Zarządzenie Nr 0050.18.2016
Wójta Gminy Lisków
z dnia 18.05.2016 r.

w sprawie zatwierdzenia „Planu ochrony informacji niejawnych w Urzędzie Gminy w Liskowie".

Na podstawie art. 33 ust. 1 i 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t. j. Dz. U. z 2016 r. poz. 446) w związku z art. 15 ust. 1 pkt 5 ustawy o ochronie informacji niejawnych (tj. Dz. U. z 2010 r. Nr 182 poz. 1228 z późniejszymi zmianami) zarządzam, co następuje:

§ 1.

W celu zapewnienia właściwej realizacji zadań w zakresie ochrony informacji niejawnych w Urzędzie Gminy w Liskowie zatwierdzam i wprowadzam do użytku opracowany przez Pełnomocnika ds. ochrony informacji niejawnych: **„Plan ochrony informacji niejawnych w Urzędzie Gminy w Liskowie",** stanowiący Załącznik do niniejszego zarządzenia.

§ 2.

„Plan ochrony informacji niejawnych w Urzędzie Gminy w Liskowie" dotyczy wszystkich pracowników Urzędu Gminy w Liskowie, którzy przetwarzają informacje niejawne.

§ 3.

Wykonanie zarządzenia powierzam Pełnomocnikowi ds. ochrony informacji niejawnych.

§ 4.

Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT
Maria Krawiec

Rozdzielnik:

1. Pełnomocnik ds. ochrony informacji niejawnych
2. Pracownik Kancelarii Materiałów Niejawnych
3. Pracownicy Urzędu Gminy w Liskowie
4. a/a

Załącznik do
Zarządzenia Nr 0050.18.2016
Wójta Gminy Lisków
z dnia 18.05.2016

PLAN OCHRONY INFORMACJI NIEJAWNYCH

W URZĘDZIE GMINY W LISKOWIE

Opracował: Katarzyna Włodarczyk

Pełnomocnik ds. Ochrony
Informacji Niejawnych

Zatwierdzam
WÓJT
Mariel Krawiec
/Kierownik Jednostki/

Spis treści:

I. AKTY PRAWNE ZWIĄZANE Z OCHRONĄ INFORMACJI NIEJAWNYCH.

- **DZIENNIK USTAW Nr 182 z 2010 r., poz. 1228**
  Ustawa o ochronie informacji niejawnych z dnia 5 sierpnia 2010 r.

- **DZIENNIK USTAW Nr 276 z 2011 r., poz. 1631**
  Rozporządzenie Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych

- **DZIENNIK USTAW Nr 258 z 2010 r., poz. 1752**
  Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie wzorów poświadczeń bezpieczeństwa

- **DZIENNIK USTAW Nr 258 z 2010 r., poz. 1751**
  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.

- **DZIENNIK USTAW Nr 159 z 2011 r., poz. 948**
  Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego

- **DZIENNIK USTAW Nr 271 z 2011 r., poz. 1603**
  Rozporządzenie Prezesa Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne

- **DZIENNIK USTAW Nr 288 z 2011 r., poz. 1692**
  Rozporządzenie Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności

- **DZIENNIK USTAW Nr 93 z 2011 r., poz. 541**
  Rozporządzenie Prezesa Rady Ministrów z dnia 27 kwietnia 2011 r. w sprawie przygotowania i przeprowadzania kontroli stanu zabezpieczenia informacji niejawnych

- **DZIENNIK USTAW Nr 115 z 2012 r., poz. 683**
  Rozporządzenie Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych.

II. DEFINICJE UŻYWANE W PLANIE OCHRONY INFORMACJI NIEJAWNYCH

W rozumieniu planu ochrony informacji niejawnych:
1. ustawą - jest ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228),
2. służbą ochrony państwa - jest Agencja Bezpieczeństwa Wewnętrznego
3. rękojmią zachowania tajemnicy — jest zdolność osoby do spełnienia ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem, stwierdzona w wyniku przeprowadzenia postępowania sprawdzającego;
4. dokumentem — jest każda utrwalona informacja niejawna;
5. materiałem — jest dokument lub przedmiot albo dowolna ich część, chronione jako informacja niejawna, a zwłaszcza urządzenie, wyposażenie lub broń wyprodukowane albo będące w trakcie produkcji, a także składnik użyty do ich wytworzenia;
6. przetwarzaniem informacji niejawnych — są wszelkie operacje wykonywane w odniesieniu do informacji niejawnych i na tych informacjach, w szczególności ich wytwarzanie, modyfikowanie, kopiowanie, klasyfikowanie, gromadzenie, przechowywanie, przekazywanie lub udostępnianie;
7. Urzędem - jest Urząd Gminy w Liskowie;
8. Wójtem – jest Wójt Gminy Lisków;
9. pełnomocnikiem ochrony - jest Pełnomocnik ds. Ochrony Informacji Niejawnych w Urzędzie Gminy w Liskowie.

III. KLASYFIKACJA INFORMACJI NIEJAWNYCH.

Informacjom niejawnym nadaje się klauzulę „**poufne**", jeżeli ich nieuprawnione ujawnienie spowoduje szkodę dla Rzeczypospolitej Polskiej przez to, że:

1) utrudni prowadzenie bieżącej polityki zagranicznej Rzeczypospolitej Polskiej;
2) utrudni realizację przedsięwzięć obronnych lub negatywnie wpłynie na zdolność bojową Sił Zbrojnych Rzeczypospolitej Polskiej;
3) zakłóci porządek publiczny lub zagrozi bezpieczeństwu obywateli;
4) utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za ochronę bezpieczeństwa lub podstawowych interesów Rzeczypospolitej Polskiej;
5) utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za ochronę porządku publicznego, bezpieczeństwa obywateli lub ściganie sprawców przestępstw i przestępstw skarbowych oraz organom wymiaru sprawiedliwości;
6) zagrozi stabilności systemu finansowego Rzeczypospolitej Polskiej;
7) wpłynie niekorzystnie na funkcjonowanie gospodarki narodowej.

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.

