125

ZARZĄDZENIE Nr 18/ 2019

Wójta Gminy Miedzichowo

z dnia 29.07.2019r.

W sprawie: zatwierdzenia Planu -Instrukcji sposobu i trybu przetwarzania informacji niejawnych o klauzuli „ZASTRZEŻONE" w Urzędzie Gminy Miedzichowo.

Na podstawie: Art. 43 ust. 5 ustawy z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych (tekst jednolity – Dz.U z 2019 Nr 742) zarządzam co następuje:

§1. Zatwierdzam do realizacji Plan-Instrukcję sposobu i trybu przetwarzania informacji niejawnych o klauzuli „ZASTRZEŻONE" w Urzędzie Gminy Miedzichowo w treści stanowiącej załącznik do niniejszego zarządzenia.

§ 2. Traci moc dotychczasowy Plan Ochrony Informacji Niejawnych w Urzędzie Gminy Miedzichowo zatwierdzony Zarządzeniem nr 4/2009 Wójta Gminy Miedzichowo z dnia 21 stycznia 2009 roku.

§ 3. Zarządzenie wchodzi w życie z dniem podjęcia.

WÓJT GMINY
MIEDZICHOWO
64-361 Miedzichowo
Ul. Poznańska 12

WÓJT
dr Stanisław Piechota

Sporządziła: Karolina Łotecka

Zatwierdzam

WÓJT
dr Stanisław Piechota

.....

/Kierownik Jednostki/

PLAN-INSTRUKCJA SPOSOBU I TRYBU PRZETWARZANIA INFORMACJI NIEJAWNYCH O KLAUZULI

„ZASTRZEŻONE"

W *URZĘDZIE GMINY MIEDZICHOWO*

OPRACOWAŁ:

Pełnomocnik ds. Ochrony Informacji Niejawnych
Karolina Łotocka

Pełnomocnik ds. Ochrony Informacji Niejawnych

Spis treści:

XVII. Kopie, odpisy, wypisy, wyciągi lub tłumaczenia.

XVIII. Zasady dostępu do informacji niejawnych.

XIX. Nadzór w zakresie ochrony informacji niejawnych.

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

XXI. Archiwizowanie, gromadzenie i niszczenie materiałów niejawnych.

XXII. Przechowywanie kluczy i pieczęci.

- **ZAŁĄCZNIKI DO INSTRUKCJI**

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.

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 w sprawie wzorów poświadczeń bezpieczeństwa,

- **DZIENNIK USTAW Nr 258 z 2010 r., poz. 1751**
Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 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.

I. DEFINICJE W ROZUMIENIU INSTRUKCJI

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.

1) **rękojmia zachowania tajemnicy** – jest zdolność osoby do spełnienia ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem , stwierdzona w wyniku przeprowadzenia postępowania sprawdzającego;

2) **dokumentem** - jest każda utrwalona informacja niejawna;

3) **materiałem** - jest dokument lub przedmiot jak też chroniony jako informacja niejawna przedmiot lub dowolna jego część.

4) **jednostką organizacyjną** - jest podmiot wymieniony w art. 1 ust. 2 ustawy o ochronie informacji niejawnych;

5) **systemem teleinformatycznym** - jest system, teleinformatyczny w rozumieniu art.2 pkt 3 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U.Nr 144,poz.1204,z późn.zm.);

6) **siecią teleinformatyczną** - jest organizacyjne i techniczne połączenie systemów teleinformatycznych;

7) **akredytacją bezpieczeństwa teleinformatycznego** - jest dopuszczenie systemu lub sieci teleinformatycznej do wytwarzania, przetwarzania, przechowywania lub przekazywania informacji niejawnych, na zasadach określonych w ustawie;

8) **dokumentacją bezpieczeństwa systemu lub sieci informatycznej** - są Szczególne Wymagania Bezpieczeństwa oraz Procedury Bezpiecznej Eksploatacji danego systemu lub sieci teleinformatycznej, sporządzone zgodnie z zasadami określonymi w ustawie.

9) **ryzykiem** – jest kombinacja prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji;

10) **szacowaniem ryzyka** – jest całościowy proces analizy i oceny ryzyka;

11) **zarządzaniem ryzyka** – są skoordynowane działania w zakresie zarządzania bezpieczeństwem informacji , z uwzględnieniem ryzyka,

12) **kancelaria materiałów niejawnych** – wydzielone, wyodrębnione pomieszczenie przeznaczone do ewidencjonowania, opracowywania przechowywania dokumentów niejawnych oznaczonych klauzulą „zastrzeżone"

13) **pracownik kancelarii materiałów niejawnych** – osoba wyznaczona przez kierownika jednostki do prowadzenia kancelarii materiałów niejawnych.

14) **informatyczny nośnik danych** – należy przez to rozumieć materiał służący do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej;

15) **dokument elektroniczny** – należy przez to rozumieć dokument przetwarzany w systemie teleinformatycznym podlegający rejestracji w odpowiedniej ewidencji przed przekazaniem go drogą elektroniczną;

16) **dokumencie nieelektroniczny** – należy przez to rozumieć dokument utrwalony na nośniku innym, niż informatyczny nośnik danych, podlegający rejestracji w odpowiedniej ewidencji;

17) **poczta elektroniczna** – należy przez to rozumieć środek komunikacji elektronicznej w rozumieniu art. 2 pkt. 5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. Nr 144, poz. 1204, z pożn. zm.1);

18) **metadane** – należy przez to rozumieć zestaw powiązanych z dokumentem elektronicznym usystematyzowanych danych przetwarzanych w systemie teleinformatycznym opisujących ten dokument, w szczególności ułatwiających kontrolę jego obiegu, wyszukiwanie lub przechowywanie;

19) **konwersja** – należy przez to rozumieć przekształcenie dokumentu nieelektronicznego w dokument elektroniczny dokonywane w szczególności poprzez jego zeskanowanie oraz odwzorowanie oznaczeń w metadanych;

20) **kopiowanie** – należy przez to rozumieć każdą formę powielania całości lub części dokumentu, w szczególności wykonywanie kopii, odpisu, wypisu, konwersji, wydruku, nagrania.

II. OCENA ZAGROŻEŃ ZEWNĘTRZNYCH I WEWNĘTRZNYCH

1.1. OCENA ZAGROŻEŃ ZEWNĘTRZNYCH

Zagrożeniami zewnętrznymi dla Urzędu Gminy Miedzichowo są:

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

1.2. 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 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)

1.3. WNIOSKI:

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

1/ systematyczną , skrupulatną i wnikliwą kontrolę systemu ochrony przez osoby odpowiedzialne za jego organizację,

2/ pracownicy pionu ochrony w czasie dnia pracy powinny zwracać szczególną uwagę na możliwość zaistnienia ewentualnych zagrożeń,

3/ stosować zasadę niedopuszczania osób niepowołanych do penetracji strefy bezpieczeństwa,

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

2.1. OCENA ZAGROŻEŃ WEWNĘTRZNYCH:

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

2.2. WNIOSKI

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

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

4. zastosowanie zasady, że do informacji niejawnych mogą mieć dostęp tylko pracownicy posiadający poświadczenie bezpieczeństwa lub właściwe upoważnienie wydane przez kierownika jednostki.
5. zwracanie szczególnej uwagi na osoby, których zachowanie wskazuję na spożycie alkoholu.

III. PRZEDMIOT OCHRONY

1. Informacje niejawne oznaczone klauzulą:

   - „zastrzeżone".
   - pomieszczenia , w których są przechowywane i opracowywane materiały niejawne o klauzuli „zastrzeżone".

IV. 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.

- **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 jako(***niski , średni, wysoki***) wobec klauzuli informacji niejawnych **„zastrzeżone",**
4. W celu określenia poziomu zagrożeń przeprowadzono analizę, w której uwzględniono wszystkie istotne czynniki mogące mieć wpływ na bezpieczeństwo informacji niejawnych, w szczególności:
   - klauzule tajności przetwarzanych informacji niejawnych;
   - postać i ilość informacji niejawnych;
   - sposób przechowywania informacji niejawnych;
   - otoczenie i strukturę budynków lub obszarów, w których przetwarzane są informacje niejawne;
   - ilość osób mających lub mogących mieć dostęp do informacji niejawnych, a także posiadane przez nich uprawnienia oraz uzasadnioną potrzebę dostępu

do informacji niejawnych;

- szacowane zagrożenie ze strony obcych służb specjalnych oraz zagrożenie sabotażem, zamachem terrorystycznym, kradzieżą lub inną działalnością przestępczą.

5. Zatwierdzenie 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.
6. Poziom zagrożeń określa się przed rozpoczęciem przetwarzania informacji niejawnych, a także po każdej zmianie czynników, mogącej mieć istotny wpływ na bezpieczeństwo informacji niejawnych.
7. W ramach systemu bezpieczeństwa fizycznego informacji niejawnych stosuje się środki bezpieczeństwa fizycznego w celu zapewnienia poufności, integralności i dostępności tych informacji.

