ZARZĄDZENIE NR VII/14/2014
BURMISTRZA MIASTA ORZESZE

z dnia 18 grudnia 2014 r.

w sprawie: zatwierdzenia „ Planu Ochrony Informacji Niejawnych w Urzędzie Miejskim w Orzeszu”

Na podstawie art. 15 ust. 1 pkt 5 oraz art. 43 ust. 5 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2010 r. Nr 182 poz. 1228) oraz art. 33 ust. 3 i art. 30 ust. 1 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz.U. z 2013 r. poz.594 z późn. zm.),

zarządzam, co następuje:

§ 1. 1. Zatwierdzam Plan Ochrony Informacji Niejawnych w Urzędzie Miejskim w Orzeszu stanowiący załącznik Nr 1 do niniejszego zarządzenia.

2. Zatwierdzam Tabelę Oceny Istotności Czynników Zagrożenia, stanowiącą załącznik Nr 2 do niniejszego zarządzenia.

§ 2. Zobowiązuję pracowników do wprowadzenia i stosowania ustaleń zawartych w planie i tabeli.

§ 3. Wyłącza się jawność informacji publicznych zawartych w załącznikach do niniejszego zarządzenia. Wyłączenie jawności informacji ma na celu zwiększenie bezpieczeństwa postępowania z informacjami niejawnymi wytwarzanymi i przechowywanymi w Urzędzie Miejskim w Orzeszu.

§ 4. Nadzór nad wykonaniem Zarządzenia powierzam Pełnomocnikowi ds. Ochrony Informacji Niejawnych

§ 5. Zarządzenie wchodzi w życie z dniem podpisania.

Burmistrz Miasta Orzesze

inż. Mirosław Blaski

Załącznik Nr 1 do zarządzenia Nr VII/14/2014
Burmistrza Miasta Orzesze
z dnia 18 grudnia 2014 r.

ZATWIERDZAM

……

PLAN
OCHRONY INFORMACJI NIEJAWNYCH
W URZĘDZIE MIEJSKIM W ORZESZU
Opracował:
Sonia Janecka
Pełnomocnik
Ochrony Informacji Niejawnych

Orzesze, grudzień 2014 r.

Spis treści

1. **Postanowienia ogólne**

1. Plan Ochrony Informacji niejawnych w Urzędzie Miejski w Orzeszu określa zasady i tryb postępowania z informacjami niejawnymi oraz zapewnia jednolity sposób postępowania z tymi informacjami w Urzędzie Miejskim w Orzeszu.

2. Podstawy prawne ochrony informacji niejawnych:

· ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (t. j. Dz. U. Nr 182, poz. 1228);

· rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 roku w sprawie wzoru decyzji o cofnięciu poświadczenia bezpieczeństwa (Dz.U.2010.258.1754);

· rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 roku w sprawie wzoru decyzji o odmowie wydania poświadczenia bezpieczeństwa (Dz.U.2010.258.1753);

· rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 roku w sprawie wzorów poświadczeń bezpieczeństwa (Dz.U.2010.258.1752);

· rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 roku 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.2010.258.1751);

· rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 roku w sprawie przekazywania informacji, udostępniania dokumentów oraz udzielania pomocy służbom i instytucjom uprawnionym do prowadzenia poszerzonych postępowań sprawdzających, kontrolnych postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego (Dz.U.2010.258.1750);

· rozporządzenie Prezesa Rady Ministrów z dnia 13 sierpnia 2010 roku w sprawie sposobu oznaczania materiałów, umieszczania na nich klauzul tajności, a także zmiany nadanej klauzuli tajności (Dz.U.2010.159.1069);

· rozporządzenie Rady Ministrów z dnia 01 czerwca 2010 roku w sprawie organizacji i funkcjonowania kancelarii tajnych (Dz.U.2010.114.765);

· rozporządzenie Prezesa Rady Ministrów z dnia 26 lutego 2010 roku w sprawie postępowania z dokumentacją w komórkach organizacyjnych wykonujących zadania w zakresie obronności i bezpieczeństwa państwa (Dz.U.2010.34.181)

2. **Definicje używane w Planie ochrony informacji niejawnych**

W rozumieniu planu ochrony informacji niejawnych:

1. **ustawą** - jest ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (t. j. Dz. U. Nr 182, poz. 1228),

2. **służbą ochrony państwa** - jest Agencja Bezpieczeństwa Wewnętrznego

3. **rękojmią zachowania tajemnicy** — jest zdolność osoby do spełnienia ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem, stwierdzona w wyniku przeprowadzenia postępowania sprawdzającego;

4. **dokumentem** — jest każda utrwalona informacja niejawna;

5. **materiałem** — jest dokument lub przedmiot albo dowolna ich część, chronione jako informacja niejawna, a zwłaszcza urządzenie, wyposażenie lub broń wyprodukowane albo będące w trakcie produkcji, a także składnik użyty do ich wytworzenia;

6. **przetwarzaniem informacji niejawnych** — są wszelkie operacje wykonywane w odniesieniu do informacji niejawnych i na tych informacjach, w szczególności ich wytwarzanie, modyfikowanie, kopiowanie, klasyfikowanie, gromadzenie, przechowywanie, przekazywanie lub udostępnianie;

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

8. **Urzędem** - jest Urząd Miejski w Orzeszu,

9. **Burmistrzem** - jest Burmistrz Miasta Orzesze,

10. **pełnomocnikiem ochrony** - jest Pełnomocnik ds. Ochrony Informacji Niejawnych w Urzędzie Miejskim w Orzeszu,

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

12. 12**. dokumentacja bezpieczeństwa systemu lub sieci informatycznej** - są szczególne Wymagania Bezpieczeństwa oraz Procedury Bezpiecznej Eksploatacji danego systemu lub sieci teleinformatycznej, sporządzone zgodnie z zasadami określonymi w ustawie.