IV. OCENA ZAGROŻEŃ ZEWNĘTRZNYCH I WEWNĘTRZNYCH .

1. Ocena zagrożeń zewnętrznych:

a) Zagrożeniami zewnętrznymi dla Urzędu Gminy w Liskowie są:

- możliwość napadu lub włamania przez zorganizowane grupy przestępcze i terrorystyczne, działające w sposób profesjonalny, przemyślany i zorganizowany,
- możliwość napadu lub włamania przez pojedynczych przestępców, możliwość napadu przez przypadkowe osoby wykorzystujące nadarzającą się okazję z powodu nieprawidłowości i niewystarczającej ochronie mienia urzędu.

b) Symptomy mogące świadczyć o przygotowaniu napadu lub włamania do budynku:

- wzmożone zainteresowanie osób postronnych obiektem, pomieszczeniem urzędu objawiające się między innymi: podejmowaniem prób uzyskania informacji o danym obiekcie, pomieszczeniu etc. od pracowników podczas luźnych rozmów po "przypadkowym" spotkaniu,
- nawiązaniem rozmów przez osoby postronne z pracownikami,
- podszywaniem się pod byłych pracowników urzędu pracujących w urzędzie i przejawianie zainteresowaniem tym, co się po latach zmieniło,
- interesowaniem się osobami funkcyjnymi, w tym także ich przywarami oraz sposobem wykonywania obowiązków służbowych,
- obserwacja sposobu działania systemu ochronnego, sekretariatu, sprzątaczki itp.,
- rozpoznawanie systemu technicznych zabezpieczeń, w tym stosowanych urządzeń alarmowych,
- celowe uszkadzanie urządzeń alarmowych, linii telefonicznych, oświetlenia itp.,
- próby pozyskania do grup przestępczych pracowników urzędu (dotyczy głównie osób mających problemy finansowe, towarzyskie, a także służbowe).
-

c) Wnioski:

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

- systematyczną, skrupulatną i wnikliwą kontrolę budynku Urzędu Gminy i wyznaczonych stref bezpieczeństwa,
- stosować zasadę niedopuszczania osób niepowołanych do penetracji strefy bezpieczeństwa,
- wykonywanie prac porządkowych, remontowych itp. w strefie bezpieczeństwa wyłącznie pod nadzorem osób odpowiedzialnych.

2. Ocena zagrożeń wewnętrznych:

- próby pozyskania dokumentów lub mienia przez pracowników urzędu,
- próby powielania, kserowania dokumentów służbowych dla celów prywatnych,
- byli pracownicy urzędu zwolnieni dyscyplinarnie,
- rozpoznanie organizacji pracy Urzędu Gminy celem łatwiejszej pracy grup przestępczych na terenie urzędu,
- próby wglądu w dokumenty niejawne przez osoby nieuprawnione,
- nadmierne spożywanie alkoholu - przesłanką do wykroczeń dyscyplinarnych i przestępstw.

3. Wnioski:

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

a) zwracanie szczególnej uwagi na osoby, które mogą być zainteresowane uzyskaniem dokumentu,
b) prowadzić szczególny nadzór, by nie dokonywano prób kserowania, kopiowania bez zgody przełożonego,
c) uwrażliwianie pracowników w trakcie prowadzonych szkoleń na możliwość prób kontaktu grup przestępczych z pracownikami, którzy mają dostęp do dokumentów szczególnie ważnych,
d) zastosowanie zasady, że do informacji niejawnych mogą mieć dostęp tylko pracownicy posiadający poświadczenie bezpieczeństwa lub właściwe upoważnienie jednorazowe wydane przez kierownika jednostki,
e) wprowadzenie szczególnej uwagi na osoby, których zachowanie wskazuje na nadmierne spożywanie alkoholu.

V. PRZEDMIOT OCHRONY.

1. Przedmiotem ochrony w Urzędzie Gminy w Liskowie są informacje niejawne oznaczone klauzulą:

   - „zastrzeżone".

VI. SZACOWANIE RYZYKA.

Szacowanie ryzyka i poziomu zagrożeń związany z dostępem do informacji niejawnych osób nieuprawnionych lub ich utratą zawiera Załącznik Nr 1 do Planu Ochrony.

A. POZIOM ZAGROŻEŃ

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

2. W celu doboru adekwatnych środków bezpieczeństwa fizycznego określa się poziom zagrożeń związanych z utratą poufności, integralności lub dostępności informacji niejawnych, zwany dalej „poziomem zagrożeń".
3. Poziom zagrożeń określono dla pomieszczenia lub obszaru, w którym przetwarzane są informacje niejawne.
4. Poziom zagrożeń określono się jako **niski** dla najwyższej klauzuli informacji niejawnych **„zastrzeżone".**
5. W celu określenia poziomu zagrożeń przeprowadzono analizę, w której uwzględniono wszystkie istotne czynniki mogące mieć wpływ na bezpieczeństwo informacji niejawnych, w szczególności:

a) klauzule tajności przetwarzanych informacji niejawnych;
b) postać i ilość informacji niejawnych;
c) sposób przechowywania informacji niejawnych;
d) otoczenie i strukturę budynków lub obszarów, w których przetwarzane są informacje niejawne;
e) ilość osób mających lub mogących mieć dostęp do informacji niejawnych, a także posiadane przez nich uprawnienia oraz uzasadnioną potrzebę dostęp do informacji niejawnych;
f) szacowane zagrożenie ze strony obcych służb specjalnych oraz zagrożenie sabotażem, zamachem terrorystycznym, kradzieżą lub inną działalnością przestępczą.

6. Zatwierdzenie dokumentacji, o której mowa w art. 43 ust. 4 ustawy (**poufne i wzwyż**), lub instrukcji, o której mowa w art. 43 ust. 5 ustawy (**zastrzeżone**) jest równoznaczne z formalnym zaakceptowaniem przez kierownika jednostki organizacyjnej określonego poziomu zagrożeń wraz z jego ewentualnymi konsekwencjami.
7. Poziom zagrożeń określa się przed rozpoczęciem przetwarzania informacji niejawnych, a także po każdej zmianie czynników, mogącej mieć istotny wpływ na bezpieczeństwo informacji niejawnych.
8. W ramach systemu bezpieczeństwa fizycznego informacji niejawnych stosuje się środki bezpieczeństwa fizycznego w celu zapewnienia poufności, integralności i dostępności tych informacji.
9. Cel, o którym mowa osiąga się przez:

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 nieuprawnionych działań;

d) uniemożliwianie lub opóźnianie wtargnięcia osób nieuprawnionych w sposób niezauważony lub z użyciem siły do pomieszczenia lub obszaru, w którym przetwarzane są informacje niejawne.

