środek bezpieczeństwa K2S2</i>	1
<i>Liczba punktów za kategorię K2 stanowiącą iloczyn liczby punktów za oba powyższe środki bezpieczeństwa ($K2=K2S1 \times K2S2$)</i>	1
<u>KATEGORIA K3 – BUDYNKI</u>	
<i>Liczba punktów za kategorię K3 – TYP 3</i>	3
<i>Ogólna liczba punktów stanowiąca sumę punktów za wszystkie kategorie</i> <i>PUNKTY = $K1+K2+K3$</i>	5

Ogólna liczba punktów stanowiąca sumę punktów za wszystkie kategorie $K1+K2+K3=5$ jest większa od wymaganej do osiągnięcia (2) - w związku z tym nie jest konieczne stosowanie dodatkowych środków bezpieczeństwa z kategorii K4, K5 lub K6.

PLAN OCHRONY INFORMACJI NIEJAWNYCH

W wyniku przeprowadzonej analizy w Urzędzie Gminy Wilczyn zostały zastosowane następujące środki w zakresie bezpieczeństwa fizycznego w celu zapewnienia poufności, integralności i dostępności informacji niejawnych oznaczonych klauzulą „zastrzeżone”.

3. Wykaz stanowisk, z którymi może łączyć się dostęp do informacji niejawnych o klauzuli „ZASTRZEŻONE”

LP.	STANOWISKO	UWAGI
1.	Wójt Gminy	
2.	Sekretarz Gminy	
3.	Pełnomocnik ds. ochrony informacji niejawnych	
4.	Pracownik ds. ewidencji ludności, spraw wojskowych i obronnych	
5.	Inspektor Bezpieczeństwa Teleinformatycznego	
6.	Administrator Systemu Informatycznego	
7.	Kurierzy wykonawcy Akcji Kurierskiej	

4. Wykaz informacji niejawnych stanowiących tajemnicę służbową o klauzuli „zastrzeżone”

LP.	RODZAJ INFORMACJI	UWAGI
1	Plan Akcji Kurierskiej	
2	Sprawozdanie roczne z Akcji Kurierskiej	
3	Plan Operacyjny Funkcjonowania Gminy Wilczyn w warunkach zewnętrznego zagrożenia bezpieczeństwa i w czasie wojny	
4	Karty realizacji zadań operacyjnych	
5	Dokumenty postępowań sprawdzających w tym ankiety bezpieczeństwa osobowego	
7	Korespondencja z Agencją Bezpieczeństwa Wewnętrznego w sprawach postępowań sprawdzających wg potrzeb.	

5. Wzór protokołu oceny dokumentacji niearchiwalnej.

PROTOKÓŁ OCENY DOKUMENTACJI NIEARCHIWALNEJ

Komisja w składzie:

.....
imię i nazwisko, stanowisko

.....
imię i nazwisko, stanowisko

.....
imię i nazwisko, stanowisko

dokonała oceny i wydzielenia przeznaczonej do przekazania na makulaturę lub zniszczenie dokumentacji niearchiwalnej w ilościmb. i stwierdziła, że stanowi ona dokumentację niearchiwalną dla celów praktycznych jednostki organizacyjnej, oraz że upłynęły terminy jej przechowywania określone w jednolitym rzeczowym wykazie akt.

Przewodniczący komisji:

Członkowie komisji :

.....

.....

.....

Załączniki:

.....kart spisu

.....pozycji spisu

Przekazujący przekazuje, a Przyjmujący przyjmuje teczki, rejestry i pisma ewidencyjne o numerach:

[illegible]

PRZEKAZUJĄCY

.....
(imię, nazwisko, podpis)

7. Wzór protokołu otwarcia szafy, sejfu.

PROTOKÓŁ OTWARCIA SEJFU (Szafy)

W dniu.....

Komisja w składzie :

1.
(imię i nazwisko)

2.
(imię i nazwisko)

3.
(imię i nazwisko)

dokonała otwarcia sejfu (szafy) znajdującej się w pomieszczeniu nr....., którego Użytkownikiem jest.....

(imię i nazwisko oraz stanowisko służbowe)

Z sejfu (szafy) zostały zabrane następujące dokumenty (materiały, przedmioty):

1.
2.
3.

którymi obecnie dysponuje Pan/i

.....
(imię i nazwisko oraz stanowisko służbowe)

Sejf (szafę) zamknięto i zaplombowano pieczęcią (referentką do plasteliny nr.....) w obecności członków komisji.

