

Zatwierdzam

29.12.2023 roku

Rafał Kuciński
/Kierownik Jednostki/

PIN.1410.9.2023

URZĄD GMINY DZIERZGOWO
06-520 Dzierzgowo
ul. T. Kościuszki 1

PLAN OCHRONY INFORMACJI NIEJAWNYCH W URZĘDZIE GMINY DZIERZGOWO.

OPRACOWAŁ

Rafał Wólkowski
Pełnomocnik ds. Ochrony
Informacji Niejawnych
w Urzędzie Gminy Dzierzgowo
06-520 Dzierzgowo
ul. T. Kościuszki 1

29.12.2023 roku

Pełnomocnik ds. Ochrony
Informacji Niejawnych

SPIS TREŚCI:

Akty prawne związane z ochroną informacji niejawnych,

- I. Definicje w rozumieniu Planu ochrony informacji niejawnych,**
- II. Ocena zagrożeń zewnętrznych i wewnętrznych,**
- III. Przedmiot ochrony,**
- IV. Szacowanie ryzyka,**
- V. Ewidencja materiałów niejawnych,**
- VI. Zabezpieczenie informacji niejawnych,**
- VII. Dostęp do informacji niejawnych oznaczonych klauzulą „zastrzeżone” ,**
- VIII. Punkt ewidencji informacji niejawnych,**
- IX. Postępowanie z przesyłkami,**
- X. Obowiązki pracownika punktu ewidencji informacji niejawnych,**
- XI. Zakres udostępniania informacji niejawnych,**
- XII. Zasady wykonywania dokumentów niejawnych,**
- XIII. Wykonywanie dokumentów niejawnych z wykorzystaniem sprzętu komputerowego,**
- XIV. Gromadzenie dokumentów zawierających informacje niejawne,**
- XV. Oznaczanie, nadawanie, zmiana i znoszenie klauzuli niejawności materiałom niejawnym,**
- XVI. Okresy ochronne,**
- 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 PLANU**

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 - Wzór zgody na udostępnienie informacji niejawnych o klauzuli „zastrzeżone” osobie, wobec której wszczęto postępowanie sprawdzające,

ZAŁĄCZNIK Nr 7 - Instrukcja alarmowa w przypadku zgłoszenia o podłożeniu lub znalezieniu ładunku wybuchowego w Urzędzie,

ZAŁĄCZNIK Nr 8 - Instrukcja postępowania w przypadku otrzymania przesyłki niewiadomego pochodzenia,

ZAŁĄCZNIK Nr 9 - Instrukcja dotycząca sposobu i trybu przetwarzania informacji niejawnych o klauzuli „zastrzeżone” w podległych komórkach organizacyjnych oraz zakres i warunki stosowania środków bezpieczeństwa fizycznego w celu ich ochrony.

ZAŁĄCZNIK NR 10 - Instrukcja postępowania z dokumentami niejawnymi w przypadku wprowadzenia stanu nadzwyczajnego.

AKTY PRAWNE ZWIĄZANE Z OCHRONĄ INFORMACJI NIEJAWNYCH

➤ **DZIENNIK USTAW z 2023 r., poz. 756 t. j. ze zm.**

Ustawa o ochronie informacji niejawnych z dnia 5 sierpnia 2010 r.,

➤ **DZIENNIK USTAW z 2017 r., poz. 1558 t. j.**

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 z 2015 r., poz. 220 t. j.**

Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie wzorów poświadczeń bezpieczeństwa,

➤ **DZIENNIK USTAW z 2020 r., poz. 1256 t. j.**

Rozporządzenie Prezesa Rady Ministrów z dnia 9 lipca 2020 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 ze zm.**

Rozporządzenie Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych.

I. DEFINICJE W ROZUMIENIU PLANU OCHRONY INFORMACJI NIEJAWNYCH.

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. z 2020 roku, poz. 344 t. j. ze 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) **punkt ewidencji informacji niejawnych** – wydzielone, wyodrębnione pomieszczenie przeznaczone do ewidencjonowania, opracowywania przechowywania dokumentów niejawnych oznaczonych klauzulą „zastrzeżone”,
- 13) **pracownik punktu ewidencji informacji niejawnych** – osoba wyznaczona przez kierownika jednostki do prowadzenia punktu ewidencji informacji 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) **dokument 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. z 2020 roku, poz. 344 t. j. ze zm.),
- 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 Dzierzgowo 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 ochrony mienia urzędu.