10. Środki bezpieczeństwa fizycznego stosuje się we wszystkich pomieszczeniach i obszarach, w których są przetwarzane informacje niejawne, w tym w miejscach, w których znajdują się systemy teleinformatyczne przetwarzające informacje niejawne (jeżeli takie są stosowane w jednostce).
11. W zależności od poziomu zagrożeń określonego w wyniku przeprowadzenia analizy, stosuje się odpowiednią kombinację następujących środków bezpieczeństwa fizycznego:

a) bariery fizyczne – środki chroniące granice miejsca, w którym przetwarzane są informacje niejawne, w szczególności są to ogrodzenia, ściany, bramy, drzwi i okna;

b) szafy i zamki – stosowane do przechowywania informacji niejawnych lub zabezpieczające te informacje przed nieuprawnionym dostępem.

12. W celu zapewnienia poufności, integralności i dostępności informacji niejawnych można zastosować również środki bezpieczeństwa fizycznego inne niż wymienione powyżej, jeżeli wynika to z analizy poziomu zagrożeń.

B. METODYKA DOBORU ŚRODKÓW BEZPIECZEŃSTWA FIZYCZNEGO

1. Proces doboru środków bezpieczeństwa fizycznego zapewnia elastyczność ich stosowania w zależności od określonego poziomu zagrożeń oraz w oparciu o ustalone podstawowe wymagania doboru środków bezpieczeństwa fizycznego.

2. Zastosowano najbardziej odpowiednie i ekonomiczne kombinacje środków bezpieczeństwa fizycznego, których celem jest ochrona informacji niejawnych.

3. Proces doboru środków bezpieczeństwa fizycznego:

PIERWSZY ETAP procesu doboru środków bezpieczeństwa fizycznego	odczytanie z tabeli w cz. II „Podstawowe wymagania bezpieczeństwa fizycznego" minimalnej łącznej sumy punktów wymaganych do osiągnięcia założonego poziomu ochrony informacji w wyniku zastosowania odpowiednich środków bezpieczeństwa fizycznego. Liczba wymaganych punktów zależy od najwyższej klauzuli tajności informacji przetwarzanych w danej lokalizacji oraz poziomu zagrożeń, określonego wcześniej zgodnie z § 3 rozporządzenia.
DRUGI ETAP procesu doboru środków bezpieczeństwa fizycznego	odczytanie z tej samej tabeli w cz. II, odpowiadającej założonemu poziomowi ochrony informacji, minimalnej liczby punktów koniecznych do uzyskania w każdej z grup obejmującej kategorie wymaganych do zastosowania środków bezpieczeństwa fizycznego (oznaczonej „obowiązkowo").

TRZECI ETAP procesu doboru środków bezpieczeństwa fizycznego	dokonanie wyboru określonych środków bezpieczeństwa fizycznego, przy którym należy posługiwać się tabelą w cz. III „Klasyfikacja środków bezpieczeństwa fizycznego". W tej tabeli należy odczytać liczbę punktów odpowiadającą wybranemu środkowi bezpieczeństwa i wpisać ją w odpowiednie miejsce w tabeli w cz. IV „Punktacja zastosowanych środków bezpieczeństwa fizycznego". Przy dokonywaniu wyboru konieczne jest uwzględnienie wymagań określonych w rozporządzeniu, jak też w samej tabeli w cz. III „Klasyfikacja środków bezpieczeństwa fizycznego". Dobór adekwatnych środków bezpieczeństwa fizycznego w konkretnym przypadku musi zapewnić uzyskanie zarówno minimalnej łącznej sumy punktów wymaganych do osiągnięcia założonego poziomu ochrony informacji niejawnych (w zależności od najwyższej klauzuli tajności informacji przetwarzanych w danej jednostce oraz poziomu zagrożeń), jak również uzyskanie minimalnej liczby punktów odpowiadających każdej z grup kategorii środków bezpieczeństwa fizycznego (oznaczonych jako „obowiązkowo"). W przypadku, gdy liczba punktów uzyskanych po zastosowaniu środka należącego do grup kategorii oznaczonych jako „obowiązkowo" jest mniejsza od minimalnej łącznej sumy punktów wymaganych do osiągnięcia założonego poziomu ochrony informacji niejawnych, należy zastosować środki z kategorii oznaczonych „dodatkowo" zapewniające uzyskanie minimalnej łącznej sumy punktów.

VII. EWIDENCJA MATERIAŁÓW NIEJAWNYCH POSTĘPOWANIE Z PRZESYŁKAMI

1. Informacje niejawne o klauzuli „zastrzeżone" mogą być ewidencjonowane przez pracownika kancelarii materiałów niejawnych, na zasadach określonych przez kierownika jednostki, opisanych w Instrukcji dotyczącej 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 Liskowie oraz w Planie Ochrony Informacji Niejawnych.

2. Sposób właściwego opisania dokumentu niejawnego został przedstawiony w załączniku nr 2 do Planu Ochrony Informacji Niejawnych.

VIII. DOSTĘP DO INFORMACJI NIEJAWNYCH OZNACZONYCH KLAUZULĄ „ZASTRZEŻONE".

1. Informacje niejawne oznaczone klauzulą „zastrzeżone" mogą być udostępniane wyłącznie osobie uprawnionej do dostępu do informacji niejawnych o określonej klauzuli niejawności.

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

a) po uzyskaniu przez pracownika upoważnienia dostępu do informacji niejawnych oznaczonych klauzulą „zastrzeżone" wydanego przez kierownika jednostki,
b) po przeszkoleniu tej osoby w zakresie przepisów ustawy o ochronie informacji niejawnych i uzyskaniu odpowiedniego zaświadczenia. Szkolenie dla pracowników urzędu organizuje Pełnomocnik ochrony.

