

ZARZĄDZENIE Nr 7/2011

Starosty Nowodworskiego
z dnia 3 marca 2011 roku

w sprawie: wprowadzenia planu ochrony informacji niejawnych i instrukcji dotyczącej sposobu i trybu przetwarzania informacji niejawnych o klauzuli „zastrzeżone” w Starostwie Powiatowym w Nowym Dworze Gdańskim.

Na podstawie ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2010 r. Nr 182, poz.1228), zarządza się co następuje:

§ 1

Wprowadza się Plan Ochrony informacji niejawnych w Starostwie Powiatowym w Nowym Dworze Gdańskim.

§ 2

Wprowadza się Załącznik Nr 1 Instrukcję dotyczącą sposobu i trybu przetwarzania informacji niejawnych o klauzuli „zastrzeżone” w Starostwie Powiatowym w Nowym Dworze Gdańskim.

§ 3

1. Uchyla się Zarządzenie Nr 12/2000 z dnia 21 kwietnia 2000 r. Starosty Powiatu Nowodworskiego w sprawie szczegółowego wymagania w zakresie ochrony informacji niejawnych oznaczonych klauzulą „zastrzeżone” w Starostwie Powiatowym w Nowym Dworze Gdańskim.

2. Uchyla się Zarządzenie Nr 14/2001 z dnia 29 czerwca 2001 r. Starosty Powiatu Nowodworskiego w sprawie wprowadzenia planu ochrony informacji niejawnych.

§ 4

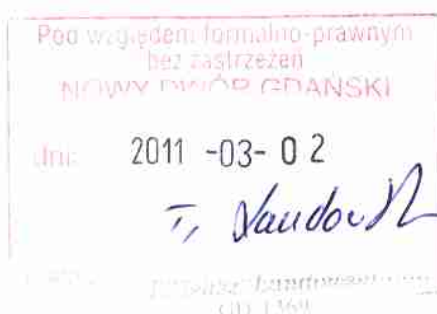
Wykonanie Zarządzenia powierzam Kierownikom Wydziałów, Zespołom i Samodzielnym stanowiskom pracy w Starostwie Powiatowym w Nowym Dworze Gdańskim.

§ 5

Nadzór nad wykonaniem Zarządzenia powierza się Pełnomocnikowi Ochrony.

§ 6

Zarządzenie wchodzi w życie z dniem jego podpisania.



STAROSTA

inż. Zbigniew Piórkowski

PLAN OCHRONY INFORMACJI NIEJAWNYCH STAROSTWA POWIATOWEGO W NOWYM DWORZE GDAŃSKIM

opracowany na podstawie ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych Art.15, ust.1, pkt 5 (Dz. U. z 2010 r. Nr 182, poz. 1228).

I. PRZEDMIOT OCHRONY

Przedmiotem ochrony w Starostwie Powiatowym w Nowym Dworze Gdańskim są:

1. Informacje niejawne oznaczone klauzulą „poufne” i „zastrzeżone”.
2. Informacje niejawne w razie wprowadzenia stanu nadzwyczajnego.

II. POSTANOWIENIA OGÓLNE

1. Użyte w niniejszym planie:

- 1) określenie „komórka organizacyjna” oznacza wydział (jednostkę organizacyjną) w Starostwie Powiatowym;
- 2) rękojmią zachowania tajemnicy oznacza zdolność osoby do spełnienia ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem, stwierdzona w wyniku przeprowadzenia postępowania sprawdzającego;
- 3) dokumentem – jest każda utrwalona informacja niejawna;
- 4/ materiałem – jest dokument lub przedmiot albo dowolna jego część, chronione jako informacja niejawna;
- 5) przetwarzaniem informacji niejawnych – są wszelkie operacje wykonane w odniesieniu do informacji niejawnych i na tych informacjach, w szczególności ich wytwarzanie, modyfikowanie, kopiowanie, klasyfikowanie, gromadzenie, przechowywanie, przekazywanie lub udostępnianie;
- 6) 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.).
- 7) dokumentem szczególnych wymagań bezpieczeństwa – jest systematyczny opis sposobu zarządzania bezpieczeństwem systemu teleinformatycznego;
- 8) dokumentem procedur bezpiecznej eksploatacji systemu teleinformatycznego – jest opis sposobu i trybu postępowania w sprawach związanych z bezpieczeństwem informacji niejawnych przetwarzanych w systemie teleinformatycznym oraz zakres odpowiedzialności użytkowników systemu teleinformatycznego i pracowników mających do niego dostęp;
- 9) dokumentacją bezpieczeństwa systemu teleinformatycznego – jest dokument szczególnych wymagań bezpieczeństwa oraz dokument procedur bezpiecznej eksploatacji systemu teleinformatycznego, opracowany zgodnie z zasadami określonymi w ustawie;
- 10) akredytacją bezpieczeństwa teleinformatycznego – jest dopuszczenie systemu teleinformatycznego do przetwarzania informacji niejawnych;
- 11) ryzykiem – jest kombinacja prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji;
- 12) zatrudnieniem – jest również odpowiednio powołanie, mianowanie lub wyznaczenie.

