

**ZARZĄDZENIE NR 27 /09
BURMISTRZA RYCHWAŁA
z dnia 30 września 2009 r.**

**w sprawie wprowadzenia do użytku służbowego „Planu Ochrony Informacji
Niejawnych w Urzędzie Gminy i Miasta w Rychwale”.**

Na podstawie art.33 ust.1 i 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2001 r. Nr 142, poz. 1591 ze zm.) oraz art.18 ust.4 pkt 5 oraz art. 20 ust. 2 i art. 26 ust. 1 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 2005 r. Nr 196, poz. 1631 ze zm.) zarządzam, co następuje :

§ 1.

W celu zapewnienia ochrony informacji niejawnych oraz przestrzegania przepisów o ochronie informacji niejawnych, wprowadzam do użytku służbowego „Plan ochrony informacji niejawnych w Urzędzie Gminy i Miasta w Rychwale” (wraz z załącznikami do tego planu), stanowiący załącznik do zarządzenia.

§ 2.

Tracą moc : Zarządzenie Nr 27/2005 Burmistrza Rychwała z dnia 15 lipca 2005 r. w sprawie określenia stanowisk i rodzajów prac zleconych, z którymi może łączyć się dostęp do informacji niejawnych w Urzędzie Gminy i Miasta w Rychwale, Zarządzenie Nr 20/07 Burmistrza Rychwała z dnia 31 grudnia 2007 r. w sprawie ochrony informacji niejawnych w Urzędzie Gminy i Miasta w Rychwale, Zarządzenie Nr 21/07 Burmistrza Rychwała z dnia 31 grudnia 2007 r. w sprawie zatwierdzenia szczegółowych wymagań w zakresie ochrony informacji niejawnych oznaczonych klauzulą „zastrzeżone”.

§ 3.

Wykonanie zarządzenia powierza się Pełnomocnikowi ds. ochrony informacji niejawnych.

§ 4.

Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ
Gminy i Miasta Rychwał

Jan Bariczak

Załącznik do Zarządzenia Nr 27/09
Burmistrza Rychwała
z dnia 30 września 2009 r.

Plan Ochrony Informacji Niejawnych

w Urzędzie Gminy i Miasta w Rychwale

Rychwał, wrzesień 2009 r.

I. PODSTAWY PRAWNE OCHRONY INFORMACJI NIEJAWNYCH

1. Ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 2005 r. Nr 196, poz. 1631 z późn. zm.),
2. Rozporządzenie Prezesa Rady Ministrów z dnia 25 lutego 1999 r. w sprawie szczegółowego zakresu, warunków i trybu współdziałania organów, służb i innych państwowych jednostek organizacyjnych ze służbami ochrony państwa w toku prowadzonych postępowań sprawdzających (Dz. U. Nr 18, poz. 159),
3. Rozporządzenie Prezesa Rady Ministrów z dnia 25 sierpnia 2005 r. w sprawie szczegółowego trybu przygotowania i prowadzenia przez służby ochrony państwa kontroli w zakresie ochrony informacji niejawnych (Dz. U. Nr 171, poz. 1430),
4. Rozporządzenie Prezesa Rady Ministrów z dnia 25 sierpnia 2005 r. w sprawie wzorów poświadczenia bezpieczeństwa, decyzji o odmowie wydania poświadczenia bezpieczeństwa oraz decyzji o cofnięciu poświadczenia bezpieczeństwa (Dz. U. Nr 171, poz. 1431),
5. Rozporządzenie Prezesa Rady Ministrów z dnia 25 sierpnia 2005 r. w sprawie wzorów zaświadczeń stwierdzających odbycie szkolenia w zakresie ochrony informacji niejawnych (Dz. U. Nr 171, poz. 1432),
6. Rozporządzenie Prezesa Rady Ministrów z dnia 25 sierpnia 2005 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. Nr 171, poz. 1433),
7. Rozporządzenie Prezesa Rady Ministrów z dnia 29 sierpnia 2005 r. w sprawie wysokości i trybu pobierania, przez służbę ochrony państwa, opłat za przeprowadzenie postępowania bezpieczeństwa przemysłowego, sprawdzeń oraz postępowań sprawdzających (Dz. U. Nr 174, poz. 1447),
8. Rozporządzenie Rady Ministrów z dnia 8 września 2005 r. w sprawie wzorów kwestionariusza bezpieczeństwa przemysłowego, świadectwa bezpieczeństwa przemysłowego, decyzji o odmowie wydania świadectwa bezpieczeństwa przemysłowego oraz decyzji o cofnięciu świadectwa bezpieczeństwa przemysłowego (Dz. U. Nr 181, poz. 1504),
9. Rozporządzenie Prezesa Rady Ministrów z dnia 29 września 2005 r. w sprawie trybu i sposobu przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne (Dz. U. Nr 200, poz. 1650),
10. Rozporządzenie Prezesa Rady Ministrów z dnia 30 września 2005 r. w sprawie wysokości opłat za przeprowadzenie przez służbę ochrony państwa czynności z zakresu bezpieczeństwa teleinformatycznego (Dz. U. Nr 200, poz. 1652),
11. Rozporządzenie Prezesa Rady Ministrów z dnia 5 października 2005 r. w sprawie sposobu oznaczania materiałów, umieszczania na nich klauzul tajności, a także zmiany nadanej klauzuli tajności (Dz. U. Nr 205, poz. 1696),
12. Rozporządzenie Rady Ministrów z dnia 18 października 2005 r. w sprawie organizacji kancelarii tajnych (Dz. U. Nr 208, poz. 1741).

II. DEFINICJE UŻYWANE W PLANIE OCHRONY INFORMACJI NIEJAWNYCH

W rozumieniu planu ochrony informacji niejawnych:

1. Ustawą - jest ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 2005 r. Nr 196, poz. 1631 z późn. zm.),
2. Tajemnicą służbową - jest informacja niejawna niebędąca tajemnicą państwową, uzyskana w związku z czynnościami służbowymi albo wykonywaniem prac zleconych, której

nieuprawnione ujawnienie mogłoby narazić na szkodę interes państwa, interes publiczny lub prawnie chroniony interes obywateli albo jednostki organizacyjnej,

3. Służbami ochrony państwa - jest Agencja Bezpieczeństwa Wewnętrznego,

4. Rękojmnia zachowania tajemnicy - oznacza spełnienie ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem,

5. Dokumentem - jest każda utrwalona informacja niejawna, w szczególności na piśmie, mikrofilmach, negatywach i fotografiach, nośnikach do zapisów informacji w postaci cyfrowej i na taśmach elektromagnetycznych, także w formie mapy, wykresu, rysunku, obrazu, grafiki, fotografii, broszury, książki, kopii, odpisu, wypisu, wyciągu i tłumaczenia dokumentu, zbędnego lub wadliwego wydruku, odbitki, kliszy, matrycy i dysku optycznego, kalki, taśmy atramentowej, jak również informacja niejawna utrwalona na elektronicznych nośnikach danych,

6. Materiałem - jest dokument, jak też chroniony jako informacja niejawna przedmiot lub dowolna jego część, a zwłaszcza urządzenie, wyposażenie lub broń wyprodukowana albo będąca w trakcie produkcji, a także składnik użyty do ich wytworzenia;

7. Systemem teleinformatycznym - jest system, który tworzą urządzenia, narzędzia, metody postępowania i procedury stosowane przez wyspecjalizowanych pracowników, w sposób zapewniający wytwarzanie, przechowywanie, przetwarzanie lub przekazywanie informacji,

8. Siecią teleinformatyczną - jest organizacyjne i techniczne połączenie systemów teleinformatycznych,

9. Akredytacją bezpieczeństwa teleinformatycznego - jest dopuszczenie systemu lub sieci teleinformatycznej do wytwarzania, przetwarzania, przechowywania lub przekazywania informacji niejawnych, na zasadach określonych w ustawie,

10. Dokumentacją bezpieczeństwa systemu lub sieci informatycznej - są Szczególne Wymagania Bezpieczeństwa Systemu oraz Procedury Bezpiecznej Eksploatacji danego systemu lub sieci teleinformatycznej, sporządzone zgodnie z zasadami określonymi w ustawie,

11. Urzędem - jest Urząd Gminy i Miasta w Rychwale,

12. Burmistrzem - jest Burmistrz Rychwała,

13. Pełnomocnikiem ochrony - jest Pełnomocnik do Spraw Ochrony Informacji Niejawnych w Urzędzie Gminy i Miasta w Rychwale,

14. Pionem ochrony - jest wyspecjalizowana komórka Urzędu wykonująca zadania z zakresu ochrony informacji niejawnych.

III. OCENA ZAGROŻEŃ ZEWNĘTRZNYCH I WEWNĘTRZNYCH DLA INFORMACJI NIEJAWNYCH

a. OCENA ZAGROŻEŃ ZEWNĘTRZNYCH

1. Zagrożeniami zewnętrznymi dla Urzędu są:

- 1) możliwość napadu przez zorganizowane grupy przestępcze i terrorystyczne, działające w sposób profesjonalny, przemyślany i zorganizowany,
- 2) możliwość napadu przez pojedynczych przestępców, przypadkowe osoby wykorzystujące nadarżającą się okazję z powodu nieprawidłowości w ochronie mienia Urzędu,
- 3) zagrożenia naturalne (związane z działalnością sił przyrody) i cywilizacyjne (związane z działalnością człowieka).