3. Osoba przeszkolona, o którym mowa w pkt.2 i 3 , zgodnie z art.20 ust.1 ustawy o ochronie informacji niejawnych składa pisemne oświadczenie o zapoznaniu się z przepisami o ochronie informacji niejawnych. Wzór oświadczenia stanowi Załącznik nr 3 do Planu ochrony.

4. Szkolenie kierownika jednostki w związku z przewidywanym dostępem do informacji niejawnych oznaczonych klauzulą „zastrzeżone" organizuje pełnomocnik ochrony wydając stosowne zaświadczenie.

IX . ZAKRES i ZASADY UDOSTĘPNIANIA INFORMACJI NIEJAWNYCH.

Udostępnianie informacji niejawnych oznaczonych klauzulą „zastrzeżone" określonej osobie może nastąpić w oparciu o ważne Poświadczenie Bezpieczeństwa lub pisemne upoważnienie kierownika jednostki - wzór upoważnienia stanowi Załącznik nr 5 do Planu Ochrony Informacji Niejawnych.

X. ZASADY WYKONYWANIA DOKUMENTÓW NIEJAWNYCH.

1. W Urzędzie Gminy w Liskowie dokumenty niejawne o klauzuli „zastrzeżone" są sporządzane ręcznie. Docelowo planuje się wdrożenie wykonywania dokumentów niejawnych z wykorzystaniem sprzętu komputerowego.

2. Klauzulę tajności na sporządzonym dokumencie niejawnym nadaje osoba, która jest uprawniona do podpisania dokumentu lub oznaczenia innego niż dokument materiału.

3. Propozycje przyznania klauzuli niejawności na wykonywanym dokumencie przedstawia osoba sporządzająca dokument.

4. Dokumenty niejawne powinny być opisane i oznaczone zgodnie Rozporządzeniem Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów,

umieszczania na nich klauzul tajności (Dz. U. Nr 288 z 2011 roku, poz.1692). Wzór sposobu opisania dokumentu stanowi Załącznik nr 2 do Planu.

XI. GROMADZENIE DOKUMENTÓW ZAWIERAJĄCYCH INFORMACJE NIEJAWNE.

1. Dokumenty zawierające informacje niejawne powinny być przechowywane zgodnie z rzeczowym podziałem akt.
2. Dokumenty ostatecznie załatwione wymagają wszycia w teczkę pism, po zakończeniu roku kalendarzowego, klauzule niejawności teczek określa się według dokumentu o najwyższej klauzuli tajności.
3. Dokumenty niejawne o klauzuli „zastrzeżone" mogą być przechowywane w kancelarii materiałów niejawnych lub na stanowiskach pracy w meblach biurowych zamykanych na klucz.

XII. OZNACZANIE, NADAWANIE, ZMIANA I ZNOSZENIE KLAUZULI NIEJAWNOŚCI MATERIAŁOM NIEJAWNYM.

1. Klauzulę tajności nadaje osoba, która jest uprawniona do podpisania dokumentu lub oznaczenia innego niż dokument materiału.

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

3. Osoba wymieniona w pkt.1 może określić datę lub wydarzenie, po którym nastąpi zniesienie lub zmiana klauzuli tajności.

4. Zniesienie lub zmiana klauzuli tajności jest możliwe wyłącznie po wyrażeniu pisemnej zgody przez osobę, o której mowa w pkt. 1, albo jej przełożonego w przypadku ustania lub zmiany ustawowych przesłanek ochrony.

5. Należy nie rzadziej niż raz na 5 lat dokonać przeglądu materiałów celem ustalenia, czy spełniają ustawowe przesłanki ochrony.

6. Po zniesieniu lub zmianie klauzuli tajności podejmuje się czynności polegające na naniesieniu odpowiednich zmian w oznaczeniu materiału i poinformowaniu o nich odbiorców. Odbiorcy materiału, którzy przekazali go kolejnym odbiorcom, są odpowiedzialni za poinformowanie ich o zniesieniu lub zmianie klauzul tajności.

7. Poszczególne części materiału mogą być oznaczone różnymi klauzulami tajności.

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

9. Wprowadza się następujące oznaczenia klauzul tajności:

„Z" – dla klauzuli „zastrzeżone".

10. Materiały zawierające informacje niejawne utrwalone na piśmie - „dokument nieelektroniczny" oraz „elektroniczny", oznacza się w sposób zgodny z Rozporządzeniem Prezesa Rady Ministrów z dnia 22 grudnia 2011r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności (Dz. U. Nr 288 z 2011r., poz.1692). Wzór opisania dokumentu niejawnego stanowi Załącznik nr 2 do Planu ochrony .

11. W przypadkach uzasadnionych organizacją ochrony informacji niejawnych na materiałach zawierających informacje niejawne można nanosić dodatkowe oznaczenia.

12. Na trwale oprawionych zbiorach dokumentów, rejestrach, książkach, broszurach i reprodukcjach klauzule tajności umieszcza się po prawej stronie na górze i dole zewnętrznych ścianek okładki oraz, jeżeli jest, na stronie tytułowej.

XIII. OKRESY OCHRONNE.

1. Na pismach zawierających informacje niejawne, wobec których minął ustawowy okres ochrony ustanowiony przez osobę uprawnioną do nadania klauzuli:
a) skreśla się klauzulę tajności na każdej stronie w prawym górnym i dolnym rogu;
b) na pierwszej stronie nad skreśloną klauzulą tajności w prawym górnym rogu umieszcza się dodatkowo napis „Jawne" oraz datę, imię, nazwisko i podpis osoby dokonującej tych adnotacji.

2. Na pismach zawierających informacje niejawne, wobec których zniesiono lub zmieniono przyznaną klauzulę tajności:

a) na każdej stronie w prawym górnym i dolnym rogu skreśla się dotychczasowe klauzule tajności;
b) nad skreślonymi klauzulami tajności umieszcza się nowe klauzule tajności;
c) na pierwszej stronie nad skreśloną klauzulą tajności w prawym górnym rogu umieszcza się datę, imię, nazwisko i podpis osoby dokonującej tych adnotacji oraz wskazuje się podstawy dokonanej zmiany.