13. **ryzykiem** – jest kombinacja prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji;

14. **szacowaniem ryzyka** – jest całościowy proces analizy i oceny ryzyka;

15. **zarządzaniem ryzyka** – są skoordynowane działania w zakresie zarządzania bezpieczeństwem informacji , z uwzględnieniem ryzyka,

16. **kancelaria materiałów niejawnych –** wydzielone, wyodrębnione pomieszczenie przeznaczone do ewidencjonowania, opracowywania przechowywania dokumentów niejawnych oznaczonych klauzula „poufne”,

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

3. **Przedmiot ochrony**

Przedmiotem ochrony w Urzędzie są:

1. Informacje niejawne oznaczone:

– klauzulą „poufne",

– klauzulą „zastrzeżone",

2. Pomieszczenia, w których są przechowywane i opracowane materiały niejawne.

4. **Klasyfikacja informacji niejawnych**

Informacjom niejawnym nadaje się następujące klauzule:

1. "poufne", jeżeli ich nieuprawnione ujawnienie informacji spowoduje szkodę dla Rzeczypospolitej Polskiej przez to, że:

1) utrudni prowadzenie bieżącej polityki zagranicznej Rzeczypospolitej Polskiej;

2) utrudni realizacje przedsięwzięć obronnych lub negatywnie wpłynie na zdolność bojową Sił Zbrojnych Rzeczypospolitej Polskiej;

3) zakłóci porządek publiczny lub zagrozi bezpieczeństwu obywateli;

4) utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za ochronę bezpieczeństwa lub podstawowych interesów Rzeczypospolitej Polskiej;

5) utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za ochronę porządku publicznego, bezpieczeństwa obywateli lub ściganie sprawców przestępstw i przestępstw skarbowych oraz organom wymiaru sprawiedliwości;

6) zagrozi stabilności systemu finansowego Rzeczypospolitej Polskiej;

7) wpłynie niekorzystnie na funkcjonowanie gospodarki narodowej.

Informacjom niejawnym nadaje się klauzule **„zastrzeżone”,** jeżeli nie nadano im wyższej klauzuli tajności, a ich nieuprawnione ujawnienie może mieć szkodliwy wpływ na wykonywanie przez organy władzy publicznej lub inne jednostki organizacyjne zadań w zakresie obrony narodowej, polityki zagranicznej, bezpieczeństwa publicznego, przestrzegania praw i wolności obywateli, wymiaru sprawiedliwości albo interesów ekonomicznych Rzeczypospolitej Polskiej.

5. **Dostęp do informacji niejawnych**

5.1 Uprawnienia do dostępu do informacji niejawnych

1. Informacje niejawne 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 o klauzuli „poufne” może nastąpić:

- po uzyskaniu przez pracownika poświadczenia bezpieczeństwa po przeprowadzonym przez Pełnomocnika ochrony zwykłym postępowaniu sprawdzającym,
- po przeszkoleniu danej osoby w zakresie ochrony informacji niejawnych i uzyskaniu odpowiedniego zaświadczenia o przeszkoleniu.

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

- po uzyskaniu przez pracownika upoważnienia dostępu do informacji niejawnych oznaczonych klauzula „zastrzeżone” wydanego przez kierownika jednostki,
- po przeszkoleniu danej osoby w zakresie przepisów ustawy o ochronie informacji niejawnych i uzyskaniu odpowiedniego zaświadczenia.

4. Zwykle postępowanie sprawdzające wobec pracowników jednostki w związku z dostępem do informacji niejawnych oznaczonych klauzula „poufne” na pisemne polecenie kierownika jednostki przeprowadza Pełnomocnik ds. 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 klauzula „poufne” może skutkować:

- przeniesieniem danej osoby na stanowisko nie związane z informacjami niejawnymi o klauzuli „poufne”,
- rozwiązaniem umowy o prace w przypadku niemożności zmiany stanowiska,
- niemożnością zatrudnienia na danym stanowisku , w przypadku ubiegania się o zatrudnienie w Urzędzie.

5.2 Udostępnianie informacji niejawnych

1. Informacje niejawne mogą być udostępniane wyłącznie osobie dającej rękojmię zachowania tajemnicy tylko w takim zakresie, jaki jest niezbędny do załatwienia konkretnej sprawy a wynikającym z zakresu czynności.

2. Informacje niejawne mogą być udostępnione tylko osobom uprawnionym do dostępu do informacji określonych tą klauzulą i z uwzględnieniem ograniczenia określonego w pkt a.

6. **Zasady wykonywania i przetwarzania dokumentów niejawnych**

6.1 Zasady wykonywania i przetwarzania dokumentów niejawnych

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

2. Uprawnienie do przyznania, obniżenia i znoszenia klauzuli tajności przysługuje wyłącznie w zakresie posiadanego prawa dostępu do informacji niejawnych.

