- dziennik korespondencyjny,
- dziennik ewidencji wykonanych dokumentów, oznaczonych klauzulą „poufne" i „zastrzeżone",
- książkę doręczeń przesyłek miejscowych,

17. W przypadkach uzasadnionych organizacją ochrony informacji niejawnych kancelaria może prowadzić także inne rejestry niż wymienione wyżej wymienione, w tym odrębne rejestry dla dokumentów oznaczonych różnymi klauzulami tajności.

18. Za zgodą kierownika jednostki organizacyjnej, w porozumieniu z pełnomocnikiem ochrony, w kancelarii mogą być przyjmowane, rejestrowane, przechowywane i wysyłane dokumenty i materiały oznaczone klauzulą „zastrzeżone"

POSTĘPOWANIE Z PRZESYŁKAMI

1. Kierownik 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 kierownik kancelarii 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 kierownik lub pracownik kancelarii:
- sprawdza, czy zawartość przesyłki odpowiada wyszczególnionym na niej numerom ewidencyjnym;
- ustala, czy liczba załączników i stron jest zgodna z liczbą oznaczoną na poszczególnych dokumentach

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

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

7. W kancelarii 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 kancelarii przesyłki, o której mowa w ust. 1, kierownik lub pracownik kancelarii uzupełnia dane dotyczące przesyłki w odpowiednim dzienniku lub rejestrze.

11. Jeżeli adresat podjął decyzję o przechowywaniu przesyłki „do rąk własnych" w kancelarii w stanie zamkniętym, kierownik kancelarii dokonuje czynności, o których mowa w ust. 5, przy udziale adresata. Przesyłka jest w takim przypadku przechowywana w formie zapieczętowanego pakietu, a fakt ten odnotowuje się w rubryce „Informacje uzupełniające/Uwagi".

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

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

14. Wszelkich adnotacji, w dziennikach ewidencyjnych, dokonuje się atramentem lub tuszem. Zmian dokonuje się kolorem czerwonym, umieszczając datę i czytelny podpis dokonującego zmiany.

15. Zabrania się wycierania i zamazywania adnotacji,

16. Dokumenty, materiały oraz zbiory dokumentów dotyczące spraw ostatecznie zakończonych przechowuje się w kancelarii nie dłużej niż 2 lata. Po upływie tego okresu przekazuje się je do archiwum zakładowego, spełniającego wymogi bezpieczeństwa odpowiednie dla ich klauzuli tajności, jeżeli jednostka organizacyjna takim dysponuje.

OBOWIĄZKI OSÓB FUNKCYJNYCH

- *Przed otwarciem drzwi sprawdzić stan zamków i zabezpieczenie drzwi,*
- *Sprawdzić stan zabezpieczeń szaf, sprzętu komputerowego.*
- *Przestrzegać zasad zakazu wstępu osobom nieuprawnionym do kancelarii tajnej,*
- *W miarę możliwości niezbędne sprawy załatwiać w strefie bezpieczeństwa,*
- *Stosować zasadę, że do kancelarii tajnej wstęp mogą mieć tylko osoby posiadające poświadczenie bezpieczeństwa*

VIII. ZAKRES UDOSTĘPNIANIA INFORMACJI NIEJAWNYCH

1. Udostępnianie pracownikowi informacji niejawnych uwarunkowane jest posiadaniem właściwego i ważnego poświadczenia osobowego.

2. Udostępnianie informacji niejawnych stanowiących tajemnice służbowa o klauzuli „poufne" lub „zastrzeżone" określonej osobie może nastąpić również w oparciu o pisemne jednorazowe upoważnienie kierownika jednostki.

IX. ZASADY WYKONYWANIA DOKUMENTÓW NIEJAWNYCH

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

2. Klauzulę niejawności na danym dokumencie przyznaje osoba, która jest upoważniona do podpisania dokumentu,

3. Rękopisy sporządzanych dokumentów niejawnych powinny być opracowywane w brulionach (zeszytach pracy) uprzednio zarejestrowanych kancelarii tajnej.

4.Dokumenty niejawne powinny być opisane i oznaczone zgodnie z Rozporządzeniem Prezesa Rady Ministrów z dnia 29 września 2005 r. w sprawie sposobu oznaczania materiałów, umieszczania na nich klauzul tajności, a także zmiany nadanej klauzuli tajności (Dz.U. z 2005 roku, nr 205, poz.1696).

X. 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 Burmistrz, 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;
- zapewnia 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 „poufne" .