2. Symptomy mogące świadczyć o przygotowaniu napadu lub włamania do budynku:

- 1) wzmożone zainteresowanie osób postronnych obiektami, pomieszczeniami Urzędu, objawiające się m. in. podejmowaniem prób uzyskania informacji o obiektach lub pomieszczeniach podczas rozmów z pracownikami,
- 2) nawiązanie rozmów przez osoby postronne z pracownikami,
- 3) podszywanie się pod byłych pracowników Urzędu i przejawianie zainteresowania tym, co się po latach zmieniło,
- 4) interesowanie się osobami funkcyjnymi, w tym także ich przywarami oraz sposobem wykonywania obowiązków służbowych,
- 5) obserwacja sposobu działania systemu ochronnego, sekretariatu, sprzątaczk, itp.,
- 6) rozpoznawanie systemu technicznych zabezpieczeń, w tym stosowanych urządzeń alarmowych,
- 7) celowe uszkodzanie urządzeń alarmowych, linii telefonicznych, oświetlenia itp.,
- 8) próby pozyskania do grup przestępczych pracowników Urzędu.

3. Wnioski:

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

- 1) systematyczną, skrupulatną i wnikliwą kontrolę systemu ochrony przez osoby odpowiedzialne za jego organizację,
- 2) pracownicy pionu ochrony w czasie dnia pracy powinni zwracać szczególną uwagę na możliwość zaistnienia ewentualnych zagrożeń,
- 3) stosować zasadę niedopuszczania osób niepowołanych do penetracji strefy bezpieczeństwa,
- 4) wykonywanie prac porządkowych, remontowych itp. w strefie bezpieczeństwa wyłącznie pod nadzorem osób odpowiedzialnych,
- 5) wykorzystanie ostrzeżeń dotyczących zagrożeń naturalnych i cywilizacyjnych dla budynku Urzędu.

b. OCENA ZAGROŻEŃ WEWNĘTRZNYCH

1. Zagrożeniami wewnętrznymi dla Urzędu są:

- 1) próby zaboru dokumentów lub mienia przez pracowników Urzędu,
- 2) próby powielania, kserowania dokumentów służbowych dla celów prywatnych,
- 3) byli pracownicy Urzędu zwolnieni dyscyplinarnie,
- 4) rozpoznanie organizacji pracy Urzędu celem łatwiejszej pracy grup przestępczych na terenie Urzędu,
- 5) próby wglądu w dokumenty niejawne przez osoby nieuprawnione,
- 6) spożywanie alkoholu lub używanie środków odurzających - przesłanka do wykroczeń dyscyplinarnych i przestępstw,
- 7) świadome lub nieświadome, nieupoważnione zapoznanie się z dokumentami niejawnymi,
- 8) niezajomość przepisów o ochronie informacji niejawnych,
- 9) bagatelizowanie przepisów o ochronie informacji niejawnych oraz potencjalnych zagrożeń.

2. Wnioski:

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

- 1) zwracanie szczególnej uwagi na osoby, które mogą być zainteresowane zaborem dokumentu,
- 2) prowadzenie szczególnego nadzoru by nie dokonywano prób kserowania, kopiowania bez zgody przełożonego,

- 3) uwrażliwienie pracowników w trakcie prowadzonych szkoleń na możliwość prób kontaktu grup przestępczych z pracownikami, którzy mają dostęp do dokumentów szczególnie ważnych,
- 4) zastosowanie zasady, że do informacji niejawnych mogą mieć dostęp tylko pracownicy posiadający poświadczenie bezpieczeństwa lub właściwe upoważnienie jednorazowe wydane przez Burmistrza,
- 5) staranne szkolenie osób w zakresie ochrony informacji niejawnych,
- 6) materiały zawierające informacje niejawne muszą być przetwarzane i wykonywane tak, aby minimalizować ryzyko ich zniszczenia na skutek wypadków losowych,
- 7) zwrócenie szczególnej uwagi na osoby, których zachowanie wskazuje na spożywanie alkoholu.

c. POSTĘPOWANIE W SYTUACJACH KRYZYSOWYCH

1. W przypadku wystąpienia sytuacji kryzysowych np. pożar, powódź, należy w pierwszej kolejności powiadomić Burmistrza oraz osoby odpowiedzialne za pomieszczenia, w których przechowywane są dokumenty o klauzuli „zastrzeżone” i pracowników Kancelarii Tajnej.
2. W pierwszej kolejności należy zabezpieczyć:
 - a) pieczęcie,
 - b) dokumenty o najwyższej klauzuli tajności,
 - c) kopie zapasowe, jeżeli są przechowywane,
 - d) inne dokumenty i materiały.
3. Dokumenty ewakuuje się w opłombowanych, brezentowych workach ewakuacyjnych. Za ewakuację odpowiedzialny jest kierownik Kancelarii Tajnej.
4. W sytuacji, gdy ewakuacja jest niemożliwa, w pierwszej kolejności należy zniszczyć dokumenty o najwyższych klauzulach, pieczęcie i w miarę możliwości pozostałe dokumenty i materiały.
5. W przypadku zaistnienia stanów nadzwyczajnych (stan wojny, stan wyjątkowy, stan klęski żywiołowej), powiadamia się Burmistrza Rychwała i inne osoby odpowiedzialne, przy pomocy dostępnych środków teletechnicznych, lub gdy to jest niemożliwe, za pomocą gońca.
6. Sposób i kolejność powiadamiania zamieszczono w planie stałego dyżuru, który przechowywany jest w Kancelarii Tajnej. Powiadamia się także Policję, Straż Pożarną i inne służby oraz instytucje, w zależności od zaistniałej sytuacji.
7. Metody postępowania w stanach nadzwyczajnych określone są w Planie stałego dyżuru w Urzędzie Gminy i Miasta w Rychwale.

IV. PRZEDMIOT OCHRONY

Przedmiotem ochrony w Urzędzie, są:

1. Informacje niejawne stanowiące tajemnicę służbową oznaczone klauzulą „poufne” oraz klauzulą „zastrzeżone”.
2. Pomieszczenia, w których są przechowywane i opracowane materiały niejawne.

V. EWIDENCJA INFORMACJI NIEJAWNYCH PODLEGAJĄCYCH OCHRONIE

1. Informacje niejawne stanowiące tajemnicę służbową oznaczone klauzulą „poufne” podlegają ewidencjonowaniu w Kancelarii Tajnej.
2. Dokumenty niejawne oznaczone klauzulą „zastrzeżone” mogą być przechowywane w Kancelarii Tajnej lub poza Kancelarią Tajną.

3. Dokumenty niejawne wpływające do Urzędu podlegają ewidencjonowaniu w dzienniku korespondencji.
4. Dokumenty niejawne wytworzone - wychodzące z Urzędu rejestruje się w dzienniku ewidencji wykonanych dokumentów.
5. Każdy dokument niejawny przychodzący lub wychodzący z Urzędu ewidencjonuje się w odrębnej pozycji właściwego dziennika ewidencyjnego.
6. Numer ewidencyjny każdego dokumentu niejawnego stanowiącego tajemnicę służbową o klauzuli „poufne” lub „zastrzeżone” poprzedzony jest skrótem literowym, odpowiednio - „Pf” lub „Z”.
7. Ewidencjonowaniu w Kancelarii Tajnej podlegają wszystkie dokumenty zawierające informacje stanowiące tajemnicę służbową.
8. Sposób właściwego opisanie dokumentu niejawnego został przedstawiony w załączniku nr 3 do planu ochrony.

VI. ZABEZPIECZENIE INFORMACJI NIEJAWNYCH, FIZYCZNA OCHRONA DOKUMENTACJI NIEJAWNEJ

1. W celu zmniejszenia ryzyka zapoznania się z informacjami niejawnymi przez osoby do tego nieuprawnione tworzy się strefy ograniczonego dostępu. Wyróżniane są 3 strefy:
 - 1) administracyjna - służąca do kontroli „przepływu” osób i pojazdów,
 - 2) bezpieczeństwa - obejmująca pomieszczenia, w których przechowywane są dokumenty niejawne,
 - 3) specjalne pomieszczenie, zabezpieczone przed podglądem z zewnątrz, wyposażone w odpowiednie szafy metalowe, zwane Kancelarią Tajną.Schemat rozmieszczenia stref zawiera załącznik nr 8 do planu ochrony.
2. Informacje niejawne stanowiące tajemnicę służbową oznaczone klauzulą „poufne”, wymagają przechowywania i zabezpieczania w Kancelarii Tajnej, oddzielnie w odrębnych szafach metalowych.
3. W przypadkach uzasadnionych, podyktowanych względami dłuższego okresu czasu, niezbędnego do realizacji zadań związanych z dostępem do informacji niejawnych, dokumenty oznaczone klauzulą „poufne”, mogą być wydawane poza Kancelarię Tajną, ale jedynie w sytuacji, gdy odbiorca dokumentu zapewnia warunki ochrony tych dokumentów przechowując je w szafach metalowych z odpowiednim zamknięciem.
4. Szafy metalowe, w których przechowywane są dokumenty oznaczone klauzulą „poufne”, podlegają codziennemu, po zakończeniu pracy, zamykaniu i plombowaniu.
5. Informacje niejawne stanowiące tajemnicę służbową oznaczone klauzulą „zastrzeżone” można przechowywać w pomieszczeniu Kancelarii Tajnej lub na stanowiskach pracy w meblach biurowych zamykanych na klucz.
6. Zakres specjalnych środków ochrony fizycznej dokumentacji niejawnej określa rozporządzenie Rady Ministrów w sprawie organizacji i funkcjonowania kancelarii tajnych (Dz. U. z 2005 r. Nr 208, poz. 1741).

VII. ZASADY DOSTĘPU DO INFORMACJI NIEJAWNYCH STANOWIĄCYCH TAJEMNICĘ SŁUŻBOWĄ - POSTĘPOWANIE SPRAWDZAJĄCE

1. Informacje niejawne stanowiące tajemnicę służbową oznaczone klauzulą „poufne” lub „zastrzeżone” mogą być udostępniane wyłącznie osobie uprawnionej do dostępu do informacji niejawnych o określonej klauzuli niejawności.