3. Zawyżanie lub zaniżanie klauzuli tajności jest niedopuszczalne.

4. Dokumenty niejawne wpływające do Urzędu podlegają ewidencjonowaniu w dzienniku ewidencji.

5. Dokumenty niejawne wytworzone w Urzędzie rejestruje się w dzienniku ewidencji.

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

7. Numer ewidencyjny każdego dokumentu niejawnego stanowiącego tajemnicę o klauzuli „poufne" lub „zastrzeżone" poprzedzony jest skrótem literowym, odpowiednio, „Pf" lub „Z".

8. Dokumenty niejawne wytworzone w Urzędzie powinny być oznaczone w sposób określony w rozporządzeniu Prezesa Rady Ministrów z dnia 13 sierpnia 2010 r. w sprawie sposobu oznaczania materiałów, umieszczania na nich klauzul tajności, a także zmiany nadanej klauzuli tajności (Dz. U. Nr 159, poz. 1069).

6.2 Okresy ochronne

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

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

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

2. **Na pismach zawierających informacje niejawne, wobec których zniesiono lub zmieniono przyznana klauzule 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 skreślona klauzula tajności w prawym górnym rogu umieszcza się datę, imię, nazwisko
i podpis osoby dokonującej tych adnotacji oraz wskazuje się podstawy dokonanej zmiany.

3. W stosunku do pism znajdujących się w zbiorach dokumentów zawierających informacje niejawne, wobec których minął ustawowy lub ustanowiony okres ochrony, czynności, o których mowa w ust. 1—2, można dokonać najpóźniej w przypadku ich udostępniania lub przekazywania osobom spoza jednostki lub komórki organizacyjnej.

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

- **na wszystkich stronach** w prawym górnym rogu odpowiednio napis:

  „Kopia", „Odpis", „Wypis", „Wyciąg" lub „Tłumaczenie z języka –

  (nazwa języka) – (imię i nazwisko tłumacza)";

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

- **na ostatniej stronie dodatkowo** napis „Za zgodność" i odcisk tuszowej pieczęci urzędowej z nazwa jednostki lub komórki organizacyjnej (numerem jednostki wojskowej), w której sporządzono kopie, odpis, wypis, wyciąg lub tłumaczenie.

- zgodność z oryginałem kopii, odpisu, wypisu lub wyciągu potwierdza podpisem kierownik jednostki lub komórki organizacyjnej albo inna osoba przez niego upoważniona, a tłumaczenia – osoba dokonująca tłumaczenia.

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

- nazwie jednostki lub komórki organizacyjnej, w której sporządzono kopie, odpis, wypis, wyciąg lub tłumaczenie;
- liczbie egzemplarzy sporządzonych kopii, odpisów, wypisów, wyciągów lub tłumaczeń;
- dacie sporządzenia kopii, odpisu, wypisu, wyciągu lub tłumaczenia;
- numerze, pod jakim kopia, odpis, wypis, wyciąg lub tłumaczenie zostały zarejestrowane w dzienniku ewidencji wykonanych dokumentów.
- adnotacje, o których mowa , wpisuje się przed wykonaniem kopii, odpisu, wypisu, wyciągu lub tłumaczenia, natomiast numer, pod jakim zostały zarejestrowane w dzienniku ewidencyjnym , nanosi się po wykonaniu kopii, odpisu, wypisu, wyciągu lub tłumaczenia.

7. **Wykonywanie dokumentów zawierających informacje niejawne za pomocą komputera**

Pracownicy, którzy do opracowywania i wykonywania dokumentów zawierających informacje 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 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 kontrolowanego dostępu

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

8. **Ochrona fizyczna**

1. Budynek i znajdujące się w nim pomieszczenia stanowiące siedzibę Urzędu podlegają ochronie. Ochrona fizyczna polega na stałym monitoringu budynku i znajdujących się w nim pomieszczeń poprzez system alarmowy.

2. Kody do instalacji alarmowej do budynku Urzędu posiadają: Burmistrz Miasta Orzesze, Z-ca Burmistrza Orzesze, Sekretarz Miasta, Kierownik USC oraz upoważnieni pracownicy odpowiedzialni za otworzenie i zamknięcie budynku Urzędu.

3. Pomieszczenia, w których znajdują się informacje niejawne z klauzulą „poufne" i „ zastrzeżone " po godzinach pracy powinny być zamykane, a klucze zabierane.

4. Sprzątanie pomieszczenia w którym są przechowywane informacje niejawne powinno odbywać się w obecności upoważnionego pracownika przed zakończeniem pracy

5. Informacje niejawne oznaczone klauzulą „poufne” należy przechowywać w szafach metalowych z zamkami o skomplikowanym mechanizmie,

6. W uzasadnionych przypadkach podyktowanych względami dłuższego okresu czasu, niezbędnego do wykonania zadań związanych z dostępem do informacji niejawnych, dokumenty o klauzuli „poufne” mogą być wydawane poza pomieszczenie służące do przechowywania lecz pod warunkiem, że odbiorca dokumentu zapewni warunki ochrony tych dokumentów przechowując je w szafach metalowych z odpowiednim zamknięciem.

7. Szafę metalowe, w której przechowuje się dokumenty o klauzuli „poufne” po zakończeniu pracy należy zamknąć i wychodząc z pomieszczenia zakodować.

8. Informacje niejawne oznaczone klauzulą „zastrzeżone” można przechowywać na stanowiskach pracy, w meblach biurowych zamykanych na klucz.

