

Zarządzenie Nr 0050.158.2018

Burmistrza Stąporkowa z dnia 22 listopada 2018 roku

w sprawie zatwierdzenia „Planu Ochrony Informacji Niejawnych w Urzędzie Miejskim w Stąporkowie”.

Na podstawie art. 30 ust. 1 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2018 r., poz. 944 ze zm.) oraz art. 15 ust. 1 pkt 5 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2018 r., poz. 412 ze zm.) zarządzam, co następuje:

§ 1

W celu zapewnienia ochrony informacji niejawnych oraz przestrzegania przepisów o ochronie informacji niejawnych zatwierdzam i wprowadzam do stosowania „Plan Ochrony Informacji Niejawnych w Urzędzie Miejskim w Stąporkowie” stanowiący załącznik do niniejszego zarządzenia.

§ 2

„Plan Ochrony Informacji Niejawnych w Urzędzie Miejskim w Stąporkowie” określony w załączniku do niniejszego zarządzenia dotyczy wszystkich pracowników urzędu, którzy przetwarzają informacje niejawne.

§ 3

Nadzór nad wykonaniem zarządzenia powierzam pełnomocnikowi ds. ochrony informacji niejawnych.

§ 4

Traci moc zarządzenie Nr 88/2012 Burmistrza Stąporkowa z dnia 10 maja 2012 roku w sprawie zatwierdzenia „Planu Ochrony Informacji Niejawnych w Urzędzie Miejskim w Stąporkowie”.

§ 5

Zarządzenie wchodzi w życie z dniem podpisania.

Sporządziła: *Bogumiła Józwiak*
PEŁNOMOCNIK
Ochrony Informacji Niejawnych
Bogumiła Józwiak

BURMISTRZ
mgr Dorota Łukomska

Załącznik do Zarządzenia Nr 0050.158.2018

Burmistrza Stąporkowa z dnia 22 listopada 2018 r.

ZATWIERDZAM

BURMISTRZ

mgr Dorota Łukomska

Burmistrz

**PLAN OCHRONY INFORMACJI NIEJAWNYCH
W URZĘDZIE MIEJSKIM W STĄPORKOWIE**

OPRACOWAŁA: Bogumiła Jóźwik

Pełnomocnik Ochrony Informacji Niejawnych

Stąporków, dnia 22 listopada 2018 r.

SPIS TREŚCI:

I. Akty prawne związane z ochroną informacji niejawnych.....	4
II. Definicje używane w Planie Ochrony Informacji Niejawnych	5
III. Ocena zagrożeń zewnętrznych i wewnętrznych	6
IV. Przedmiot ochrony	8
V. Ewidencja informacji niejawnych podlegających ochronie	8
VI. Zabezpieczenie informacji niejawnych	9
VII. Zasady dostępu do informacji niejawnych oznaczonych klauzulą „zastrzeżone”	10
VIII. Kancelaria materiałów niejawnych	11
IX. Zakres udostępniania informacji niejawnych	14
X. Zasady wykonywania dokumentów niejawnych	15
XI. Wykonywanie dokumentów niejawnych z wykorzystaniem sprzętu komputerowego.....	15
XII. Gromadzenie dokumentów zawierających informacje niejawne	19
XIII. Oznaczanie, nadawanie, zmiana i znoszenie klauzuli niejawności materiałom niejawnym.....	20
XIV. Okresy ochronne i nadzór w zakresie ochrony informacji niejawnych	23
XV. Odpowiedzialność karna, dyscyplinarna i służbowa za naruszenie przepisów o ochronie informacji niejawnych	23
XVI. Archiwizowanie, gromadzenie i niszczenie materiałów niejawnych	24
XVII. Przechowywanie kluczy i pieczęci	26
Wykaz załączników do Planu Ochrony Informacji Niejawnych	27
Wzory pism i upoważnień	42
Plan postępowania z materiałami zawierającymi informacje niejawne stanowiące tajemnicę państwową i służbową w razie wprowadzenia stanu nadzwyczajnego w Urzędzie Miejskim w Stąporkowie	53
Wymagania w zakresie ochrony informacji niejawnych oznaczonych klauzulą „zastrzeżone”	58
Instrukcja alarmowa w przypadku zgłoszenia o podłożeniu lub znalezieniu ładunku wybuchowego w Urzędzie	62
Instrukcja postępowania w przypadku otrzymania przesyłki niewiadomego pochodzenia	65

I. Akty prawne związane z ochroną informacji niejawnych

Plan Ochrony Informacji Niejawnych w Urzędzie Miejskim w Stąporkowie określa zasady i tryb postępowania z informacjami niejawnymi oraz zapewnia jednolity sposób postępowania z tymi informacjami.

Podstawowe akty prawne regulujące realizację zadań:

1. Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2018 r., poz. 412 ze zm.).
2. Rozporządzenie Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych (Dz. U. z 2017 r., poz. 1558).
3. Rozporządzenie Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzuli tajności (Dz. U. z 2011 r., Nr 288, poz. 1692) .
4. Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie wzorów zaświadczeń stwierdzających odbycie szkolenia w zakresie ochrony informacji niejawnych oraz sposobu rozliczania kosztów przeprowadzenia szkolenia przez Agencję Bezpieczeństwa Wewnętrznego lub Służbę Kontrwywiadu Wojskowego (Dz. U. z 2015 r., poz. 205).
5. Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie wzorów poświadczeń bezpieczeństwa (Dz. U. z 2015 r., poz. 220).
6. Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań teleinformatycznych (Dz. U. z 2011 r., Nr 159, poz. 948).
7. Rozporządzenie Prezesa Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne (Dz. U. z 2011 r., Nr 271, poz. 1603).

II. Definicje używane w Planie 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 organ 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** – zdolność osoby do spełniania ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem, stwierdzona w wyniku przeprowadzenia postępowania sprawdzającego.
- 2) **Dokument** - każda utrwalona informacja niejawna.
- 3) **Material** – dokument lub przedmiot albo dowolna ich część, chronione jako informacja niejawna.
- 4) **Przetwarzanie informacji niejawnych** – wszelkie operacje wykonywane w odniesieniu do informacji niejawnych i na tych informacjach, w szczególności ich wytwarzanie, modyfikowanie, kopiowanie, klasyfikowanie, gromadzenie, przechowywanie, przekazywanie lub udostępnienie.
- 5) **Jednostka organizacyjna** – podmiot wymieniony w art. 1 ust. 2 ustawy o ochronie informacji niejawnych.
- 6) **System teleinformatyczny** – jest to system w rozumieniu art. 2 pkt 3 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2017 r., poz. 1219 ze zm.).
- 7) **Sieć teleinformatyczna** – organizacyjne i techniczne połączenie systemów teleinformatycznych.
- 8) **Akredytacja bezpieczeństwa teleinformatycznego** – dopuszczenie systemu teleinformatycznego do przetwarzania informacji niejawnych.
- 9) **Dokumentacja bezpieczeństwa systemu teleinformatycznego** – dokument szczególnych wymagań bezpieczeństwa oraz dokument procedur bezpiecznej eksploatacji systemu teleinformatycznego, opracowane zgodnie z zasadami określonymi w ustawie.
- 10) **Urząd** – Urząd Miejski w Stąporkowie.
- 11) **Kierownik jednostki organizacyjnej** – burmistrz Stąporkowa.
- 12) **Pełnomocnik** – pełnomocnik do spraw ochrony informacji niejawnych w Urzędzie Miejskim w Stąporkowie.
- 13) **Kierownik kancelarii materiałów niejawnych** – osoba wyznaczona przez kierownika

jednostki organizacyjnej do prowadzenia kancelarii materiałów niejawnych.

- 14) **Pion ochrony** – zespół pracowników Urzędu Miejskiego w Stąporkowie wykonujących zadania związane z ochroną informacji niejawnych.
- 15) **Kancelaria materiałów niejawnych** – wydzielone, wyodrębnione miejsce (pomieszczenie), w którym odbywają się czynności związane z przetwarzaniem informacji niejawnych, tj. ewidencjonowanie, opracowywanie, przechowywanie, zapewnianie prawidłowego obiegu, wydawanie dokumentów lub materiałów zawierających informacje niejawne o klauzuli „zastrzeżone”.
- 16) **Ryzyko** – kombinacja prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji.
- 17) **Szacowanie ryzyka** – całościowy proces analizy i oceny ryzyka.
- 18) **Zarządzanie ryzykiem** – skoordynowane działania w zakresie zarządzania bezpieczeństwem informacji, z uwzględnieniem ryzyka.
- 19) **Poświadczenie bezpieczeństwa** – dokument uprawniający do dostępu do informacji niejawnych o wskazanej w nim klauzuli tajności przez okres na jaki zostało wydane.

III. Ocena zagrożeń zewnętrznych i wewnętrznych

Ocena zagrożeń zewnętrznych

Zagrożeniami zewnętrznymi dla Urzędu Miejskiego w Stąporkowie są:

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

Symptomy mogące świadczyć o przygotowaniu napadu lub włamania do budynku:

- wzmożone zainteresowanie osób postronnych obiektem, pomieszczeniami urzędu, przejawiające się m.in. podejmowaniem prób uzyskania informacji o danym obiekcie, pomieszczeniu, od pracowników podczas luźnych rozmów po „przypadkowym” spotkaniu,
- nawiązaniem rozmów przez osoby postronne z pracownikami,
- podszywanie się pod byłych pracowników urzędu i przejawianie zainteresowania tym, co zmieniło się po latach,
- interesowanie się osobami funkcyjnymi, w tym także ich przywarami oraz sposobem wykonywania obowiązków służbowych,
- obserwacja sposobu działania systemu ochronnego, sekretariatu, sprzątaczk, 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 to głównie osób mających problemy finansowe, towarzyskie, a także służbowe).

WNIOSKI:

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

- prowadzić systematyczną, skrupulatną i wnikliwą kontrolę systemu ochrony przez osoby odpowiedzialne za jego organizację,
- pracownicy pionu ochrony w czasie dnia pracy powinni zwracać szczególną uwagę na możliwość zaistnienia ewentualnych zagrożeń,
- stosować zasadę niedopuszczenia osób niepowołanych do penetracji miejsc przechowywania dokumentów niejawnych,
- wykonywać prace porządkowe, remontowe itp. wyłącznie pod nadzorem osób odpowiedzialnych.

Ocena zagrożeń wewnętrznych

Zagrożeniami wewnętrznymi dla Urzędu Miejskiego w Stąporkowie są:

- 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 Miejskiego w celu łatwiejszej pracy grup przestępczych na terenie urzędu,
- próby wglądu w dokumenty niejawne przez osoby nieuprawnione.

WNIOSKI:

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

- zwracać szczególną uwagę na osoby, które mogą być zainteresowane zaborem dokumentów,
- prowadzić szczególny nadzór, by nie dokonywano prób kserowania, kopiowania bez zgody przełożonego,
- uwrażliwić pracowników w trakcie prowadzonych szkoleń na możliwość prób kontaktu grup przestępczych z pracownikami, którzy mają dostęp do dokumentów szczególnie

wrażliwych,

- zastosować zasady, że do informacji niejawnych mogą mieć dostęp tylko pracownicy posiadający poświadczenie bezpieczeństwa lub właściwe upoważnienie wydane przez kierownika jednostki organizacyjnej.

IV. Przedmiot ochrony

Przedmiotem ochrony w Urzędzie Miejskim w Stąporkowie są

- informacje niejawne oznaczone klauzulą „zastrzeżone” i „poufne”.
- pomieszczenia, w których są przechowywane i opracowywane materiały niejawne.