2. Uzyskanie uprawnień do dostępu do informacji niejawnych może nastąpić:

1) po przeprowadzeniu zwykłego postępowania sprawdzającego i po uzyskaniu przez daną osobę poświadczenia bezpieczeństwa,

2) po przeszkoleniu tej osoby, w zakresie ochrony informacji niejawnych, kończącym się wydaniem określonego przepisami zaświadczenia.

3. Postępowanie sprawdzające zwykłe do dostępu do informacji niejawnych stanowiących tajemnicę służbową oznaczonych klauzulą „poufne”, a także w związku z dostępem do informacji niejawnych stanowiących tajemnicę służbową oznaczonych klauzulą „zastrzeżone” przeprowadza pełnomocnik ochrony, na pisemne polecenie Burmistrza Rychwała.

4. Każda osoba, w odniesieniu do której będzie przeprowadzane postępowanie sprawdzające obowiązana jest do:

1) wypełnienia określonej przepisami ankiety bezpieczeństwa osobowego,

2) wypełnienia ankiety w sposób dokładny i zgodny z prawdą.

5. Odmowa poddania się postępowaniu sprawdzającemu, ze strony osoby, która jest lub będzie zatrudniona na stanowisku związanym z dostępem do informacji niejawnych stanowiących tajemnicę służbową o klauzuli „poufne” lub „zastrzeżone”, a w związku z tym nieuzyskanie poświadczenia bezpieczeństwa warunkującego dostęp do informacji podlegających ochronie skutkować może:

1) przeniesieniem danej osoby na stanowisko nie związane z informacjami niejawnymi,

2) rozwiązaniem umowy o pracę w przypadku niemożności zmiany stanowiska,

3) niemożnością zatrudnienia na danym stanowisku, w odniesieniu do osoby ubiegającej się o zatrudnienie w Urzędzie.

6. Burmistrz może wyrazić w formie pisemnej zgodę na udostępnienie informacji niejawnych stanowiących tajemnicę służbową osobie, która jest zatrudniona lub wykonuje prace zlecone, wobec której wszczęto zwykłe postępowanie sprawdzające.

7. W wyjątkowych, szczególnie uzasadnionych przypadkach, Burmistrz może wyrazić pisemną zgodę na jednorazowe udostępnienie określonych informacji niejawnych osobie nieposiadającej odpowiedniego poświadczenia bezpieczeństwa w trybie art. 49 ust. 2 ustawy o ochronie informacji niejawnych. Jednorazowe wyrażenie zgody na udostępnienie informacji niejawnych powinno określać zakres podmiotowy i przedmiotowy udostępnienia oraz nie oznacza zmiany lub zniesienia ich klauzul tajności - wzór upoważnienia stanowi załącznik nr 7 do planu ochrony.

VIII. POSTĘPOWANIE Z INFORMACJAMI NIEJAWNymi OZNACZONYMI KLAUZULĄ „ZASTRZEŻONE”

1. Do obiegu dokumentów zawierających informacje niejawne stanowiące tajemnicę służbową oznaczone klauzulą „zastrzeżone” stosuje się przepisy instrukcji kancelaryjnej obowiązującej w Urzędzie.

2. Zasady postępowania z dokumentami zawierającymi informacje niejawne stanowiące tajemnicę służbową oznaczone klauzulą „zastrzeżone” określają „Szczegółowe wymagania w

zakresie ochrony informacji niejawnych oznaczonych klauzulą „zastrzeżone”, obowiązujące w Urzędzie Gminy i Miasta w Rychwale”, określono w załączniku nr 3 do planu ochrony.

IX. KANCELARIA TAJNA

a. POSTANOWIENIA OGÓLNE

W Urzędzie funkcjonuje Kancelaria Tajna, która wymaga zabezpieczenia i wyposażenia zgodnie z rozporządzeniem Rady Ministrów z dnia 18 października 2005 r. w sprawie organizacji i funkcjonowania kancelarii tajnych (Dz. U. Nr 208, poz. 1741).

1. Kancelarię Tajną tworzy Burmistrz Rychwała.

2. Kancelarią kieruje kierownik Kancelarii wyznaczony przez Burmistrza na wniosek pełnomocnika ochrony.

3. Do obowiązków kierownika Kancelarii Tajnej należy:

1) bezpośredni nadzór nad obiegiem dokumentów niejawnych w referatach i na innych stanowiskach pracy Urzędu,

2) udostępnianie lub wydawanie dokumentów osobom do tego uprawnionym,

3) egzekwowanie zwrotu dokumentów,

4) kontrola przestrzegania właściwego oznaczania dokumentów zawierających informacje niejawne, wykonanych w Urzędzie,

5) prowadzenie bieżącej kontroli postępowania z dokumentami,

6) wykonywanie poleceń pełnomocnika ochrony.

4. W przypadku zmiany na stanowisku kierownika Kancelarii Tajnej sporządza się protokół zdawczo-odbiorczy.

5. Protokół, o którym mowa w pkt 4 sporządza się w obecności Kierownika zdającego obowiązki, osoby przejmującej obowiązki Kierownika oraz pełnomocnika ochrony. Protokół sporządza się w dwóch egzemplarzach, pierwszy egzemplarz przechowywany jest w Kancelarii Tajnej, drugi u pełnomocnika ochrony.

6. W przypadku czasowej nieobecności kierownika Kancelarii jego obowiązki przejmuje upoważniony pracownik pionu ochrony, w razie jego braku Kancelarię Tajną przejmuje protokolarnie inny pracownik wyznaczony przez Burmistrza na wniosek pełnomocnika ochrony.

7. Dokumenty lub materiały niejawne oznaczone klauzulą „poufne” przechowywane są w szafach o odpowiedniej klasie odporności - w szafach stalowych klasy A.

8. Dokumenty i materiały oznaczone różnymi klauzulami tajności są przechowywane w odrębnych szafach lub pomieszczeniach, chyba, że wchodzi one w skład zbioru dokumentów.

9. Dokumenty i materiały, o których mowa w pkt 8, mogą być przechowywane w jednej szafie lub pomieszczeniu pod warunkiem ich fizycznego oddzielenia w sposób umożliwiający osobne zamknięcie. W takim przypadku szafa lub pomieszczenie musi spełniać wymagania dla najwyższej klauzuli tajności przechowywanych w nich dokumentów lub materiałów.

10. Po zakończeniu pracy kierownik Kancelarii Tajnej jest obowiązany sprawdzić prawidłowość zamknięcia szaf i pomieszczeń Kancelarii.

11. Zasady i sposób zdawania, przechowywania i wydawania kluczy oraz ich duplikatów do pomieszczeń oraz szaf Kancelarii Tajnej określa pkt XVIII Planu ochrony.

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

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

14. W Kancelarii Tajnej przyjmuje się, rejestruje, przechowuje, przekazuje i wysyła dokumenty oraz prowadzi:

- 1) rejestr dzienników, książek ewidencyjnych i teczek,
- 2) dziennik korespondencyjny,
- 3) dziennik ewidencji wykonanych dokumentów oznaczonych klauzulą „poufne” i „zastrzeżone”,
- 4) książkę doręczeń przesyłek miejscowych.

Wzory w/w dokumentów określają załączniki do rozporządzenia Rady Ministrów z dnia 18 października 2005 r. w sprawie organizacji i funkcjonowania kancelarii tajnych. *

15. W przypadkach uzasadnionych organizacją ochrony informacji niejawnych Kancelaria Tajna może prowadzić także inne rejestry niż wymienione w pkt 14, w tym odrębne rejestry dla dokumentów oznaczonych różnymi klauzulami tajności.

b. POSTĘPOWANIE Z PRZESYŁKAMI

1. Kierownik lub pracownik Kancelarii Tajnej przyjmuje przesyłki lub dokumenty za pokwitowaniem i odciska na nich pieczęć oraz datę wpływu do Urzędu.

2. Przyjmując przesyłkę sprawdza:

- 1) prawidłowość adresu,
- 2) całość pieczęci i opakowania,
- 3) zgodność odcisku pieczęci na opakowaniu z nazwą jednostki nadawcy,
- 4) zgodność numeru na przesyłce z numerem tej przesyłki w wykazie lub w książce doręczeń.

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

4. Po otwarciu przesyłki kierownik Kancelarii Tajnej:

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

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

6. Kierownik Kancelarii Tajnej odnotowuje fakt sporządzenia protokołu, o którym mowa w pkt 3 i 5, w odpowiednim dzienniku w rubryce „Informacje uzupełniające/Uwagi”.

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

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

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

10. W przypadku zwrotu do Kancelarii Tajnej przesyłki, o której mowa w pkt 1, kierownik Kancelarii Tajnej uzupełnia dane dotyczące przesyłki w odpowiednim dzienniku.

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

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

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

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

15. Zabrania się wycierania i zamazywania adnotacji.

16. Dokumenty, materiały oraz zbiory dokumentów dotyczące spraw ostatecznie zakończonych przechowuje się w Kancelarii Tajnej jako materiały archiwalne.

c. OBOWIĄZKI OSÓB FUNKCYJNYCH

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

2. Sprawdzić stan zabezpieczeń szaf i sprzętu komputerowego.

3. Przestrzegać zasad zakazu wstępu osobom nieuprawnionym do Kancelarii Tajnej.

4. W miarę możliwości niezbędne sprawy załatwiać w strefie bezpieczeństwa.

5. Stosować zasadę, że do Kancelarii Tajnej wstęp mogą mieć tylko osoby posiadające poświadczenie bezpieczeństwa oraz zaświadczenie o przeszkoleniu.