9 Ocena zagrożeń zewnętrznych i wewnętrznych

9.1 Zagrożenia zewnętrzne

1. **Rodzaje zagrożeń:**

Zagrożeniami zewnętrznymi dla Urzędu są:

• możliwość napadu przez zorganizowane grupy przestępcze i terrorystyczne, działające w sposób profesjonalny, przemyślany i zorganizowany,

• możliwość napadu przez pojedynczych przestępców, możliwość napadu przez przypadkowe osoby wykorzystujące nadarzającą się okazję z powodu nieprawidłowości w ochronie mienia Urzędu.

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

• wzmożone zainteresowanie osób postronnych obiektem, pomieszczeniami urzędu objawiające się między innymi: podejmowaniem prób uzyskania informacji o danym obiekcie, pomieszczeniu od pracowników podczas luźnych rozmów po „przypadkowym” spotkaniu,

• nawiązanie rozmów przez osoby postronne z pracownikami,

• podszywanie się pod byłych pracowników Urzędu i przejawianie zainteresowaniem tym, co się po latach zmieniło,

• interesowanie się osobami funkcyjnymi, w tym także ich przywarami oraz sposobem wykonywania obowiązków służbowych,

• obserwacja sposobu działania systemu ochronnego, sekretariatu, sprzątaczki itp.,

• rozpoznawanie systemu technicznych zabezpieczeń, w tym stosowanych urządzeń alarmowych,

• celowe uszkadzanie urządzeń alarmowych, linii telefonicznych, oświetlenia itp.,

• próby pozyskania do grup przestępczych pracowników Urzędu (dotyczy głównie osób mających problemy finansowe, towarzyskie, a także służbowe).

3. **Wnioski**

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

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

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

• stosować zasadę niedopuszczania osób niepowołanych do penetracji strefy bezpieczeństwa,

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

9.2 Zagrożenia wewnętrzne

1. **Rodzaje zagrożeń:**

• 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 celem łatwiejszej pracy grup przestępczych na terenie urzędu,

• próby wglądu w dokumenty niejawne przez osoby nieuprawnione,

• spożywanie alkoholu – przesłanka do wykroczeń dyscyplinarnych i przestępstw.

2. **Wnioski**

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

• zwracanie szczególnej uwagi na osoby, które mogą być zainteresowane zaborem prowadzenie szczególnego nadzoru, by nie dokonywano prób kserowania, kopiowania bez zgody przełożonego,

• uwrażliwianie pracowników w trakcie prowadzonych szkoleń na możliwość prób kontaktu grup przestępczych z pracownikami, którzy mają dostęp do dokumentów szczególnie ważnych,

• zastosowanie zasady, że do informacji niejawnych mogą mieć dostęp tylko pracownicy posiadający poświadczenie bezpieczeństwa lub właściwe upoważnienie jednorazowe wydane przez Burmistrza.

• wprowadzenie szczególnej uwagi na osoby, których zachowanie wskazuje na nadmierne spożywanie alkoholu.

10. **Postępowanie w przypadku naruszenia ustawy o ochronie informacji**

niejawnych i przepisów wykonawczych do ustawy.

1. Za ochronę informacji niejawnych w Urzędzie odpowiada Burmistrz. Zadania określone ustawą o ochronie informacji niejawnych w imieniu Burmistrza wykonuje pełnomocnik ochrony poprzez:

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

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

2. W przypadku ujawnienia informacji niejawnych przez podległych pracowników Burmistrz lub upoważniony przez niego pracownik zawiadamia na piśmie pełnomocnika ochrony podając jaka informacja niejawna została ujawniona lub jakie naruszenie przepisów zostało stwierdzone.

3. Pełnomocnik ochrony przeprowadza okresowe kontrole przestrzegania ustawy o ochronie informacji niejawnych w Urzędzie. W przypadku stwierdzenia naruszenia przepisów o ochronie informacji niejawnych pełnomocnik ochrony przekłada Burmistrzowi pisemną informację o naruszeniu przepisów i wnioski do podjęcia decyzji.

4. W przypadku naruszenia przepisów o ochronie informacji niejawnych oznaczonych klauzulą „poufne" lub wyższą pełnomocnik ochrony powiadamia Burmistrza oraz właściwe Służby Ochrony Państwa.

11 Instrukcja postępowania w przypadku otrzymania przesyłki niewiadomego pochodzenia

W przypadku otrzymania jakiejkolwiek przesyłki niewiadomego pochodzenia lub budzącej

podejrzenia z jakiegokolwiek innego powodu:

- brak nadawcy,

- brak adresu nadawcy,

- przesyłka pochodzi od nadawcy lub z miejsca, z którego nie spodziewamy się,

- inne podejrzenia.

Nie należy otwierać tej przesyłki .

Należy:

1. Umieścić przesyłkę w grubym worku plastikowym, szczelnie zamknąć.

2. Worek należy umieścić w drugim plastikowym worku, szczelnie zamkniętym, zakleić taśmą lub plastrem.

3. Paczki nie należy przemieszczać, należy pozostawić ją na miejscu.

4. Powiadomić:

- Komendę Powiatową Policji tel. 997;

- Komendę Powiatową Państwowej Straży Pożarnej tel. 998;

Służby te podejmą wszelkie niezbędne kroki w celu bezpiecznego przejęcia przesyłki. W przypadku, gdy podejrzana przesyłka została otwarta i zawiera jakąkolwiek podejrzaną

zawartość w formie stałej (galaretę, pianę, pył lub inną).