V. Ewidencja informacji niejawnych podlegających ochronie

1. Klauzulę tajności nadaje osoba, która jest uprawniona do wytworzenia i podpisywania dokumentu wyłącznie w zakresie posiadanego prawa dostępu do informacji niejawnych.
2. Informacje niejawne oznaczone klauzulą „zastrzeżone” muszą być ewidencjonowane w wydzielonym, wyodrębnionym pomieszczeniu spełniającym wymogi wynikające z przepisów ustawy o ochronie 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 opisu dokumentu niejawnego został przedstawiony w **Załączniku Nr 1** do Planu Ochrony Informacji Niejawnych.
9. Prowadzi się również Rejestr Dzienników służący do ewidencjonowania książek, rejestrów i Dzienników Ewidencyjnych.
10. Pracownik Urzędu dokonujący odbioru przesyłki niejawnej sprawdza:
 - 1) prawidłowość oznaczenia adresu;

-
- 2) całość pieczęci i opakowania;
 - 3) zgodność odcisku pieczęci na opakowaniu z nazwą jednostki organizacyjnej nadawcy,
 - 4) zgodność numerów na przesyłce z numerami na wykazie przesyłek nadanych lub w książce doręczeń.

11. W przypadku stwierdzenia uszkodzenia przesyłki lub śladów jej otwarcia, osoba kwitująca odbiór przesyłki sporządza wraz z doręczającym, protokół uszkodzenia. Jeden egzemplarz protokołu przekazuje się nadawcy, drugi – pełnomocnikowi do spraw ochrony informacji niejawnych w Urzędzie, a w przypadku, gdy w obiegu przesyłek pośredniczył przewoźnik – kolejny egzemplarz protokołu przekazuje się także jemu. Fakt sporządzenia protokołu kierownik kancelarii materiałów niejawnych odnotowuje w Dzienniku Ewidencyjnym w rubryce nr 18 (Informacje uzupełniające/Uwagi). Wzór Protokołu uszkodzenia przesyłki niejawnej stanowi **Załącznik Nr 2 do Planu Ochrony Informacji Niejawnych**.

12. Pracownik kancelarii materiałów niejawnych:

- 1) sprawdza, czy zawartość przesyłki odpowiada wyszczególnionym na niej numerom ewidencyjnym;
- 2) ustala, czy liczba stron lub innych jednostek miary oraz załączników jest zgodna z liczbą podaną na poszczególnych dokumentach.

13. W przypadku stwierdzenia nieprawidłowości w wyniku czynności, o których mowa powyżej, pracownik kancelarii materiałów niejawnych sporządza w dwóch egzemplarzach protokół z otwarcia przesyłki zawierający opis tych nieprawidłowości, przykazując jeden egzemplarz do kancelarii nadawcy. Wzór Protokołu otwarcia przesyłki niejawnej stanowi **Załącznik Nr 3 do Planu Ochrony Informacji Niejawnych**.

14. Pracownik kancelarii materiałów niejawnych odnotowuje fakt sporządzenia protokołu, o którym mowa w pkt. 12 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 kancelarii materiałów niejawnych, zabezpieczone zgodnie z przepisami ustawy o ochronie informacji niejawnych.
2. Informacje niejawne oznaczone klauzulą „zastrzeżone” można przechowywać na stanowisku pracy, w meblach biurowych zamykanych na klucz, pod warunkiem spełniania wymogów bezpieczeństwa odpowiednich do tej klauzuli.

VII. Zasady dostępu do informacji niejawnych oznaczonych klauzulą „zastrzeżone”

1. Informacje niejawne mogą być udostępniane wyłącznie osobie uprawnionej do dostępu do informacji niejawnych o określonej klauzuli tajności.

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; **Wzór Upoważnienia stanowi załącznik Nr 4 do Planu Ochrony Informacji Niejawnych.**
- po przeszkoleniu danej osoby w zakresie przepisów ustawy o ochronie informacji niejawnych i uzyskaniu odpowiedniego zaświadczenia stwierdzającego odbycie takiego szkolenia. **Wzór Zaświadczenia stwierdzającego odbycie szkolenia stanowi Załącznik Nr 5 do Planu Ochrony Informacji Niejawnych.**

3. Uzyskanie uprawnień dostępu do informacji o klauzuli „poufne” może nastąpić:

- po uzyskaniu przez pracownika poświadczenia bezpieczeństwa po przeprowadzonym przez Pełnomocnika do spraw ochrony informacji niejawnych zwykłym postępowaniu sprawdzającym. **Wzór Poświadczenia Bezpieczeństwa stanowi Załącznik Nr 6 do Planu Ochrony Informacji Niejawnych.**
- po przeszkoleniu danej osoby w zakresie przepisów ustawy o ochronie informacji niejawnych i uzyskaniu odpowiedniego zaświadczenia o przeszkoleniu.

4. Zwykłe postępowanie sprawdzające wobec pracowników jednostki w związku z dostępem do informacji niejawnych oznaczonych klauzulą „poufne” na pisemne polecenie kierownika jednostki przeprowadza Pełnomocnik do spraw ochrony informacji niejawnych. **Wzór Polecenia wszczęcia zwykłego postępowania sprawdzającego stanowi Załącznik Nr 7 do Planu Ochrony Informacji Niejawnych.**

5. Osoba podlegająca procedurze postępowania sprawdzającego zobowiązana jest do:

- wypełnienia określonej przepisami ustawy ankiety bezpieczeństwa osobowego,
- 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 „poufne”, a w związku z tym nie uzyskanie poświadczenia bezpieczeństwa warunkującego dostęp do informacji oznaczonych klauzulą „poufne” może skutkować:

- przeniesieniem danej osoby na stanowisko nie związane z informacjami niejawnymi o klauzuli „poufne”
- rozwiązaniem umowy o pracę w przypadku niemożności zmiany stanowiska,

- niemożnością zatrudnienia na danym stanowisku, w przypadku ubiegania się o zatrudnienie w Urzędzie.

7. Szkolenie kierownika jednostki organizacyjnej w związku z dostępem do informacji niejawnych oznaczonych klauzulą „zastrzeżone” przeprowadza Pełnomocnik do spraw ochrony informacji niejawnych, wydając stosowne zaświadczenie.

VIII. Kancelaria materiałów niejawnych

1. W Urzędzie Miejskim w Stąporkowie funkcjonuje kancelaria materiałów niejawnych, która została utworzona dla potrzeb jednostki, dla właściwego przechowywania, ewidencjonowania materiałów niejawnych oznaczonych klauzulą „zastrzeżone”.

2. Organizacja pracy kancelarii materiałów 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. **Wzór Karty zapoznania się z dokumentem stanowi Załącznik Nr 8 do Planu Ochrony Informacji Niejawnych.**

3. Dla zapewnienia prawidłowej organizacji pracy kancelarii prowadzi się następujące dzienniki ewidencji:

- 1) rejestr dzienników ewidencji i teczek,
- 2) dziennik ewidencyjny,
- 3) książkę doręczeń przesyłek miejscowych,
- 4) wykaz przesyłek nadanych,
- 5) rejestr wydanych przedmiotów.

4. Kancelaria materiałów niejawnych odmawia udostępnienia lub wydania materiału osobie nieuprawnionej.

5. Kancelarię materiałów niejawnych tworzy kierownik jednostki organizacyjnej.

6. Kancelarią kieruje wyznaczony przez kierownika jednostki organizacyjnej kierownik kancelarii materiałów niejawnych, który bezpośrednio podlega pełnomocnikowi do spraw ochrony informacji niejawnych. Do podstawowych zadań kierownika kancelarii należy:

- bezpośredni nadzór nad obiegiem dokumentów;
- udostępnianie, wydawanie materiałów zawierających informacje niejawne osobom do tego uprawnionym;
- egzekwowanie zwrotu materiałów,
- kontrola przestrzegania właściwego oznaczenia i rejestrowania materiałów niejawnych w kancelarii;

-
- prowadzenie bieżącej kontroli postępowania z dokumentami zawierającymi informacje niejawne;
 - współpraca z Pełnomocnikiem do spraw ochrony informacji niejawnych w zakresie przepisów wynikających z ustawy o ochronie informacji niejawnych.

7. W przypadku zmiany na stanowisku kierownika kancelarii materiałów niejawnych sporządza się protokół zdawczo-odbiorczy. **Wzór Protokołu zdawczo-odbiorczego materiałów i dokumentów zawierających informacje niejawne stanowi Załącznik Nr 9 do Planu Ochrony Informacji Niejawnych.**

8. Protokół, o którym mowa w pkt. 7 sporządza się w obecności pracownika zdającego obowiązki, osoby przejmującej oraz Pełnomocnika do spraw ochrony informacji niejawnych. Protokół sporządza się w dwóch egzemplarzach: pierwszy przechowywany jest w kancelarii materiałów niejawnych, drugi – u Pełnomocnika ochrony informacji niejawnych.

9. W przypadku czasowej nieobecności pracownika kancelarii jego obowiązki przejmuje upoważniony pracownik pionu ochrony (pełnomocnik oin). W razie braku tych osób, kancelarię przejmuje protokolarnie inny pracownik wyznaczony przez kierownika jednostki na wniosek pełnomocnika do spraw ochrony informacji niejawnych.

10. W pomieszczeniach kancelarii można wydzielić miejsce, w którym osoby upoważnione mogą zapoznać się z dokumentami – czytelną. Organizacja czytelną:

- czytelną powinna być zorganizowana w sposób umożliwiający stały nadzór ze strony pracownika kancelarii;
- w czytelną zabrania się instalowania systemu nadzoru wizyjnego.

11. Po zakończeniu pracy pracownik kancelarii lub upoważniony pracownik kancelarii jest obowiązany sprawdzić prawidłowość zamknięcia szafy i pomieszczenia kancelarii.

12. Klucze do szafy metalowej należy złożyć w pomieszczeniu kancelarii w miejscu niewidocznym. Po zakończeniu pracy pracownik kancelarii zamyka na klucz drzwi wejściowe kancelarii, a klucze pozostawia w miejscu niewidocznym.

13. Wszelkie nieprawidłowości związane z naruszeniem zasad określonych powyżej należy niezwłocznie zgłaszać pełnomocnikowi do spraw ochrony informacji niejawnych.

POSTĘPOWANIE Z PRZESYŁKAMI

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

2. Przyjmując przesyłkę sprawdza:

- prawidłowość adresu;

-
- całość pieczęci i opakowania;
 - zgodność odcisku pieczęci na opakowaniu z nazwą jednostki nadawcy;
 - 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 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. Wzór Protokołu uszkodzenia przesyłki niejawnej stanowi Załącznik Nr 2 do Planu Ochrony Informacji Niejawnych.

4. Po otwarciu przesyłki 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, pracownik kancelarii sporządza protokół z otwarcia przesyłki zawierający opis nieprawidłowości, przekazując jeden egzemplarz do kancelarii nadawcy. Wzór Protokołu otwarcia przesyłki niejawnej stanowi Załącznik Nr 3 do Planu Ochrony Informacji Niejawnych.

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

7. W kancelarii 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 pisemnie 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 materiałów niejawnych przesyłki adresowanej „do rąk własnych” pracownik kancelarii uzupełnia dane dotyczące przesyłki w odpowiednim dzienniku

lub rejestrze.