8. Cel, o którym mowa osiąga się przez:

1) zapewnienie właściwego przetwarzania informacji niejawnych;
2) umożliwienie zróżnicowania dostępu do informacji niejawnych dla pracowników zgodnie z posiadanymi przez nich uprawnieniami oraz uzasadnioną potrzebą dostępu do informacji niejawnych;
3) wykrywanie, udaremnianie lub powstrzymywanie nieuprawnionych działań;
4) uniemożliwianie lub opóźnianie wtargnięcia osób nieuprawnionych w sposób niezauważony lub z użyciem siły do pomieszczenia lub obszaru, w którym przetwarzane są informacje niejawne.
2. 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.

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

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

2) **systemy sygnalizacji włamania i napadu** – stosowane w celu podwyższenia poziomu bezpieczeństwa, który dają bariery fizyczne, a w pomieszczeniach i budynkach w celu zastąpienia lub wsparcia pracowników jednostki organizacyjnej lub personelu bezpieczeństwa;

3) **kontrola dostępu** – stosowana w celu zagwarantowania, że dostęp do chronionego obszaru uzyskują wyłącznie osoby posiadające odpowiednie uprawnienia;

4) **personel bezpieczeństwa** – osoby przeszkolone, nadzorowane, a w razie konieczności posiadające odpowiednie uprawnienie dostępu do informacji niejawnych, zatrudnione w celu wykonywania czynności związanych z fizyczną ochroną informacji niejawnych, w tym kontroli dostępu, nadzoru nad systemem monitoringu wizyjnego, a także reagowania na alarmy lub sygnały awaryjne;

5) **szafy i zamki** – stosowane do przechowywania informacji niejawnych lub zabezpieczające te informacje przed nieuprawnionym dostępem;

7) **system kontroli osób i przedmiotów** polegający na użyciu odpowiednich urządzeń technicznych lub zwracaniu się o dobrowolne poddanie się kontroli lub udostępnienie do kontroli rzeczy osobistych, a także przedmiotów wnoszonych lub wynoszonych – stosowany w celu zapobiegania próbom nieuprawnionego wnoszenia na chroniony obszar rzeczy zagrażających bezpieczeństwu informacji niejawnych lub nieuprawnionego wynoszenia informacji niejawnych z budynków lub obiektów.

5. 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.

6. Jeżeli istnieje zagrożenie podglądu, także przypadkowego, informacji niejawnych, podejmuje się środki w celu wyeliminowania takiego zagrożenia zarówno w świetle dziennym, jak i w warunkach sztucznego oświetlenia.

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.

PROCES DOBORU ŚRODKOW 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 lokalizacji 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.

V. EWIDENCJA MATERIAŁÓW NIEJAWNYCH

1. Informacje niejawne oznaczone klauzulą „zastrzeżone" mogą być ewidencjonowane w wydzielonym ,wyodrębnionym pomieszczeniu spełniającym wymogi wynikające z przepisów ustawy o ochronie informacji niejawnych ,

2. Informacje niejawne o klauzuli „zastrzeżone" mogą być ewidencjonowane na zasadach określonych przez kierownika jednostki , opisanych w Instrukcji ,

3. Dokumenty niejawne wpływające do Urzędu ewidencjonuje się w dzienniku ewidencyjnym

4. Dokumenty niejawne wytworzone – wychodzące z Urzędu rejestruje się w dzienniku ewidencyjnym,

5. Każdy dokument niejawny przychodzący lub wychodzący z Urzędu ewidencjonuje się w odrębnej pozycji dziennika ewidencyjnego,

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

7. Ewidencjonowaniu podlegają wszystkie dokumenty niejawne oznaczone klauzulą „zastrzeżone"

8. Sposób właściwego opisania dokumentu niejawnego został przedstawiony w załączniku nr 2 do niniejszego Planu Ochrony Informacji Niejawnych (Instrukcji),

9. Prowadzi się również Rejestr Dzienników służący do ewidencjonowania książek i dzienników ewidencyjnych ,rejestrów.

10. Pracownik odpowiedzialny za ewidencjonowanie materiałów niejawnych przyjmuje przesyłki za pokwitowaniem i odciska na nich pieczęć oraz datę wpływu do jednostki organizacyjnej.
    Przyjmując przesyłkę, sprawdza się:

    1) prawidłowość adresu;
    2) całość opakowania;
    3) zgodność odcisku pieczęci na opakowaniu z nazwą jednostki organizacyjnej nadawcy;

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

12. Pracownik odpowiedzialny :
    1) sprawdza, czy zawartość przesyłki odpowiada wyszczególnionym na niej numerom ewidencyjnym;
    2) ustala, czy liczba załączników i stron jest zgodna z liczbą oznaczoną na poszczególnych dokumentach.

13. W przypadku stwierdzenia nieprawidłowości w wyniku czynności, o których mowa w pkt.12, pracownik sporządza w dwóch egzemplarzach protokół z otwarcia przesyłki zawierający opis nieprawidłowości, jeden egzemplarz przekazując do kancelarii nadawcy.

14. Pracownik odnotowuje fakt sporządzenia protokołu, o którym mowa w pkt. 11 i 13, w odpowiednim dzienniku lub rejestrze w rubryce "Informacje uzupełniające/Uwagi".

VI. ZABEZPIECZENIE INFORMACJI NIEJAWNYCH O KLAUZULI "ZASTRZEŻONE"

1. Informacje niejawne oznaczone klauzulą „zastrzeżone" można przechowywać w pomieszczeniu kancelarii materiałów niejawnych lub na stanowiskach pracy, w meblach biurowych zamykanych na klucz.
2. 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.

3.Funkcje i cechy zamków typu 1, 2, 3 lub 4 zostały określone w załączniku do Rozporządzenia Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych.

VII. DOSTĘP DO INFORMACJI NIEJAWNYCH OZNACZONYCH KLAUZULĄ „ZASTRZEŻONE''

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

2. Uzyskanie uprawnień dostępu do informacji niejawnych o klauzuli „zastrzeżone" może nastąpić:
   - po uzyskaniu przez pracownika upoważnienia dostępu do informacji niejawnych oznaczonych klauzulą „zastrzeżone" wydanego przez kierownika jednostki,
   - po przeszkoleniu danej osoby w zakresie przepisów ustawy o ochronie informacji niejawnych i uzyskaniu odpowiedniego zaświadczenia.
4. 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 niniejszego Planu ochrony(Instrukcji).

VIII.STANOWISKO DO EWIDENCJONOWANIA MATERIAŁÓW NIEJAWNYCH O KLAUZULI „ZASTRZEŻONE"

1. W urzędzie funkcjonuje stanowisko , które zostało utworzone dla potrzeb jednostki , dla właściwego przechowywania , ewidencjonowania materiałów niejawnych oznaczonych klauzulą „zastrzeżone".

2. Organizacja stanowiska pracy zapewnia możliwość ustalenia w każdych okolicznościach, gdzie znajduje się materiał o klauzuli „zastrzeżone" pozostający w dyspozycji jednostki organizacyjnej oraz kto z tym materiałem się zapoznał.

3. Pracownik odmawia udostępnienia lub wydania materiału osobie nieuprawnionej.

4. W celu uniemożliwienia osobom nieuprawnionym dostępu do informacji niejawnych o klauzuli „zastrzeżone" należy w szczególności:
   1) zorganizować strefy ochronne;
   2) wprowadzić system kontroli wejść i wyjść ze stref ochronnych;
   3) określić uprawnienia do przebywania w strefach ochronnych;
   4) stosować wyposażenie i urządzenia służące ochronie informacji niejawnych, którym przyznano certyfikaty.

5. Wyznaczone stanowisko tworzy kierownik jednostki organizacyjnej na wniosek Pełnomocnika,.

6. Do podstawowych zadań wyznaczonego pracownika należy:

   1) bezpośredni nadzór nad obiegiem dokumentów niejawnych;

2) udostępnianie lub wydawanie dokumentów osobom do tego uprawnionym;

3) egzekwowanie zwrotu dokumentów;

4) kontrola przestrzegania właściwego oznaczania dokumentów niejawnych w jednostce organizacyjnej;

5) prowadzenie bieżącej kontroli postępowania z dokumentami;

6) wykonywanie poleceń pełnomocnika ochrony;

7. W przypadku zmiany na stanowisku, pracownik zdający sporządza protokół zdawczo-odbiorczy.

8. Protokół, o którym mowa w pkt. 7, sporządza się w obecności pracownika zdającego obowiązki, osoby przejmującej obowiązki oraz pełnomocnika ochrony. Protokół sporządza się w dwóch egzemplarzach; pierwszy egzemplarz przechowywany jest na stanowisku a drugi – u pełnomocnika ochrony. Wzór protokołu określa załącznik nr 4 do niniejszego Planu Ochrony (Instrukcji).