1.2. SYMPTOMY MOGĄCE ŚWIADCZYĆ O PRZYGOTOWANIU NAPADU LUB WŁAMANIA DO BUDYNKU

- wzmożone zainteresowanie osób postronnych obiektem, помещением urzędu objawiające się między innymi: podejmowaniem prób uzyskania informacji o danym obiekcie, помещению 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 przejawianiem zainteresowaniem tym, co się po latach zmieniło,
- interesowaniem się osobami funkcyjnymi, w tym także ich przywarami oraz sposobem wykonywania obowiązków służbowych,
- obserwacją sposobu działania systemu ochronnego, sekretariatu, sprzątaczkę itp.,
- rozpoznawanie systemu technicznych zabezpieczeń, w tym stosowanych urządzeń alarmowych,
- celowe uszkodzanie 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 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.

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 jednorazowe wydane przez kierownika jednostki,
5. wprowadzenie szczególnej uwagi na osoby, których zachowanie wskazuje na nadmierne spożywanie alkoholu.

III. PRZEDMIOT OCHRONY.

1. Informacje niejawne oznaczone klauzulą:
 - „zastrzeżone”.
 - pomieszczenia, w których są przechowywane i opracowywane materiały niejawne.

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 zagrożeniem”.
3. Poziom zagrożeń określono dla pomieszczenia lub obszaru, w którym przetwarzane są informacje niejawne.
3. Poziom zagrożeń określono się jako **niski** i najwyższej 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 dokumentacji, 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) **system monitoringu wizyjnego** – stosowany przez pracowników jednostki organizacyjnej lub personel bezpieczeństwa w celu bieżącego monitorowania ochronnego lub sprawdzania incydentów bezpieczeństwa i sygnałów alarmowych pochodzących z systemów sygnalizacji włamania i napadu,
 - 6) **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.

4. 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.
5. 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 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 kategorii 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” muszą ewidencjonowane w wydzielonym ,wyodrębnionym pomieszczeniu spełniającym wymogi wynikające z przepisów ustawy o ochronie informacji niejawnych,
2. Dokumenty niejawne o klauzuli „zastrzeżone” mogą być ewidencjonowane na zasadach określonych przez kierownika jednostki, opisanych w Planie Ochrony Informacji Niejawnych,
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 opisanie dokumentu niejawnego został przedstawiony w załączniku nr 2 do Planu Ochrony Informacji Niejawnych,
9. Prowadzi się również Rejestr Dzienników służący do ewidencjonowania ksiąg i dzienników ewidencyjnych, rejestrów.
10. Pracownik punktu ewidencji informacji 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 punktu ewidencji informacji niejawnych:
 - 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 punktu ewidencji informacji niejawnych sporządza w dwóch egzemplarzach protokół z otwarcia przesyłki zawierający opis nieprawidłowości, jeden egzemplarz przekazując do kancelarii nadawcy.
14. Pracownik punktu ewidencji informacji niejawnych 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.

1. Informacje niejawne oznaczone klauzulą „zastrzeżone” należy przechowywać w punkcie ewidencji informacji niejawnych, zabezpieczonych zgodnie z przepisami ustawy o ochronie informacji niejawnych, w szafie klasy A lub w meblu/szafie biurowym drewnianym zamykanym na klucz,