X. ZASADY WYKONYWANIA DOKUMENTÓW ZAWIERAJĄCYCH INFORMACJE NIEJAWNE

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

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

3. Rękopisy sporządzonych dokumentów, zawierające informacje niejawne, muszą być wykonane w brulionach uprzednio zarejestrowanych w Kancelarii Tajnej. Z wykorzystanych brulionów osoba za nie odpowiedzialna rozlicza się w Kancelarii Tajnej.

4. Dokumenty niejawne powinny być opisane i oznaczone zgodnie z rozporządzeniem Prezesa Rady Ministrów z dnia 29 września 2005 r. w sprawie sposobu oznaczania materiałów, umieszczania na nich klauzul tajności, a także zmiany nadanej klauzuli tajności (Dz. U. Nr 205, poz. 1696). Wzór sposobu opisanie dokumentu stanowi załącznik nr 2 do Planu ochrony.

XI. WYKONYWANIE DOKUMENTÓW ZAWIERAJĄCYCH INFORMACJE NIEJAWNE ZA POMOCĄ KOMPUTERA

ZABRANIA SIĘ PRZETWARZANIA I WYKONYWANIA DOKUMENTÓW ZAWIERAJĄCYCH INFORMACJE NIEJAWNE POZA KANCELARIĄ TAJNĄ.

Pracownicy, którzy do opracowywania i wykonywania dokumentów zawierających informacje stanowiące tajemnicę służbową, oznaczone klauzulami „poufne” lub „zastrzeżone”, wykorzystują urządzenia komputerowe, obowiązani są zabezpieczać informacje podlegające ochronie przed ich nieuprawnionym ujawnieniem, a także przed dotarciem do tych informacji przez osoby, które nie powinny zapoznać się z ich treścią.

1. Bezpieczeństwo teleinformatyczne zapewnia się, chroniąc informacje przetwarzane w systemach i sieciach teleinformatycznych przed utratą właściwości gwarantujących to bezpieczeństwo, w szczególności przed utratą poufności, dostępności i integralności.

2. Bezpieczeństwo teleinformatyczne zapewnia się przed rozpoczęciem oraz w trakcie przetwarzania informacji niejawnych w systemie lub sieci teleinformatycznej.

3. Za właściwą organizację bezpieczeństwa teleinformatycznego odpowiada Burmistrz, który w szczególności:

1) zapewnia opracowanie dokumentacji bezpieczeństwa teleinformatycznego,

2) realizuje ochronę fizyczną, elektromagnetyczną i kryptograficzną systemu lub sieci teleinformatycznej,

3) zapewnia niezawodność transmisji oraz kontrolę dostępu do urządzeń systemu lub sieci teleinformatycznej,

4) dokonuje analizy stanu bezpieczeństwa teleinformatycznego oraz zapewnia usunięcie stwierdzonych nieprawidłowości,

5) zapewnia przeszkolenie z zakresu bezpieczeństwa teleinformatycznego dla osób uprawnionych do pracy w systemie lub sieci teleinformatycznej,

6) zawiadamia właściwą służbę ochrony państwa o zaistniałym incydencie bezpieczeństwa teleinformatycznego dotyczącym informacji niejawnych oznaczonych co najmniej klauzulą „poufne”.

4. Ochrona fizyczna systemu lub sieci teleinformatycznej polega na:

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

a) klauzuli tajności,

b) ilości,

c) zagrożeń dla poufności, integralności lub dostępności informacji niejawnych,

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

a) nieuprawnionym dostępem,

b) podglądem,

c) podsłuchem.

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

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

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

6. Ochronę elektromagnetyczną systemu lub sieci teleinformatycznej zapewnia się w szczególności przez umieszczenie urządzeń teleinformatycznych, połączeń i linii w strefach kontrolowanego dostępu spełniających wymagania w zakresie tłumienności elektromagnetycznej odpowiednio do wyników szacowania ryzyka dla informacji niejawnych lub zastosowanie odpowiednich urządzeń teleinformatycznych, połączeń i linii o obniżonym

poziomie emisji lub ich ekranowanie z jednoczesnym filtrowaniem zewnętrznych linii zasilających i sygnałowych.

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

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

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

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

9. Systemy i sieci teleinformatyczne, w których mają być wytwarzane, przetwarzane, przechowywane lub przekazywane informacje niejawne podlegają akredytacji bezpieczeństwa teleinformatycznego przez służby ochrony państwa.

10. Akredytacja następuje na podstawie dokumentów szczególnych wymagań bezpieczeństwa i procedur bezpiecznej eksploatacji.

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

12. Burmistrz wyznacza:

1) osobę odpowiedzialną za funkcjonowanie systemów i sieci teleinformatycznych oraz za przestrzeganie zasad i wymagań bezpieczeństwa systemów i sieci teleinformatycznych zwaną administratorem systemu,

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

XII. GROMADZENIE DOKUMENTÓW ZAWIERAJĄCYCH INFORMACJE NIEJAWNE

1. Dokumenty zawierające informacje niejawne stanowiące tajemnicę służbową oznaczone klauzulą „poufne” i „zastrzeżone” podlegają gromadzeniu w teczkach akt oznaczonych właściwą klauzulą tajności.

2. Dokumenty ostatecznie załatwionych spraw, po zakończeniu roku, wymagają wszywania do teczek akt, zgodnie z rzeczowym wykazem akt. Całość zawartości teczki kwalifikuje się według dokumentu o najwyższej klauzuli tajności.

3. Dokumenty niejawne o klauzuli „poufne” muszą być przechowywane w Kancelarii Tajnej. W szczególnie uzasadnionych przypadkach dokumenty te mogą być przechowywane poza Kancelarią Tajną, Burmistrz lub pełnomocnik ochrony mogą wyrazić pisemną zgodę na przechowywanie dokumentów poza pomieszczeniami Kancelarii Tajnej, pod warunkiem spełnienia wymogów bezpieczeństwa odpowiednich do tej klauzuli, na czas niezbędny do realizacji zadań związanych z dostępem do tych dokumentów.

XIII. NADAWANIE, ZMIANA I ZNOSZENIE KLAUZULI TAJNOŚCI MATERIAŁOM NIEJAWNYM

a. NADAWANIE KLAUZULI TAJNOŚCI

1. Oznaczenie materiału klauzulą tajności polega na umieszczeniu na nim odpowiedniej klauzuli tajności. Przyznaną klauzulę tajności nanosi się w sposób wyraźny i w pełnym jej brzmieniu.
2. Informacje niejawne zaklasyfikowane jako stanowiące tajemnicę służbową oznacza się klauzulą:
 - 1) „poufne” - w przypadku, gdy ich nieuprawnione ujawnienie powodowałoby szkodę dla interesów państwa, interesu publicznego lub prawnie chronionego interesu obywateli;
 - 2) „zastrzeżone” - w przypadku, gdy ich nieuprawnione ujawnienie mogłoby spowodować szkodę dla prawnie chronionych interesów obywateli albo jednostki organizacyjnej.
3. Stosuje się następujące oznaczenia klauzul tajności dla dokumentów niejawnych stanowiących tajemnicę służbową:
 - 1) „Pf” - dla klauzuli „poufne”,
 - 2) „Z” - dla klauzuli „zastrzeżone”.
4. Materiały zawierające informacje niejawne utrwalone na piśmie oznacza się w następujący sposób:
 - 1) na pierwszej stronie pisma umieszcza się:
 - a) w lewym górnym rogu nazwę jednostki lub komórki organizacyjnej,
 - b) w prawym górnym rogu, w kolejności pionowej:
nazwę miejscowości i datę podpisania pisma,
klauzulę tajności,
numer egzemplarza pisma, a w przypadku, gdy pismo sporządzono w jednym egzemplarzu napis „Egz. pojedynczy”, napis o treści: „podlega ochronie do ...”, jeżeli został określony krótszy niż wskazany w art. 25 ust. 3 ustawy o ochronie informacji niejawnych okres ochrony informacji niejawnych stanowiących tajemnicę służbową
 - c) w lewym dolnym rogu numer, pod jakim pismo zostało zarejestrowane w dzienniku ewidencji wykonanych dokumentów,
 - d) w prawym dolnym rogu klauzulę tajności oraz numer strony łamany przez liczbę stron całego pisma,
 - 2) w przypadku pisma, któremu nadano bieg korespondencyjny dodatkowo:
 - a) w lewym górnym rogu pod nazwą jednostki lub komórki organizacyjnej sygnaturę literowo-cyfrową, na którą składają się: literowe oznaczenia jednostki lub komórki organizacyjnej oraz numer, pod którym pismo zostało zarejestrowane w odpowiednim dzienniku, łamany przez rok lub dwie ostatnie cyfry roku, w którym pismo zostało sporządzone, poprzedzone literami „Pf” -w przypadku pisma oznaczonego klauzulą „poufne”, literą „Z” -w przypadku pisma oznaczonego klauzulą „zastrzeżone”, oddzielonymi od numeru rejestracyjnego myślnikiem, a także w zależności od potrzeb - inne oznaczenia ułatwiające ustalenie miejsca jego sporządzenia w jednostce lub komórce organizacyjnej nadawcy lub też przynależność pisma do określonej sprawy,
 - b) w prawym górnym rogu pod numerem egzemplarza w kolejności pionowej: nazwę stanowiska adresata, imię i nazwisko oraz nazwę miejscowości, jednakże w przypadku wielu adresatów dopuszcza się umieszczenie jedynie adnotacji „adresaci według rozdzielnika”,
 - 3) na kolejnych stronach pisma umieszcza się:
 - a) w prawym górnym rogu w kolejności pionowej:
klauzulę tajności,
numer egzemplarza pisma, a w przypadku sporządzenia go w jednym egzemplarzu napis „Egz. pojedynczy”,
 - b) w lewym dolnym rogu numer, pod jakim pismo zostało zarejestrowane w dzienniku ewidencji wykonanych dokumentów,

c) w prawym dolnym rogu klauzulę tajności, numer strony łamany przez liczbę stron całego pisma,