3. W stosunku do pism znajdujących się w zbiorach dokumentów zawierających informacje niejawne, wobec których minął ustawowy lub ustanowiony okres ochrony, czynności, o których mowa w ust. 1—2, można dokonać najpóźniej w przypadku ich udostępniania lub przekazywania osobom spoza jednostki lub komórki organizacyjnej.

4. Na dokumentach elektronicznych nie dokonuje się skreśleń i adnotacji, o których mowa powyżej. Informacje o skreśleniach i adnotacjach umieszcza się we właściwych ewidencjach lub metadanych dokumentu elektronicznego.

5. Skreśleń i adnotacji, dokonuje pracownik kancelarii materiałów niejawnych lub inne upoważnione osoby.

6. Skreślenia klauzul tajności oraz adnotacji, dokonuje się kolorem czerwonym, w sposób czytelny. Wycieranie, wywabianie lub zamazywanie klauzuli tajności i dokonanych zmian jest niedozwolone.

7. W stosunku do pism znajdujących się w zbiorach dokumentów zawierających informacje niejawne, wobec których minął ustanowiony okres ochrony, czynności, o których mowa, można dokonać najpóźniej w przypadku ich udostępniania lub przekazywania osobom spoza jednostki lub komórki organizacyjnej.

8. W stosunku do materiałów innych niż pismo, na trwale oprawionych zbiorach dokumentów, rejestrach, książkach, broszurach i reprodukcjach sposoby dokonywania skreśleń i adnotacji stosuje się odpowiednio, uwzględniając sposób oznakowania tych materiałów.

XIV. KOPIE, ODPISY, WYPISY, WYCIĄGI LUB TŁUMACZENIA.

1. Na kopiach, odpisach, wypisach, wyciągach lub tłumaczeniach pism umieszcza się:

   a) na wszystkich stronach w prawym górnym rogu odpowiednio napis: „Kopia", „Odpis", „Wypis", „Wyciąg" lub „Tłumaczenie z języka – (nazwa języka) – (imię i nazwisko tłumacza)";

   b) na pierwszej stronie dodatkowo numer, pod jakim zostały zarejestrowane w dzienniku ewidencyjnym , numer egzemplarza wykonanej kopii, odpisu, wypisu, wyciągu lub tłumaczenia;

   c) na ostatniej stronie dodatkowo napis „Za zgodność" i odcisk tuszowej pieczęci urzędowej z nazwą jednostki lub komórki organizacyjnej (numerem jednostki wojskowej), w której sporządzono kopię, odpis, wypis, wyciąg lub tłumaczenie.

2. Zgodność z oryginałem kopii, odpisu, wypisu lub wyciągu potwierdza podpisem kierownik jednostki lub komórki organizacyjnej albo inna osoba przez niego upoważniona, a tłumaczenia – osoba dokonująca tłumaczenia.

3. Fakt sporządzenia kopii, odpisu, wypisu, wyciągu lub tłumaczenia odnotowuje **się** na dokumencie, z którego sporządzono kopię, odpis, wypis, wyciąg lub tłumaczenie, przez odcisk pieczęci lub umieszczenie adnotacji informującej o:

   a) nazwie jednostki lub komórki organizacyjnej, w której sporządzono kopię, odpis, wypis, wyciąg lub tłumaczenie;

   b) liczbie egzemplarzy sporządzonych kopii, odpisów, wypisów, wyciągów lub tłumaczeń;

   c) dacie sporządzenia kopii, odpisu, wypisu, wyciągu lub tłumaczenia;

d) numerze, pod jakim kopia, odpis, wypis, wyciąg lub tłumaczenie zostały zarejestrowane w dzienniku ewidencji wykonanych dokumentów.

4. Adnotacje, o których mowa wpisuje się przed wykonaniem kopii, odpisu, wypisu, wyciągu lub tłumaczenia, natomiast numer, pod jakim zostały zarejestrowane w dzienniku ewidencyjnym , nanosi się po wykonaniu kopii, odpisu, wypisu, wyciągu lub tłumaczenia.

XV. NADZÓR W ZAKRESIE OCHRONY INFORMACJI NIEJAWNYCH .

1. Za ochronę informacji niejawnych odpowiada kierownik jednostki organizacyjnej,

2. Zadania określone ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182 , poz.1228 z 2010 r.) w imieniu kierownika jednostki wykonuje pełnomocnik do spraw ochrony informacji niejawnych poprzez:

1) sprawowanie nadzoru nad przestrzeganiem zapisów Planu Ochrony Informacji Niejawnych,

2) sprawowanie nadzoru w zakresie ochrony informacji niejawnych oraz przestrzegania procedur związanych z upoważnianiem do dostępu do tych informacji.

XVI. ODPOWIEDZIALNOŚĆ KARNA, DYSCYPLINARNA I SŁUZBOWA ZA NARUSZENIE PRZEPISÓW O OCHRONIE INFORMACJI NIEJAWNYCH.

1. Zakres odpowiedzialności karnej osób, które dopuściły się przestępstwa lub czynu zabronionego przeciwko ochronie informacji został określony przepisami Kodeksu Karnego w art.266 Ustawy z dnia 6 czerwca 1997r., Kodeks Karny, Dz.U. z dnia 2 sierpnia 1997 r.

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

XVII. ARCHIWIZOWANIE, GROMADZENIE I NISZCZENIE MATERIAŁÓW NIEJAWNYCH.

1. Archiwizowanie materiałów niejawnych odbywa się z zachowaniem zasad określonych w Rozporządzeniu Ministra Kultury z dnia 16 września 2002 r. w sprawie postępowania z dokumentacją, zasad jej klasyfikowania i kwalifikowania oraz zasad i trybu przekazywania materiałów archiwalnych do archiwów państwowych (Dz. U. Nr 167, poz.1375,z dnia 9 października 2002 r.).

2. Zasady postępowania z dokumentacją w komórkach organizacyjnych wykonujących zadania w zakresie obronności i bezpieczeństwa państwa zostały określone w rozporządzeniu Prezesa Rady Ministrów z dnia 26 lutego 2010 roku (Dz.U. Nr 34 poz.181).