9. W przypadku czasowej nieobecności pracownika jego obowiązki przejmuje upoważniony pracownik pionu ochrony. W razie ich braku obowiązki przejmuje pełnomocnik ochrony lub inny pracownik wyznaczony pisemnie przez kierownika jednostki na wniosek pełnomocnika ochrony.

10. W pomieszczeniu można wydzielić miejsce, w którym osoby upoważnione mogą zapoznać się z dokumentami,.

1) wydzielone miejsce powinno być zorganizowana w sposób umożliwiający stały nadzór ze strony pracownika kancelarii .
2) w wydzielonym miejscu zabrania się instalowania systemu nadzoru wizyjnego.

11. Dokumenty i materiały oznaczone klauzulą 'zastrzeżone" oraz bez klauzuli tajności są przechowywane w oddzielnych teczkach , chyba że wchodzą one w skład zbioru dokumentów.

12. Po zakończeniu pracy wyznaczony pracownik jest obowiązany sprawdzić prawidłowość zamknięcia szaf i pomieszczenia.

13. Zasady i sposób zdawania, przechowywania i wydawania kluczy oraz ich duplikatów do pomieszczeń oraz szaf kancelarii, a także zasady ustalania, zmiany i deponowania haseł lub szyfrów, w przypadku stosowania zamków szyfrowych, określa Instrukcja,

14. Wszelkie nieprawidłowości związane z naruszeniem zasad, określonych powyżej należy niezwłocznie zgłaszać pełnomocnikowi ochrony.

15. Zasady określone obowiązują odpowiednio w stosunku do innych pomieszczeń, w których są przechowywane dokumenty lub materiały, oraz osób za te pomieszczenia odpowiedzialnych.

16. Na wydzielonym stanowisku przyjmuje się, rejestruje, przechowuje, przekazuje i wysyła dokumenty oraz prowadzi:

    1) rejestr dzienników, książek ewidencyjnych i teczek,
    2) dziennik ewidencji,
    3) książkę doręczeń przesyłek miejscowych,

W przypadkach uzasadnionych organizacją ochrony informacji niejawnych pracownik może prowadzić także inne rejestry niż wymienione wyżej wymienione

IX. POSTĘPOWANIE Z PRZESYŁKAMI

1. Pracownik przyjmuje przesyłki lub dokumenty za pokwitowaniem i odciska na nich pieczęć oraz datę wpływu do jednostki organizacyjnej.

2. Przyjmując przesyłkę, sprawdza się:

    1) prawidłowość adresu;

    2) całość pieczęci i opakowania;

    3) zgodność odcisku pieczęci na opakowaniu z nazwą jednostki nadawcy;

    4) zgodność numeru na przesyłce z numerem tej przesyłki w wykazie, książce doręczeń a także na zwrotnym potwierdzeniu odbioru.

3. W przypadku stwierdzenia uszkodzenia przesyłki lub śladów jej otwierania pracownik kwitujący odbiór przesyłki sporządza, wraz z doręczającym, protokół uszkodzenia. Jeden egzemplarz protokołu przekazuje się nadawcy, drugi pełnomocnikowi ochrony w jednostce organizacyjnej odbiorcy, a w przypadku gdy w obiegu przesyłek pośredniczył przewoźnik – kolejny egzemplarz protokołu przekazuje się także jemu.

4. Po otwarciu przesyłki pracownik :
   1) sprawdza, czy zawartość przesyłki odpowiada wyszczególnionym na niej numerom ewidencyjnym;

   2) ustala, czy liczba załączników i stron jest zgodna z liczbą oznaczoną na poszczególnych dokumentach

5. W przypadku stwierdzenia nieprawidłowości pracownik sporządza w dwóch egzemplarzach protokół z otwarcia przesyłki zawierający opis nieprawidłowości, jeden egzemplarz przekazując do kancelarii nadawcy,

6. Pracownik odnotowuje fakt sporządzenia protokołu, w odpowiednim dzienniku lub rejestrze w rubryce „Informacje uzupełniające/Uwagi".

7. Pracownik nie otwiera przesyłek oznaczonych „do rąk własnych". W odpowiednim dzienniku lub rejestrze wpisuje s nadawcę, numer i datę wpływu dokumentu; w rubryce „Informacje uzupełniające/Uwagi" odnotowuje się, że przesyłka była oznaczona „do rąk własnych",

8. Na opakowaniu przesyłek, wpisuje się datę wpływu, pozycję i numer, pod którym zarejestrowano przesyłkę. Przesyłkę przekazuje się – za pokwitowaniem – bezpośrednio adresatowi, a w razie jego nieobecności – osobie przez niego upoważnionej do odbioru,

9. Zatrzymanie przez adresata dokumentu, adresowanego „do rąk własnych", odnotowuje się w rubryce „Informacje uzupełniające/Uwagi".

10. W przypadku zwrotu do pracownika przesyłki adresowanej „do rąk własnych", pracownik uzupełnia dane dotyczące przesyłki w odpowiednim dzienniku lub rejestrze.

11. Jeżeli adresat podjął decyzję o przechowywaniu przesyłki „do rąk własnych" w w stanie zamkniętym, pracownik dokonuje czynności, o których mowa w pkt. 10, przy udziale adresata. Przesyłka jest w takim przypadku przechowywana w formie zapieczętowanego pakietu, a fakt ten odnotowuje się w rubryce „Informacje uzupełniające/Uwagi".

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

13. Otrzymaną i wysyłaną przesyłkę bądź wytworzony dokument rejestruje się odpowiednio w kolejności wytworzenia lub otrzymania.

14. Wszelkich adnotacji, w dziennikach ewidencyjnych , dokonuje się tuszem w kolorze niebieskim lub czarnym . Zmian dokonuje się kolorem czerwonym, umieszczając datę , imię i nazwisko oraz podpis dokonującej zmiany.

15. Zabrania się wycierania , zamazywania lub nadpisywania zapisów dokonanych w dziennikach ewidencyjnych .

X. OBOWIĄZKI PRACOWNIKA

1. Przed otwarciem drzwi sprawdzić stan zamków i zabezpieczenie drzwi pomieszczenia,

2. Sprawdzić stan zabezpieczeń szaf, sprzętu biurowego,

3. Przestrzegać zasad zakazu wstępu w miejsca wydzielone osobom nieuprawnionym,

XI . ZAKRES 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 Instrukcji

XII. ZASADY WYKONYWANIA DOKUMENTÓW NIEJAWNYCH

1. Klauzulę tajności nadaje osoba. Która jest uprawniona do oznaczenia innego niż dokument materiału,

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

3. Klauzulę niejawności na danym dokumencie przyznaje osoba która jest upoważniona do odpisania dokumentu,

4. Rękopisy sporządzanych dokumentów niejawnych powinny być opracowywane w brulionach (zeszytach pracy) uprzednio zarejestrowanych w odpowiednim dzienniku,

5. 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 Instrukcji.

XIII. WYKONYWANIE DOKUMENTÓW NIEJAWNYCH Z WYKORZYSTANIEM SPRZĘTU KOMPUTEROWEGO

1. Bezpieczeństwo teleinformatyczne zapewnia się, chroniąc informacje przetwarzane w systemach i sieciach teleinformatycznych przed utratą właściwości gwarantujących to bezpieczeństwo, w szczególności przed utratą poufności, dostępności i integralności.
2. Bezpieczeństwo teleinformatyczne zapewnia się przed rozpoczęciem oraz w trakcie przetwarzania informacji niejawnych w systemie lub sieci teleinformatycznej.
3. Za właściwą organizację bezpieczeństwa teleinformatycznego odpowiada kierownik jednostki organizacyjnej, który w szczególności:
   1) zapewnia opracowanie dokumentacji bezpieczeństwa teleinformatycznego;
   2) realizuje ochronę fizyczną, elektromagnetyczną systemu lub sieci.
   3) zapewnia niezawodność transmisji oraz kontrolę dostępu do urządzeń systemu lub sieci teleinformatycznej;
   4) dokonuje analizy stanu bezpieczeństwa teleinformatycznego oraz zapewnia usunięcie stwierdzonych nieprawidłowości;
   5) zapewnia przeszkolenie z zakresu bezpieczeństwa teleinformatycznego dla osób uprawnionych do pracy w systemie lub sieci teleinformatycznej;
4. Ochrona fizyczna systemu lub sieci teleinformatycznej polega na:

   1) umieszczeniu urządzeń systemu lub sieci teleinformatycznej w strefie ochronnej, zwanej również „strefą kontrolowanego dostępu" w zależności od ilości, zagrożeń dla poufności, integralności lub dostępności informacji niejawnych;
   2) zastosowaniu środków zapewniających ochronę fizyczną, w szczególności przed:

      a) nieuprawnionym dostępem,
      b) podglądem,
      c) podsłuchem.