11. Jeżeli adresat podjął decyzję o przechowaniu w kancelarii przesyłki oznaczonej „do rąk własnych” w stanie zamkniętym, pracownik kancelarii dokonuje czynności, o których mowa powyżej, 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 albo wysłaną przesyłkę bądź wytworzony dokument rejestruje się odpowiednio w kolejności otrzymania, wysłania lub wytworzenia.

14. Wszelkich adnotacji w Dzienniku Ewidencyjnym dokonuje się atramentem lub tuszem w kolorze niebieskim lub czarnym, natomiast zmiany kolorem czerwonym, umieszczając datę i czytelny podpis osoby dokonującej zmiany. Zabrania się wycierania i zamazywania zapisów dokonanych w Dzienniku Ewidencyjnym.

15. W przypadku anulowania pozycji w Dzienniku Ewidencyjnym podaje się powód anulowania, umieszczając datę, imię i nazwisko oraz podpis osoby dokonującej anulowania. Anulowania pozycji dokonuje się kolorem czerwonym.

16. Dokumenty, materiały oraz zbiory dokumentów dotyczące spraw ostatecznie zakończonych przechowuje się w kancelarii materiałów niejawnych do czasu zniesienia okresu ochronnego. Po upływie tego okresu przekazuje się do archiwum zakładowego.

OBOWIĄZKI PRACOWNIKA KANCELARII MATERIAŁÓW NIEJAWNYCH

1. Przed otwarciem drzwi należy sprawdzić stan zamków i zabezpieczeń.
2. Sprawdzić stan zabezpieczenia szafy lub mebli biurowych, w których przechowywane są materiały niejawne.
3. Przestrzegać zasad zakazu wstępu osobom nieuprawnionym do kancelarii materiałów niejawnych.

IX. Zakres udostępniania informacji niejawnych

1. Informacje niejawne mogą być udostępniane wyłącznie osobie dającej rękojmię zachowania tajemnicy i tylko w zakresie niezbędnym do wykonywania przez nią pracy lub pełnienia służby na zajmowanym stanowisku albo wykonywania czynności zleconych.
2. Udostępnianie informacji niejawnych o klauzuli „poufne” lub „zastrzeżone” osobie może

nastąpić w oparciu o ważne Poświadczenie Bezpieczeństwa lub pisemne Upoważnienie kierownika jednostki organizacyjnej.

X. Zasady wykonywania dokumentów niejawnych

1. Informacje niejawne oznaczone klauzulą „zastrzeżone” wytworzone w Urzędzie w formie dokumentu pisanego mogą być: sporządzane odręcznie, na wcześniej przygotowanych szablonach (szablony przygotowuje się w komputerze, a treść niejawną wpisuje się odręcznie w pomieszczeniu kancelarii materiałów niejawnych), na maszynie do pisania (bez pamięci) lub na komputerze, który uzyskał akredytację bezpieczeństwa teleinformatycznego zatwierdzoną przez Burmistrza.
2. Propozycję przyznania klauzuli tajności na wykonywanym dokumencie przedstawia osoba sporządzająca ten dokument.
3. Klauzulę tajności na danym dokumencie przyznaje osoba, która jest upoważniona do opisanie dokumentu.
4. Dokumenty niejawne powinny być opisane i oznaczone zgodnie z Rozporządzeniem Prezesa rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania i umieszczania na nich klauzuli tajności (Dz. U. z 2011 r., Nr 288, poz. 1692).

XI. 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;
 - 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.

4. Ochrona fizyczna systemu lub sieci teleinformatycznej polega na:

- umieszczeniu urządzeń systemu lub sieci teleinformatycznej w strefie ochronnej, zwanej również „strefą kontrolowanego dostępu”, w zależności od:
 - klauzuli tajności;
 - ilości;
 - zagrożeń dla poufności, integralności lub dostępności informacji niejawnych.
 - zastosowaniu środków zapewniających ochronę fizyczną, w szczególności przed:
 - nieuprawnionym dostępem;
 - podglądem;
 - podsłuchem.

5. Ochrona elektromagnetyczna systemu lub sieci teleinformatycznej polega na:

- niedopuszczaniu 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;
- 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 specjalnych wymagań 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:

- kierownik jednostki organizacyjnej lub osoba przez niego upoważniona ustala warunki i sposób przydzielania uprawnień osobom uprawnionym do pracy w systemie lub sieci teleinformatycznej;
- 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. Systemy i sieci teleinformatyczne, w których mają być wytwarzane, przetwarzane,

przechowywane lub przekazywane informacje niejawne, podlegają akredytacji bezpieczeństwa teleinformatycznego przez służby ochrony państwa.

10. Akredytacji udziela się na czas określony, nie dłuższy niż 5 lat.

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

12. ABW udziela akredytacji bezpieczeństwa teleinformatycznego dla systemu teleinformatycznego przeznaczonego do przetwarzania informacji niejawnych.

13. ABW udziela lub odmawia udzielenia akredytacji, o której mowa w pkt. 12 w terminie 6 miesięcy od otrzymania kompletnej dokumentacji bezpieczeństwa systemu teleinformatycznego. W uzasadnionych przypadkach, w szczególności wynikających z rozległości systemu i stopnia jego skomplikowania, termin ten może być przedłużony o kolejne 6 miesięcy. Od odmowy udzielenia akredytacji nie służy odwołanie.

14. Potwierdzeniem udzielenia przez ABW akredytacji, o której mowa w pkt. 13, jest świadectwo akredytacji bezpieczeństwa systemu teleinformatycznego.

15. Świadectwo, o którym mowa w pkt. 14, wydaje się na podstawie:

- zatwierdzonej przez ABW dokumentacji bezpieczeństwa systemu teleinformatycznego;
- wyników audytu bezpieczeństwa systemu teleinformatycznego przeprowadzonego przez ABW.

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

17. W ciągu 30 dni od udzielenia akredytacji bezpieczeństwa teleinformatycznego, o której mowa w pkt. 16, kierownik jednostki organizacyjnej przekazuje ABW dokumentację bezpieczeństwa systemu teleinformatycznego.

18. 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.

19. 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.

20. Dokument szczególnych wymagań bezpieczeństwa opracowuje się na etapie projektowania, w razie potrzeby konsultuje się z ABW, na bieżąco uzupełnia się na etapie wdrażania i modyfikuje na etapie eksploatacji przed dokonaniem zmian w systemie teleinformatycznym.

21. **Dokument procedur bezpiecznej eksploatacji** opracowuje się na etapie wdrażania oraz modyfikuje na etapie eksploatacji przed dokonaniem zmian w systemie teleinformatycznym.

22. Podstawą dokonania wszelkich zmian w systemie teleinformatycznym jest przeprowadzenie procesu szacowania ryzyka dla bezpieczeństwa informacji niejawnych przetwarzanych w tym systemie.

23. Kierownik jednostki organizacyjnej akceptuje wyniki procesu szacowania ryzyka dla bezpieczeństwa informacji niejawnych oraz jest odpowiedzialny za właściwą organizację bezpieczeństwa teleinformatycznego.

24. 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.

25. Kierownik jednostki organizacyjnej wyznacza:

- 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;
- osobę lub zespół osób nie pełniących funkcji inspektora bezpieczeństwa teleinformatycznego, odpowiedzialnych za funkcjonowanie systemu teleinformatycznego oraz za przestrzeganie zasad i wymagań bezpieczeństwa przewidzianych dla systemu teleinformatycznego, zwanych „administratorem systemu”.

26. W sytuacjach wymagających konsultacji lub uzgodnień, kierownik jednostki organizacyjnej może zwrócić się do ABW o wydanie opinii lub zaleceń w zakresie bezpieczeństwa

teleinformatycznego.

27. Stanowiska lub funkcje Administratora Systemu oraz Inspektora Bezpieczeństwa Teleinformatycznego mogą zajmować lub pełnić osoby posiadające poświadczenie 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.

28. 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.
2. Sposób przechowywania zapasowych kopii jest identyczny jak przechowywanie dokumentów wykonywanych 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 to niemożliwe – na ich obudowie lub opakowaniu.

XII. Gromadzenie dokumentów zawierających informacje niejawne

1. Dokumenty zawierające informacje niejawne powinny być przechowywane zgodnie z rzeczowym podziałem akt.
2. Dokumenty niejawne o klauzuli „zastrzeżone” są przechowywane w kancelarii materiałów niejawnych lub na stanowiskach pracy w meblach biurowych zamykanych na klucz, pod warunkiem spełniania wymogów bezpieczeństwa odpowiednich do tej klauzuli.

XIII. Oznaczanie, nadawanie, zmiana i znoszenie klauzuli niejawności materiałom niejawnym

1. Poprzez oznaczanie należy rozumieć czynność techniczną nanoszenia na materiał informacji określonych w Rozporządzeniu Prezesa Rady Ministrów z 22 grudnia 2011 r. w sprawie sposobu oznaczania i umieszczania na nich klauzuli tajności (Dz. U. z 2011 r., Nr 288, poz. 1692), w tym umieszczania na nim klauzuli tajności oraz nanoszenia informacji o zmianie lub zniesieniu nadanej klauzuli, a także umieszczania informacji w metryce dokumentu

elektronicznego.

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

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

4. Osoba, o której mowa w pkt. 2 może określić datę lub wydarzenie, po których nastąpi zniesienie lub zmiana klauzuli tajności.

5. Zniesienie lub zmiana klauzuli tajności są możliwe wyłącznie po wyrażeniu zgody przez osobę, o której mowa w pkt. 2 albo jej przełożonego w przypadku ustania lub zmiany ustawowych przesłanek ochrony.

6. Nie rzadziej niż raz na 5 lat należy dokonać przeglądu materiałów niejawnych celem ustalenia, czy spełniają ustawowe przesłanki ochrony.

7. 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 klauzuli tajności.

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

9. Oznaczenie materiału klauzulą tajności polega na umieszczeniu na nim klauzuli tajności.

10. Przyznaną klauzulę tajności nanosi się w sposób wyraźny i w pełnym jej brzmieniu.

11. Dla klauzuli tajności „zastrzeżone” wprowadza się oznaczenie „Z”.

12. Materiały zawierające informacje niejawne utrwalone na piśmie oznacza się w następujący sposób:

1) na każdej stronie pisma umieszcza się:

a) na środku, jako pierwszy element w nagłówku strony, klauzulę tajności,

b) numer egzemplarza, a w przypadku gdy dokument wykonano w jednym egzemplarzu, napis „egz. pojedynczy”,

c) sygnaturę literowo-cyfrową, na którą składają się: literowe oznaczenie jednostki lub komórki organizacyjnej, symbol oznaczenia klauzuli tajności, numer, pod którym ten dokument został zarejestrowany i rok, w którym dokonano rejestracji, a także, w zależności od potrzeb, inne oznaczenia ułatwiające ustalenie miejsca wykonywania dokumentu w jednostce lub komórce organizacyjnej lub też jego przynależność do określonej sprawy,

d) numer strony oraz liczbę stron całego dokumentu,

e) na środku, jako ostatni element w stopce strony, klauzulę tajności;

2) na pierwszej stronie umieszcza się również:

-
- a) nazwę jednostki lub komórki organizacyjnej,
 - b) nazwę miejscowości i datę podpisania dokumentu,
 - c) pod numerem egzemplarza dodatkowe dyspozycje takie jak, np. „jawne po odłączeniu załączników” lub „podlega ochronie do dnia ...”, jeżeli został określony krótszy okres ochronny niż wynika to z ustawy,
 - d) w przypadku dokumentu, któremu nadano bieg korespondencyjny, 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";

3) na ostatniej stronie pod treścią umieszcza się:

- a) liczbę załączników,
- b) liczbę stron lub innych jednostek miary wszystkich załączników lub informację określającą rodzaj załączonego materiału i jego odpowiednią jednostkę miary,
- c) klauzulę tajności załączników wraz z numerami, pod jakimi zostały zarejestrowane w „Dzienniku Ewidencyjnym” oraz liczbę stron każdego załącznika lub informację określającą rodzaj załączonego materiału i jego odpowiednią jednostkę miary,
- d) 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, lub napis "do zwrotu" - jeżeli załączniki mają zostać zwrócone nadawcy,
- e) stanowisko oraz imię i nazwisko lub inne oznaczenie wskazujące osobę uprawnioną do jego podpisania,
- f) liczbę wykonanych egzemplarzy,
- g) adresatów poszczególnych egzemplarzy dokumentu albo adnotację "adresaci według rozdzielnika",
- h) dyspozycję "ad acta" w przypadku egzemplarza pozostającego w aktach nadawcy,
- i) imię i nazwisko lub inne oznaczenie wskazujące wykonawcę.