XVIII. PRZECHOWYWANIE KLUCZY I PIECZĘCI.

1. Osobą odpowiedzialną za przechowywanie kluczy i pieczęci jest pracownik kancelarii materiałów niejawnych.

2. Klucze i pieczęci przechowywane są w zamykanej szafie, do której dostęp ma pracownik kancelarii materiałów niejawnych oraz Pełnomocnik.

3. Kopie zapasowe kluczy znajdują się w Sekretariacie Urzędu Gminy w Liskowie.

ZAŁĄCZNIKI

DO PLANU OCHRONY INFORMACJI NIEJAWNYCH

ZAŁĄCZNIK Nr 1 – Szacowanie ryzyka i poziomu zagrożeń związany z dostępem osób nieuprawnionych do informacji niejawnych o klauzuli „zastrzeżone" lub ich utratą.

ZAŁĄCZNIK Nr 2 - Oznaczanie materiałów niejawnych.

ZAŁĄCZNIK Nr 3 - Wzór oświadczenia o zapoznaniu z przepisami o ochronie informacji niejawnych.

ZAŁĄCZNIK Nr 4 - Wzór protokołu zdawczo-odbiorczego.

ZAŁĄCZNIK Nr 5 - Wzór upoważnienia uprawniające dostęp do informacji niejawnych oznaczonych klauzulą „zastrzeżone".

ZAŁĄCZNIK Nr 6 – instrukcja alarmowa w przypadku zgłoszenia o podłożeniu lub znalezieniu ładunku wybuchowego w Urzędzie.

ZAŁĄCZNIK Nr 7 – Instrukcja postępowania w przypadku otrzymania przesyłki niewiadomego pochodzenia.

ZAŁĄCZNIK Nr 1 – Szacowanie ryzyka i poziomu zagrożeń związany z dostępem osób nieuprawnionych do informacji niejawnych o klauzuli „zastrzeżone" lub ich utratą.

Dla **niskiego** poziomu zagrożeń i najwyższej klauzuli informacji niejawnych „**zastrzeżone**" - minimalna liczba punktów do osiągnięcia, wskazana w tabeli „PODSTAWOWE WYMAGANIA BEZPIECZEŃSTWA FIZYCZNEGO" wynosi **2**.

Suma 2 punktów musi obowiązkowo składać się z jednego elementu:

- K1+K2+K3, która musi wynieść minimum **2** punkty.

Dodatkowo - w przypadku nieuzyskania wymaganej liczby 2 punktów - należy zastosować środki z kategorii K4, K5 lub K6.

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= K1S1x K1S2) = **1 pkt**

KATEGRIA 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=K2S1x K2S2 = **1 pkt**

KATEGORIA K3: **budynki**:
typ 3
Liczba punktów za kategorię K3=3 pkt

ŁĄCZNA LICZBA PUNKTÓW ZA KATEGORIE K1+K2+K3 = 5 pkt

ŁĄCZNA LICZBA PUNKTÓW ZA KATEGORIE K1+K2+K3= 5, czyli jest większa od wymaganej do osiągnięcia 2 pkt. W związku z tym nie jest konieczne stosowanie dodatkowych środków bezpieczeństwa z kategorii K4, K5 lub K6.

TABELA WYZNACZONEJ PUNKTACJI ZA ZASTOSOWANE ŚRODKI BEZPIECZEŃSTWA FIZYCZNEGO

ŚRODEK BEZPIECZEŃSTWA	PUNKTACJA
KATEGORIA K1: SZAFY DO PRZECHOWYWANIA INFORMACJI NIEJAWNYCH	
ŚRODEK BEZPIECZEŃSTWA K1S1*- Konstrukcja szafy – *TYP 1	
Liczba punktów za środek bezpieczeństwa K1S1	1
***ŚRODEK BEZPIECZEŃSTWA K1S2* – Zamek do szafy**	
Liczba punktów za środek bezpieczeństwa K1S2	1
Liczba punktów za kategorię K1 stanowiąca iloczyn punktów za oba powyższe środki bezpieczeństwa (K1=K1S1xK1S2)	**1**
KATEGORIA K2: POMIESZCZENIA	
***ŚRODEK BEZPIECZEŃSTWA K2S1* – Konstrukcja pomieszczenia**	
Liczba punktów za środek bezpieczeństwa K2S1	1
***ŚRODEK BEZPIECZEŃSTWA K2S2*- Zamek do drzwi pomieszczenia**	
Liczba punktów za środek bezpieczeństwa K2S2	1

Liczba punktów za kategorię K2 stanowiącą iloczyn liczby punktów za oba powyższe środki bezpieczeństwa (K2=K2S1xK2S2)	**1**
KATEGORIA K3 - BUDYNKI	
Liczba punktów za kategorię K3 – TYP 3	**3**
Ogólna liczba punktów stanowiąca sumę punktów za wszystkie kategorie ***PUNKTY = K1+K2+K3***	**5**

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

W wyniku przeprowadzonej analizy w Urzędzie Gminy w Liskowie zostały zastosowane następujące środki w zakresie bezpieczeństwa fizycznego w celu zapewnienia poufności, integralności i dostępności informacji niejawnych oznaczonych klauzulą **„zastrzeżone":**

1. SZAFY DO PRZECHOWYWANIA INFORMACJI NIEJAWNYCH

Konstrukcja szafy :

W szafie tego typu można przechowywać informacje niejawne o klauzuli tajności „zastrzeżone" w strefach ochronnych.
Szafa charakteryzuje się następującymi cechami:

1) jest to zamykany na klucz mebel biurowy, nie wyposażony w żadne szczególne funkcje zabezpieczające, ale charakteryzujący się umiarkowaną odpornością na nieuprawnione próby otwarcia;
2) jest zabezpieczona zamkiem typu 1, 2, 3 lub 4.

Zamek do szafy:
Zamek:

1) charakteryzuje się umiarkowaną odpornością na nieuprawnione próby otwarcia;
2) może być wykorzystywany wyłącznie w szafach typu 1.