4. Ochrona fizyczna systemu lub sieci teleinformatycznej polega na:

1).umieszczeniu urządzeń systemu lub sieci teleinformatycznej w strefie bezpieczeństwa, strefie administracyjnej lub specjalnej strefie bezpieczeństwa, zwanych również „strefą kontrolowanego dostępu" w zależności od:

- klauzuli tajności, klauzuli tajności
- ilości,
- zagrożeń dla poufności, integralności lub dostępności- informacji niejawnych;

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

- podglądem,
- podsłuchem.

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

   - Utrata poufności następuje w szczególności na skutek wykorzystania elektromagnetycznej emisji ujawniającej pochodzącej z tych urządzeń.

   - 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:

   - Burmistrz lub osoba przez niego upoważniona ustala warunki i sposób przydzielania uprawnień osobom uprawnionym do pracy w systemie lub sieci teleinformatycznej;

   - administrator systemu 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. System lub sieć teleinformatyczną wyposaża się w mechanizmy kontroli, w których mają być wytwarzane, przetwarzane, przechowywane lub przekazywane informacje niejawne, podlegają akredytacji bezpieczeństwa teleinformatycznego przez służby ochrony państwa.

10. Akredytacja, o której mowa następuje na podstawie dokumentów szczególnych wymagań bezpieczeństwa i procedur bezpiecznej eksploatacji.

11. Urządzenia i narzędzia kryptograficzne, służące do ochrony informacji niejawnych stanowiących tajemnicę państwową lub tajemnicę służbową oznaczonych klauzulą „poufne", podlegają badaniom i certyfikacji prowadzonym przez służby ochrony państwa.

12. Szef właściwej służby ochrony państwa po zapoznaniu się z wynikiem analizy ryzyka dla bezpieczeństwa informacji niejawnych może, bez spełnienia niektórych wymagań w zakresie ochrony fizycznej, elektromagnetycznej lub kryptograficznej, dokonać, na czas określony, nie dłuższy jednak niż na 2 lata, akredytacji bezpieczeństwa

teleinformatycznego systemu lub sieci teleinformatycznej, którym przyznano określoną klauzulę tajności w przypadku, gdy brak możliwości ich eksploatacji powodowałby zagrożenie dla porządku publicznego, obronności, bezpieczeństwa albo interesów międzynarodowych państwa.

13. W wyniku oceny i badań, Departament Bezpieczeństwa Teleinformatycznego ABW wydaje certyfikaty ochrony elektromagnetycznej.

14. Burmistrz wyznacza:

- osobę odpowiedzialną za funkcjonowanie systemów lub sieci teleinformatycznych oraz za przestrzeganie zasad i wymagań bezpieczeństwa systemów i sieci teleinformatycznych, zwaną dalej **„administratorem systemu"**,

- pracownika pionu ochrony pełniącego funkcje **inspektora bezpieczeństwa teleinformatycznego,** odpowiedzialnego za bieżącą kontrolę zgodności funkcjonowania sieci lub systemu teleinformatycznego ze szczególnymi wymaganiami bezpieczeństwa oraz za kontrolę przestrzegania procedur bezpiecznej eksploatacji,

15. W sytuacjach wymagających konsultacji lub uzgodnień Burmistrz może zwrócić się do Agencji Bezpieczeństwa Wewnętrznego o wydanie opinii lub zaleceń w zakresie bezpieczeństwa teleinformatycznego

16. Stanowiska lub funkcje administratora systemu oraz inspektora bezpieczeństwa teleinformatycznego mogą zajmować lub pełnić osoby, posiadające poświadczenia bezpieczeństwa 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.

Zaświadczenie o odbytym szkoleniu jest przechowywane w aktach osobowych pracownika oraz dokumentacji Pełnomocnika ds. ochrony informacji niejawnych

KOPIE ZAPASOWE:

- Zaleca się wykonywanie kopii zapasowych wykonanych dokumentów niejawnych.
- 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 literowocyfrową 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.

XI. GROMADZENIE DOKUMENTÓW ZAWIERAJACYCH INFORMACJE NIEJAWNE

- Dokumenty zawierające informacje niejawne powinny być przechowywane zgodnie z rzeczowym podziałem akt.,

1. Dokumenty ostatecznie załatwione wymagają wszycia w teczkę pism, po zakończeniu roku kalendarzowego, klauzule niejawności teczek określa się według dokumentu o najwyższej klauzuli tajności,
2. Dokumenty niejawne o klauzuli „poufne" muszą być przechowywane w kancelarii tajnej. W