4) Na dokumencie nieelektronicznym można zamieścić dyspozycję dotyczącą:

- a) braku zgody na kopiowanie lub tłumaczenie części albo całości dokumentu;
- b) braku zgody na udzielanie informacji o treści dokumentu;
- c) określenia daty lub wydarzenia, po którym nastąpi zniesienie lub zmiana klauzuli tajności całości lub części dokumentu.

5) W przypadkach uzasadnionych organizacją ochrony informacji niejawnych na materiałach zawierających informacje niejawne można nanosić w sposób czytelny, widoczny i trwały dodatkowe oznaczenia, inne niż wymienione powyżej.

6) Na pismach stanowiących załączniki:

- a) na pierwszej stronie umieszcza się dodatkowo informację: „Załącznik nr ... do dokumentu nr ... z dnia ...”,
- b) jeżeli wraz z dokumentem przesyła się załączniki zawierające informacje niejawne to dokument oznacza się klauzulą tajności nie niższą niż najwyższa klauzula tajności załączników,
- c) na dokumencie – jeżeli po trwałym odłączeniu załączników dokument jest jawny albo jego klauzula tajności jest inna niż określona zgodnie z pkt b) – na każdej stronie pod numerem egzemplarza umieszcza się adnotację o jawności albo klauzulę tajności dokumentu po odłączeniu załączników.

7) Na materiałach innych niż pismo:

- a) 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 możliwe – na ich obudowie lub opakowaniu.

8) Na trwale oprawionych zbiorach dokumentów, rejestrach, książkach, broszurach i reprodukcjach:

- a) klauzulę tajności umieszcza się po środku, na górze i na dole zewnętrznych ścianek okładki oraz jeżeli jest – na stronie tytułowej.

13. Zgody na zniesienie lub zmianę klauzuli tajności udziela się w odrębnym dokumencie podlegającym rejestracji i przechowywaniu w kancelarii materiałów niejawnych lub przez oznaczenie w postaci umieszczenia informacji:

- a) na dokumencie – w przypadku dokumentu nieelektronicznego;
- b) w metryce dokumentu – w przypadku dokumentu elektronicznego.

14. Oznaczenia zniesienia klauzuli tajności na dokumencie nieelektronicznym utrwalonym w formie pisma dokonuje się następująco:

- a) skreśla się wszystkie dotychczasowe oznaczenia znoszonej klauzuli tajności;
- b) nad pierwszym w kolejności skreślonym oznaczeniem klauzuli tajności umieszcza się napis "Zniesiono klauzulę tajności" oraz datę, podpis, imię i nazwisko lub inne oznaczenie wskazujące osobę dokonującą tych adnotacji oraz wskazuje się podstawę dokonania czynności.

15. Oznaczenia zmiany klauzuli tajności na dokumencie nieelektronicznym, dokonuje się następująco:

- a) skreśla się wszystkie dotychczasowe oznaczenia klauzuli tajności;
- b) nad skreślonymi oznaczeniami klauzul tajności umieszcza się oznaczenie nowej klauzuli tajności;

c) nad pierwszym w kolejności skreślonym oznaczeniem klauzuli tajności umieszcza się datę, podpis, imię i nazwisko lub inne oznaczenie wskazujące osobę dokonującą tych adnotacji oraz wskazuje się podstawę dokonania czynności.

16. Skreśleń i adnotacji, o których mowa powyżej dokonują: kierownik kancelarii materiałów niejawnych, kierownik archiwum lub jego zastępca, w której są rejestrowane materiały niejawne lub inne osoby upoważnione przez nich bądź przez kierownika jednostki organizacyjnej.

17. Skreśleń i adnotacji, o których mowa powyżej dokonuje się kolorem czerwonym w sposób czytelny. Wycieranie, wywabianie lub zamazywanie klauzuli tajności i dokonywanych zmian jest niedozwolone.

18. Pozostałe czynności związane z oznaczaniem, zmianą lub znoszeniem klauzuli tajności wynikają z Rozporządzenia Prezesa Rady Ministrów z 22 grudnia 2011 r. w sprawie sposobu oznaczania i umieszczania na nich klauzuli tajności (Dz. U. z 2011 r., Nr 288, poz. 1692).

XIV. Okresy ochronne i nadzór w zakresie ochrony informacji niejawnych

1. Informacje niejawne podlegają ochronie do czasu zniesienia lub zmiany klauzuli tajności.
2. Zniesienie lub zmiana klauzuli tajności są możliwe wyłącznie po wyrażeniu pisemnej zgody przez osobę, która nadała klauzulę tajności i jest uprawniona do podpisywania dokumentu lub oznaczenia innego niż dokument materiału albo jej przełożonego w przypadku ustania lub zmiany ustawowych przesłanek.

XV. 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 (Dz. U. z 2018 r., poz. 1600 ze zm.) - 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 zabezpieczenia dokumentów, stwarzają warunki do ujawnienia tajemnicy osobom nieuprawnionym, mogą być zastosowane sankcje służbowe i dyscyplinarne.

XVI. Archiwizowanie, gromadzenie i niszczenie materiałów niejawnych

1. Archiwizowanie materiałów niejawnych odbywa się z zachowaniem zasad określonych w Rozporządzeniu Ministra Kultury i Dziedzictwa Narodowego z dnia 20 października 2015 r. w sprawie klasyfikowania i kwalifikowania dokumentacji, przekazywania materiałów archiwalnych do archiwów państwowych i brakowania dokumentacji niearchiwalnej (Dz. U. z 2015 r., poz. 1743).

2. Dokumentacja wytworzona i gromadzona dzieli się na:

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

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

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

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

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

7. Brakowanie dokumentacji niearchiwalnej następuje na podstawie zgody.

8. Zgodę, o której mowa, wyraża dyrektor miejscowo właściwego archiwum państwowego.

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

10. 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.

11. 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 kierownik kancelarii materiałów niejawnych.

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

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

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

15. 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.

16. Opisywanie materiałów archiwalnych polega na umieszczeniu na wierzchniej stronie każdejteczki:

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

17. Czynności związane z brakowaniem materiałów niearchiwalnych, wobec których archiwum państwowe wyraziło zgodę, są dokumentowane przez sporządzenie protokołu komisijnego zniszczenia dokumentów niearchiwalnych.

18. Protokół komisijnego zniszczenia materiałów niearchiwalnych sporządzony jest w dwóch egzemplarzach, z czego jeden egzemplarz należy przesłać do właściwego archiwum państwowego.

XVII. Przechowywanie kluczy i pieczęci

Ustala się zasady gospodarki kluczami i pieczęciami:

1. Dokumenty niejawne oraz pieczęcie przechowuje się w szafie metalowej zamykanej na klucz. Dodatkowo może być zabezpieczona szyfrem trójliczbowym.
2. Klucze od szafy metalowej kancelarii materiałów niejawnych po zakończeniu pracy należy złożyć w pomieszczeniu kancelarii w miejscu niewidocznym i nieznanym powszechnie.
3. Drzwi do pomieszczenia, w którym przechowywane są dokumenty zastrzeżone są zamykane na klucz oraz dodatkowo zabezpieczane kratą metalową zamykaną na kłódkę. Klucze przechowuje się w miejscu niewidocznym. Okna pomieszczenia zabezpieczane są roletą metalową.
4. Zabrania się wynoszenia poza Urząd, jak również udostępniania kluczy do pomieszczeń oraz urządzeń biurowych, w których przechowywane są dokumenty niejawne oznaczone klauzulą „zastrzeżone” osobom nieuprawnionym. Pracownikom Urzędu zabrania się samodzielnego dokonywania wymiany zamków bez zgody ze strony pełnomocnika ochrony informacji niejawnych.
5. Pracownik kancelarii materiałów niejawnych po przybyciu do Urzędu sprawdza, czy nie zostały naruszone kłódki i zamki zabezpieczające dostęp do pomieszczenia, w którym przechowywane są dokumenty niejawne.

WYKAZ ZAŁĄCZNIKÓW

DO PLANU OCHRONY INFORMACJI NIEJAWNYCH

Załącznik Nr 1 – Sposób oznaczania dokumentów niejawnych oznaczonych klauzulą „zastrzeżone” oraz umieszczania klauzuli na tych dokumentach.

Załącznik Nr 2 Wzór protokołu uszkodzenia przesyłki niejawnej.

Załącznik Nr 3 Wzór Protokołu otwarcia przesyłki niejawnej.

Załącznik Nr 4 Wzór Upoważnienia uprawniającego do informacji niejawnych oznaczonych klauzulą „zastrzeżone”.

Załącznik Nr 5 Wzór Zaświadczenia stwierdzającego odbycie szkolenia w zakresie ochrony informacji niejawnych.

Załącznik Nr 6 Wzór Poświadczenia Bezpieczeństwa.

Załącznik Nr 7 Wzór Polecenia wszczęcia zwykłego postępowania sprawdzającego.

Załącznik Nr 8 Wzór Karty zapoznania się z dokumentem.

Załącznik Nr 9 Wzór protokołu zdawczo-odbiorczego materiałów/dokumentów zawierających informacje niejawne.

**ZAŁĄCZNIK Nr 1 SPOSÓB OZNACZANIA DOKUMENTÓW NIEJAWNYCH
OZNACZONYCH KLAUZULĄ ZASTRZEŻONE ORAZ UMIESZCZANIA KLAUZULI NA
TYCH DOKUMENTACH**

Pismo bez załączników – pierwsza strona

Zastrzeżone	
Egz. Nr lub egz. pojedynczy	
np. jawne po odłączeniu załączników	
lub Podlega ochronie do dnia	
Nazwa jednostki lub komórki organizacyjnej	Stąporków, dn.
Sygnatura literowo-cyfrowa	Imię i nazwisko lub nazwa adresata albo „adresaci według rozdzielnika”
Treść pisma	
<u>Pierwsza strona pisma</u>	
1/3	
Zastrzeżone	

Objaśnienie:

- 1) na środku, jako pierwszy element w nagłówku strony, klauzulę tajności;
- 2) nazwę jednostki lub komórki organizacyjnej;
- 3) nazwę miejscowości i datę podpisania dokumentu;
- 4) sygnaturę literowo-cyfrową, na którą składają się: literowe oznaczenie jednostki lub komórki organizacyjnej, symbol oznaczenia klauzuli tajności „zastrzeżone”, numer, pod którym ten dokument został zarejestrowany i rok, w którym dokonano rejestracji, a także, w zależności od potrzeb inne oznaczenia;
- 5) numer egzemplarza, a w przypadku, gdy dokument wykonano w jednym egzemplarzu, napis „egz. pojedynczy”;
- 6) w przypadku dokumentu, któremu nadano bieg korespondencyjny, 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”;

- 7) numer strony oraz liczbę stron całego dokumentu;
- 8) na środku, jako ostatni element w stopce strony, klauzulę tajności.