Szafa stalowa klasy A

- 1/ Korpus szafy, drzwi, skrytki i inne elementy konstrukcyjne muszą być wykonane z blachy ze stali konstrukcyjnej, o grubości co najmniej 1 mm, zabezpieczonej przed korozją. Połączenia korpusu szafy powinny zapewnić mu dostateczną sztywność.
- 2/ Szafa może być wyposażona w zamykane skrytki.
- 3/ Drzwi szafy mogą być jednoskrzydłowe lub dwuskrzydłowe, zabezpieczone rygłem co najmniej na trzech krawędziach.
- 4/ Szafa musi być wyposażona w zamek mechaniczny kluczowy, co najmniej klasy A wg Polskiej Normy PN-EN 1300, zabezpieczony przed działaniem destrukcyjnym, w tym przed przewierceniem.
- 5/ Szafy jednoskrzydłowe powinny być wyposażone w mechanizm ryglowy blokujący je na co najmniej trzech krawędziach (rygle w średnicy min. 12 mm lub przekroju min. 112 mm², rozstaw rygli max. 450 mm).
- 6/ Szafy dwuskrzydłowe powinny być wyposażone w mechanizm dźwigowy, umieszczony na skrzydle aktywnym, blokujący je na co najmniej 3 krawędziach (rygle w średnicy min. 12 mm lub przekroju min. 112 mm², rozstaw rygli max. 450 mm); skrzydło aktywne musi blokować skrzydło bierne na całej ich wysokości. W przypadku niezależnego zamykania obu skrzydeł każde z nich powinno być wyposażone w oddzielny mechanizm ryglujący.
- 7/ Podstawa szafy musi posiadać te same rozmiary co wierzch. W szafie może znajdować się zaślepiiony otwór umożliwiający jej zakotwienie.
- 8/ Szafa musi posiadać certyfikat wydany przez jednostkę certyfikującą akredytowaną w krajowym systemie akredytacji, potwierdzający zgodność wyrobu z wymaganiami klasy A.

9/ Szafa musi posiadać tabliczkę, wydaną przez jednostkę certyfikującą akredytowaną w krajowym systemie akredytacji, zamontowaną na wewnętrznej, górnej stronie drzwi, zawierającą następujące dane:

- 1) nazwę wyrobu,
- 2) nazwę i kod identyfikacyjny producenta, typ i numer modelu,
- 3) numer fabryczny, rok produkcji, klasę wyrobu, numer certyfikatu,
- 4) masę.

2. W uzasadnionych przypadkach podyktowanych względami dłuższego okresu czasu, niezbędnego do wykonania zadań związanych z dostępem do informacji niejawnych, dokumenty o klauzuli „zastrzeżone” mogą być wydawane poza wydzielone pomieszczenie, lecz pod warunkiem, że odbiorca dokumentu zapewni warunki ochrony tych dokumentów spełniając wymogi określone w pkt 2, przechowując je w szafach metalowych klasy „A” z odpowiednim zamknięciem lub ;
3. Dokumenty lub materiały oznaczone klauzulą „zastrzeżone” mogą być przechowywane poza szafami stalowymi w pomieszczeniach punktu odpowiadające jednak co najmniej klasie o odporności na włamanie wg Polskiej Normy PN-EN 1143-1,
4. Szafy metalowe, w których przechowuje się dokumenty o klauzuli „zastrzeżone” po zakończeniu pracy należy zamknąć i sprawdzić sposób ich zabezpieczenia;
5. Informacje niejawne oznaczone klauzulą „zastrzeżone” można przechowywać w pomieszczeniu punktu ewidencji informacji niejawnych lub na stanowiskach pracy, w meblach biurowych zamykanych na klucz.