2. POMIESZCZENIA

Konstrukcja pomieszczenia :
Konstrukcja pomieszczenia charakteryzuje się następującymi cechami:

1) jest to pomieszczenie lub pokój biurowy, który może zostać zamknięty (w przypadku pozostawienia bez nadzoru), zapewniający poziom bezpieczeństwa odpowiedni dla materiałów tam przechowywanych;
2) ściany, podłoga i strop są wykonane z gipsokartonu, lekkiej cegły, drewna, płyt pilśniowych lub innego materiału o podobnej wytrzymałości;
3) drzwi i okna spełniają wymagania kategorii 1 lub wyższej, określone w Polskiej Normie PN-EN 1627 .

Zamek do drzwi pomieszczenia:
Zamek charakteryzuje się następującymi cechami:

1) zapewnia umiarkowaną odporność na nieuprawnione próby otwarcia;
2) zamek i jego komponenty spełniają wymagania kategorii 2 lub wyższej, określone w Polskiej Normie PN-EN 1627.

3. BUDYNKI :

Budynek charakteryzuje się następującymi cechami:

1) zapewnia średni poziom odporności na próby włamania;

2) stanowi wytrzymałą konstrukcję, zazwyczaj z cegły lub pustaków, opartą na ścianach szczelinowych lub podobnej budowie;

3) okna i drzwi są wykonane w standardzie odpowiadającym standardowi budynku w zakresie odporności na włamanie; okna nie muszą być zabezpieczone w powyższy sposób, jeżeli:

- dolne krawędzie okien znajdują się na wysokości przynajmniej 5,5 m nad gruntem lub innym elementem budynku (np. balkonem lub balustradą),
- nie można uzyskać do nich dostępu z dachu lub z wykorzystanie znajdującego się w pobliżu elementu (rynna, drabina, drzewo) ułatwiającego potencjalny dostęp i penetrację.

ZAŁĄCZNIK NR 2 - Oznaczanie materiałów niejawnych.

DOKUMENT NIEELEKTRONICZNY

„ZASTRZEŻONE" („Z")

W przypadku dokumentów nieelektronicznych o klauzuli tajności „zastrzeżone" dopuszcza się odstąpienie od umieszczania oznaczeń:

w prawym górnym rogu:
- numer egzemplarza, a w przypadku, gdy dokument wykonano w jednym egzemplarzu napis "Egz. pojedynczy",

oraz

w lewym dolnym rogu w kolejności pionowej:
– liczbę wykonanych egzemplarzy,
– adresatów poszczególnych egzemplarzy dokumentu, adnotację "adresaci według rozdzielnika pozostającego przy oryginale" lub wskazanie „ad acta",
– imię i nazwisko lub inne dane identyfikujące wykonawcę.

Załącznik Nr 3

.....
/miejscowość, data/

.....
/imię i nazwisko/

.....
/stanowisko/

O Ś W I A D C Z E N I E

Zgodnie z art. 20 ust.1 ustawy o ochronie informacji niejawnych (Dz. U. Nr 182 z 2010r., poz.1228) oświadczam, iż w dniu .....zostałem/am zapoznany/a z przepisami o ochronie informacji niejawnych.

.....
/data i czytelny podpis/

ZAŁĄCZNIK NR 4 - Wzór protokołu zdawczo-odbiorczego.

PROTOKÓŁ ZDAWCZO – ODBIORCZY

sporządzony w dniu .....

w obecności .....
(imię i nazwisko Pełnomocnika Ochrony)

PRZYJMUJĄCY.....
(imię i nazwisko)

ZDAJĄCY .....
(imię i nazwisko)

W oparciu o dokonane sprawdzenie dokumentów i materiałów znajdujących się w kancelarii materiałów niejawnych w Urzędzie Gminy w Liskowie stwierdzam, że stan ewidencyjny dokumentów ujęty w książkach i dziennikach ewidencyjnych jest zgodny ze stanem faktycznym.

W czasie przyjmowania obowiązków nie stwierdziłem nieprawidłowości / stwierdziłem następujące niedociągnięcia:

1. .....
2. .....
3. .....

WNIOSKI

1. .....
2. .....
3. .....

Wykaz przyjętych dokumentów i materiałów stanowią załączniki do niniejszego protokołu.
Załączniki .....na .....str.

Obowiązki zdał

.....
(podpis)

Obowiązki przyjął

.....
(podpis)

w obecności

.....
(podpis Pełnomocnika Ochrony)

SPIS DOKUMENTÓW

Załącznik nr ..... do Protokołu zdawczo –odbiorczego z dnia .....

Lp.	NAZWA DOKUMENTU	NR EWID.	KLAUZULA	ILOŚC STRON	UWAGI

<u>ZAŁĄCZNIK Nr 5</u> - Wzór upoważnienia uprawniające dostęp do informacji niejawnych oznaczonych klauzulą „zastrzeżone".

Nr IN.1412..... Lisków, dn. .....

Pani /Pan

.....

Zgodnie z art. 21 ust. 4 ustawy z dnia 5 sierpnia 2010 r. (Dz. U. Nr 182, poz.1228 ze zmianami) o ochronie informacji niejawnych,

u p o w a ż n i a m

Panią/Pana ..... do dostępu do informacji niejawnych oznaczonych klauzulą **„zastrzeżone",** zatrudnioną w Urzędzie Gminy w Liskowie na stanowisku ..... Niniejsze upoważnienie ważne jest na czas zatrudnienia w Urzędzie Gminy w Liskowie.

.....

/kierownik jednostki/

*Dostęp do informacji niejawnych o klauzuli „zastrzeżone" może nastąpić po odbyciu szkolenia w zakresie przepisów ustawy o ochronie informacji niejawnych.

Otrzymują:
1. .....
2. Akta osobowe pracownika
3. a/a

ZAŁĄCZNIK NR 6 - Instrukcja alarmowa w przypadku zgłoszenia o podłożeniu lub znalezieniu ładunku wybuchowego w urzędzie.

INSTRUKCJA ALARMOWA W PRZYPADKU ZGŁOSZENIA O PODŁOŻENIU LUB ZNALEZIENIU ŁADUNKU WYBUCHOWEGO W URZĘDZIE.