Pismo bez załączników – kolejna strona

Zastrzeżone Egz. Nr lub „egz. pojedynczy” Sygnatura literowo-cyfrowa Treść pisma <u>Kolejna strona pisma</u> 2/3 Zastrzeżone

Objaśnienie:

- 1) na środku, jako pierwszy element w nagłówku strony, klauzulę tajności;
- 2) sygnaturę literowo-cyfrową, na którą składają się: literowe oznaczenie jednostki lub komórki organizacyjnej, symbol oznaczenia klauzuli tajności „zastrzeżone”, numer, pod którym ten dokument został zarejestrowany i rok, w którym dokonano rejestracji, a także, w zależności od potrzeb inne oznaczenia;
- 3) numer egzemplarza, a w przypadku, gdy dokument wykonano w jednym egzemplarzu, napis „egz. pojedynczy”;
- 4) numer strony oraz liczbę stron całego dokumentu;
- 5) na środku, jako ostatni element w stopce strony, klauzulę tajności.

Pismo bez załączników - ostatnia strona

Zastrzeżone	
Egz. Nr lub „egz. pojedynczy”	
Sygnatura literowo-cyfrowa	
Treść pisma	
<u>Ostatnia strona pisma</u>	
Stanowisko oraz imię i nazwisko osoby uprawnionej do podpisania	
<u>Wykonano w 2 egz.</u>	
Egz. Nr 1 – adresat	
Egz. Nr 2 – a/a	
lub	
„adresaci według rozdzielnika”	
Wykonał:	
3/3	
Zastrzeżone	

Objaśnienie:

- 1) na środku, jako pierwszy element w nagłówku strony, klauzulę tajności;
- 2) sygnaturę literowo-cyfrową, na którą składają się: literowe oznaczenie jednostki lub komórki organizacyjnej, symbol oznaczenia klauzuli tajności „zastrzeżone”, numer, pod którym ten dokument został zarejestrowany i rok, w którym dokonano rejestracji, a także, w zależności od potrzeb inne oznaczenia;
- 3) numer egzemplarza, a w przypadku, gdy dokument wykonano w jednym egzemplarzu, napis „egz. pojedynczy”;
- 4) stanowisko oraz imię i nazwisko lub inne oznaczenie wskazujące osobę uprawnioną do jego podpisania;
- 5) liczbę wykonanych egzemplarzy;
- 6) adresatów poszczególnych egzemplarzy dokumentu albo adnotację „adresaci według rozdzielnika”;
- 7) dyspozycję „ad acta” w przypadku egzemplarza pozostającego w aktach nadawcy;
- 8) imię i nazwisko;
- 9) numer strony oraz liczbę stron całego dokumentu;
- 10) na środku, jako ostatni element w stopce strony, klauzulę tajności.

Wzór załącznika do pisma o klauzuli „zastrzeżone”

Zastrzeżone	
Egz. Nr lub egz. pojedynczy	
np. jawne po odłączeniu załączników	
lub Podlega ochronie do dnia	
Nazwa jednostki lub komórki organizacyjnej	Staporków, dn.
Sygnatura literowo-cyfrowa	
Treść pisma	
<u>Ostatnia strona pisma</u>	
Stanowisko oraz imię i nazwisko	
osoby uprawnionej do podpisania	
Załączników: 3, na 6 stronach.	
Załącznik Nr 1 – „zastrzeżone”, sygnatura literowo cyfrowa, na 2 stronach;	
Załącznik Nr 2 – „zastrzeżone”, sygnatura literowo cyfrowa, na 3 stronach, - „do zwrotu”;	
Załącznik Nr 3 – „zastrzeżone”, sygnatura literowo cyfrowa, na 1 stronie, - „tylko adresat”.	
<u>Wykonano w 2 egz.</u>	
Egz./ Nr 1 – adresat	
lub „adresaci według rozdzielnika”	
Egz. Nr 2 - a/a	
Wykonał:	
1/1	
Zastrzeżone	

Objaśnienie:

- 1) na środku, jako pierwszy element w nagłówku strony, klauzulę tajności;
- 2) sygnaturę literowo-cyfrową, na którą składają się: literowe oznaczenie jednostki lub komórki organizacyjnej, symbol oznaczenia klauzuli tajności „zastrzeżone”, numer, pod którym ten dokument został zarejestrowany i rok, w którym dokonano rejestracji, a także, w zależności od potrzeb inne oznaczenia;

-
- 3) numer egzemplarza, a w przypadku, gdy dokument wykonano w jednym egzemplarzu, napis „egz. pojedynczy”;
 - 4) stanowisko oraz imię i nazwisko lub inne oznaczenie wskazujące osobę uprawnioną do jego podpisania;
 - 5) liczbę załączników;
 - 6) liczbę stron lub innych jednostek miary wszystkich załączników;
 - 7) klauzule tajności załączników wraz z numerami, pod jakimi zostały zarejestrowane, oraz liczbę stron każdego załącznika;
 - 8) w przypadku, gdy adresatowi wysyła się inną liczbę załączników, niż pozostawia w aktach, dodatkowo napis „tylko adresat”-jeżeli załączniki mają być przekazane adresatowi bez pozostawienia ich w aktach, lub napis „do zwrotu”-jeżeli załączniki mają zostać zwrócone nadawcy;
 - 9) liczbę wykonanych egzemplarzy;
 - 10) adresatów poszczególnych egzemplarzy dokumentu albo adnotację „adresaci według rozdzielnika”;
 - 11) imię i nazwisko;
 - 12) numer strony oraz liczbę stron całego dokumentu;
 - 13) na środku, jako ostatni element w stopce strony, klauzulę tajności.

(Pieczęć nagłówkowa Urzędu)

Stąporków, dn.

Nr sprawy

Egz. Nr

PROTOKÓŁ USZKODZENIA PRZESYŁKI NIEJAWNEJ

W dniu do Kancelarii materiałów niejawnych Urzędu Miejskiego
w Stąporkowie wpłynęła uszkodzona przesyłka doręczona przez

.....
której nadawcą jest

Opis uszkodzonej przesyłki:

Uwagi i wnioski:

Protokół sporządzono w jednobrzmiących egzemplarzach.

Sporządził:

.....
(imię i nazwisko, stanowisko)

.....
(podpis)

Protokół sporządzono w obecności doręczającego przesyłkę:

I
(podpis)

Wykonano w egzemplarzach:

1. nadawca przesyłki;
2. doręczający przesyłkę;
3. kancelaria materiałów niejawnych

ZAŁĄCZNIK Nr 3 WZÓR PROTOKOŁU OTWARCIA PRZESYŁKI NIEJAWNEJ

(Pieczęć nagłówkowa Urzędu)

Stąporków, dn.

Nr sprawy

Egz. Nr

PROTOKÓŁ OTWARCIA PRZESYŁKI NIEJAWNEJ

W dniu do Kancelarii materiałów niejawnych Urzędu Miejskiego w Stąporkowie wpłynęła przesyłka z:

.....
(nazwa nadawcy)
o numerze/ liczbie dziennika ewidencyjnego, którą otwarto w celu zaewidencjonowania w tut. Dzienniku Ewidencyjnym.

W trakcie sprawdzania zgodności ilości liczby stron pisma oraz liczby załączników i stron załączników z ilością wskazaną w piśmie przewodnim stwierdzono nieprawidłowości.

W celu udokumentowania tych nieprawidłowości Komisja w składzie:

- | | |
|-------------------|----------|
| 1. | |
| (imię i nazwisko) | (podpis) |
| 2. | |
| (imię i nazwisko) | (podpis) |
| 3. | |
| (imię i nazwisko) | (podpis) |

stwierdziła, że:

.....

Protokół sporządzono w 3 jednobrzmiących egzemplarzach.

Sporządził:

.....
(imię i nazwisko, stanowisko)

.....
(podpis)

Wykonano w 3 egzemplarzach:

1. nadawca przesyłki;
2. doręczający przesyłkę;
3. kancelaria materiałów niejawnych

**ZAŁĄCZNIK NR 4 WZÓR UPOWAŻNIENIA UPRAWNIAJĄCEGO DO INFORMACJI
NIEJAWNYCH OZNACZONYCH KLAUZULĄ „ZASTRZEŻONE”.**

.....

(pieczęć nagłówkowa jednostki organizacyjnej)

UPOWAŻNIENIE NR

z dnia

Na podstawie art. 21 ust. 4 pkt 1 i 2 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji
niejawnych (Dz. U. z 2018 r., poz. 412 ze zm.)

u p o w a ż n i a m:

....., ur.

do dostępu do informacji niejawnych oznaczonych klauzulą „zastrzeżone”, zatrudnionej/go
w na stanowisku

.....

(podpis kierownika jednostki organizacyjnej)

*Upoważnienie jest ważne na czas zatrudnienia w lub do odwołania.

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

**ZAŁĄCZNIK NR 5 WZÓR ZAŚWIADCZENIA STWIERDZAJĄCEGO ODBYCIE SZKOLENIA
W ZAKRESIE OCHRONY INFORMACJI NIEJAWNYCH**

**ZAŚWIADCZENIE NR z dnia
stwierdzające odbycie szkolenie w zakresie ochrony informacji niejawnych**

Stwierdza się, że Pani (Pan):

- imię i nazwisko:

- numer PESEL¹⁾ :

odbyła szkolenie w zakresie ochrony:

- informacji niejawnych*,

- informacji niejawnych²⁾ :

.....

(nazwa organizacji międzynarodowej)

na podstawie przepisów ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych
(Dz. U. z 2018 r., poz. 412 ze zm.) zorganizowane przez pełnomocnika do spraw ochrony
informacji niejawnych w :

.....

(nazwa i adres siedziby jednostki organizacyjnej)

.....

(miejscowość i data)

(podpis imienna pełnomocnika ochrony informacji niejawnych)

* Niepotrzebne skreślić.

1) W przypadku braku numeru PESEL należy wpisać datę urodzenia.

2) W przypadku przeszkolenia w zakresie ochrony informacji niejawnych więcej niż jednej organizacji międzynarodowej kolejne ich nazwy, np. Organizacja Traktatu Północnoatlantyckiego, Unia Europejska, Europejska Agencja Kosmiczna, należy wpisać poniżej.