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 do dostępu do informacji niejawnych o klauzuli „zastrzeżone” może nastąpić:
 - po uzyskaniu przez pracownika poświadczenia bezpieczeństwa po przeprowadzonym przez Pełnomocnika ochrony zwykłym postępowaniu sprawdzającym lub uzyskaniu stosownego upoważnienia kierownika jednostki,
 - po przeszkoleniu danej osoby w zakresie ochrony informacji niejawnych i uzyskaniu odpowiedniego zaświadczenia o przeszkoleniu.
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. Zwykle postępowanie sprawdzające wobec pracowników jednostki w związku z dostępem do informacji niejawnych oznaczonych klauzulą „zastrzeżone” na pisemne polecenie kierownika jednostki przeprowadza Pełnomocnik ds. Ochrony Informacji Niejawnych.
5. Osoba podlegająca procedurze postępowania sprawdzającego zobowiązana jest do:
 - a. wypełnienia określonej przepisami ustawy ankiety bezpieczeństwa
 - b. osobowego,
 - c. wypełnienia ankiety w sposób dokładny i zgodny z prawdą.
6. Odmowa poddania się postępowaniu sprawdzającemu ze strony osoby, która jest lub będzie zatrudniona na stanowisku związanym z dostępem do informacji niejawnych o klauzuli „zastrzeżone”, a w związku z tym nie uzyskanie poświadczenia bezpieczeństwa warunkującego dostęp do informacji oznaczonych klauzulą „poufne” może skutkować:
 - a. przeniesieniem danej osoby na stanowisko nie związane z informacjami
 - b. niejawnymi o klauzuli „poufne”,
 - c. rozwiązaniem umowy o pracę w przypadku niemożności zmiany stanowiska,
 - d. niemożnością zatrudnienia na danym stanowisku, w przypadku ubiegania się
 - e. zatrudnienie w Urzędzie.

VIII. PUNKT EWIDENCJI INFORMACJI NIEJAWNYCH.

1. W urzędzie funkcjonuje punkt ewidencji informacji niejawnych (pokój nr 8), który został utworzony dla potrzeb jednostki, dla właściwego przechowywania, ewidencjonowania materiałów niejawnych oznaczonych klauzulą „zastrzeżone”.
2. Organizacja pracy w punkcie ewidencji informacji niejawnych 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. Punkt ewidencji informacji niejawnych 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. Punkt ewidencji informacji niejawnych tworzy kierownik jednostki organizacyjnej.

6. Punktem ewidencji informacji niejawnych kieruje pracownik, wyznaczany przez kierownika jednostki organizacyjnej na wniosek pełnomocnika ochrony.
7. Do podstawowych zadań pracownika punktu ewidencji informacji niejawnych należy:
 - 1) bezpośredni nadzór nad obiegiem dokumentów,
 - 2) udostępnianie lub wydawanie dokumentów osobom do tego uprawnionym,
 - 3) egzekwowanie zwrotu dokumentów,
 - 4) kontrola przestrzegania właściwego oznaczania i rejestrowania dokumentów w punkcie ewidencji informacji niejawnych oraz jednostce organizacyjnej,
 - 5) prowadzenie bieżącej kontroli postępowania z dokumentami,
 - 6) wykonywanie poleceń pełnomocnika ochrony.
8. W przypadku zmiany na stanowisku pracownika punktu ewidencji informacji niejawnych sporządza się protokół zdawczo-odbiorczy.
9. Protokół, o którym mowa w pkt 8, sporządza się w obecności pracownika zdającego obowiązki, osoby przejmującej obowiązki oraz pełnomocnika ochrony. Protokół sporządza się w dwóch egzemplarzach; pierwszy egzemplarz przechowywany jest w punkcie ewidencji informacji niejawnych, drugi – u pełnomocnika ochrony. Wzór protokołu określa załącznik nr 4 do Planu Ochrony.
10. W przypadku czasowej nieobecności pracownika punktu ewidencji informacji niejawnych jego obowiązki przejmuje upoważniony pracownik pionu ochrony. W razie ich braku punkt przejmuje pełnomocnik ochrony lub inny pracownik wyznaczony pisemnie przez kierownika jednostki na wniosek pełnomocnika ochrony.
11. W pomieszczeniach punktu ewidencji informacji niejawnych można wydzielić miejsce, w którym osoby upoważnione mogą zapoznawać się z dokumentami – czytelną:
 - 1) czytelnia powinna być zorganizowana w sposób umożliwiający stały nadzór ze strony pracownika punktu,
 - 2) w czytelni zabrania się instalowania systemu nadzoru wizyjnego.
12. Dokumenty i materiały oznaczone różnymi klauzulami tajności są przechowywane w odrębnych szafach lub pomieszczeniach, chyba że wchodzi one w skład zbioru dokumentów.