4) na ostatniej stronie pisma umieszcza się:

a) w prawym górnym rogu w kolejności pionowej:

klauzulę tajności,

numer egzemplarza pisma, a w przypadku sporządzenia go w jednym egzemplarzu napis „Egz. pojedynczy”,

b) z lewej strony pod treścią:

liczbę załączników, jeżeli są dołączone do pisma,

klauzule tajności załączników wraz z numerami, pod jakimi zostały zarejestrowane w odpowiednim dzienniku,

liczbę stron każdego załącznika,

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, oraz napis „do zwrotu” - jeżeli załączniki mają zostać zwrócone osobie podpisującej pismo,

c) z prawej strony pod treścią pisma i adnotacją o załącznikach w kolejności pionowej: stanowisko oraz imię i nazwisko osoby je podpisującej,

d) w lewym dolnym rogu w kolejności pionowej:

liczbę wykonanych egzemplarzy,

adresatów poszczególnych egzemplarzy pisma lub adnotację „Adresaci według rozdzielnika”,

nazwisko lub inne dane identyfikujące sporządzającego i wykonawcę,

numer, pod jakim pismo zostało zarejestrowane w dzienniku ewidencji wykonanych dokumentów,

e) w prawym dolnym rogu klauzulę tajności oraz numer strony łamany przez liczbę stron całego pisma,

5) W przypadku pisma, któremu nadano bieg korespondencyjny, na pierwszej stronie w prawym górnym rogu pod numerem egzemplarza można zamieścić dyspozycję dla adresata o treści:

a) „udzielanie informacji tylko za pisemną zgodą nadawcy”,

b) „kopiowanie tylko za pisemną zgodą nadawcy”,

c) „odpis tylko za pisemną zgodą nadawcy

d) „kopiowanie stron ... tylko za pisemną zgodą nadawcy”,

e) „odpis od ... do ... tylko za pisemną zgodą nadawcy”,

f) „wypis (wyciąg) od ... do ... tylko za pisemną zgodą nadawcy”.

5. Na pismach stanowiących załączniki:

1) na pierwszej stronie w prawym górnym rogu umieszcza się dodatkowo napis: „Załącznik nr... do pisma nr... z dnia ...”,

2) napis, o którym mowa w ppkt 1, zamieszcza się - w miarę możliwości - na innych niż pismo materiałach.

6. Jeżeli przy piśmie przewodnim przesyła się załączniki oznaczone różnymi klauzulami tajności, to:

1) klauzula pisma przewodniego lub dokumentu uwzględnia klauzulę załącznika o najwyższym stopniu tajności,

2) na piśmie przewodnim zamieszcza się dyspozycję co do klauzuli tajności pisma po trwałym odłączeniu załączników; na każdej stronie pod numerem egzemplarza zamieszcza się napis: „...(nazwa klauzuli tajności) po odłączeniu załączników” lub „jawne po odłączeniu załączników”.

7. Na piśmie przewodnim, jeżeli jego treść jest jawna, nie umieszcza się numeru według dziennika ewidencji wykonanych dokumentów, a przy jego rejestracji, w rubryce „Informacje uzupełniające/Uwagi” dziennika korespondencyjnego, należy wpisać adnotację „pismo przewodnie jawne”.

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

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

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

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

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

2) na pierwszej stronie dodatkowo numer, pod jakim zostały zarejestrowane w dzienniku ewidencji wykonanych dokumentów, numer egzemplarza wykonanej kopii, odpisu, wypisu, wyciągu lub tłumaczenia,

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

12. Zgodność z oryginałem kopii, odpisu, wypisu lub wyciągu potwierdza podpisem Burmistrz, Zastępca Burmistrza albo pełnomocnik ochrony, a tłumaczenia - osoba dokonująca tłumaczenia.

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

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

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

3) dacie sporządzenia kopii, odpisu, wypisu, wyciągu lub tłumaczenia,

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

14. Adnotacje, o których mowa w pkt 11 ppkt 1-3, wpisuje się przed wykonaniem kopii, odpisu, wypisu, wyciągu lub tłumaczenia, natomiast numer, pod jakim zostały zarejestrowane w dzienniku ewidencji wykonanych dokumentów, nanosi się po wykonaniu kopii, odpisu, wypisu, wyciągu lub tłumaczenia.

b. ZMIANA I ZNOSZENIE KLAUZULI TAJNOŚCI

1. Na pismach zawierających informacje niejawne, wobec których zniesiono przyznaną klauzulę tajności lub minął ustawowy okres ochrony lub ustanowiony przez osobę, o której mowa w art. 21 ust. 1 ustawy o ochronie informacji niejawnych:

1) skreśla się klauzulę tajności na każdej stronie w prawym górnym i dolnym rogu,

2) na pierwszej stronie nad skreśloną klauzulą tajności w prawym górnym rogu umieszcza się dodatkowo napis „Jawne” oraz datę, imię, nazwisko i podpis osoby dokonującej tych adnotacji.

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

1) na każdej stronie w prawym górnym i dolnym rogu skreśla się dotychczasowe klauzule tajności,

2) nad skreślonymi klauzulami tajności umieszcza się nowe klauzule tajności,

3) na pierwszej stronie nad skreśloną klauzulą tajności w prawym górnym rogu umieszcza się datę, imię, nazwisko i podpis osoby dokonującej tych adnotacji.

3. Na pismach zawierających informacje niejawne, których okres ochrony uległ skróceniu lub przedłużeniu, na pierwszej stronie w prawym górnym rogu nad klauzulą tajności umieszcza się odpowiednio napis: „Skrócono okres ochrony do dnia ...” albo „Przedłużono okres ochrony do dnia ...”, a także datę, imię i nazwisko oraz podpis osoby dokonującej tych adnotacji.

4. Skreśleń i adnotacji, dokonuje odpowiednio kierownik Kancelarii Tajnej lub pełnomocnik ochrony.

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

6. W stosunku do pism znajdujących się w zbiorach dokumentów zawierających informacje niejawne, wobec których minął ustanowiony okres ochrony, czynności, o których mowa w ust 2 - 5 można dokonać najpóźniej w przypadku ich udostępniania lub przekazywania osobom spoza jednostki lub komórki organizacyjnej.

7. W stosunku do materiałów innych niż pisma przepisy pkt 2 - 5 stosuje się odpowiednio, uwzględniając sposób oznakowania tych materiałów.

XIV. OKRESY OCHRONNE DLA DOKUMENTÓW NIEJAWNYCH

1. Informacje niejawne stanowiące tajemnicę służbową podlegają ochronie przez okres:

1) 5 lat od daty wytworzenia - oznaczone klauzulą „poufne”,

2) 2 lat od daty wytworzenia - oznaczone klauzulą „zastrzeżone”.

2. Wytwórca dokumentu po dokonaniu przeglądu dokumentu może określić:

1) krótszy okres ochronny,

2) przedłużać okres ochrony tych informacji na kolejne okresy nie dłuższe niż 5 lat - dla oznaczonych klauzulą „poufne” i 2 lat - dla oznaczonych klauzulą „zastrzeżone”, nie dłużej jednak niż na okres do 20 lat od daty wytworzenia tych informacji.

3. Akta spraw zakończonych oznaczonych klauzulą „poufne” przechowuje się w Kancelarii Tajnej przez okres 5 lat, „zastrzeżone” przez okres 2 lat. Po zniesieniu okresu ochronnego dokumenty te można przekazać do archiwum zakładowego celem dalszego przechowywania.

XV. NADZÓR W ZAKRESIE OCHRONY INFORMACJI NIEJAWNYCH

1. Za ochronę informacji niejawnych w Urzędzie Gminy i Miasta w Rychwale odpowiada Burmistrz.

2. Zadania określone ustawą o ochronie informacji niejawnych w imieniu Burmistrza wykonuje pełnomocnik ochrony poprzez:

1) sprawowanie nadzoru nad realizacją zadań i przestrzeganiem przepisów określonych w Planie ochrony,

2) sprawowanie kontroli w zakresie ochrony informacji niejawnych oraz przestrzegania związanych z upoważnianiem do dostępu do tych informacji, w odniesieniu do wszystkich komórek organizacyjnych Urzędu.

XVI. 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 niejawnych został określony przepisami kodeksu karnego w art. 266 (ustawa z dnia 06 czerwca 1997 r. kodeks karny, Dz. U. Nr 88, poz. 553 z późn. zm.): § 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 stanowiącą tajemnicę służbową 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. W stosunku do pracowników, którzy nie przestrzegając wymagań związanych z ochroną informacji niejawnych i nierzetelnie wykonując swoje obowiązki, dopuszczają się uchybień w zakresie zabezpieczenia dokumentów i informacji podlegających ochronie, stwarzając warunki do ujawnienia tajemnicy osobom nieuprawnionym, zastosowane być mogą przewidziane prawem sankcje dyscyplinarne i służbowe.

XVII. ARCHIWIZOWANIE, GROMADZENIE I NISZCZENIE MATERIAŁÓW NIEJAWNYCH

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

2. Dokumentacja wytwarzana i gromadzona dzieli się na:

1) materiały archiwalne - wchodzące do państwowego zasobu archiwalnego,

2) dokumentację niearchiwalną - inną dokumentację, niestanowiącą 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 w pkt 3 stanowią podstawę gromadzenia dokumentacji w akta 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, wydzieleniu dokumentacji nieprzydatnej i przekazaniu jej na makulaturę.