POŚWIADCZENIE BEZPIECZEŃSTWA NR

Na podstawie art. 28 pkt 1 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych
(Dz. U. z 2018 r., poz. 412 ze zm.) po przeprowadzeniu na wniosek/polecenie*

.....
(nazwa wnioskodawcy albo stanowisko osoby, która poleciła przeprowadzenie postępowania*)

.....
(nazwa i adres siedziby organu, który przeprowadził postępowanie)

zwykłego/poszerzonego* postępowania sprawdzającego, stwierdza się, że Pan(i)

.....
(imię i nazwisko, data urodzenia)

daje rękojmię zachowania tajemnicy

w zakresie dostępu do informacji niejawnych oznaczonych klauzulą

..... na okres do:
(nazwa klauzuli tajności) (termin ważności)

..... na okres do*:
(nazwa klauzuli tajności) (termin ważności)*

..... na okres do*:
(nazwa klauzuli tajności) (termin ważności)*

..... mp.
(miejscowość i data)(podpis i imienna pieczęć osoby upoważnionej)

* niepotrzebne skreślić

**ZALĄCZNIK NR 7 WZÓR POLECENIA WSZCZĘCIA ZWYKŁEGO POSTĘPOWANIA
SPRAWDZAJĄCEGO**

.....
(nazwa jednostki organizacyjnej)

Miejscowość i data

Pełnomocnik ds. Ochrony Informacji Niejawnych
w

POLECENIE WSZCZĘCIA ZWYKŁEGO POSTĘPOWANIA SPRAWDZAJĄCEGO

Na podstawie art. 23 ust 1 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji
niejawnych (Dz. U. z 2018 r., poz. 412 ze zm.) polecam przeprowadzenie zwykłego
postępowania sprawdzającego w celu wydania poświadczenia bezpieczeństwa,
upoważniającego do dostępu do informacji niejawnych oznaczonych klauzulą tajności
„poufne” wobec:

1. Imię (imiona)
2. Nazwisko (w tym przybrane)
3. Nr PESEL
4. Imię ojca

.....
/Pieczęć i podpis kierownika jednostki organizacyjnej/

Załącznik nr 8 Wzór karty zapoznania się z dokumentem

KARTA ZAPOZNANIA SIĘ Z DOKUMENTEM NR.....

[illegible]

(nazwa komórki organizacyjnej)

dokonano przekazania materiałów i dokumentów zawierających informacje niejawne.

(imię i nazwisko – stanowisko służbowe)

(imię i nazwisko – stanowisko służbowe)

(imię i nazwisko)

Przekazaniu podlegają niżej wymienione materiały i dokumenty zawierające informacje niejawne:

[illegible]

Informacje dotyczące zgodności (lub niezgodności) stanu faktycznego ze stanem ewidencyjnym:

.....
.....
.....
.....

Uwagi lub wnioski dotyczące ujawnionych nieprawidłowości w zakresie ewidencjonowania i obiegu dokumentów oraz ewentualne inne informacje i uwagi:

.....
.....
.....
.....

Do protokołu załączono:

.....
.....

Protokół sporządzono w dwóch jednobrzmiących egzemplarzach.

Zdający:

.....

(imię i nazwisko)

Przyjmujący:

.....

(imię i nazwisko)

W obecności pełnomocnika ds. ochrony informacji niejawnych oraz członków komisji:

.....

(imię i nazwisko – stanowisko)

.....

(podpis)

.....

(imię i nazwisko – stanowisko)

.....

(podpis)

.....

(imię i nazwisko – stanowisko)

.....

(podpis)

WZORY PISM I UPOWAŻNIEŃ

1. PISMO DO DELEGATURY AGENCJI BEZPIECZEŃSTWA WEWNĘTRZNEGO.
2. WNIOSEK O SPRAWDZENIE W EWIDENCJACH I KARTOTEKACH NIEDOSTĘPNYCH POWSZECHNIE.
3. WNIOSEK W SPRAWIE UDZIELENIA INFORMACJI Z KRAJOWEGO REJESTRU KARNEGO.
4. WNIOSEK – ZGODA NA UDOSTĘPNIENIE INFORMACJI NIEJAWNYCH O KLAUZULI „POUFNE” OSOBIE, WOBEC KTÓREJ WSZCZĘTO POSTĘPOWANIE SPRAWDZAJĄCE ZWYKŁE.
5. WNIOSEK O PRZEPROWADZENIE POSZERZONEGO POSTĘPOWANIA SPRAWDZAJĄCEGO.
6. WZÓR - PROTOKÓŁ OCENY DOKUMENTACJI NIEARCHIWALNEJ.
7. SPIS DOKUMENTACJI NIEARCHIWALNEJ PRZEZNACZONEJ NA MAKULATURĘ LUB ZNISZCZENIE.
8. WZÓR - PROTOKÓŁ KOMISYJNEGO ZNISZCZENIA DOKUMENTÓW NIEARCHIWALNYCH.
9. WZÓR - PROTOKÓŁ OTWARCIA SZAFY, SEJFU.

1/ PISMO DO DELEGATURY AGENCJI BEZPIECZEŃSTWA WEWNĘTRZNEGO

.....

(nazwa jednostki organizacyjnej)

L.dz.

Miejscowość i data

Dyrektor

Delegatury Agencji

Bezpieczeństwa Wewnętrznego

W

Na podstawie art. 14 ust 1-3 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji
niejawnych (Dz. U. z 2018 r., poz. 412 ze zm.) wykonując nałożone zadania wynikające
z przepisów Ustawy o ochronie informacji niejawnych w załączeniu przesyłam Ankietę
Bezpieczeństwa Osobowego z wnioskiem o przeprowadzenie poszerzonego postępowania
sprawdzającego wobec Pana/i, kandydata na
pełnomocnika ochrony informacji niejawnych w
(nazwa jednostki)

Jednocześnie proszę o wyznaczenie miejsca i terminu szkolenia dla kandydata na
pełnomocnika w

(nazwa jednostki)

Załącznik: Ankieta Bezpieczeństwa Osobowego na stronach.

.....

(podpis kierownika jednostki)

**2/ WNIOSEK O SPRAWDZENIE W EWIDENCJACH I KARTOTEKACH
NIEDOSTĘPNYCH POWSZECHNIE**

.....
(nazwa jednostki organizacyjnej występującej
o sprawdzenie osoby upoważnionej do dostępu
do informacji niejawnych)

Miejscowość i data

Dyrektor
Delegatury Agencji
Bezpieczeństwa Wewnętrznego
w

**WNIOSEK O SPRAWDZENIE W EWIDENCJACH I KARTOTEKACH
NIEDOSTĘPNYCH POWSZECHNIE**

Na podstawie art. 25 ust 1 pkt 2 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji
niejawnych (Dz. U. z 2018 r., poz. 412 ze zm.) wykonując nałożone zadania w związku
z przeprowadzanym zwykłym postępowaniem sprawdzającym wobec następującej osoby:

1. Nr PESEL
2. Nazwisko (w tym przybrane)
3. Imię (imiona)
4. Imię ojca
5. Imię matki
6. Nazwisko rodowe matki
7. Data urodzenia
8. Miejsce urodzenia
9. Miejsce zameldowania
10. Miejsce zamieszkania

Proszę o poinformowanie, czy Agencja Bezpieczeństwa Wewnętrznego posiada
informacje, które mają wpływ na wynik postępowania.

.....
Pieczęć i podpis pełnomocnika ochrony lub zastępcy pełnomocnika ochrony

**3/ WNIOSEK W SPRAWIE UDZIELENIA INFORMACJI Z KRAJOWEGO REJESTRU
KARNEGO**

.....
(nazwa jednostki organizacyjnej występującej
o sprawdzenie osoby upoważnionej do dostępu
do informacji niejawnych)

Miejscowość i data

Krajowy Rejestr Karny
Biuro Informacyjne
ul. Czerniakowska 100
00-454 Warszawa

lub Punkt Informacyjny
Krajowego Rejestru Karnego
przy Sądzie Powszechnym

Na podstawie art. 6 ust. 1 pkt 10 ustawy z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym (Dz. U. z 2018 r., poz. 1218 ze zm.) oraz art. 25 ust 1 pkt 1 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2018 r., poz. 412 ze zm.) w załączeniu przekazuję zapytanie stanowiące załącznik nr 2 do rozporządzenia Ministra Sprawiedliwości z dnia 7 lipca 2015 r. w sprawie udzielania informacji o osobach oraz o podmiotach zbiorowych na podstawie danych zgromadzonych w Krajowym Rejestrze Karnym (Dz. U. z 2015 r., poz. 1025 ze zm.) dotyczy

1. Imię (imiona).....
2. Nazwisko (w tym przybrane)
3. Nr PESEL
4. Imię ojca

Zapytanie proszę odesłać na adres:
.....

.....
Pieczęć i podpis pełnomocnika ochrony lub zastępcy pełnomocnika ochrony

**4/ WNIOSEK – ZGODA NA UDOSTĘPNIENIE INFORMACJI NIEJAWNYCH
O KLAUZULI „POUFNE” OSOBIE, WOBEC KTÓREJ WSZCZĘTO POSTĘPOWANIE
SPRAWDZAJĄCE ZWYKŁE**

.....
(nazwa jednostki organizacyjnej)

Miejscowość i data

**ZGODA NA UDOSTĘPNIENIE INFORMACJI NIEJAWNYCH O KLAUZULI
„POUFNE” OSOBIE, WOBEC KTÓREJ WSZCZĘTO POSTĘPOWANIE
SPRAWDZAJĄCE ZWYKŁE**

Postępowanie sprawdzające zostało wszczęte w dniu

Na podstawie art. 34 ust 9 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych
(Dz. U. z 2018 r., poz. 412 ze zm.) wyrażam zgodę na udostępnienie informacji niejawnych
oznaczonych klauzulą tajności „poufne” następującej osobie:

1. Imię (imiona)
2. Nazwisko (w tym przybrane)
3. Nr PESEL
4. Imię ojca
5. Imię matki
6. Nazwisko rodowe matki
7. Data urodzenia
8. Miejsce urodzenia

.....
Pieczętka i podpis pełnomocnika ochrony lub zastępcy pełnomocnika ochrony

**5/ WNIOSEK O PRZEPROWADZENIE POSZERZONEGO POSTĘPOWANIA
SPRAWDZAJĄCEGO**

.....

Miejscowość i data

(nazwa jednostki organizacyjnej występującej
o sprawdzenie osoby upoważnionej do dostępu
do informacji niejawnych)

L.dz

Dyrektor

Delegatury Agencji

Bezpieczeństwa Wewnętrznego

w

**WNIOSEK O PRZEPROWADZENIE POSZERZONEGO POSTĘPOWANIA
SPRAWDZAJĄCEGO**

Na podstawie art. 23 ust 2 pkt 1 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji
niejawnych (Dz. U. z 2018 r., poz. 412 ze zm.) wnoszę o przeprowadzenie poszerzonego
postępowania sprawdzającego w celu wydania poświadczenia bezpieczeństwa,
upoważniającego do dostępu do informacji niejawnych o klauzuli*
wobec:

1. Imię (imiona)
2. Nazwisko.....
3. Nr PESEL

.....
Pieczątką i podpis pełnomocnika ochrony lub zastępcy pełnomocnika ochrony

Załącznik:

Załącznik – Ankieta Bezpieczeństwa Osobowego – nastr. – tylko adresat

- wpisać odpowiednią klauzulę lub klauzulę tajności

INFORMACJA DODATKOWE:

Zgodnie z art. 73 ust. 1 ustawy o ochronie informacji niejawnych, Agencja Bezpieczeństwa Wewnętrznego prowadzi ewidencję osób uprawnionych na podstawie przepisów ustawy do dostępu do informacji niejawnych o klauzuli „poufne” i wyższej (tj. poprzez poświadczenie bezpieczeństwa lub zgodę, o której mowa w art. 34 ust. 9 ustawy) oraz ewidencję osób, którym odmówiono wydania lub cofnięto poświadczenie bezpieczeństwa. Ewidencja ta prowadzona jest w oparciu o dane przekazywane do ABW przez pełnomocnika ochrony na podstawie art. 15 ust. 1 pkt 9 ustawy.

Wypełnione karty pełnomocnicy przesyłają do właściwej Delegatury ABW.