13. Po zakończeniu pracy kierownik punktu ewidencji informacji niejawnych lub upoważniony pracownik punktu ewidencji informacji niejawnych jest obowiązany sprawdzić prawidłowość zamknięcia szaf i pomieszczeń punktu.
14. Zasady i sposób zdawania, przechowywania i wydawania kluczy oraz ich duplikatów do pomieszczeń oraz szaf punktu, a także zasady ustalania, zmiany i deponowania haseł lub szyfrów, w przypadku stosowania zamków szyfrowych, określa plan ochrony informacji niejawnych.
15. Wszelkie nieprawidłowości związane z naruszeniem zasad, określonych powyżej należy niezwłocznie zgłaszać pełnomocnikowi ochrony.
16. Zasady określone obowiązują odpowiednio w stosunku do innych pomieszczeń, w których są przechowywane dokumenty lub materiały, oraz osób za te pomieszczenia odpowiedzialnych.
17. W punkcie ewidencji informacji niejawnych 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 (jeżeli zachodzi taka potrzeba).
18. W przypadkach uzasadnionych organizacją ochrony informacji niejawnych punkt ewidencji informacji niejawnych może prowadzić także inne rejestry niż wymienione wyżej wymienione, w tym odrębne rejestry dla dokumentów oznaczonych różnymi klauzulami tajności – np. kartę zapoznania się z dokumentem niejawnym oznaczonym klauzulą „zastrzeżone”.
19. Za zgodą kierownika jednostki organizacyjnej, w porozumieniu z pełnomocnikiem ochrony, w punkcie ewidencji informacji niejawnych mogą być przyjmowane, rejestrowane, przechowywane i wysyłane dokumenty i materiały oznaczone klauzulą „zastrzeżone”

IX. POSTĘPOWANIE Z PRZESYŁKAMI.

1. Pracownik punktu ewidencji informacji niejawnych 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 lub w książce doręczeń.
3. W przypadku stwierdzenia uszkodzenia przesyłki lub śladów jej otwierania pracownik punktu ewidencji informacji niejawnych 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 punktu ewidencji informacji niejawnych:
 - 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 punktu ewidencji informacji niejawnych sporządza w dwóch egzemplarzach protokół z otwarcia przesyłki zawierający opis nieprawidłowości, jeden egzemplarz przekazując do punktu ewidencji informacji niejawnych nadawcy,
 6. Pracownik punktu ewidencji informacji niejawnych odnotowuje fakt sporządzenia protokołu, w odpowiednim dzienniku lub rejestrze w rubryce „Informacje uzupełniające/Uwagi”.
 7. W punkcie ewidencji informacji niejawnych materiałów niejawnych nie otwiera się przesyłek oznaczonych „do rąk własnych”. W odpowiednim dzienniku lub rejestrze wpisuje się nadawcę, numer i datę wpływu dokumentu; w rubryce „Informacje uzupełniające/Uwagi” odnotowuje się, że przesyłka była oznaczona „do rąk własnych”,
 8. Na opakowaniu przesyłek, wpisuje się datę wpływu, pozycję i numer, pod którym zarejestrowano przesyłkę. Przesyłkę przekazuje się – za pokwitowaniem – bezpośrednio adresatowi, a w razie jego nieobecności – osobie przez niego upoważnionej do odbioru,
 9. Zatrzymanie przez adresata dokumentu, adresowanego „do rąk własnych”, odnotowuje się w rubryce „Informacje uzupełniające/Uwagi”.

10. W przypadku zwrotu do punktu ewidencji informacji niejawnych przesyłki adresowanej „do rąk własnych”, pracownik punktu ewidencji informacji niejawnych uzupełnia dane dotyczące przesyłki w odpowiednim dzienniku lub rejestrze.
 11. Jeżeli adresat podjął decyzję o przechowywaniu przesyłki „do rąk własnych” w punkcie ewidencji informacji niejawnych w stanie zamkniętym, pracownik punktu ewidencji informacji niejawnych 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. Otrzymałą 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 PUNKTU EWIDENCJI INFORMACJI NIEJAWNYCH MATERIAŁÓW NIEJAWNYCH.