7. Brakowanie dokumentacji niearchiwalnej następuje na wniosek Burmistrza na podstawie zgody właściwego archiwum.

8. Do wniosku o zgodę 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.

9. Protokół oraz spis dokumentacji niearchiwalnej sporządza komisja powołana przez Burmistrza, w której skład wchodzi: kierownik referatu zarządzania, osoba prowadząca archiwum zakładowe, przedstawiciel komórki organizacyjnej, której dokumentacja niearchiwalna podlega brakowaniu oraz kierownik Kancelarii Tajnej.

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

11. W archiwum zakładowym przechowuje się dokumenty brakowania, wraz z dowodami przekazania nieprzydatnej dokumentacji niearchiwalnej na makulaturę bądź protokołami jej zniszczenia.

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

13. 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.

14. Opisanie 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) tytułu teczki, to jest nazwy hasła klasyfikacyjnego według wykazu akt, obowiązującego w danej jednostce organizacyjnej, i informacji o rodzaju materiałów archiwalnych, znajdujących się w teczce,
- 4) rocznych dat krańcowych, to jest dat najwcześniejszego i najpóźniejszego materiału archiwalnego w teczce,
- 5) sygnatury teczki, to jest numeru spisu zdawczo-odbiorczego i numeru pozycji teczki w spisie zdawczo-odbiorczym,
- 6) symbolu kwalifikacyjnego materiałów archiwalnych (kategoria A),
- 7) liczby stron w teczce.

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

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

XVIII. PRZECHOWYWANIE KLUCZY I PIECZĘCI

1. Pieczęcie, którymi posługuje się kierownik Kancelarii Tajnej przechowywane są w szafach metalowych w Kancelarii Tajnej.

2. Szafy metalowe Kancelarii Tajnej po zamknięciu powinny być dodatkowo plombowane pieczęcią do plasteliny.

3. Klucze od szaf metalowych po zakończeniu pracy należy złożyć w pomieszczeniu Kancelarii Tajnej w miejscu niewidocznym.

4. Po zakończeniu pracy kierownik Kancelarii Tajnej zamyka i plombuje pieczęcią do plasteliny szafy w Kancelarii Tajnej.

5. Klucz od drzwi wejściowych oraz pieczęć do plasteliny kierownik Kancelarii Tajnej powinien zabezpieczyć tak, by osoby nieuprawnione nie mogły z nich korzystać.

6. Tworzy się zapasowy komplet kluczy Kancelarii Tajnej.
7. Zapasowy komplet kluczy należy umieścić w pojemniku na klucze, który dodatkowo powinien być zabezpieczony pieczęcią do plasteliny.
8. Tak przygotowany komplet kluczy zapasowych należy złożyć za pokwitowaniem do zdeponowania u pełnomocnika ochrony.

XIX. USTALENIA KOŃCOWE

1. Kierownicy Referatów, przełożeni pracowników, a także pełnomocnik ochrony:
 - 1) zapoznają podległych pracowników z ustaleniami Planu ochrony informacji niejawnych w Urzędzie,
 - 2) zapewnią bieżące przestrzeganie postanowień Planu ochrony w zakresie ochrony informacji niejawnych, mogących występować w działalności kierowanej komórki organizacyjnej.
2. Osoby wymienione w pkt 1, wprowadzą jako obowiązującą zasadę, zapoznawania z Planem ochrony wszystkie osoby, które podejmują pracę w komórkach organizacyjnych.
3. W przypadku wystąpienia wątpliwości, a także potrzeby przybliżenia zasad dotyczących realizacji zadań związanych z ochroną informacji niejawnych, sporządzania i wykonania dokumentów zawierających informacje stanowiące tajemnicę służbową, pracownicy Urzędu mogą w każdym czasie zwracać się o wyjaśnienia czy też instruktaż do:
 - 1) pełnomocnika ochrony,
 - 2) kierownika Kancelarii Tajnej.
4. Integralną część Planu ochrony stanowią załączniki w ilości 8, wymienione w dołączonym do Planu ochrony wykazie załączników.

WYKAZ ZAŁĄCZNIKÓW DO PLANU OCHRONY INFORMACJI NIEJAWNYCH W URZĘDZIE GMINY I MIASTA W RYCHWALE

Załącznik nr 1	
Wykaz stanowisk i funkcji oraz rodzajów prac zleconych, z którymi może łączyć się dostęp do informacji niejawnych stanowiących tajemnicę służbową.....	21
Załącznik nr 2	
Sposób oznaczania dokumentów niejawnych stanowiących tajemnicę służbową oraz umieszczania klauzul na tych dokumentach.....	22
Załącznik nr 3	
Szczegółowe wymagania w zakresie ochrony informacji niejawnych stanowiących tajemnicę służbową oznaczonych klauzulą „zastrzeżone”.....	25
Załącznik nr 4	
Instrukcja postępowania na wypadek otrzymania zgłoszenia o podłożeniu ładunku wybuchowego w budynku Urzędu Gminy i Miasta w Rychwale.....	29
Załącznik nr 5	
Instrukcja postępowania w przypadku otrzymania przesyłki niewiadomego pochodzenia.....	32
Załącznik nr 6	
Protokół otwarcia sejfu (szafy metalowej) Kancelarii Tajnej Urzędu Gminy i Miasta w Rychwale.....	33
Załącznik nr 7	
Wzór upoważnienia jednorazowego.....	34
Załącznik nr 8	
Schemat organizacji stref ochronnych.....	35

Wykaz stanowisk i funkcji oraz rodzajów prac zleconych, z którymi może łączyć się dostęp do informacji niejawnych stanowiących tajemnicę służbową.

a. Oznaczonych klauzulą „poufne”

1. Burmistrz Rychwała,
2. Z-ca Burmistrza Rychwała,
3. Sekretarz Gminy,
4. Stanowisko pracy ds. ochrony przeciwpożarowej, wojskowości i zarządzania kryzysowego,
5. Pełnomocnik ds. ochrony niejawnych,
6. Kierownik kancelarii tajnej.

b. Oznaczonych klauzulą „zastrzeżone”

1. Skarbnik Gminy,
2. Informatyk,
3. Inspektor – sekretariat.

c. Rodzaje prac zleconych z których wykonywaniem może łączyć się dostęp do informacji niejawnych stanowiących tajemnicę służbową.

- Projektowanie, instalacja, konserwacja i naprawa systemów zabezpieczeń technicznych,
- Opinie, analizy i ekspertyzy dotyczące ochrony informacji niejawnych, w tym ich ochrony fizycznej,
- Opinie, analizy i ekspertyzy dotyczące ochrony fizycznej i technicznej obiektów,
- Opinie, analizy i ekspertyzy dotyczące bezpieczeństwa mieszkańców i zarządzania kryzysowego, w tym programów współpracy z policją,
- Opinie, analizy i ekspertyzy dotyczące obrony cywilnej, w tym świadczeń na rzecz systemu obronności kraju,
- Opinie, analizy i ekspertyzy wraz ze szczegółową dokumentacją obejmującą bazy danych, systemy teleinformatyczne przetwarzające informacje prawnie chronione, ważne dla interesu publicznego,
- Inne prace służące ochronie interesu publicznego.

**SPOSÓB OZNACZANIA DOKUMENTÓW NIEJAWNYCH
STANOWIĄCYCH TAJEMNICĘ SŁUŻBOWĄ ORAZ UMIESZCZANIA
KLAUZUL NA TYCH DOKUMENTACH**

STRONA PIERWSZA DOKUMENTU

.....
Nazwa jednostki organizacyjnej

.....
Miejscowość, data

KLAUZULA TAJNOŚCI

Egz. Nr

- sygnatura literowo-cyfrowa
- numer z dziennika korespondencji łamany przez dwie ostatnie cyfry roku

ADRESAT

TREŚĆ DOKUMENTU

Nr DEWD

KLAUZULA TAJNOŚCI
Nr strony / ilość stron dokumentu

STRONA DRUGA I KOLEJNE DOKUMENTU

KLAUZULA TAJNOŚCI

Egz. Nr

TREŚĆ DOKUMENTU

Nr DEWD

KLAUZULA TAJNOŚCI
Nr strony / ilość stron dokument

KLAUZULA TAJNOŚCI

Egz. Nr

TREŚĆ DOKUMENTU

Pod treścią- informacja o załącznikach (jeśli występują) :

- liczba załączników
- klauzule tajności załączników wraz z nr ewidencyjnym z DEWD
- liczba stron lub kart każdego załącznika
- w przypadku, gdy adresatowi wysyła się inną liczbę załączników niż pozostawia w aktach, dodatkowo napis „tylko adresat”
- w przypadku, gdy załączniki należy zwrócić - napis „do zwrotu”

.....
stanowisko oraz imię i
nazwisko osoby podpisującej
dokument

- liczba wykonanych egzemplarzy
- adresaci poszczególnych egzemplarzy
- nazwisko osoby, która sporządziła dokument
- nazwisko osoby, która wykonała dokument
- Nr DEWD

KLAUZULA TAJNOŚCI
Nr strony / ilość stron dokumentu

**Szczegółowe wymagania
w zakresie ochrony informacji niejawnych oznaczonych
klauzulą „zastrzeżone” obowiązujące w Urzędzie Gminy i Miasta
w Rychwale**

Rozdział 1

Przestrzeganie zasad ogólnych

§ 1

Zezwala się wszystkim wykonawcom dokumentów (materiałów) o klauzuli „zastrzeżone” na wykonywanie tych dokumentów w pomieszczeniach wykonawcy.

§ 2

Zezwala się na przechowywanie dokumentów (materiałów) o klauzuli „zastrzeżone” w segregatorach lub teczkach tematycznych, razem z dokumentami jawnymi w szafach (lub biurkach) zamykanych na klucz.