5. Ochrona elektromagnetyczna systemu lub sieci teleinformatycznej polega na niedopuszczeniu do utraty poufności i dostępności informacji niejawnych przetwarzanych w urządzeniach teleinformatycznych.

   1) utrata poufności następuje w szczególności na skutek wykorzystania elektromagnetycznej emisji ujawniającej pochodzącej z tych urządzeń.

2) utrata dostępności następuje w szczególności na skutek zakłócania pracy urządzeń teleinformatycznych za pomocą impulsów elektromagnetycznych o dużej mocy.

6. Ochronę elektromagnetyczną systemu lub sieci teleinformatycznej zapewnia się w szczególności przez umieszczenie urządzeń teleinformatycznych, połączeń i linii w strefach kontrolowanego dostępu odpowiednio do wyników szacowania ryzyka dla informacji niejawnych.

7. W celu zapewnienia kontroli dostępu do systemu lub sieci teleinformatycznej

1) kierownik jednostki organizacyjnej lub osoba przez niego upoważniona ustala warunki i sposób przydzielania uprawnień osobom uprawnionym do pracy w systemie lub sieci teleinformatycznej;

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

8.System lub sieć teleinformatyczną wyposaża się w mechanizmy kontroli dostępu odpowiednie do klauzuli tajności informacji niejawnych w nich przetwarzanych.

9. Kierownik jednostki organizacyjnej udziela akredytacji bezpieczeństwa teleinformatycznego dla systemu teleinformatycznego przeznaczonego do przetwarzania informacji niejawnych o klauzuli „zastrzeżone" przez zatwierdzenie dokumentacji bezpieczeństwa systemu teleinformatycznego.

10. W ciągu 30 dni od udzielenia akredytacji bezpieczeństwa teleinformatycznego, o której mowa w pkt. 17, kierownik jednostki organizacyjnej przekazuje ABW dokumentację bezpieczeństwa systemu teleinformatycznego.

11. W ciągu 30 dni od otrzymania dokumentacji bezpieczeństwa systemu teleinformatycznego ABW może przedstawić kierownikowi jednostki organizacyjnej, który udzielił akredytacji bezpieczeństwa teleinformatycznego, zalecenia dotyczące konieczności przeprowadzenia dodatkowych czynności związanych z bezpieczeństwem informacji niejawnych. Kierownik jednostki organizacyjnej w terminie 30 dni od otrzymania zalecenia informuje ABW o realizacji zaleceń. W szczególnie uzasadnionych przypadkach ABW może nakazać wstrzymanie przetwarzania informacji niejawnych w systemie teleinformatycznym posiadającym akredytację bezpieczeństwa teleinformatycznego.

12. Dokument szczególnych wymagań bezpieczeństwa systemu teleinformatycznego powinien zawierać w szczególności wyniki procesu szacowania ryzyka dla bezpieczeństwa informacji niejawnych przetwarzanych w systemie teleinformatycznym oraz określać przyjęte w ramach zarządzania ryzykiem sposoby osiągania i utrzymywania odpowiedniego poziomu bezpieczeństwa systemu, a także opisywać aspekty jego budowy, zasady działania i eksploatacji, które mają związek z bezpieczeństwem systemu lub wpływają na jego bezpieczeństwo. Przebieg i wyniki procesu szacowania ryzyka mogą zostać przedstawione w odrębnym dokumencie niż dokument szczególnych wymagań bezpieczeństwa.

13. Dokument szczególnych wymagań bezpieczeństwa opracowuje się na etapie projektowania, w razie potrzeby konsultuje z ABW , bieżąco uzupełnia na etapie wdrażania i modyfikuje na etapie eksploatacji przed dokonaniem zmian w systemie teleinformatycznym.
14. Dokument procedur bezpiecznej eksploatacji opracowuje się na etapie wdrażania oraz modyfikuje na etapie eksploatacji przed dokonaniem zmian w systemie teleinformatycznym.
15. Podstawą dokonywania wszelkich zmian w systemie teleinformatycznym jest przeprowadzenie procesu szacowania ryzyka dla bezpieczeństwa informacji niejawnych przetwarzanych w tym systemie.
16. Kierownik jednostki organizacyjnej akceptuje wyniki procesu szacowania ryzyka dla bezpieczeństwa informacji niejawnych oraz jest odpowiedzialny za właściwą organizację bezpieczeństwa teleinformatycznego.
17. Bez konieczności przeprowadzania badań i oceny Szef ABW może dopuścić do stosowania w systemie teleinformatycznym przeznaczonym do przetwarzania informacji niejawnych o klauzuli „zastrzeżone" urządzenia lub narzędzia kryptograficzne, jeżeli otrzymały stosowny certyfikat wydany przez krajową władzę bezpieczeństwa państwa będącego członkiem NATO lub Unii Europejskiej lub inny uprawniony organ w NATO lub w Unii Europejskiej.

18. Kierownik jednostki organizacyjnej wyznacza:
    1) pracownika pionu ochrony pełniącego funkcję **INSPEKTORA BEZPIECZEŃSTWA TELEINFORMATYCZNEGO**, odpowiedzialnych za weryfikację i bieżącą kontrolę zgodności funkcjonowania systemu teleinformatycznego ze szczególnymi wymaganiami bezpieczeństwa oraz przestrzegania procedur bezpiecznej eksploatacji;

2) osobę lub zespół osób, niepełniących funkcji inspektora bezpieczeństwa teleinformatycznego, odpowiedzialnych za funkcjonowanie systemu teleinformatycznego oraz za przestrzeganie zasad i wymagań bezpieczeństwa przewidzianych dla systemu teleinformatycznego, zwanych **„ADMINISTRATOREM SYSTEMU".**

19. W sytuacjach wymagających konsultacji lub uzgodnień kierownik jednostki może zwrócić się do Agencji Bezpieczeństwa Wewnętrznego o wydanie opinii lub zaleceń w zakresie bezpieczeństwa teleinformatycznego .
20. Stanowiska lub funkcje administratora systemu oraz inspektora bezpieczeństwa teleinformatycznego mogą zajmować lub pełnić osoby, posiadające poświadczenia bezpieczeństwa lub upoważnienie odpowiednie do klauzuli informacji wytwarzanych, przetwarzanych, przechowywanych lub przekazywanych w systemach lub sieciach teleinformatycznych, po odbyciu specjalistycznych szkoleń z zakresu bezpieczeństwa teleinformatycznego prowadzonych przez służby ochrony państwa.
21. Zaświadczenie o odbytym szkoleniu jest przechowywane w aktach osobowych oraz dokumentacji Pełnomocnika ds. ochrony informacji niejawnych.

KOPIE ZAPASOWE:

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

XIV. GROMADZENIE DOKUMENTÓW ZAWIERAJACYCH INFORMACJE NIEJAWNE

1. Dokumenty zawierające informacje niejawne o klauzuli „zastrzeżone" 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" są przechowywane w wydzielonym pomieszczeniu lub na stanowiskach pracy w meblach biurowych zamykanych na klucz,

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

8. Wprowadza się następujące oznaczenia klauzul tajności:

   „Z" – dla klauzuli „zastrzeżone".

9. 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 Instrukcji .
10. W przypadku pisma, któremu nadano bieg korespondencyjny, na pierwszej stronie w prawym górnym rogu pod numerem egzemplarza można zamieścić dyspozycję dla adresata o treści:
    1) „udzielanie informacji tylko za pisemną zgodą nadawcy";
    2) „kopiowanie tylko za pisemną zgodą nadawcy";
    3) „odpis tylko za pisemną zgodą nadawcy";
    4) „kopiowanie stron od ... do ... tylko za pisemną zgodą nadawcy";
    5) „odpis od ... do ... tylko za pisemną zgodą nadawcy";
    6) „wypis (wyciąg) od ... do ... tylko za pisemną zgodą nadawcy".

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

12. **Dokumenty elektroniczne** przetwarzane wyłącznie w systemie teleinformatycznym,, podlegające ewidencji w elektronicznym rejestrze dokumentów, oznacza się w sposób określony w Rozporządzeniu Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności, (Dz.U. z 2011r. nr 288 poz. 1692),

13. W przypadku dokumentów elektronicznych, o których mowa w pkt. 13, na każdej stronie w prawym górnym rogu pod klauzulą tajności zamiast oznaczenia numeru egzemplarza umieszcza się napis „Egz. elektroniczny".