1. Przed otwarciem drzwi sprawdzić stan zamków i zabezpieczenie drzwi,
2. Sprawdzić stan zabezpieczeń szaf, sprzętu biurowego.
3. Przestrzegać zasad zakazu wstępu osobom nieuprawnionym do punktu ewidencji informacji niejawnych materiałów niejawnych,

XI. ZAKRES UDOSTĘPNIANIA INFORMACJI NIEJAWNYCH.

1. Udostępnianie pracownikowi informacji niejawnych oznaczonych klauzulą „zastrzeżone” uwarunkowane jest posiadaniem właściwego i ważnego poświadczenia osobowego.
 2. 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.

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 punkcie ewidencji informacji niejawnych.
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 opisanie dokumentu stanowi załącznik nr 2 do Planu OIN.

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:
 - zapewnia opracowanie dokumentacji bezpieczeństwa teleinformatycznego,
 - realizuje ochronę fizyczną, elektromagnetyczną systemu lub sieci,

- zapewnia niezawodność transmisji oraz kontrolę dostępu do urządzeń systemu lub sieci teleinformatycznej,
- dokonuje analizy stanu bezpieczeństwa teleinformatycznego oraz zapewnia usunięcie stwierdzonych nieprawidłowości,
- przeszkolenie z zakresu bezpieczeństwa teleinformatycznego dla osób uprawnionych do pracy w systemie lub sieci teleinformatycznej,
- zawiadamia właściwą służbę ochrony państwa o zaistniałym incydencie bezpieczeństwa teleinformatycznego dotyczącym informacji niejawnych oznaczonych co najmniej klauzulą „zastrzeżone”.

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:
 - a) klauzuli tajności,
 - b) ilości,
 - c) zagrożeń dla poufności, integralności lub dostępności- informacji niejawnych;
- 2) zastosowaniu środków zapewniających ochronę fizyczną, w szczególności przed:
 - a) nieuprawnionym dostępem,
 - b) podglądem,
 - c) podsłuchem.

5. 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 spełniających wymagania w zakresie tłumienności elektromagnetycznej odpowiednio do wyników szacowania ryzyka

dla informacji niejawnych, lub zastosowanie odpowiednich urządzeń teleinformatycznych, połączeń i linii o obniżonym poziomie emisji lub ich ekranowanie z jednoczesnym filtrowaniem zewnętrznych linii zasilających i sygnałowych.

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 Systemu 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 lub pracowników pionu ochrony pełniących 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**”.

18. W sytuacjach wymagających konsultacji lub uzgodnień kierownik jednostki może zwrócić się do Agencji Bezpieczeństwa Wewnętrznego o wydanie opinii lub zaleceń w zakresie bezpieczeństwa teleinformatycznego .
19. 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.
20. Zaświadczenie o odbytym szkoleniu jest przechowywane w aktach osobowych oraz dokumentacji Pełnomocnika art. ochrony informacji niejawnych.

KOPIE ZAPASOWE.

1. Zaleca się wykonywanie kopii zapasowych wykonanych dokumentów niejawnych.
2. Sposób przechowywania zapasowych kopii jest identyczny jak przechowywanie dokumentów wykonanych w formie tradycyjnej (pismo), w przypadku gdy nośnikiem informacji jest materiał inny niż pismo, 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 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” muszą być przechowywane w punkcie ewidencji informacji niejawnych. W szczególnie uzasadnionych przypadkach dokumenty te mogą być przechowywane poza punktem, kierownik jednostki organizacyjnej lub inna upoważniona przez niego osoba mogą wyrazić pisemną zgodę na przechowywanie dokumentów poza pomieszczeniami punktu, pod warunkiem spełnienia wymogów bezpieczeństwa odpowiednich do tej klauzuli, na czas niezbędny do realizacji zadań związanych z dostępem do tych dokumentów.

4. Dokumenty niejawne o klauzuli „zastrzeżone” są przechowywane w punkcie ewidencji informacji niejawnych 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. 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 2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności, (Dz. U. Nr

- 288 z 2011 r., poz. 1692). Wzór opisanego dokumentu niejawnego stanowi załącznik nr 2 do Planu ochrony.
11. 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”.
12. W przypadkach uzasadnionych organizacją ochrony informacji niejawnych na materiałach zawierających informacje niejawne można nanosić dodatkowe oznaczenia.
13. **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 2011 r. nr 288 poz. 1692),
14. 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”.
15. **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 ...”,
16. **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;

17. 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”.