§ 3

Zabrania się przekazywania informacji niejawnych o klauzuli „zastrzeżone” w czasie prowadzenia rozmów przez techniczne środki łączności oraz systemy teleinformatyczne, które nie zapewniają właściwego zabezpieczenia tajemnicy.

§ 4

Zabrania się przekazywania w rozmowach i korespondencji prywatnej informacji stanowiących tajemnicę służbową o klauzuli „zastrzeżone”.

§ 5

Zabrania się wykonywania kopii, kserokopii, odpisu, wypisu lub udzielania informacji o treściach zawartych w dokumentach o klauzuli „zastrzeżone”, wytworzonych w Urzędzie bez zgody Burmistrza lub osób upoważnionych przez Burmistrza.

§ 6

Wszystkie dokumenty (materiały) oraz informacje niejawne o klauzuli „zastrzeżone” podlegają okresowej kontroli przez pion ochrony i Pełnomocnika ds. ochrony informacji niejawnych.

§ 7

Dokumenty (materiały) mogą wykonywać wyłącznie osoby uprawnione do dostępu do wiadomości zawierających informacje niejawne i w warunkach gwarantujących ochronę tych informacji.

Rozdział 2

Obieg dokumentów służbowych

§ 8

Dokumenty niejawne oznaczone klauzulą „zastrzeżone” wpływające do Urzędu lub wysyłane przez Urząd, podlegają ewidencjonowaniu i rejestrowaniu (jako przesyłka), w sekretariacie Urzędu, w „Dzienniku Korespondencyjnym” zgodnie z Instrukcją kancelaryjną (w rubryce uwagi należy wpisać- „Z”).

§ 9

Adresat dokumentu o klauzuli „zastrzeżone”, pobiera go osobiście z sekretariatu Urzędu za pokwitowaniem (podpis z datą), a następnie rejestruje dokument w formularzu spisu spraw segregatora tematycznego zgodnie z rzeczowym wykazem akt i tam go przechowuje.

§ 10

Do ewidencji dokumentów niejawnych o klauzuli „zastrzeżone” wykonanych w komórce organizacyjnej lub na stanowisku pracy, służył będzie „DZIENNIK EWIDENCJI WYKONANYCH DOKUMENTÓW” (DEWD), który prowadzi się w ramach kancelarii tajnej.

§ 11

Przy wykonywaniu dokumentu o klauzuli „zastrzeżone”, wykonawca takiego dokumentu postępuje zgodnie z rozporządzeniem Prezesa Rady Ministrów z dnia 5 października 2005 r. w sprawie sposobu oznaczania materiałów, umieszczania na nich klauzul tajności, a także zmiany nadanej klauzuli tajności (Dz.U. Nr 205, poz. 1696).

§ 12

Dokument (materiał) wykonawca rejestruje w „DZIENNIKU EWIDENCJI WYKONANYCH DOKUMENTÓW” (DEWD) o klauzuli „zastrzeżone” po ustaleniu, w jakim segregatorze tematycznym, wykonany dokument będzie przechowywany, nadając mu odpowiedni numer.

§ 13

Wysyłając dokument o klauzuli „zastrzeżone” wykonawca pakuje dokument w dwie nieprzezroczyste i mocne koperty, przy czym na kopertach muszą być umieszczone:

1) na kopercie wewnętrznej:

- a) klauzula tajności i ewentualne dodatkowe oznaczenie,
- b) imienne określenie adresata,
- c) imię, nazwisko i podpis osoby pakującej,
- d) numer, pod którym dokument został zarejestrowany w DEWD;

2) na kopercie zewnętrznej:

- a) nazwa jednostki organizacyjnej adresata,
- b) adres siedziby adresata,
- c) nazwa jednostki organizacyjnej nadawcy,
- d) numer wykazu i pozycji w wykazie przesyłek nadanych.

§ 14

Po sporządzeniu przesyłki, kierownik kancelarii tajnej udaje się z nią i z DEWD do sekretariatu Urzędu, w celu uzyskania potwierdzenia przekazania dokumentu do wysłania.

§ 15

W przypadku wysyłania przesyłki za dowodem doręczenia, kierownik kancelarii tajnej zobowiązany jest dołączyć wypisany druk potwierdzenia odbioru.

Rozdział 3

Archiwizacja dokumentów

§ 16

Dokumenty, materiały lub aktowe zbiory dokumentów, dotyczące spraw ostatecznie zakończonych, mogą być przechowywane w kancelarii (lub innym wydzielonym pomieszczeniu, zapewniającym ich ochronę odpowiednio do przyznanej im klauzuli tajności) nie dłużej niż 2 lata. Po upływie tego okresu przekazuje się je do archiwum/składnicy akt, na podstawie spisów zdawczo-odbiorczych.

§ 17

1. Za logiczne uporządkowanie zbioru dokumentów, stanowiących akta sprawy oraz kwalifikowanie i klasyfikowanie zgodnie z Jednolitym Rzeczowym Wykazem Akt, odpowiada pracownik merytoryczny prowadzący sprawę.

2. Przed przekazaniem akt spraw ostatecznie zakończonych do kancelarii tajnej, archiwum/składnicy, pracownik merytoryczny ma obowiązek dokonania przeglądu oraz dostosowania klauzul zgodnie z art. 25 ust. 3 i 4 ustawy.

3. W przypadku akt spraw ostatecznie zakończonych pozostających na stanie kancelarii czynności, o których mowa w ust. 2, dokonuje kierownik kancelarii tajnej.

4. Sposób porządkowania akt spraw zakończonych, przejmowania ich przez archiwa, wydzielania dokumentacji niearchiwalnej oraz jej brakowania określają odrębne przepisy., w tym § 35 rozporządzenia Prezesa Rady Ministrów z dnia 22 grudnia 1999 r. w sprawie instrukcji kancelaryjnej dla organów gmin i związków międzygminnych (Dz. U. Nr 112, poz. 1319, z późn. zm.).

INSTRUKCJA POSTĘPOWANIA NA WYPADEK OTRZYMANIA ZGŁOSZENIA O PODŁOŻENIU ŁADUNKU WYBUCHOWEGO W BUDYNKU URZĘDU GMINY I MIASTA W RYCHWALE.

I. PROCEDURY POSTĘPOWANIA PO OTRZYMANIU ZGŁOSZENIA O PODŁOŻENIU ŁADUNKU WYBUCHOWEGO W GODZINACH PRACY - TELEFONICZNE ODEBRANIE ZGŁOSZENIA O PODŁOŻENIU ŁADUNKU WYBUCHOWEGO.

1. Gdy usłyszysz słowa: „Podłożyłem ładunek wybuchowy - bombę” nie wpadaj w panikę, zachowaj spokój, postępuj wg poniższych wskazań.
2. Po przyjęciu informacji nie odkładaj słuchawki na widelki, połóż ją obok aparatu telefonicznego.
3. Powiadom natychmiast Burmistrza Rychwała, Zastępcę Burmistrza lub w razie ich nieobecności pełnomocnika ochrony, Komisariat Policji w Rychwale lub Komendę Miejską Policji w Koninie.
4. W przypadku, gdy nie jest to możliwe lub utrudnione:
 - a. powiadom policję dzwoniąc pod numer alarmowy 997 lub 112,
 - b. powiadom służby administracyjno-techniczne,
 - c. upewnij się, że informacja dotarła do przełożonych,
 - d. sprawdź czy wszystkie informacje, które otrzymałeś podczas zgłoszenia dokładnie przekazałeś przełożonym lub policji,
 - e. nie rozpowszechniaj samowolnie informacji o otrzymanym zgłoszeniu o podłożeniu bomby, może to spowodować panikę wśród pracowników oraz osób postronnych, utrudni działania policji oraz ewentualną ewakuację,
 - f. wykonuj polecenia przełożonych i funkcjonariuszy policji,
 - g. bądź świadom, że przejmując zgłoszenie stałeś się świadkiem zdarzenia i będziesz przesłuchany przez policję.

II. WSKAZÓWKI DLA OSOBY PROWADZĄCEJ ROZMOWĘ TELEFONICZNĄ Z OSOBĄ INFORMUJĄCĄ O FAKCIE PODŁOŻENIA „BOMBY” W OBIEKCIE.

Uwaga !!! Nie odkładać słuchawki po zakończeniu rozmowy telefonicznej.

1. Osoba, która przyjęła zgłoszenie o podłożeniu ładunku wybuchowego albo zauważyła w obiekcie przedmiot niewiadomego pochodzenia mogący być ładunkiem wybuchowym, natychmiast zawiadamia Burmistrza Rychwała, Zastępcę Burmistrza lub w razie ich nieobecności pełnomocnika ochrony oraz Policję.
2. Zawiadamiając dyżurnego oficera Policji należy podać:
 - a. treść rozmowy z osobą zgłaszającą o podłożeniu ładunku wybuchowego, którą należy prowadzić według poniższych wskazówek,
 - b. miejsce i opis zlokalizowanego przedmiotu, który może być ładunkiem wybuchowym,
 - c. numer telefonu, z którego prowadzona jest rozmowa oraz swoje imię i nazwisko,
 - d. uzyskać od policji potwierdzenie przyjętego zawiadomienia,
3. Pracownik przyjmujący informacje o zdarzeniu terrorystycznym powinien:
 - a. w czasie rozmowy wykazać maksymalny spokój i opanowanie oraz dążyć do uzyskania możliwie największej liczby szczegółów dotyczących zagrożenia, jak i osoby przekazującej

informację. Każdy zapamiętany szczegół z rozmowy lub przedłużenia czasu rozmowy mogą mieć istotny wpływ na późniejsze postępowanie dochodzeniowe.

b. uzyskaną informację przekazać natychmiast przełożonym, podając w szczególności treść rozmowy oraz miejsce, czas i źródło jej uzyskania.