Należy:

1. Nie naruszyć 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.

6. Powiadomić:

- Komendę Powiatową Policji tel. 997;

- Komendę Powiatową Państwowej Straży Pożarnej tel. 998;

- Powiatową Stację Sanitarno-Epidemiologiczną. 76 8702348

- Pogotowie Ratunkowe tel. 999;

Po przybyciu właściwej służby należy bezwzględnie stosować się do jej zaleceń.

12. **Instrukcja alarmowa w przypadku zgłoszenia o podłożeniu lub znalezieniuładunku wybuchowego w budynku Urzędu**

12.1 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:

1) Burmistrza ,

2) Komendanta Powiatowego Policji.

2. Zawiadamiając Policję należy podać treść rozmowy ze zgłaszającym o podłożeniu ładunku wybuchowego, którą należy prowadzić wg poniższych wskazówek:

1) miejsce i opis zlokalizowanego przedmiotu, który może być ładunkiem wybuchowym,

2) numer telefonu, z którego prowadzona jest rozmowa i swoje stanowisko,

3) uzyskać od Policji potwierdzenie przyjętego zawiadomienia.

12.2 Akcja poszukiwawcza ładunku wybuchowego po uzyskaniu informacji o jego podłożeniu

1. Do czasu przybycia Policji akcją kieruje Burmistrz, a w czasie jego nieobecności Z- ca Burmistrza, Sekretarz bądź Pełnomocnik Ochrony.

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

a) przedmioty, rzeczy lub urządzenia, paczki itp., których wcześniej nie było i nie wnieśli ich użytkownicy pomieszczeń,

b) ślady przemieszczania elementów wyposażenia pomieszczeń,

c) zmiany w wyglądzie zewnętrznym przedmiotów, rzeczy, urządzeń, które przedtem w pomieszczeniu były oraz emitowane z nich sygnały (np. dźwięki mechanizmów zegarowych itp.).

3. Pomieszczenia ogólnodostępne takie jak: korytarze, klatki schodowe, hale, windy, toalety, piwnice, strychy itp. oraz najbliższe otoczenie zewnętrzne obiektu powinny być sprawdzone przez wyznaczonych do tego pracowników.

4. Zlokalizowanych przedmiotów, rzeczy, urządzeń, 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 Burmistrza 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 decyzje ewakuacji osób z zagrożonego obiektu przed przybyciem Policji.

6. Należy zachować spokój i opanowanie, aby nie dopuścić do przejawów paniki.

Współpraca z policją w czasie akcji

1. Po przybyciu do obiektu policjanta bądź policyjnej grupy interwencyjnej kierujący akcją powinien przekazać im wszelkie informacje dotyczące zdarzenia oraz wskazać miejsce zlokalizowanych przedmiotów, rzeczy, urządzeń obcego pochodzenia i punkty newralgiczne w obiekcie.

2. Policjant lub dowódca grupy interwencyjnej przejmuje kierowanie akcją, a kierujący dotychczas akcją winien udzielić mu wszechstronnej pomocy.

3. Na wniosek policjanta kierującego akcją Burmistrz 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 Burmistrzowi.

12.3 Postanowienia końcowe dotyczące działań w przypadku zgłoszenia o podłożeniu ładunku wybuchowego:

1. Osobom przyjmującym zgłoszenie o podłożeniu ładunku wybuchowego oraz Burmistrzowi nie wolno lekceważyć żadnej informacji na ten temat. Każdorazowo osoby te winny zawiadamiać o tym Policję, która z urzędu dokona sprawdzenia wiarygodności każdego zgłoszenia.

2. Burmistrz powinien na bieżąco organizować szkolenie pracowników w zakresie sposobu zachowania w sytuacjach wymienionych w tej części Planu oraz winien znać rozmieszczenie newralgicznych punktów -węzły energetyczne i wodne, które udostępnia się na żądanie policjanta kierującego akcją

13. **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 dokumentacja, zasad jej klasyfikowania i kwalifikowania oraz zasad i trybu przekazywania materiałów archiwalnych do archiwów państwowych.(Dz. U. z 2002 r. Nr 167, poz.1375),

2. Zasady postępowania z dokumentacja w komórkach organizacyjnych wykonujących zadania w zakresie obronności i bezpieczeństwa państwa zostały określone w rozporządzeniu Prezesa Rady Ministrów z dnia 26 lutego 2010 roku (Dz. U. Nr 34 poz.181),

3. Dokumentacja wytwarzana i gromadzona dzieli się na :

1) materiały archiwalne - wchodzące do państwowego zasobu archiwalnego;

2) dokumentacje niearchiwalna - inna dokumentacje, niestanowiąca materiałów archiwalnych.