18. 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.

19. Utrwalanie informacji niejawnych w formie dźwięku, obrazu lub poczty elektronicznej,

- 1) powinno być poprzedzone i kończyć się informacją o nadanej klauzuli tajności, jeżeli istnieją takie możliwości techniczne.

20. 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 ustawowy 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 „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:

- 1) na każdej stronie w prawym górnym i dolnym rogu skreśla się dotychczasowe klauzule tajności,
- 2) nad skreślonymi klauzulami tajności umieszcza się nowe klauzule tajności;
- 3) 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 punktu ewidencji informacji 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.

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. Informacje niejawne stanowiące oznaczone klauzulą „zastrzeżone” mogą być udostępniane wyłącznie osobie uprawnionej do dostępu do informacji niejawnych o określonej klauzuli niejawności,
2. Uzyskanie uprawnień do dostępu do informacji niejawnych o klauzuli „poufne” może nastąpić:
 - 1) po przeprowadzeniu zwykłego postępowania sprawdzającego wobec kandydata do dostępu do tych informacji,

- 2) po uzyskaniu przez daną osobę poświadczenia bezpieczeństwa ,
 - 3) po przeszkoleniu danej osoby w zakresie przepisów o ochronie informacji niejawnych i uzyskaniu właściwego zaświadczenia o przeszkoleniu.
3. Zwykle postępowanie sprawdzające w związku z dostępem do informacji niejawnych o klauzuli „zastrzeżone” na pisemne polecenie kierownika jednostki organizacyjnej przeprowadza Pełnomocnik ds. Ochrony Informacji Niejawnych ,
4. Osoba podlegająca postępowaniu sprawdzającemu zwykłemu zobowiązana jest do:
- 1) wypełnienia określonej przepisami ankiety bezpieczeństwa osobowego, w sposób dokładny i zgodny z prawdą,
 - 2) odbyć szkolenie z zakresu znajomości przepisów ustawy o ochronie informacji niejawnych prowadzone przez Pełnomocnika .
5. Odmowa poddania się postępowaniu sprawdzającemu ze strony osoby, która jest lub będzie zatrudniona na stanowisku związanym z dostępem do informacji niejawnych, a w związku z tym nie uzyskanie poświadczenia bezpieczeństwa warunkującego dostęp do informacji niejawnych o klauzuli „zastrzeżone” może skutkować:
- 1) przeniesieniem danej osoby na stanowisko nie związane z dostępem do informacji niejawnych,
 - 2) rozwiązaniem umowy o pracę w przypadku niemożności zmiany stanowiska,
 - 3) niemożnością zatrudnienia na danym stanowisku, w przypadku ubiegania się o zatrudnienie w Urzędzie.
6. Kierownik jednostki organizacyjnej może wyrazić w formie pisemnej zgodę na udostępnienie informacji niejawnych o klauzuli „zastrzeżone” osobie która jest zatrudniona lub wykonuje prace zlecone , wobec której wszczęto zwykle postępowanie sprawdzające ,wzór zgody pisemnej stanowi załącznik nr 6 do Planu ochrony,
7. Kierownik jednostki organizacyjnej uzyskuje dostęp do informacji niejawnych oznaczonych klauzulą „zastrzeżone” po uzyskaniu Poświadczenia Bezpieczeństwa lub upoważnienia kierownika jednostki oraz uzyskaniu zaświadczenia stwierdzającego odbycie szkolenia z zakresu przepisów ustawy o ochronie informacji niejawnych.
8. Postępowanie sprawdzające wobec kierownika jednostki , w przypadku potrzeby uzyskania uprawnień dostępu do informacji niejawnych oznaczonych klauzulą „poufne” przeprowadza Agencja Bezpieczeństwa Wewnętrznego,
9. Szkolenie kierownika jednostki w związku z przewidywanym dostępem do informacji niejawnych oznaczonych klauzulą „poufne” organizuje pełnomocnik ochrony wydając stosowne zaświadczenie,

10. 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,

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. z 2023 roku, poz. 756 t. j. ze zm.) w imieniu kierownika jednostki wykonuje pełnomocnik do spraw ochrony informacji niejawnych poprzez:

- 1) sprawowanie nadzoru nad przestrzeganiem przepisów zawartych w Planie Ochrony Informacji Niejawnych,
- 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 1997 r., Kodeks Karny, Dz. U. z 2023 roku, poz. 1138 t. j. ze zm.) w art. 266.