UWAGA:

Kartę informacyjną należy przesłać w przypadku:

- 1) Wydania Poświadczenia Bezpieczeństwa
- 2) Odmowy wydania Poświadczenia Bezpieczeństwa
- 3) Cofnięcia Poświadczenia Bezpieczeństwa
- 4) Wydania zgody na udostępnienie informacji niejawnych w oparciu o art. 34 ust. 9

Aktualny wzór Karty Informacyjnej można pobrać na stronie:

<https://bip.abw.gov.pl/bip/informacje-niejawne-1/nadzor-nad-systemem-oc/materialy-do-pobrania/152,MATERIALY-DO-POBRANIA.html>

.....

(nazwa jednostki organizacyjnej)

PROTOKÓŁ OCENY DOKUMENTACJI NIEARCHIWALNEJ

Komisja w składzie:

.....

imię i nazwisko, stanowisko

.....

imię i nazwisko, stanowisko

.....

imię i nazwisko, stanowisko

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

Przewodniczący komisji:

Członkowie komisji:

.....

.....

Załączniki:

..... kart spisu

..... Pozycji spisu

**7/SPIS DOKUMENTACJI NIEARCHIWALNEJ PRZEZNACZONEJ NA MAKULATURĘ
LUB ZNISZCZENIE**

.....

nazwa i adres jednostki organizacyjnej

**SPIS DOKUMENTACJI NIEARCHIWALNEJ PRZEZNACZONEJ NA
MAKULATURĘ LUB ZNISZCZENIE**

LP.	TYTUŁ TECZKI	SYMBOL Z WYKAZU RZECZOWEGO	DATY SKRAJNE	UWAGI

**PROTOKÓŁ KOMISYJNEGO ZNISZCZENIA DOKUMENTÓW
NIEARCHIWALNYCH**

W dniu komisja w składzie:

1. Przewodniczący komisji
(kierownik lub pracownik archiwum zakładowego)
2. Członek komisji
(przedstawiciel komórek org, których dokumenty są brakowane)
3. Członek komisji
(pełnomocnik ochrony lub pracownik pionu ochrony)

dokonała zniszczenia dokumentów niearchiwalnych, w oparciu o zgodę Archiwum Państwowego – pismo nr z dnia wydaną na podstawie Protokołu oceny dokumentacji niearchiwalnej oraz Spisu dokumentacji niearchiwalnej przeznaczonej na makulaturę lub zniszczenie, pismo nr z dnia

Dokumenty zostały komisyjnie zniszczone w dniu przez
(spalenie, zniszczenie itp.).

Podpisy członków komisji:

1. Przewodniczący komisji
2. Członek komisji
3. Członek komisji

PROTOKÓŁ OTWARCIA SZAFY, SEJFU

W dniu

Komisja w składzie:

1.

(imię i nazwisko)

2.

(imię i nazwisko)

3.

(imię i nazwisko)

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

(imię i nazwisko oraz stanowisko służbowe)

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

1.

2.

3.

którymi obecnie dysponuje Pan/i

.....

(imię i nazwisko oraz stanowisko służbowe)

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

Podpisy członków komisji:

1.

2.

3.

**PLAN POSTĘPOWANIA Z MATERIAŁAMI ZAWIERAJĄCYMI INFORMACJE
NIEJAWNE STANOWIĄCE TAJEMNICĘ PAŃSTWOWĄ I SŁUŻBOWĄ W RAZIE
WPROWADZENIA STANU NADZWYCZAJNEGO W URZĘDZIE MIEJSKIM
W STĄPORKOWIE**

Na podstawie art. 15 ust. 1 pkt 5 ustawy z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych (Dz. U. z 2018 r., poz. 412 ze zm.) ustala się w niniejszym Planie zasady postępowania w razie konieczności zabezpieczenia materiałów niejawnych w przypadku wprowadzenia stanu nadzwyczajnego. Jako stany nadzwyczajne uważa się stany określone w art. 228 Konstytucji RP (Dz. U. z 1997 r., Nr 78, poz. 483 ze zm.).

§ 1

1. Konieczność podjęcia działań zmierzających do zabezpieczenia materiałów zawierających informacje niejawne stanowiące tajemnicę państwową może mieć miejsce w przypadkach:

1. Spodziewanego zagrożenia państwa,
2. Wprowadzenia stanu nadzwyczajnego,
3. Wybuchu konfliktu zbrojnego mającego bezpośredni związek z Państwem Polskim,
4. Zagrożeń wewnętrznych spowodowanych klęskami żywiołowymi.

§ 2

1. Zabezpieczeniu podlegają wszystkie materiały zawierające informacje niejawne stanowiące tajemnicę państwową, jeśli ilość materiałów niejawnych znajdujących się w Kancelarii Materiałów Niejawnych jest niewielka.

2. Szczególnej ochronie w związku z podjętymi działaniami podlegają:

- a) materiały mające bezpośredni związek z funkcjonowaniem jednostki organizacyjnej w warunkach zagrożenia,
- b) materiały wytworzone w ciągu ostatnich 5 lat.

§ 3

1. Priorytet w zakresie zabezpieczenia dokumentów oznaczonych klauzulą „zastrzeżone” mają dokumenty dotyczące:

- a) Akcji Kurierskiej,
- b) zadań związanych z podwyższeniem gotowości obronnej jednostki organizacyjnej (Plan operacyjny funkcjonowania Urzędu)

2. Zabezpieczenie materiałów wymienionych w pkt. 1 jest niezbędne do zapewnienia realizacji zadań jednostki organizacyjnej na rzecz Sił Zbrojnych, Urzędu oraz mieszkańców.

§ 4

1. Decyzję w sprawie zabezpieczenia i ewakuacji materiałów podejmuje Burmistrz Stąporkowa, a koordynatorem akcji jest Pełnomocnik ds. ochrony informacji niejawnych.
2. W przypadkach uzasadnionych, pod nieobecność Burmistrza Stąporkowa i Pełnomocnika ds. ochrony informacji niejawnych, decyzję podejmuje kierownik komórki organizacyjnej, w której przechowywane są dokumenty podlegające zabezpieczeniu i ewakuacji.
3. Miejsce zabezpieczenia materiałów podlegających ewakuacji, wymienionych powyżej, ustala osoba podejmująca decyzję o ewakuacji.
4. Zabezpieczenie dokumentów, o których mowa w Planie, dokonuje się poprzez ich ewakuowanie z pomieszczeń kancelarii materiałów niejawnych. Ewakuacja tych dokumentów następuje w warunkach pozwalających doprowadzić do ulokowania ich w miejscu zapewniającym wystarczające bezpieczeństwo w zaistniałej sytuacji zagrożenia, możliwie spełniając wymagania ustawy o ochronie informacji niejawnych.

§ 5

1. Ewakuacji materiałów z zagrożonych pomieszczeń dokonywać należy, w zależności od stopnia i umiejscowienia zagrożenia:
 - a) korytarzami i klatką schodową do głównego lub awaryjnego wyjścia z budynku Urzędu,
 - b) przez okno przy bezwzględnym zagwarantowaniu bezpiecznego odbioru materiałów na zewnątrz budynku Urzędu.

§ 6

1. W celu wykonania zadań związanych z zabezpieczeniem materiałów będących przedmiotem zabezpieczenia, merytoryczni pracownicy – wytwórcy dokumentów niejawnych na żądanie Pełnomocnika ds. ochrony informacji niejawnych zobowiązani są do udzielenia pomocy, w szczególności w zakresie:
 - a) zorganizowania przeniesienia zasobów z kancelarii materiałów niejawnych, czy ze stanowisk pracy, na których znajdują się takie dokumenty,
 - b) organizowania stanowiska przeznaczonego do zabezpieczenia dokumentów po ewakuacji.

§ 7

1. W stanie nadzwyczajnym sporządza się dwa egzemplarze spisu materiałów niejawnych przeznaczonych do ewakuacji oraz niepodlegających ewakuacji, z których w razie ewakuacji jeden pozostawia się w pomieszczeniu pracy a drugi zabiera wraz z ewakuowanymi materiałami do nowego miejsca.

2. Zabezpieczenie ewakuowanych dokumentów odbywa się poprzez dokonanie niżej wymienionych czynności:

- a) wydanie stosownych poleceń Pełnomocnikowi do spraw ochrony informacji niejawnych, innym pracownikom odpowiedzialnym za te dokumenty,
- b) w przypadku konieczności zabezpieczenia materiałów w godzinach pozasłużbowych, osoba podejmująca decyzję o konieczności ewakuacji materiałów zarządza wezwaniem osób odpowiedzialnych przy użyciu wszelkich dostępnych środków,
- c) zapewnienie niezbędnego środka transportu oraz pracowników w ilości niezbędnej do zapakowania i przemieszczenia materiałów wymagających zabezpieczenia,
- d) w przypadku zabezpieczenia materiałów niejawnych Pełnomocnik do spraw ochrony informacji niejawnych wyznacza dwuosobową komisję spośród pracowników Urzędu posiadających uprawnienia do dostępu do dokumentów niejawnych podlegających ewakuacji, która dokona komisyjnego otwarcia szafy.

3. Komisja realizująca powyższe zadania sporządza protokół z otwarcia, z którego musi wynikać:

- a) zasadność otwarcia szafy pod nieobecność pracownika kancelarii materiałów niejawnych,
- b) określenie rodzaju i ilości materiałów poddanych zabezpieczeniu i ewakuacji,
- c) określenie materiałów, które ewentualnie pozostały w szafie, a więc tych materiałów, które nie zostały objęte zabezpieczeniem,
- d) określenie sposobu zabezpieczenia materiałów w nowym miejscu ich przechowywania,
- e) określenie sposobu zabezpieczenia materiałów, które pozostały w ewakuowanym pomieszczeniu. **Wzór protokołu otwarcia szafy/biurka, gdzie znajdują się dokumenty zawierające informacje niejawne stanowi Załącznik nr 1 do niniejszego Planu.**

4. Komisja przystępując do otwarcia szafy, a więc wykonując polecenie zarządzającego dokonania zabezpieczenia materiałów, wykorzystuje klucze do Kancelarii Materiałów Niejawnych deponowane u Pełnomocnika ds. ochrony informacji niejawnych.

5. Komisja, realizując powyższe zadania w przypadku ewentualnego pozostawienia części materiałów, których nie zdołano zabezpieczyć i ewakuować, obowiązana jest zamknąć szafę i

ją zaplombować. Powyższy fakt komisja obowiązkowo uwzględni w treści sporządzonego przez siebie protokołu dotyczącego zarówno otwarcia pomieszczenia, jak też zabezpieczenia materiałów.

§ 8

1. Celem sprawnej realizacji Planu w Urzędzie należy:

- a) oznaczyć szafę z materiałami podlegającymi zabezpieczeniu i ewakuacji w sposób trwały i widoczny na zewnątrz poprzez umieszczenie na niej napisu „Ewakuacja”.
- b) worki i pojemniki, w miarę możliwości, przechowywać należy w szafie lub w miejscach dostępnych i nie wymagających korzystania z kluczy,
- c) w szafie na drzwiach powinna być informacja jakie dokumenty podlegają zabezpieczeniu mając na względzie ważność i aktualność materiałów wymagających zabezpieczenia

§ 9

Realizację postanowień Planu powierza się Pełnomocnikowi do spraw ochrony informacji niejawnych w zakresie:

- a) przygotowania materiałów już posiadanych do ewentualnego zabezpieczenia,
- b) bieżącego gromadzenia materiałów, z myślą o wymaganiach związanych z ewentualnością ich zabezpieczenia.