I. ALARMOWANIE

1. Osoba, która przyjęła zgłoszenie o podłożeniu ładunku wybuchowego, albo zauważyła w obiekcie przedmiot niewiadomego pochodzenia, mogący być ładunkiem wybuchowym, jest obowiązana powiadomić o tym:
   - Kierownika obiektu lub jego zastępcę;
   - Policję.

2. Zawiadamiając Policję należy podać:
- Treść rozmowy ze zgłaszającym o podłożeniu ładunku wybuchowego, którą należy prowadzić wg poniższych wskazówek ;
  - miejsce i opis zlokalizowanego przedmiotu, który może być ładunkiem wybuchowym;
  - numer telefonu, z którego prowadzona jest rozmowa i swoje stanowisko;
  - uzyskać od policji potwierdzenie przyjętego powyższego zawiadomienia.

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

1. Do czasu przybycia Policji akcją kieruje administrator obiektu, a w czasie jego nieobecności osoba przez niego upoważniona.
2. Kierujący akcją zarządza, aby użytkownicy pomieszczeń dokonali sprawdzenia, czy w tych pomieszczeniach znajdują się :
   - przedmioty rzeczy lub urządzenia, paczki itp., których wcześniej nie było i nie wnieśli ich użytkownicy pomieszczeń (np. interesanci);
   - ślady przemieszczania elementów wyposażenia pomieszczeń;
   - zmiany w wyglądzie zewnętrznym przedmiotów, rzeczy, urządzeń, które przedtem w pomieszczeniu były oraz emitowane z nich sygnały (np. dźwięki mechanizmów zegarowych, świecące elementy elektroniczne itp.).
3. Pomieszczenia ogólnodostępne takie jak: korytarze, klatki schodowe, halle, toalety, strychy itp. oraz najbliższe otoczenie zewnętrzne obiektu powinno być sprawdzone przez pracowników obsługi.
4. Zlokalizowanych przedmiotów, rzeczy, urządzeń, których – w ocenie użytkowników obiektu – przedtem nie było, a zachodzi podejrzenie, iż mogą to być ładunki wybuchowe, nie wolno dotykać. O ich umiejscowieniu należy natychmiast powiadomić administratora obiektu i policję .
5. W przypadku, gdy użytkownicy pomieszczeń faktycznie stwierdzą obecność przedmiotów (rzeczy, urządzeń), których wcześniej nie było lub zmiany w wyglądzie i usytuowaniu przedmiotów stale znajdujących się w tych pomieszczeniach, należy domniemywać, że pojawienie się tych przedmiotów lub

zmiany w ich wyglądzie i usytuowaniu mogły nastąpić na skutek działania sprawcy podłożenia ładunku wybuchowego. W takiej sytuacji kierujący akcją może wydać decyzję ewakuacji osób z zagrożonego obiektu przed przybyciem policji.

6. Należy zachować spokój i opanowanie, aby nie dopuścić do przejawów paniki.

III. WSPÓŁPRACA Z POLICJĄ W CZASIE AKCJI

1. Po przybyciu do obiektu policjanta lub policyjnej grupy interwencyjnej administrator obiektu powinien przekazać im wszelkie informacje dotyczące zdarzenia oraz wskazać miejsca zlokalizowanych przedmiotów, rzeczy, urządzeń obcego pochodzenia i punkty newralgiczne w obiekcie.
2. Policjant lub dowódca grupy policjantów przejmuje kierowanie akcją, a administrator obiektu winien udzielić mu wszechstronnej pomocy podczas jej prowadzenia.
3. Na wniosek policjanta kierującego akcją, administrator obiektu podejmuje decyzje 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 administratorowi.

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

1. Osobom przyjmującym zgłoszenie o podłożeniu ładunku wybuchowego oraz administratorowi obiektu nie wolno lekceważyć żadnej informacji na ten temat i każdorazowo powinni powiadamiać o tym policję, która z urzędu dokona sprawdzenia wiarygodności każdego zgłoszenia.
2. Administrator obiektu powinien na bieżąco organizować szkolenie pracowników w zakresie sposobu zachowania w sytuacjach wymienionej w tej części planu oraz winien znać rozmieszczenie newralgicznych punktów - węzły energetyczne i wodne, które udostępnia się na żądanie policjanta kierującego akcją.
3. Z informacjami tej części planu powinni być zapoznani wszyscy pracownicy urzędu.

ZAŁĄCZNIK NR 7 - Instrukcja postępowania w przypadku otrzymania przesyłki niewiadomego pochodzenia.

1. W przypadku otrzymania jakiejkolwiek przesyłki niewiadomego pochodzenia lub budzącej podejrzenia z następujących powodów:

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

wtedy: **Nie należy otwierać tej przesyłki!**

Należy natomiast:

- umieścić tę przesyłkę w grubym worku plastikowym, szczelnie zamknąć,
- worek ten należy umieścić w drugim plastikowym worku, szczelnie należy zamknąć, zawiązać supeł i zakleić taśmą klejącą,
- paczki nie należy przemieszczać, należy pozostawić ją na miejscu,
- powiadomić odpowiednie służby:

Policję – nr 997; tel.kom.112 lub straż pożarną- nr 998.

Służby te podejmą wszystkie niezbędne kroki w celu bezpiecznego przejęcia przesyłki.

2. W przypadku , gdy podejrzana przesyłka została otwarta i zawiera jakakolwiek podejrzaną zawartość w formie stałej (galaretę, pianę, pył lub inną) należy:

- nie naruszać tej zawartości, tzn. nie rozsypywać, nie przenosić, nie dotykać, nie wąchać nie powodować ruchu powietrza w pomieszczeniu (wyłączyć systemy wentylacji i klimatyzacji, zamknąć okna),
- całą zawartość umieścić w worku plastikowym, zamknąć go i zakleić taśmą lub plastrem,
- dokładnie umyć ręce,
- zaklejony worek umieścić w drugim worku, zamknąć go i zakleić,
- ponownie umyć ręce,
- powiadomić odpowiednie służby:

Policję –nr 997; tel.kom.112 lub straż pożarną- nr 998.

PO PRZYBYCIU WŁAŚCIWYCH SŁUŻB NALEŻY BEZWZGLĘDNIE STOSOWAĆ SIĘ DO ICH ZALECEŃ!