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

§ 2. Funkcjonariusz publiczny, który ujawnia osobie nieuprawnionej informację niejawną o klauzuli „zastrzeżone” lub „poufne” lub informację, którą uzyskał w związku z wykonywaniem czynności służbowych, a której ujawnienie

może narazić na szkodę prawnie chroniony interes, podlega karze pozbawienia wolności do lat 3.”.

2. 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 przepisach prawa w sprawie postępowania z dokumentacją, zasad jej klasyfikowania i kwalifikowania oraz zasad i trybu przekazywania materiałów archiwalnych do archiwów państwowych.
2. Zasady postępowania z dokumentacją w komórkach organizacyjnych wykonujących zadania w zakresie obronności i bezpieczeństwa państwa zostały określone w przepisach prawa,
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 w stanowią podstawę gromadzenia dokumentacji w akta 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 niearchiwalnej,
 - 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 wchodzi: osoba kierująca lub prowadząca archiwum zakładowe albo składnicę akt oraz przedstawiciele komórek organizacyjnych, których dokumentacja niearchiwalna podlega brakowaniu oraz pracownik punktu ewidencji informacji niejawnych,
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 komisijnego zniszczenia dokumentów niearchiwalnych.
19. Protokół komisijnego 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 metalowe punktu ewidencji informacji niejawnych po zamknięciu mogą być dodatkowo plombowane pieczęcią do plasteliny,
 - 2) Klucze od szaf metalowych punktu ewidencji informacji niejawnych oraz pieczęcie, po zakończeniu pracy należy złożyć w pomieszczeniu punktu ewidencji informacji niejawnych w miejscu niewidocznym,
 - 3) Po zakończeniu pracy, pracownik materiałów niejawnych zamyka i plombuje pieczęcią do plasteliny drzwi wejściowe punktu ewidencji informacji niejawnych,
 - 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 punktu ewidencji informacji niejawnych powinien zabezpieczać tak, by osoby nieuprawnione nie mogły z niej korzystać,

- 6) Tworzy się zapasowy komplet kluczy od pomieszczeń punktu ewidencji informacji niejawnych,
- 7) Zapasowy komplet kluczy 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 punktu ewidencji informacji niejawnych po przybyciu do urzędu, przed otwarciem punktu ewidencji informacji niejawnych powinien sprawdzić, czy nie zostały naruszone pieczęcie zabezpieczające klucze oraz zabezpieczające drzwi wejściowe do punktu ewidencji informacji niejawnych. W dalszej kolejności sprawdza czy nie zostały naruszone pieczęcie na szafach znajdujących się w punkcie ewidencji informacji niejawnych.

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 - Wzór zgody na udostępnienie informacji niejawnych o klauzuli „zastrzeżone” osobie, wobec której wszczęto postępowanie sprawdzające,

ZAŁĄCZNIK Nr 7 - Instrukcja alarmowa w przypadku zgłoszenia o podłożeniu lub znalezieniu ładunku wybuchowego w Urzędzie,

ZAŁĄCZNIK Nr 8 - Instrukcja postępowania w przypadku otrzymania przesyłki niewiadomego pochodzenia.

ZAŁĄCZNIK Nr 9 - Instrukcja dotycząca sposobu i trybu przetwarzania informacji niejawnych o klauzuli „zastrzeżone” w podległych komórkach organizacyjnych oraz zakres i warunki stosowania środków bezpieczeństwa fizycznego w celu ich ochrony.

ZAŁĄCZNIK NR 10 - Instrukcja postępowania z dokumentami niejawnymi w przypadku wprowadzenia stanu nadzwyczajnego.