14. **Materiały w postaci prezentacji multimedialnych oznacza się w następujący sposób:**

    1) na każdym slajdzie lub stronie stanowiącej integralną część prezentacji multimedialnej umieszcza się:

    a) w prawym górnym rogu klauzulę tajności,
    b) w prawym dolnym rogu klauzulę tajności, numer slajdu lub strony łamany przez liczbę slajdów lub stron;

    2) na pierwszym slajdzie lub stronie stanowiącej integralną część prezentacji multimedialnej umieszcza się dodatkowo:

    a) w lewym górnym rogu nazwę jednostki lub komórki organizacyjnej oraz sygnaturę

literowo-cyfrową,
b) napis o treści: „podlega ochronie do ...",

15. Na pismach stanowiących załączniki,

1) Na pierwszej stronie w prawym górnym rogu, umieszcza się dodatkowo napis: „Załącznik nr ... do pisma nr ... z dnia ...".
2) Napis, o którym mowa w ust. 1, zamieszcza się, w miarę możliwości, na innych niż pismo materiałach.
3) Jeżeli przy piśmie przewodnim przesyła się załączniki oznaczone klauzulami tajności, to:

a) klauzula pisma przewodniego lub dokumentu nie może być niższa niż klauzula załącznika o najwyższym stopniu tajności;

16. Na piśmie przewodnim, jeżeli jego klauzula jest inna po odłączeniu załączników,

1) Zamieszcza się dyspozycję co do klauzuli tajności pisma po trwałym ich odłączeniu; na każdej stronie pod numerem egzemplarza zamieszcza się napis: „..... (nazwa klauzuli tajności) po odłączeniu załączników" lub „Jawne po odłączeniu załączników".
2) Przy rejestracji pisma przewodniego, o którym mowa w pkt.1, we właściwej ewidencji, w rubryce „Informacje uzupełniające/Uwagi" wpisuje się adnotację o treści „... (nazwa klauzuli tajności) po odłączeniu załączników" lub „Jawne po odłączeniu załączników".

17.Na materiałach innych niż pismo,

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

18.Utrwalanie informacji niejawnych w formie dźwięku, obrazu lub poczty elektronicznej, powinno być poprzedzone i kończyć się informacją o nadanej klauzuli tajności, jeżeli istnieją takie możliwości techniczne.

19. Na trwale oprawionych zbiorach dokumentów, rejestrach, książkach, broszurach i reprodukcjach,

1) klauzule tajności umieszcza się po prawej stronie na górze i dole zewnętrznych ścianek okładki oraz, jeżeli jest, na stronie tytułowej.

XVI. OKRESY OCHRONNE

1. Na pismach zawierających informacje niejawne, wobec których minął okres ochrony ustanowiony przez osobę uprawnioną do nadania klauzuli :

1) skreśla się klauzulę tajności na każdej stronie w prawym górnym i dolnym rogu;
2) na pierwszej stronie nad skreśloną klauzulą tajności w prawym górnym rogu umieszcza się dodatkowo napis „zniesienie klauzuli tajności " oraz datę, imię, nazwisko i podpis osoby dokonującej tych adnotacji.

2. 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.

3. 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.

4. Skreśleń i adnotacji, dokonuje wyznaczony pracownik lub inne upoważnione osoby.

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

6.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.

XVII. KOPIE, ODPISY, WYPISY, WYCIĄGI LUB TŁUMACZENIA

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

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

2) **na pierwszej stronie dodatkowo** numer, pod jakim zostały zarejestrowane w dzienniku ewidencyjnym , numer egzemplarza wykonanej kopii, odpisu, wypisu, wyciągu lub tłumaczenia;
3) **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:

1) nazwie jednostki lub komórki organizacyjnej, w której sporządzono kopię, odpis, wypis, wyciąg lub tłumaczenie;
2) liczbie egzemplarzy sporządzonych kopii, odpisów, wypisów, wyciągów lub tłumaczeń;
3) dacie sporządzenia kopii, odpisu, wypisu, wyciągu lub tłumaczenia;
4) 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.

XVIII. ZASADY DOSTĘPU DO INFORMACJI NIEJAWNYCH

1. Postępowanie sprawdzające wobec kierownika jednostki , w przypadku potrzeby uzyskania uprawnień dostępu do informacji niejawnych oznaczonych klauzulą „poufne" przeprowadza Agencja Bezpieczeństwa Wewnętrznego,

2. Uzyskanie uprawnień do dostępu do informacji niejawnych o klauzuli „zastrzeżone" może nastąpić:
   1) po uzyskaniu przez daną osobę upoważnienia nadanego przez kierownika jednostki ,
   2) po przeszkoleniu danej osoby w zakresie przepisów o ochronie informacji niejawnych i uzyskaniu właściwego zaświadczenia o przeszkoleniu, szkolenie dla pracowników urzędu organizuje Pełnomocnik ochrony,

3) Szkolenie i w związku z przewidywanym dostępem do informacji niejawnych oznaczonych klauzulą „zastrzeżone" organizuje pełnomocnik ochrony wydając stosowne zaświadczenie,
4) Szkolenie odbywa się nie rzadziej niż raz na 5 lat

XIX. 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 przepisów zawartych w niniejszej Instrukcji,
   2) sprawowanie nadzoru w zakresie ochrony informacji niejawnych oraz przestrzegania procedur związanych z upoważnianiem do dostępu do tych informacji.

XX. ODPOWIEDZIALNOŚĆ KARNA , DYSCYPLINARNA I SŁUŻBOWA ZA NARUSZENIE PRZEPISÓW O OCHRONIE INFORMACJI NIEJAWNYCH

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

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

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

2. Wobec pracowników, którzy nie przestrzegają wymagań związanych z ochroną informacji niejawnych, dopuszczają się uchybień w zakresie niewłaściwego

zabezpieczania dokumentów, stwarzając warunki do ujawnienia tajemnicy osobom nieuprawnionym, mogą być zastosowane sankcje służbowe i dyscyplinarne.

XXI. 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),

3. Dokumentacja wytwarzana i gromadzona dzieli się na :

   1) materiały archiwalne - wchodzące do państwowego zasobu archiwalnego;
   2) dokumentację niearchiwalną - inną dokumentację, niestanowiącą materiałów archiwalnych.

4. Rzeczową klasyfikację oraz kwalifikację dokumentacji ze względu na okresy jej przechowywania, wytwarzanej i gromadzonej zawierają jednolite rzeczowe wykazy akt,

5. Wykazy akt o których mowa stanowią podstawę gromadzenia dokumentacji w aktach spraw.

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

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

8. Brakowanie dokumentacji niearchiwalnej następuje na podstawie zgody wydanej przez właściwe archiwum .

9. Zgodę, o której mowa wyraża dyrektor miejscowo właściwego archiwum państwowego lub wojskowego.

10. Wniosek o wyrażenie zgody na brakowanie dokumentacji niearchiwalnej należy złożyć dyrektorowi miejscowo właściwego archiwum państwowego lub wojskowego.

11. Do wniosku o zgodę jednorazową dołącza się:

    1) protokół oceny dokumentacji nicarchiwalnej,
    2) spis dokumentacji niearchiwalnej przeznaczonej do przekazania na makulaturę lub zniszczenie, albo spis dokumentacji technicznej niearchiwalnej przeznaczonej na makulaturę lub zniszczenie,

12. Protokół oraz spis dokumentacji niearchiwalnej, sporządza komisja powołana przez kierownika jednostki , w której skład wchodzą: osoba kierująca lub prowadząca archiwum zakładowe albo składnicę akt oraz przedstawiciele komórek organizacyjnych, których dokumentacja niearchiwalna podlega brakowaniu oraz pracownik kancelarii niejawnej,

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

14. Urząd przechowuje w archiwum zakładowym dokumenty brakowania, o których mowa wraz z dowodami przekazania nieprzydatnej dokumentacji niearchiwalnej na makulaturę bądź protokółami jej zniszczenia.

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

16. Materiały archiwalne powinny być ułożone wewnątrz teczek w kolejności spraw, a w ramach sprawy - chronologicznie, poczynając od pierwszego pisma wszczynającego sprawę. Poszczególne strony akt znajdujących się w teczce powinny być opatrzone kolejną numeracją.

17. Opisanie materiałów archiwalnych polega na umieszczeniu na wierzchniej stronie każdej teczki:

    1) nazwy jednostki organizacyjnej i komórki organizacyjnej, w której materiały powstały;
    2) znaku akt, to jest symbolu literowego komórki organizacyjnej oraz symbolu klasyfikacyjnego według wykazu akt, obowiązującego w jednostce organizacyjnej;
    3) tytułu teczki, to jest nazwy hasła klasyfikacyjnego według wykazu akt, obowiązującego w danej jednostce organizacyjnej, i informacji o rodzaju materiałów archiwalnych, znajdujących się w teczce;
    4) rocznych dat krańcowych, to jest dat najwcześniejszego i najpóźniejszego materiału archiwalnego w teczce;

5) sygnatury teczki, to jest numeru spisu zdawczo-odbiorczego i numeru pozycji teczki w spisie zdawczo-odbiorczym;
6) symbolu kwalifikacyjnego materiałów archiwalnych (kategoria A);
7) liczby stron w teczce.