III. ZASADY POSTĘPOWANIA KIEROWNICTWA URZĘDU MIASTA PO OTRZYMANIU INFORMACJI O PODŁOŻENIU ŁADUNKU WYBUCHOWEGO

1. Burmistrz, Zastępca Burmistrza lub pełnomocnik ochrony - dokonuje analizy otrzymanej informacji i podejmuje decyzję o:

- a) powiadomieniu policji o zagrożeniu terrorystycznym,
- b) ewentualnym przerwaniu pracy w Urzędzie,
- c) ewentualnym przeprowadzeniu ewakuacji pracowników z obiektu zagrożonego w trybie alarmowym,
- d) zabezpieczeniu dokumentów, w tym w szczególności niejawnych, baz danych i innego mienia posiadającego istotną wartość dla Urzędu,
- e) przekazuje zarządzenia wykonawcze dla kierowników podległych komórek organizacyjnych.

2. Do czasu przybycia Policji akcją kieruje Burmistrz, Zastępca Burmistrza lub w razie ich nieobecności pełnomocnik ochrony.

3. Kierujący akcją zarządza, aby użytkownicy pomieszczeń dokonali sprawdzenia, czy w tych pomieszczeniach znajdują się:

- a) przedmioty, rzeczy, paczki, urządzenia itp., których wcześniej nie było i nie wniesli ich użytkownicy pomieszczeń (a mogły być wniesione i pozostawione przez inne osoby np. interesantów),
- b) ślady przemieszczania elementów wyposażenia pomieszczeń,
- c) zmiany w wyglądzie zewnętrznym przedmiotów, rzeczy, urządzeń, które przedtem były w pomieszczeniu oraz emitowane z nich sygnały (dźwięki mechanizmów zegarowych, świejące elementy elektroniczne itp.).

4. Pomieszczenia ogólnodostępne, takie jak korytarze, klatki schodowe, toalety, piwnice oraz najbliższe otoczenie zewnętrzne obiektu, powinny być sprawdzane przez pracowników obsługi administracyjnej obiektu.

5. Zlokalizowanych przedmiotów, urządzeń, rzeczy, których (w ocenie użytkowników obiektu) przedtem nie było, a zachodzi podejrzenie, że mogą to być ładunki wybuchowe, nie wolno dotykać. O ich umiejscowieniu należy natychmiast powiadomić administratora obiektu i Policję.

V. WSPÓŁDZIAŁANIE ADMINISTRATORA OBIEKTU Z POLICYJĄ GRUPĄ ANTYTERRORYSTYCZNĄ

1. Burmistrz, Zastępca Burmistrza lub w razie ich nieobecności pełnomocnik ochrony zapoznaje dowódcę grupy policyjnej z posiadanymi informacjami o zagrożeniu i podjętymi w związku z tym przedsięwzięciami. Wskazuje miejsca zlokalizowanych przedmiotów, rzeczy, urządzeń obcych i punkty newralgiczne w obiekcie.

2. Z chwilą przybycia policji realizuje decyzje podejmowane przez dowódcę grupy antyterrorystycznej, administrator obiektu powinien udzielić mu wszechstronnej pomocy.

3. Burmistrz, Zastępca Burmistrza lub w razie ich nieobecności pełnomocnik ochrony wyznacza spośród pracowników osobę dobrze znającą obiekt, która towarzyszy grupie

policyjnej przy pracach rozpoznawczych udzielając informacji odnośnie rozmieszczenia poszczególnych pomieszczeń w obiekcie.

4. Identyfikacją i rozpoznawaniem zlokalizowanych przedmiotów, rzeczy, urządzeń obcych oraz neutralizowaniem ewentualnie położonych ładunków wybuchowych zajmują się uprawnione i wyspecjalizowane jednostki policji, przy wykorzystaniu specjalistycznych środków technicznych. Policjant kierujący akcją może w każdym momencie podjąć decyzję o ewakuacji użytkowników innych osób z obiektu. Ewakuacja nie jest w każdym przypadku obowiązkowa - ma charakter fakultatywny.

5. Policjant kierujący akcją po zakończeniu działań przekazuje protokolarnie obiekt administratorowi w postaci notatki z przeprowadzonej interwencji minersko - pirotechnicznej.

6. Dopiero po przyjęciu protokolarnie obiektu od dowódcy grupy minersko - pirotechnicznej przez administratora obiektu uznaje się, że nie ma w nim niebezpiecznych materiałów wybuchowych.

VI. ZASADY EWAKUACJI OSÓB I SPRZĘTU Z OBIEKTU ZAGROŻONEGO

1. Zakres ewakuacji obiektu uzależnia się od występującego zagrożenia.

2. Przed ewakuacją obiektu należy w miarę możliwości otworzyć drzwi i okna pomieszczeń zagrożonych i sąsiednich, a urządzenia i odbiorniki wyłączyć z sieci zasilania.

3. Ewakuowane osoby przed opuszczeniem budynku powinny zabrać ze sobą rzeczy osobiste, takie jak torby, torebki, plecaki, ubrania, przenośne radioodbiorniki itp., co pozwoli prowadzącym przeszukiwanie uniknąć straty czasu na identyfikowanie pozostawionych przedmiotów tego rodzaju.

4. Klucze pracownicy pozostawiają w drzwiach.

5. Miejscem ewakuacji ludzi i mienia jest remiza OSP w Rychwale.

6. Ewakuację prowadzi się w sposób zorganizowany, po oznakowanych i sprawdzonych pod względem pirotechnicznym drogach.

7. Należy sprawdzić - czy wszyscy pracownicy opuścili pomieszczenia.

8. W czasie ewakuacji należy zapewnić właściwą organizację ruchu osób opuszczających obiekt oraz umożliwić ominięcie przez ewakuowanych rejonu zagrożonego wybuchem.

9. W przypadku organizowania ewakuacji o charakterze prewencyjnym, wykorzystuje się główne wyjścia z obiektu.

10. Zdecydowanie przeciwdziałać gromadzeniu się ewakuowanych osób w bezpośrednim otoczeniu zagrożonego obiektu, terenu. Wszyscy niebiorący bezpośredniego udziału w akcji powinni znajdować się w odległości bezpiecznej od zagrożonego obiektu, terenu.

11. Po zakończeniu ewakuacji powiadomić należy grupę pirotechniczną, że wszyscy opuścili zagrożony obiekt.

INSTRUKCJA POSTĘPOWANIA W PRZYPADKU OTRZYMANIA PRZESYŁKI NIEWIADOMEGO POCHODZENIA

I. 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:

1. Umieścić przesyłkę w grubym worku plastikowym, szczelnie zamknąć.
2. Worek należy umieścić w drugim plastikowym worku, szczelnie zamknąć, zakleić taśmą lub plastrem.
3. Paczki nie należy przemieszczać, należy pozostawić ją na miejscu.
4. Powiadomić:
Komisariat Policji w Rychwale -tel. 997; 063 247 26 60; kom. 112,
Komendę Miejską Państwowej Straży Pożarnej - tel. 998;
Służby te podejmą wszelkie niezbędne kroki w celu bezpiecznego przejęcia przesyłki.
5. Powiadomić:
Burmistrza Rychwała, Zastępcę Burmistrza lub pełnomocnika ochrony.

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

Należy:

1. Nie naruszać zawartości - nie rozsypywać, nie przenosić, nie dotykać, nie wąchać, nie powodować ruchu powietrza w pomieszczeniu (wyłączyć systemy wentylacyjne, zamknąć okna).
2. Całą zawartość umieścić w worku plastikowym, zamknąć go i zakleić taśmą lub plastrem.
3. Dokładnie umyć ręce.
4. Zaklejony worek umieścić w drugim worku, zamknąć go i zakleić.
5. Ponownie umyć ręce.

**PO PRZYBYCIU WŁAŚCIWEJ SŁUŻBY NALEŻY BEZWZGLĘDnie STOSOWAĆ
SIĘ DO JEJ ZALECEŃ**

**PROTOKÓŁ OTWARCIA SEJFU (SZAFY METALOWEJ)* KANCELARII TAJNEJ
URZĘDU GMINY I MIASTA W RYCHWALE**

W dniu r. Komisja w składzie:

- 1.....
 - 2.....
 - 3.....
- (nazwisko i imię, stanowisko służbowe)

dokonała otwarcia sejfu/szafy metalowej* znajdującej się w pomieszczeniu Kancelarii Tajnej
Urzędu Gminy i Miasta w Rychwale , której użytkownikiem jest :

.....
(nazwisko i imię, stanowisko służbowe)

Z sejfu/szafy metalowej* zostały zabrane niżej wymienione dokumenty (materiały,
przedmioty):

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

którymi, w celu

dysponował będzie
(nazwisko i imię, stanowisko służbowe)

Sejf/szafę metalową* zamknięto i zaplombowano (referentką do plasteliny) w obecności
członków Komisji.

Podpisy członków Komisji:

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

* - niepotrzebne skreślić

WZÓR UPOWAŻNIENIA JEDNORAZOWEGO

UPOWAŻNIENIE NR

Na podstawie art. 49 ust. 2-4 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji
niejawnych (Dz. U. z 2005 r. Nr 196, poz. 1631 z późn. zm.)

UPOWAŻNIAM

Pana / Panią
(imię i nazwisko, stanowisko lub pełniona funkcja)

do dostępu do informacji niejawnych stanowiących tajemnicę służbową oznaczonych
klauzulą „zastrzeżone”/„poufne”* w związku z

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

Upoważnienie ważne na czas wykonania zadania/do dnia

*niepotrzebne skreślić

Schemat organizacji stref ochronnych