Podpisy członków komisji:

1. 2. 3.

8. Wzór upoważnienia jednorazowego

U P O W A Ż N I E N I E Nr.....

Na podstawie art.21, pkt 4, ust.1 ustawy z dnia 05 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2016 r., poz.1167 z późn.zm.)

u p o w a ż n i a m

Panią/ Pana:

PESEL:

Imię ojca:

do dostępu do informacji niejawnych stanowiących tajemnicę służbową oznaczonych klauzulą „zastrzeżone”

w związku z

(określić rodzaj zadania do wykonania)

- Upoważnienie ważne jest na czas wykonania zadania.
- Dostęp do informacji niejawnych o klauzuli „zastrzeżone” może nastąpić po odbyciu szkolenia w zakresie przepisów ustawy o ochronie informacji niejawnych.
- Upoważnienie może zostać cofnięte w każdym czasie. W takim wypadku upoważniony powinien zaprzestać działań, do których został upoważniony na podstawie mniejszego dokumentu oraz zwrócić upoważnienie pełnomocnikowi ochrony.

.....

(podpis kierownik jednostki organizacyjnej)

9. Wzór dokumentu potwierdzającego odbycie szkolenia z zakresu ochrony informacji niejawnych.

Z A Ś W I A D C Z E N I E Nr.....

**stwierdzające odbycie szkolenia
w zakresie ochrony informacji niejawnych**

Stwierdza się, że Pani(Pan):

- Imię i nazwisko:
- Numer PESEL:

Odbyła (odbył) szkolenie w zakresie ochrony:

- Informacji niejawnych,*
- Informacji niejawnych Organizacji Traktatu Północnoatlantyckiego,*
- Informacji niejawnych Unii Europejskiej,*

na podstawie przepisów ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2016 r., poz. 1167 z późn.zm.), zorganizowane przez pełnomocnika do spraw ochrony informacji niejawnych w Urzędzie Gminy w Wilczynie, ul. Strzełńska 12D, 62-550 Wilczyn

.....
(miejscowość i data)

.....
(podpis i imienna pieczęć pełnomocnika ochrony lub jego zastępcy)

Otrzymują:

1. Adresat
2. Pełnomocnik Ochrony Informacji Niejawnych

*niepotrzebne skreślić

10. Wzór oświadczenia osoby upoważnionej do przestrzegania przepisów dot. ochrony informacji niejawnych.

Wilczyn,
(data)

.....
(Imię i Nazwisko)

.....
(stanowisko i nazwa komórki organizacyjnej)

OŚWIADCZENIE

Ja, niżej podpisana(y) oświadczam, że zapoznała(e)m się z przepisami dotyczącymi ochrony informacji niejawnych i zobowiązuje się do przestrzegania:

- Przepisów Ustawy o ochronie informacji niejawnych z 5 sierpnia 2010 r. (Dz.U. z 2016 r., poz. 1167) oraz przepisów wynikających z rozporządzeń wydanych na podstawie ww. Ustawy.
- Procedur wewnętrznych Urzędu Gminy w Wilczynie dotyczących ochrony informacji niejawnych.
- Zachowania tajemnicy przez cały okres zatrudnienia, także po ustaniu stosunku pracy, wszelkie informacje dotyczące informacji niejawnych, przetwarzania oraz sposobów zabezpieczenia tych informacji w Urzędzie Gminy w Wilczynie.

Jednocześnie oświadczam, że:

- Zostałem/am przeszkolony przez Pełnomocnika Ochrony Informacji Niejawnych Urzędu Gminy w Wilczynie z zakresu przestrzegania przepisów dotyczących ochrony informacji niejawnych.
- Zapewnię ochronę informacji niejawnym przetwarzanym w Urzędzie Gminy w Wilczynie, a w szczególności zabezpieczę je przed dostępem osób nieupoważnionych, zabraniem, uszkodzeniem oraz nieuzasadnioną modyfikacją lub zniszczeniem.
- Natychmiast zgłoszę przełożonemu i Pełnomocnikowi ochrony informacji niejawnych stwierdzenie próby lub faktu naruszenia systemu ochrony fizycznej i teleinformatycznej informacji niejawnych.

.....
(czytelny podpis osoby upoważnionej)