18. Czynności związane z brakowaniem materiałów niearchiwalnych, wobec których archiwum państwowe wyraziło zgodę jest dokumentowany przez sporządzenie protokołu komisyjnego zniszczenia dokumentów niearchiwalnych.

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

XXII. PRZECHOWYWANIE KLUCZY I PIECZĘCI

1. Ustala się zasady gospodarki kluczami i pieczęciami :

1) Szafy , w których przechowywane są informacje niejawne o klauzuli „zastrzeżone" po zamknięciu mogą być dodatkowo plombowane pieczęcią do plasteliny,

2) Klucze od oraz pieczęcie, po zakończeniu pracy należy złożyć w miejscu niewidocznym.

3) Po zakończeniu pracy , pracownik zamyka i ewentualnie plombuje pieczęcią do plasteliny drzwi wejściowe do pomieszczenia,

4) Klucz od drzwi wejściowych należy umieścić w pojemniku lub woreczku , dodatkowo zabezpieczając pieczęcią do plasteliny, następnie tak przygotowany pojemnik lub woreczek należy umieścić w miejscu niewidocznym w wyznaczonym pomieszczeniu.

5) Pieczęć do plasteliny pracownik powinien zabezpieczać tak, by osoby nieuprawnione nie mogły z niej korzystać,

6) Tworzy się zapasowy komplet kluczy od pomieszczenia w którym są przechowywane materiały niejawne o klauzuli „zastrzeżone",,

7) Zapasowy komplet kłuczy należy umieścić w zamykanym pojemniku lub woreczku na klucze, który dodatkowo powinien być zabezpieczony pieczęcią do plasteliny.

8) Tak przygotowany komplet kluczy zapasowych należy złożyć do zdeponowania w szafie metalowej w jednym z pomieszczeń Urzędu.

9) Pracownik po przybyciu do urzędu , przed otwarciem pomieszczenia powinien sprawdzić , czy nie zostały naruszone pieczęcie zabezpieczające klucze oraz zabezpieczające drzwi wejściowe do pomieszczenia. W dalszej kolejności sprawdza czy nie zostały naruszone pieczęcie na szafach znajdujących się w pomieszczeniu – jeżeli szafy były dodatkowo w ten sposób zabezpieczone, .

ZAŁĄCZNIKI

DO INSTRUKCJI

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 Nr1 – szacowanie ryzyka i poziomu zagrożeń związany z dostępem osób nieuprawnionych do informacji niejawnych o klauzuli „zastrzeżone" lub ich utratą

OCENA ISTOTNOŚCI

CZYNNIKÓW ZAGROŻEŃ

mających lub mogących mieć wpływ na

bezpieczeństwo informacji niejawnych

w Urzędzie Gminy Miedzichowo

opracowano zgodnie z rozporządzeniem
Rady Ministrów z dnia 29 maja 2012r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych.
(Dz.U.115,poz.683, z dnia 19 czerwca 2012r.)

Opracował:

Pełnomocnik ds. Ochrony Informacji Niejawnych

.....

Karolina Łotecka

Pełnomocnik Ochrony
Informacji niejawnych

3

KLAUZULA TAJNOŚCI PRZETWARZANYCH INFORMACJI NIEJAWNYCH w
Urzędzie Gminy Miedzichowo

* *zaznaczyć*

L.p.	KLAUZULA TAJNOŚCI	TAK *	NIE *
1.	ściśle tajne	-	X
2.	tajne	-	X
3.	poufne	-	X
4.	zastrzeżone	X	-

Uwaga:
analizie podlegają wszystkie klauzule tajności wszystkich przetwarzanych informacji niejawnych. Przy ocenie istotności czynnika stosuje się zasadę: im wyższe klauzule tajności przetwarzanych informacji , tym czynnik ma istotniejsze znaczenie. Dla informacji niejawnych o klauzuli „ściśle tajne" wartość oceny jest stała i wynosi 8 pkt. (czynnik ma „ bardzo istotne znaczenie").
W przypadku nowo organizowanej jednostki organizacyjnej należy przyjąć wartości szacunkowe.

L.p.	OCENA ISTOTNOŚCI CZYNNIKA	PRZYZNANO*
1.	Bardzo istotny (8pkt.)	
2.	Istotny (4 pkt.)	
3.	Mało istotny (1 pkt.)	1

* *wpisać odpowiednią ilość punktów.*

UZASADNIENIE:

W Urzędzie Gminy Miedzichowo przetwarzane są tylko dokumenty opatrzone klauzulą „Zastrzeżone"

4

LICZBA MATERIAŁÓW NIEJAWNYCH
w Urzędzie Gminy Miedzichowo

L.p.	KLAUZULA TAJNOŚCI	LICZBA MATERIAŁÓW NIEJAWNYCH
1.	ściśle tajne	0
2.	tajne	0
3.	poufne	0
4.	zastrzeżone	ok. 100

Uwaga:

Przy ocenie istotności czynnika należy brać pod uwagę wszystkie materiały niejawne zarejestrowane w urządzeniach ewidencyjnych , pozostające w faktycznej dyspozycji jednostki organizacyjnej. W uzasadnieniu należy odnieść się do przybliżonej ogólnej liczby wszystkich materiałów stosując zasadę: im więcej informacji niejawnych o najwyższych klauzulach tajności , tym czynnik ma istotniejsze znaczenie.

W przypadku nowo organizowanej jednostki organizacyjnej należy przyjąć wartości szacunkowe.

L.p.	OCENA ISTOTNOŚCI CZYNNIKA	PRZYZNANO*
1.	Bardzo istotny (8pkt.)	
2.	Istotny (4 pkt.)	
3.	Mało istotny (1 pkt.)	**1**

* *wpisać odpowiednią ilość punktów.*

UZASADNIENIE:

Wszystkie materiały niejawne przetwarzane w Urzędzie Gminy Miedzichowo opatrzone zostały klauzulą „Zastrzeżone" i są przechowywane przez Stanowisko do Ewidencjonowania Materiałów Niejawnych.

5

POSTAĆ INFORMACJI NIEJAWNYCH
w Urzędzie Gminy Miedzichowo

L.p.	POSTAĆ INFORMACJI NIEJAWNYCH	TAK*	NIE*
1.	Dokumenty nielektroniczne	X	-
2.	Dokumenty elektroniczne	X	-
3.	Inne: nagranie dźwiękowe, obrazem itp	-	X

*zaznaczyć

Uwaga:

Przy ocenie istotności czynnika należy brać pod uwagę ogólna liczbę przetwarzanych informacji niejawnych, stosując zasadę, że im więcej informacji niejawnych przetwarzanych w systemach teleinformatycznych (w stosunku do ogólnej liczby materiałów) tym czynnik jest bardziej istotny. W przypadku nowo organizowanej jednostki należy przyjąć wartości szacunkowe.

L.p.	OCENA ISTOTNOŚCI CZYNNIKA	PRZYZNANO*
1.	Bardzo istotny (8pkt.)	
2.	Istotny (4 pkt.)	
3.	Mało istotny (1 pkt.)	**1**

* *wpisać odpowiednią ilość punktów.*

UZASADNIENIE:

Informacje niejawne („Zastrzeżone „) przetwarzane w Urzędzie zasadniczo są w postaci nieelektronicznej. Przetwarzane informacje niejawne nie są przesyłane w formie e-mail ani przekazywane poza Urząd w postaci elektronicznej elektronicznej, tylko drukowane i przesyłane/przechowywane w formie papierowej po wydrukowaniu. Wersje elektroniczne dokumentów tworzone są w celu możliwości ich odtworzenia i ewentualnej poprawy czy aktualizacji. Dostęp do stacji komputerowej, na której są przetwarzane informacje niejawne został ograniczony do minimum, a dokumenty wytwarzane są osobiście przez uprawnionych pracowników Urzędu.

6

LICZBA OSÓB
mających lub mogących mieć dostęp do informacji niejawnych
w Urzędzie Gminy Miedzichowo

L.p.	KLAUZULA TAJNOŚCI	LICZBA OSÓB
1.	ściśle tajne	0
2.	Tajne	0
3.	poufne	0
4.	zastrzeżone	10

Uwaga:
Przy ocenie istotności czynnika należy uwzględnić pracowników jednostki organizacyjnej mających lub mogących mieć dostęp do informacji niejawnych tj. osoby zajmujące stanowiska , wykonujące zadania lub prace zlecone związane z dostępem do takich informacji , a także posiadane przez nich uprawnienia oraz uzasadnioną potrzebę dostępu do informacji niejawnych . Im więcej osób (w stosunku do zatrudnionych) tym czynnik jest bardziej istotny. W przypadku nowo organizowanej jednostki organizacyjnej należy przyjąć wartości szacunkowe.