4. Rzeczowa klasyfikacje oraz kwalifikacje dokumentacji ze względu na okresy jej przechowywania, wytwarzanej i gromadzonej zawierają jednolite rzeczowe wykazy akt,

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

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

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

8. Brakowanie dokumentacji niearchiwalnej następuje na podstawie zgody.

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

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

11. Do wniosku o zgodę jednorazowa dołącza się:

1) protokół oceny dokumentacji niearchiwalnej,

2) spis dokumentacji niearchiwalnej przeznaczonej do przekazania na makulaturę lub zniszczenie, albo spis dokumentacji technicznej niearchiwalnej przeznaczonej na makulaturę lub zniszczenie,

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

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

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

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

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

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

1) nazwy jednostki organizacyjnej i komórki organizacyjnej, w której materiały powstały;

2) znaku akt, to jest symbolu literowego komórki organizacyjnej oraz symbolu klasyfikacyjnego według wykazu akt, obowiązującego w jednostce organizacyjnej;

3) tytułu teczki, to jest nazwy hasła klasyfikacyjnego według wykazu akt, obowiązującego w danej jednostce organizacyjnej, i informacji o rodzaju materiałów archiwalnych, znajdujących się w teczce;

4) rocznych dat krańcowych, to jest dat najwcześniejszego i najpóźniejszego materiału archiwalnego w teczce;

5) sygnatury teczki, to jest numeru spisu zdawczo-odbiorczego i numeru pozycji teczki w spisie zdawczo-odbiorczym;

6) symbolu kwalifikacyjnego materiałów archiwalnych (kategoria A);

7) liczby stron w teczce.

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

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

14. **PRZECHOWYWANIE KLUCZY I PIECZĘCI**

Ustala się zasady gospodarki kluczami i pieczęciami :

1. Klucze od szafy metalowej kancelarii materiałów niejawnych oraz pieczecie, po zakończeniu pracy należy złożyć w pomieszczeniu kancelarii w miejscu niewidocznym.

3. Po zakończeniu pracy , pracownik materiałów niejawnych zamyka i koduje drzwi wejściowe kancelarii,

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

5. Pieczęć do plasteliny pracownik kancelarii materiałów niejawnych powinien zabezpieczać tak, by osoby nieuprawnione nie mogły z niej korzystać,

9. Pracownik kancelarii materiałów niejawnych po przybyciu do urzędu , przed otwarciem kancelarii powinien sprawdzić , czy nie zostały naruszone pieczecie zabezpieczające klucze oraz zabezpieczające drzwi wejściowe do kancelarii.

ZAŁACZNIKI
DO PLANU OCHRONY
INFORMACJI NIEJAWNYCH

ZAŁACZNIK Nr 1 *- sposób oznaczania dokumentów niejawnych oznaczonych klauzulą*

poufne i zastrzeżone oraz umieszczania klauzuli na tych dokumentach

Pierwsza strona dokumentu zawierającego informacje niejawne

……
/miejscowość, data sporządzenia dokumentu/

Klauzula tajności

Egz. Nr .....

……..

/nazwa jednostki lub komórki organizacyjnej/

- sygnatura literowo-cyfrowa

- numer z dziennika ewidencji

łamany przez rok lub dwie ostatnie cyfry roku

/treść dokumentu/

/W przypadku gdy do pisma przewodniego dołączone są załączniki/

· Liczba załączników,

· Klauzule tajności załączników wraz z nr dziennika ewidencyjnego,

· Liczba stron lub kart każdego załącznika,

· W przypadku, gdy adresatowi wysyła się inna liczbę załączników niż pozostawia w aktach, dodatkowo napis „tylko adresat”,

· W przypadku, gdy załączniki maja być zwrócone napis -„do zwrotu”

….....

/stanowisko, oraz imię i nazwisko

osoby podpisującej dokument/

- liczba wykonanych egzemplarzy
- adresatów poszczególnych egzemplarzy
- dyspozycję „ad acta” w przypadku egzemplarza pozostającego w aktach nadawcy
- imię i nazwisko wykonawcy

numer strony/ liczba stron

Klauzula tajności

ZAŁACZNIK Nr 2

WZORY
PISM I UPOWAŻNIEŃ

SPIS TREŚCI:

POSWIADCZENIE BEZPIECZEŃSTWA NR_____

Na podstawie art.28 pkt. 1 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182 , poz.1228) po przeprowadzeniu na wniosek/polecenie*

_____

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

przez_____

(nazwa i adres siedziby organu , który przeprowadził postępowanie)

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

_____

(imię i nazwisko, data urodzenia)

daje rękojmie zachowania tajemnicy

w zakresie dostępu do informacji niejawnych oznaczonych klauzula

_____ - na okres do: _____

(nazwa klauzuli tajności) (termin ważności)

_____ - na okres do:* _____

(nazwa klauzuli tajności) (termin ważności)*

_____ - na okres do:* _____

(nazwa klauzuli tajności) (termin ważności)*

_____

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

_____

**niepotrzebne skreślić*

ZAŚWIADCZENIE NR__

stwierdzające odbycie szkolenia

w zakresie ochrony informacji niejawnych

Stwierdza się ,że Pani (Pan):

- imię i nazwisko _____

- nr PESEL _____

odbyła (odbył) szkolenie w zakresie ochrony:

- informacji niejawnych, *****

- informacji niejawnych Organizacji Traktatu Północnoatlantyckiego

- informacji niejawnych Unii Europejskiej, *****

na podstawie przepisów ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182,poz,1228), zorganizowane przez pełnomocnika do spraw ochrony informacji niejawnych w:

(nazwa i adres siedziby jednostki organizacyjnej)

.....

(miejscowość i data)

……..

(podpis i imienna pieczątka pełnomocnika lub jego

zastępcy)

***** Niepotrzebne skreślić

Upoważnienie uprawniające do dostępu do informacji niejawnych oznaczonych klauzulą „zastrzeżone”

Nr pisma…….

……..

/miejscowość ,data/

Pan /Pani

…….