**PROTOKÓŁ OTWARCIA SZAFY/BIURKA, GDZIE ZNAJDUJĄ SIĘ DOKUMENTY
ZAWIERAJĄCE INFORMACJE NIEJAWNE**

W dniu

Komisja w składzie:

1.

(imię i nazwisko)

2.

(imię i nazwisko)

3.

(imię i nazwisko)

dokonała otwarcia szafy/biurka znajdującej się w pomieszczeniu

.....

.....

(nazwa wydziału, nr pokoju)

którego użytkownikiem jest

(nazwisko i imię, stanowisko służbowe)

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

1.

2.

3.

4.

którymi obecnie dysponuje Pan/i

.....

(nazwisko i imię, stanowisko służbowe)

Szafę/biurko zamknięto i zaplombowano pieczęcią w obecności członków komisji.

Podpisy członków komisji:

1.

2.

3.

WYMAGANIA W ZAKRESIE OCHRONY INFORMACJI NIEJAWNYCH OZNACZONYCH KLAUZULĄ „ZASTRZEŻONE”

I. DEFINICJA INFORMACJI NIEJAWNYCH OZNACZONYCH KLAUZULĄ „ZASTRZEŻONE”.

1. Informacjom niejawnym nadaje się klauzulę „zastrzeżone”, jeśli nie nadano im wyższej klauzuli, 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.
2. Informacje niejawne, którym przyznano klauzulę „zastrzeżone” są chronione zgodnie z przepisami ustawy z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych (Dz. U. z 2018 r., poz. 412 ze zm.).

Oznacza to w szczególności, że informacje takie:

- 1) mogą być udostępnione wyłącznie osobie uprawnionej do dostępu do informacji niejawnych oznaczonych klauzulą „zastrzeżone”,
- 2) muszą być wytwarzane, przetwarzane lub przechowywane w warunkach uniemożliwiających ich nieuprawnione ujawnienie,
- 3) muszą być odpowiednio chronione.

II. OZNACZANIE INFORMACJI ZASTRZEŻONYCH

1. Propozycję przyznania klauzuli niejawności na wykonywanym dokumencie przedstawia osoba sporządzająca dokument.
2. Klauzulę niejawności na danym dokumencie przyznaje osoba, która jest uprawniona do odpisania dokumentu.
3. Rękopisy sporządzanych dokumentów niejawnych oznaczonych klauzulą „zastrzeżone” powinny być opracowywane w brulionach (zeszytach pracy) uprzednio zarejestrowanych w kancelarii materiałów niejawnych.
4. Dokumenty niejawne oznaczone klauzulą „zastrzeżone” powinny być opisane oznaczone zgodnie z Rozporządzeniem Prezesa Rady Ministrów z dnia 13 sierpnia 2010 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzuli tajności (Dz. U. z 2011 r., Nr 288, poz. 1692) . Wzór sposobu opisanie dokumentu stanowi załącznik do Planu Ochrony Informacji Niejawnych.

III. PRZEKAZYWANIE NA ZEWNĄTRZ INFORMACJI ZASTRZEŻONYCH

1. Materiały zawierające informacje niejawne oznaczone klauzulą „zastrzeżone”, nadawane w postaci listów, przekazuje się jako listy polecone, w dwóch nieprzezroczystych mocnych kopertach. Materiały nadawane w postaci paczek, przekazuje się jako paczki wartościowe w dwóch nieprzezroczystych warstwach mocnego papieru, które oznacza się w sposób następujący:

- na wewnętrznej kopercie (listu) lub wewnętrznej warstwie papieru (paczki) muszą być umieszczone:
 - klauzula tajności ewentualnie dodatkowe oznaczenie,
 - znak pisma,
 - imienne określenie adresata,
 - imię, nazwisko i podpis osoby pakującej.

- na zewnętrznej kopercie (listu) lub zewnętrznej warstwie papieru (paczki) muszą być umieszczone:
 - nazwa jednostki organizacyjnej adresata,
 - adres siedziby adresata,
 - znak pisma, jednak bez umieszczania informacji, że korespondencja zawiera informacje „zastrzeżone”, tj. bez symbolu „Z”, po literowym oznaczeniu komórki organizacyjnej twórcy dokumentu,
 - nazwa jednostki organizacyjnej nadawcy.

IV. WYTWARZANIE INFORMACJI ZASTRZEŻONYCH Z WYKORZYSTANIEM SPRZĘTU KOMPUTEROWEGO

1. Dokumenty oznaczone klauzulą „zastrzeżone” mogą być wytwarzane pod warunkiem zastosowania niezbędnych czynności i zabezpieczeń określonych w rozdziale 8(Bezpieczeństwo Teleinformatyczne) ustawy o ochronie informacji niejawnych.
2. Pełnomocnik określi osoby, które posiadają poświadczenie bezpieczeństwa lub upoważnienia nadane przez kierownika jednostki i są uprawnione do wytwarzania materiałów zastrzeżonych.
3. Wykaz osób uprawnionych do wytwarzania materiałów oznaczonych klauzulą „zastrzeżone” prowadzony jest przez pełnomocnika w formie rejestru.
4. Należy dokonać akredytacji bezpieczeństwa teleinformatycznego systemu i sieci teleinformatycznej, w których będą wytwarzane, przetwarzane, przechowywane

lub przekazywane informacje niejawne oznaczone klauzulą „zastrzeżone”.

5. Po akredytacji należy wydzielić stanowisko komputerowe, które będzie służyło do wytwarzania tych dokumentów.

6. Dokumenty szczególnych wymagań bezpieczeństwa oraz procedury bezpiecznej eksploatacji systemów i sieci teleinformatycznych, w których mają być wytwarzane, przetwarzane, przechowywane lub przekazywane informacje niejawne oznaczone klauzulą „zastrzeżone” są akredytowane przez kierownika jednostki, a następnie przedstawiane właściwej służbie ochrony państwa. ABW może wnieść w ciągu 30 dni od przedstawienia dokumentacji poprawki do określonych procedur.

V. KOPIE ZAPASOWE

1. Zaleca się wykonywanie kopii zapasowych wykonanych dokumentów oznaczonych klauzulą „zastrzeżone”.

2. Sposób przechowywania zapasowych kopii, w przypadku, gdy nośnikiem informacji jest materiał inny niż pismo, jest taki sam, jak sposób przechowywania dokumentów wykonanych w tradycyjnej formie, zaewidencjonowanie kopii zapasowych polega na tym, że 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 niemożliwe – na ich obudowie lub opakowaniu.

VI. PRZECHOWYWANIE INFORMACJI ZASTRZEŻONYCH W KOMÓRKACH ORGANIZACYJNYCH LUB NA STANOWISKACH PRACY

1. Informacje niejawne oznaczone klauzulą „zastrzeżone” podlegają ochronie w sposób określony w Ustawie o ochronie informacji niejawnych do czasu, gdy osoba, która nadała klauzulę niejawności nie zniesie okresu ochronnego.

2. Dokumentacja zawierająca informacje niejawne oznaczone klauzulą „zastrzeżone” może być przechowywana w kancelarii materiałów niejawnych lub w pomieszczeniach na stanowiskach pracy w meblach biurowych zamykanych na klucz (zabezpieczone przed dostępem osób nieuprawnionych).

VII. NADAWANIE, ZMIANA I ZNOSZENIE KLAUZULI „ZASTRZEŻONE”

1. Klauzulę przyznaje osoba, która jest upoważniona do podpisania dokumentu lub oznaczenia innego niż dokument materiału. Uprawnienie do przyznania, obniżania i znoszenia klauzuli tajności przysługuje wyłącznie w zakresie posiadanego dostępu do informacji niejawnych.

-
2. Zawyżanie lub zaniżanie klauzuli tajności jest niedopuszczalne.
 3. Odbiorca materiału zgłasza osobie, która przyznała daną klauzulę albo jej przełożonemu fakt wyraźnego zawyżenia lub zaniżenia klauzuli tajności. W przypadku, gdy osoba lub jej przełożony zdecyduje o zmianie klauzuli, powinna o tym poinformować odbiorców tego materiału. Odbiorcy materiału, którzy przekazali go kolejnym odbiorcom są odpowiedzialni za poinformowanie o ich zmianie klauzuli.
 4. Zmiany nadanej klauzuli dokonuje się przez jej skreślenie i wpisanie obok niej nowej z podaniem:
 - a) daty;
 - b) imienia i nazwiska,
 - c) podpisu osoby dokonującej zmiany.
 5. Skreślenie bez wpisania daty, imienia i nazwiska oraz podpisu dokonującego zmiany uważa się za niedokonane.
 6. Skreślenia oraz pozostałych wpisów dokonuje się kolorem czerwonym. Wycieranie, wywabianie lub zamazywanie klauzuli, która podlega zmianie i dokonanych zmian jest niedozwolone. Fakt dokonania zmian klauzuli należy odnotować w odpowiednich dziennikach ewidencyjnych lub rejestrach materiałów niejawnych, z podaniem przyczyny zmiany.
 7. Uprawnienia osoby, o której mowa w pkt. 1 w zakresie przyznawania, obniżania lub znoszenia klauzuli tajności materiału oraz określenia okresu, jaki informacja niejawna podlega ochronie, przechodzą w przypadku rozwiązania, zniesienia, likwidacji, przekształcenia lub reorganizacji dotyczącej stanowiska lub funkcji tej osoby, na jej następcę prawnego. W razie braku następcy prawnego, uprawnienia w tym zakresie przechodzą na właściwą służbę ochrony państwa.

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 wniesli 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, świeące elementy elektroniczne, itp.).

3. Pomieszczenia ogólnodostępne takie jak: korytarze, klatki schodowe, halle, windy, toalety, piwnice, strychy itp. oraz najbliższe otoczenia 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

obiekty 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 powinien udzielić mu wszechstronnej pomocy podczas jej prowadzenia.

3. Na wniosek policjanta, kierującego akcją, administrator obiektu podejmuje decyzję o ewakuacji użytkowników i innych osób z obiektu – o ile wcześniej to nie nastąpiło.

4. Identyfikacją i rozpoznaniem zlokalizowanych przedmiotów, rzeczy, urządzeń obcych oraz neutralizowaniem ewentualnie podłożonych ładunków wybuchowych zajmują się uprawnione i wyspecjalizowane ogniwa organizacyjne policji, przy wykorzystaniu specjalistycznych środków technicznych.

5. Policjant kierujący akcją, po zakończeniu działań, przekazuje protokolarnie obiekt administratorowi.

IV. POSTANOWIENIA KOŃCOWE DOTYCZĄCE DZIAŁAŃ W PRZYPADKU ZGŁOSZENIA O 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 powiadomić o tym policję, która z urzędu dokona sprawdzenia wiarygodności każdego zdarzenia.

2. Administrator obiektu powinien na bieżąco organizować szkolenia 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.

INSTRUKCJA POSTĘPOWANIA W PRZYPADKU OTRZYMANIA PRZESYŁKI NIEWIADOMEGO POCHODZENIA

W przypadku otrzymania jakiegokolwiek 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 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 podejmują wszystkie niezbędne kroki w celu bezpiecznego przejęcia przesyłki.

W przypadku, gdy podejrzana przesyłka została otwarta i zawiera jakąkolwiek podejrzaną zawartość w formie stałej (galarete, pianę, pył lub inną)

Należy:

- nie naruszać tej zawartości,
- nie rozsypywać, nie przenosić, nie dotykać, nie wachać, nie powodować ruchu powietrza w pomieszczeniu (wyłączyć systemy wentylacyjne i klimatyzacji, zamknąć okna),
- całą zawartość umieścić w worku 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