L.p.	OCENA ISTOTNOŚCI CZYNNIKA	PRZYZNANO*
1.	Bardzo istotny (8pkt.)	
2.	Istotny (4 pkt.)	
3.	Mało istotny (1 pkt.)	1

* *wpisać odpowiednią ilość punktów.*

UZASADNIENIE:
Faktyczny stały dostęp do dokumentów niejawnych o klauzuli „Zastrzeżone" ma jedna osoba. Ponadto Wójt i Pełnomocnik Ochrony Informacji Niejawnych oraz wyznaczeni pracownicy w ramach aktualizacji zadań operacyjnych (Plan operacyjnego funkcjonowania Gminy...).

7

LOKALIZACJA
Urzędu Gminy Miedzichowo

L.p.	Rodzaj zabudowy	Opis
1.	Budynek wolnostojący	NIE
2.	Budynek przylegający parterem do budynków mieszkalnych komunalnych.	ul. Poznańska 12 – Stanowisko do Ewidencjonowania Materiałów Niejawnych. W budynku siedzibę ma również Gminny Ośrodek Pomocy Społecznej oraz Gminny Zespół Obsługi Szkół

Uwaga:

Na wzrost oceny istotności tego czynnika ma wpływ np. to, że budynek użytkowany jest wspólnie z innymi podmiotami lub budynek , którego ściany przylegają do innego budynku). Na wzrost oceny istotności czynnika ma wpływ także najbliższe sąsiedztwo np.: obiekty przedstawicielstw dyplomatycznych, przedsiębiorstw zagranicznych , hotele, obiekty sportowe i hale widowiskowe, ogólnodostępne parkingi, garaże, zakłady przemysłowe , punkty handlowe i inne instalacje stanowiące zagrożenie dla zdrowia lub życia .

L.p.	OCENA ISTOTNOŚCI CZYNNIKA	PRZYZNANO*
1.	Bardzo istotny (8pkt.)	
2.	Istotny (4 pkt.)	4
3.	Mało istotny (1 pkt.)	

* *wpisać odpowiednią ilość punktów.*

UZASADNIENIE:
Budynek użytkowany jest z innymi podmiotami i nie jest obiektem wolnostojącym.

8

DOSTĘP DO BUDYNKU
osób niebędących pracownikami jednostki
Urzędu Gminy Miedzichowo

L.p.	ZAGADNIENIE	OPIS
1.	Osoby jakiej jednostki/*nazwa jednostki/*	Gminnego Zespołu Obsługi Szkół Gminnego Ośrodka Pomocy Społecznej
2.	Szacunkowa liczba tych osób	10
3.	Goście , interesanci	Interesanci urzędu
4.	Inne osoby	Korzystający z Sali konferencyjnej; Radni

Uwaga:
Na wzrost oceny istotności tego czynnika ma wpływ możliwość swobodnego poruszania się po budynku osób niebędących pracownikami jednostki organizacyjnej np. goście, interesanci (w obicktach użyteczności publicznej).
W przypadku nowo organizowanej jednostki organizacyjnej należy przyjąć wartości szacunkowe.

L.p.	OCENA ISTOTNOŚCI CZYNNIKA	PRZYZNANO*
1.	Bardzo istotny (8pkt.)	
2.	Istotny (4 pkt.)	4
3.	Mało istotny (1 pkt.)	

* *wpisać odpowiednią ilość punktów.*

UZASADNIENIE:
Urząd nie posiada odrębnej strefy obsługi interesantów, a dostęp w godzinach pracy do poszczególnych referatów jest nieograniczony, przy czym w pomieszczeniach gdzie przetwarzane są informacje niejawne nie ma wzmożonego ruch obsługiwanych interesantów.

9

INNE CZYNNIKI
dla Urzędu Gminy Miedzichowo

L.p.	CZYNNIK	TAK *	NIE*
1.	Działanie obcych służb specjalnych	-	X
2.	Sabotaż, zamach terrorystyczny	-	X
3.	Kradzież lub inna działalność przestępcza	X	-
4.	Pożar, działanie sił przyrody (np. powódź) lub szkody górnicze	X	-

* zaznaczyć

Uwaga:
Jeśli kierownik jednostki organizacyjnej uzna, że w jego jednostce występują inne niż wymienione czynniki mające wpływ na zagrożenie ujawnieniem lub utratą informacji niejawnych , powinien je określić . Ocenie podlegają Inne Czynniki łącznie. Jeśli wystąpią różne czynniki , należy w ocenie przyjąć czynnik o najwyższym stopniu znaczenia (np. bardzo istotny).

L.p.	OCENA ISTOTNOŚCI CZYNNIKA	PRZYZNANO*
1.	Bardzo istotny (8pkt.)	
2.	Istotny (4 pkt.)	4
3.	Mało istotny (1 pkt.)	

* *wpisać odpowiednią ilość punktów.*

UZASADNIENIE:
Ze względu na to, że stały dostęp do informacji niejawnych jest bardzo ograniczony, a klauzula chronionych dokumentów jest najniższa, mało prawdopodobne jest działanie obcych służb wywiadu, sabotaż czy zamach terrorystyczny.

10

TABELA OKREŚLAJĄCA POZIOM ZAGROŻEŃ
w Urzędzie Gminy Miedzichowo

L.P.	CZYNNIK	OCENA ISTOTNOŚCI CZYNNIKA		
		BARDZO ISTOTNY (8 pkt.)	ISTOTNY (4 pkt.)	MAŁO ISTOTNY (1 pkt.)
1.	Klauzula tajności przetwarzanych informacji niejawnych	-	-	**1**
2.	Liczba materiałów niejawnych	-	-	**1**
3.	Postać informacji niejawnych	-	-	**1**
4.	Liczba osób	-	-	**1**
5.	Lokalizacja	-	**4**	-
6.	Dostęp osób do budynku	-	**4**	-
7.	Inne czynniki	-	**4**	-
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 Miedzichowo określono jako **NISKI** .

11

TABELA WYZNACZANIA PUNKTACJI ZA ZASTOSOWANE ŚRODKI BEZPIECZEŃSTWA FIZYCZNEGO/ZASTRZEŻONE/

ŚRODEK BEZPIECZEŃSTWA	PUNKTACJA
***KATEGORIA K1:* SZAFY DO PRZECHOWYWANIA INFORMACJI NIEJAWNYCH**	
***Środek bezpieczeństwa K1S1*- Konstrukcja szafy**	
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	***2***
Ogólna liczba punktów stanowiąca sumę punktów za wszystkie kategorie PUNKTY = K1+K2+K3	***4***

Ogólna liczba punktów stanowiąca sumę punktów za wszystkie kategorie K1+K2+K3=4 – jest większa od wymaganej do osiągnięcia (2)- w związku z tym nie jest konieczne stosowanie dodatkowych środków bezpieczeństwa z kategorii K4,K5 lub K6..

W wyniku przeprowadzonej analizy w Urzędzie Gminy Miedzichowo 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 wykorzystaniem znajdującego się w pobliżu elementu (rynna, drabina, drzewo) ułatwiającego potencjalny dostęp i penetrację.

ZAŁĄCZNIK NR 2 -Oznaczanie materiałów niejawnych.

DOKUMENT NIEELEKTRONICZNY

NA KAŻDEJ STRONIE

Z A S T R Z E Ż O N E

Egz.Nr.....
Egz.pojedynczy

W lewym górnym rogu sygnaturę literowo-cyfrową, na którą składają się:

- Literowe oznaczenie jednostki lub komórki:
  OC.
- Symbol oznaczenia klauzuli:
  Z.
- Numer pod, którym dokument ten został zarejestrowany w odpowiedniej ewidencji i rok lub dwie ostatnie cyfry roku w którym dokonano rejestracji:
  2.2019
- W zależności od potrzeb inne oznaczenia ułatwiające ustalenie miejsca jego wykonania w jednostce lub komórce organizacyjnej lub też przynależność dokumentu do określonej sprawy:
  5220.I.1

Z A S T R Z E Ż O N E

strona/liczba stron całego dokumentu

DOKUMENT NIEELEKTRONICZNY

NA PIERWSZEJ STRONIE

URZĄD GMINY
w .....