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

u p o w a ż n i a m

Pana/ą…… do dostępu do informacji niejawnych oznaczonych klauzula **„zastrzeżone”** zatrudnionego/ona w …… na stanowisku …….

……..

/kierownik jednostki/

***** Upoważnienie ważne jest na czas zatrudnienia w ……lub do odwołania,

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

…….....

Nazwa jednostki organizacyjnej występującej o sprawdzenie

osoby upoważnianej do dostępu do informacji niejawnych

Miejscowość i data ……

L. dz. ……

DYREKTOR

Delegatury Agencji Bezpieczeństwa

Wewnętrznego

WNIOSEK O SPRAWDZENIE W EWIDENCJACH I KARTOTEKACH NIEDOSTEPNYCH POWSZECHNIE

Na podstawie art. 25 ust. 1 pkt 2 ustawy z dnia 5 sierpnia 2010 r. o ochronie

informacji niejawnych (Dz. U. z 2010 r., Nr 182, poz. 1228) 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. Adres zameldowania ……
10. Adres zamieszkania ……

proszę o poinformowanie, czy Agencja Bezpieczeństwa Wewnętrznego posiada informacje,

które maja wpływ na wynik postępowania.

……..…….

Pieczątka i podpis pełnomocnika ochrony

MINISTERSTWO SPRAWIEDLIWOSCI
KRAJOWY REJESTR KARNY

Data wpływu

znak opłaty

Data wystawienia…….

ZAPYTANIE O UDZIELENIE INFORMACJI O OSOBIE *

1. Nazwisko rodowe……
2. Nazwisko (w tym przybrane)……
3. Imiona……
4. Imię ojca……..….

5. Imię matki……..…

6. Data urodzenia…….…….

7. Nazwisko rodowe matki…….……...

8. Miejsce urodzenia…….……

9. Obywatelstwo……..……..

10. Miejsce zamieszkania…….

11. Wskazanie postępowania , o którym mowa w art.6 pkt 4-6 i 8-10 ustawy z dnia 24 maja 2000r o Krajowym Rejestrze Karnym (Dz.U. Nr 50,poz.580 z pózn. zm.), późn. zm. związku z którym zachodzi potrzeba uzyskania informacji o osobie – **art.25 ust.1 Ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U.Nr 182 ,poz.1228)**

12. Rodzaj danych, które mają być przedmiotem informacji o osobie:

1. Kartoteka karna 2. Kartoteka Nieletnich

3. Kartoteka Osób Pozbawionych Wolności oraz Poszukiwanych Listem Gończym **)

4. Zakres danych, które mają być przedmiotem informacji o osobie……

.....……

(podpis osoby uprawnionej)

……

Miejscowość i data

……

Nazwa jednostki organizacyjnej wnioskującej o przeprowadzenie

poszerzonego postępowania sprawdzającego

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 2010 r., Nr 182, poz. 1228) wnoszę o przeprowadzenie poszerzonego postępowania sprawdzającego w celu wydania poświadczenia bezpieczeństwa,

upoważniającego do dostępu do informacji niejawnych o klauzuli ……..*

wobec :

1. Imię …….
2. Nazwisko ……
3. Nr PESEL …….

……..

Pieczątka i podpis kierownika jednostki organizacyjnej

lub osoby upoważnionej do obsady stanowiska lub zlecenia prac

Załącznik :

Załącznik – Ankieta Bezpieczeństwa Osobowego – na …….str. - tylko adresat

· *wpisać odpowiedniąklauzulęlub klauzulętajności*

.

INFORMACJA DODATKOWA:

Zgodnie z art. 73 ust. 1 ustawy o ochronie informacji niejawnych, Agencja Bezpieczeństwa Wewnętrznego prowadzi ewidencje 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 ewidencje osób, którym odmówiono wydania lub cofnięto poświadczenie bezpieczeństwa. Ewidencja ta prowadzona jest w oparciu o dane przekazywane do ABW przez pełnomocników 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:

http://www.bip.abw.gov.pl/portal/bip/76/151/INFORMACJA_NA_TEMAT_KART_IN FORMACYJNYCH. html

ZAŁĄCZNIK NR 3 - protokół oceny dokumentacji niearchiwalnej

.....

(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 dokumentacje niearchiwalne 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

ZAŁĄCZNIK NR 4 - spis dokumentacji niearchiwalnej przeznaczonej na makulaturęlub zniszczenie

.....

nazwa i adres jednostki organizacyjnej

SPIS DOKUMENTACJI NIEARCHIWALNEJ PRZEZNACZONEJ NA MAKULATURĘLUB ZNISZCZENIE

Lp.	TYTUŁ TECZKI	SYMBOL Z WYKAZU RZECZOWEGO	DATY SKRAJNE	UWAGI

ZAŁĄCZNIK NR 5- protokół komisyjnego zniszczenia dokumentów niearchiwalnych

PROTOKÓŁ KOMISYJNEGO ZNISZCZENIA DOKUMENTÓW NIEARCHIWALNYCH

W dniu ..... komisja w składzie:

1. Przewodniczacy komisji.....

   (kierownik lub pracownik archiwum zakładowego)

2. Członek komisji.....

   (przedstawiciel komórek org., których dokumenty sa brakowane),

3. Członek komisji.....

   (Pełnomocnik ochrony lub pracownik pionu ochrony),

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

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

Podpisy członków komisji:

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

Załącznik Nr 2 do Zarządzenia Nr VII/14/2014

Burmistrza Miasta Orzesze

z dnia 18 grudnia 2014 r.