- nazwę jednostki lub komórki organizacyjnej,

w lewym górnym rogu, nad sygnaturą literowo-cyfrową,

Miejscowość,data

- nazwę miejscowości i datę podpisania dokumentu, w prawym górnym rogu, powyżej numeru egzemplarza lub napisu „Egz. pojedynczy":

ADRESAT

lub

„adresaci według rozdzielnika"

- w przypadku dokumentu, któremu nadano bieg korespondencyjny, pod numerem egzemplarza w kolejności pionowej:

✓ imię i nazwisko lub nazwę stanowiska adresata, w przypadku wielu adresatów dokumentu, któremu nadano bieg korespondencyjny, dopuszcza się możliwość umieszczenia jedynie adnotacji "adresaci według rozdzielnika";

DOKUMENT NIEELEKTRONICZNY

NA OSTATNIEJ STRONIE

- Liczba załączników
- Liczba stron lub innych jednostek miary wszystkich załączników
- Klauzule tajności załączników wraz z numerami , pod jakimi zostały zarejestrowane w odpowiedniej ewidencji oraz liczbę stron każdego załącznika lub informację określającą rodzaj załączonego materiału i jego odpowiednią jednostkę miary,
- W przypadku gdy adresatowi wysyła się inną liczbę załączników niż pozostawia w aktach , dodatkowo napis „TYLKO ADRESAT" jeżeli załączniki mają być przekazane adresatowi bez pozostawiania ich w aktach
- Napis „DO ZWROTU" - jeżeli załączniki mają zostać zwrócone osobie uprawnionej do jego podpisania;

<u>Załączniki: 2 na 4 stronach</u>
Załącznik nr 1 – zastrzeżony ,nr ewid. Z-1.2019 na 2 stronach,
Załącznik nr 2- jawny , na 2 stronach – tylko adresat

Stanowisko, imię i nazwisko osoby uprawnionej do podpisania dokumentu

- Liczba egzemplarzy
- Adresaci poszczególnych egzemplarzy/ lub adnotację „adresaci według rozdzielnika"
- Imię i nazwisko lub inne dane identyfikujące wykonawcę

<u>Wykonano w 2 egz.</u>
Egz.Nr1 - .....,
Egz.Nr 2-ad acta
Wykonał: .....

UWAGA!

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.

DOKUMENT NIEELEKTRONICZNY -WZÓR

Z A S T R Z E Ż O N E

URZĄD GMINY
w .....
OC.Z.2.2019.5220.I.1

Miejscowość,data

Egz.Nr.....
Egz.pojedynczy

ADRESAT

TREŚĆ DOKUMENTU

<u>Załączniki: 2 na 4 stronach</u>
Załącznik nr 1 – zastrzeżony ,nr ewid. Z.1.2019 na 2 stronach,
Załącznik nr 2- jawny , na 2 stronach – tylko adresat

.....
Stanowisko, imię i nazwisko osoby uprawnionej do podpisania dokumentu

<u>Wykonano w 2 egz.</u>
Egz.Nr 1 –.....,
Egz.Nr 2-a/a
Wykonał: .....

Z A S T R Z E Ż O N E

strona/liczba stron całego dokumentu

ZAŁĄCZNIKI – OZNACZANIE

Na pierwszej stronie w prawym górnym rogu umieszcza się dodatkowo napis:

„Załącznik nr ... do dokumentu nr ... z dnia ...".

Napis, o którym mowa umieszcza się – w miarę możliwości – na materiałach innych niż dokumenty.

Jeżeli wraz z dokumentem przesyła się załączniki zawierające informacje niejawne, to:

1) klauzula tajności dokumentu nie może być niższa niż najwyższa klauzula tajności załączników;

2) na dokumencie – jeżeli po trwałym odłączeniu załączników jest jawny albo jego klauzula tajności jest inna niż określona zgodnie z pkt. 1 – na każdej stronie pod numerem egzemplarza zamieszcza się adnotację o jawności albo klauzuli tajności dokumentu po ich odłączeniu./ w rubryce „Informacje uzupełniające/Uwagi" wpisuje się adnotację o jawności albo klauzuli tajności dokumentu po trwałym odłączeniu załączników.

materiały inne niż dokumenty

- klauzulę tajności i sygnaturę literowo cyfrową umieszcza się przez ostemplowanie, nadrukowanie, wpisanie odręczne, trwałe dołączenie metek, nalepek, kalkomanii lub w inny widoczny sposób, bezpośrednio, a jeżeli to nie jest możliwe – na ich obudowie lub opakowaniu.
- Utrwalanie informacji niejawnych w formie dźwięku lub obrazu powinno być poprzedzone i kończyć się informacją o nadanej klauzuli tajności, o ile istnieją takie
  możliwości techniczne.
- Na trwale oprawionych zbiorach dokumentów, rejestrach, książkach, broszurach
  i reprodukcjach klauzule tajności umieszcza się pośrodku, na górze i na dole zewnętrznych ścianek okładki oraz – jeżeli jest – na stronie tytułowej.

DOKUMENT ELEKTRONICZNY

Oznacza się tak jak dokumenty nielektroniczne z tym ,że:

1) na każdej stronie zamiast oznaczenia numeru egzemplarza, umieszcza się napis

„Egz. elektroniczny";

2) na pierwszej stronie można nie umieszczać daty podpisania dokumentu, jednak data musi zostać zapisana w metadanych tego dokumentu;

3) na ostatniej stronie zamiast liczby wykonanych egzemplarzy oraz ich adresatów umieszcza się napis **„Egz. elektroniczny"** oraz wskazuje jego adresatów, wskazanie adresatów można zastąpić adnotacją „adresaci według rozdzielnika" lub adnotacją **„przechowywany w systemie".**

Na pierwszej stronie dokumentu,

- w prawym górnym rogu pod numerem egzemplarza lub napisem **„Egz. elektroniczny",** można zamieścić dyspozycję dotyczącą:

1) zgody na kopiowanie części lub całości dokumentu – w przypadku dokumentu o klauzuli tajności „ściśle tajne";

2) braku zgody na kopiowanie części lub całości dokumentu – w przypadku dokumentu o klauzuli tajności „tajne" lub niższej;

3) braku zgody na udzielanie informacji o treści dokumentu;

4) określenia daty lub wydarzenia, po którym nastąpi zniesienie lub zmiana klauzuli tajności całości lub części dokumentu.

W przypadkach uzasadnionych organizacją ochrony informacji niejawnych, na materiałach zawierających informacje niejawne można nanosić dodatkowe oznaczenia, inne niż te, o których mowa powyżej.

KONWERSJA DOKUMENTU

1. Dokument elektroniczny powstały w wyniku konwersji dokumentu nieelektronicznego zarejestrowanego w odpowiedniej ewidencji nie wymaga odrębnej rejestracji, pod warunkiem, Że informacja o dokonaniu konwersji zostanie umieszczona przed dokonaniem tej czynności na pierwszej stronie dokumentu nieelektronicznego, a po dokonaniu tej czynności – w danych rejestrowych tego dokumentu oraz w metadanych powstałego w wyniku konwersji dokumentu elektronicznego.

2. Osoba dokonująca konwersji dokumentu nieelektronicznego odpowiedzialna jest za zapewnienie zgodności oznaczeń tego dokumentu z oznaczeniami umieszczonymi w treści oraz w metadanych dokumentu elektronicznego powstałego w wyniku konwersji.

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
SPISANY 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..... 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

Załącznik Nr 5

Miedzichowo dnia ..... 201... roku

Pan /Pani

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

u p o w a ż n i a m

Pana/ą .....do dostępu do informacji niejawnych oznaczonych klauzulą **„zastrzeżone"** zatrudnionego/oną w Urzędzie Gminy Miedzichowo na stanowisku Inspektora.

.....
/kierownik jednostki/

*Upoważnienie ważne jest na czas zatrudnienia w Urzędzie Gminy Miedzichowo
*Dostęp do informacji niejawnych o klauzuli „zastrzeżone" może nastąpić po odbyciu szkolenia w zakresie przepisów ustawy o ochronie informacji niejawnych.

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 o tym powiadomić:
   - 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, windy, toalety, piwnice, strychy itp. Oraz najbliższe otoczenie zewnętrzne obiektu powinno być sprawdzone przez pracowników obsługi administracyjnej lub ochrony .
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 akcja, po zakończeniu działań , przekazuje protokolarnie obiekt administratorowi.

IV. POSTANOWIENIA KOŃCOWE DOTYCZĄCE DZIAŁAŃ W PRZYPADKU ZGŁOSZENIA O PODŁOŻENIU 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.*

INSTRUKCJA POSTĘPOWANIA W PRZYPADKU OTRZYMANIA PRZESYŁKI NIEWIADOMEGO POCHODZENIA.

W przypadku otrzymania jakiejkolwiek przesyłki niewiadomego pochodzenia lub budzącej podejrzenia z jakiegokolwiek innego powodu:

- Brak nadawcy,
- Brak adresu nadawcy,
- Przesyłka pochodzi od nadawcy lub z miejsca z którego nie spodziewamy się ,
- Inne podejrzenia,

Nie należy otwierać tej przesyłki

Należy:

- 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:

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

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

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
  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:

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

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