TABELA OCENY ISTOTNOŚCI CZYNNIKÓW ZAGROŻEŃ

Lp.	CZYNNIK	OCENA ISTOTNOŚCI CZYNNIKA			UZASADNIENIE	WSKAZÓWKI
		BARDZO ISTOTNY (8 pkt)	ISTOTNY (4 pkt)	MAŁO ISTOTNY (1 pkt)		
1	2	3	4	5	6	7
1	Klauzula tajności przetwarzanych informacji niejawnych			1	W Urzędzie Miejskim Orzesze przetwarzane są informacje niejawne o klauzuli „zastrzeżone” oraz 1 dokument o klauzuli „poufne”	Analizie podlegają wszystkie klauzule tajności wszystkich przetwarzanych informacji niejawnych. Przy ocenie istotności czynnika stosuje się zasadę: im wyższe klauzule tajności przetwarzanych informacji, tym czynnik ma istotniejsze znaczenie. Dla informacji niejawnych o klauzuli "ściśle tajne" wartość oceny jest stała i wynosi 8 pkt (czynnik ma "bardzo istotne" znaczenie). W przypadku nowo organizowanej jednostki organizacyjnej należy przyjąć wartości szacunkowe.
2	Liczba materiałów niejawnych			2	Liczba materiałów niejawnych oznaczonych klauzulą "zastrzeżone" - 449 Liczba materiałów niejawnych oznaczonych klauzulą "poufne" - 96	Przy ocenie istotności czynnika należy brać pod uwagę wszystkie materiały niejawne zarejestrowane w urządzeniach ewidencyjnych, pozostające w faktycznej dyspozycji jednostki organizacyjnej. W uzasadnieniu należy odnieść się do przybliżonej ogólnej liczby wszystkich materiałów, stosując zasadę: im więcej informacji niejawnych o najwyższych klauzulach tajności, tym czynnik ma istotniejsze znaczenie. W przypadku nowo organizowanej jednostki organizacyjnej należy przyjąć wartości szacunkowe.
3	Postać informacji niejawnych			1	W Urzędzie Miejskim Orzesze niewiele jest przetwarzanych w systemach teleinformatycznych dokumentów w stosunku	Przy ocenie należy brać pod uwagę ogólną liczbę przetwarzanych informacji niejawnych, stosując zasadę, że im więcej informacji przetwarzanych w systemach teleinformatycznych (w stosunku do ogólnej liczby materiałów) tym czynnik jest bardziej istotny. W przypadku nowo organizowanej jednostki organizacyjnej należy przyjąć wartości szacunkowe.

					do ogólnej liczby materiałów	
4	Liczba osób			1	Liczba pracowników mających dostęp do informacji niejawnych jest niewielka w stosunku do liczby wszystkich pracowników.	Przy ocenie istotności tego czynnika należy uwzględnić pracowników jednostki organizacyjnej mających lub mogących mieć dostęp do informacji niejawnych, tj. osoby zajmujące stanowiska, wykonujące zadania lub prace zlecone związane z dostępem do takich informacji, a także posiadane przez nich uprawnienia oraz uzasadnioną potrzebę dostępu do informacji niejawnych. Im więcej osób (w stosunku do liczby zatrudnionych) tym czynnik jest bardziej istotny. W przypadku nowo organizowanej jednostki organizacyjnej należy przyjąć wartości szacunkowe.
5	Lokalizacja			1	Budynek Urzędu Miejskiego Orzesze nie jest użytkowany z innymi podmiotami zani nie jest w zwartej zabudowie. Budynek urzędu nie jest również usytuowany w sąsiedztwie obiektów sportowych i hal widowiskowych ogólnodostępne parkingi, garaże, zakłady przemysłowe i instalacje stanowiące zagrożenie dla życia lub zdrowia.	Na wzrost oceny istotności tego czynnika ma wpływ np. to, że budynek użytkowany jest wspólnie z innymi podmiotami lub budynek jest w zabudowie zwartej (np. budynek, którego ściany przylegają do innego budynku). Na wzrost oceny istotności czynnika ma wpływ także najbliższe sąsiedztwo np.: obiekty przedstawicielstw i podmiotów zagranicznych, hotele, obiekty sportowe i hale widowiskowe, ogólnodostępne parkingi, garaże, zakłady przemysłowe i instalacje stanowiące zagrożenie dla życia lub zdrowia.
6	Dostęp osób do budynku			1	Urząd Miejski Orzesze ma swobodny dostęp poruszania się po budynku osobom niezatrudnionym w urzędzie.	Na wzrost oceny istotności tego czynnika ma wpływ możliwość swobodnego poruszania się po budynku osób niebędących pracownikami jednostki organizacyjnej, np. gości, interesantów (w obiektach użyteczności publicznej).
7	Inne czynniki*)			-	-	Poziom zagrożeń powinien uwzględniać inne czynniki wynikające ze specyfiki jednostki organizacyjnej, niewykazane powyżej, a mogące mieć wpływ na ochronę informacji niejawnych, np.: działanie obcych służb specjalnych, sabotaż, zamach terrorystyczny, kradzież lub inna działalność przestępcza, pożar, działanie sił przyrody (np. obszar zagrożony powodzią) lub szkody górnicze.
Suma punktów				7		