2. Nadzór nad ochroną informacji niejawnych sprawują bezpośrednio kierownicy wydziałów.
3. Pełnomocnik ds. ochrony informacji niejawnych, zwany dalej „pełnomocnikiem ochrony” odpowiada za zapewnienie przestrzegania przepisów o ochronie informacji niejawnych.
4. Szkolenie w zakresie ochrony informacji niejawnych przeprowadza pełnomocnik ochrony w stosunku do osób zatrudnionych w Starostwie Powiatowym.

5. Kierownik komórki organizacyjnej przed rozwiązaniem stosunku pracy z pracownikiem posiadającym dostęp do informacji niejawnych oznaczonych klauzulą „zastrzeżone” przyjmuje protokolarnie całość dokumentacji /teczkę/ i wyznacza pracownika, który ma prowadzić wspomnianą dokumentację. O powyższym fakcie niezwłocznie należy powiadomić pełnomocnika ochrony.

6. Informacje niejawne mogą być udostępnione wyłącznie osobie dającej rękojmię zachowania tajemnicy i tylko w zakresie niezbędnym do wykonania przez nią pracy lub pełnienia służby na zajmowanym stanowisku albo wykonywanej pracy zleconej.

III. KLASYFIKOWANIE INFORMACJI NIEJAWNYCH

1. Informacjom niejawnym nadaje się klauzulę „poufne”, jeżeli ich nieuprawnione ujawnienie spowoduje szkodę dla Rzeczypospolitej Polskiej m. innymi przez:

- 1) utrudnienie prowadzenia bieżącej polityki zagranicznej Rzeczypospolitej Polskiej;
- 2) zakłócenie porządku publicznego lub zagrożenie bezpieczeństwu obywateli;
- 3) utrudnienie wykonanie zadań służbom lub instytucjom odpowiedzialnych za ochronę bezpieczeństwa lub podstawowych interesów Rzeczypospolitej Polskiej;
- 4) utrudnienie wykonanie zadań służbom i instytucjom odpowiedzialnym za ochronę porządku publicznego, bezpieczeństwa obywateli lub ściganie sprawców przestępstw i przestępstw skarbowych oraz organom wymiaru sprawiedliwości;
- 5) zagrożenie stabilności systemu finansowego Rzeczypospolitej Polskiej;
- 6) wpłynięcie niekorzystnie na funkcjonowanie gospodarki narodowej.

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

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

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

5. Zniesienie lub zmiana klauzuli tajności są możliwe wyłącznie po wyrażeniu pisemnej zgody przez osobę która podpisała dokument, albo jej przełożonego w przypadku ustania lub zmiany ustawowych przesłanek ochronnych.

6. Kierownicy jednostek organizacyjnych przeprowadzają nie rzadziej niż raz na 5 lat przegląd materiałów w celu ustalenia, czy spełniają ustawowe przesłanki ochrony.

7. Po zniesieniu lub zmianie klauzuli tajności należy dokonać odpowiednich zmian w oznaczeniu materiału i poinformować o nich odbiorców.

8. Informacje niejawne mogą być udostępnione wyłącznie osobie uprawnionej posiadającej poświadczenie bezpieczeństwa dostępem do określonej klauzuli tajności lub pisemnym upoważnieniem kierownika jednostki organizacyjnej, jeżeli nie posiada ona poświadczenie bezpieczeństwa.

9. Udostępnienie informacji niejawnej o klauzuli „zastrzeżone” określonej osobie lub instytucji, może nastąpić na pisemną zgodę kierownika jednostki i tylko w odniesieniu do informacji wytworzonych w Urzędzie.

10. Udostępnienie określonej osobie lub instytucji, informacji niejawnych o klauzuli „zastrzeżone” otrzymanych przez Urząd, może nastąpić po uzyskaniu pisemnej zgody jednostki, które te informacje wytworzyła.

11. Informacje niejawne muszą być chronione i przetwarzane w warunkach uniemożliwiających ich nieuprawnione ujawnienie zgodnie z przepisami dotyczące kancelarii tajnych, bezpieczeństwa systemów teleinformatycznych, obiegu materiałów i środków bezpieczeństwa fizycznego, odpowiednich do nadanej klauzuli tajności.

IV. ORGANIZACJA OCHRONY INFORMACJI NIEJAWNYCH

1. Kierownik jednostki organizacyjnej, w której są przetwarzane informacje niejawne, odpowiada za ich ochronę, w szczególności za zorganizowanie i zapewnienie funkcjonowania tej ochrony.

2. Kierownikowi jednostki organizacyjnej bezpośrednio podlega zatrudniony przez niego pełnomocnik do spraw ochrony informacji niejawnych, zwany dalej „pełnomocnikiem ochrony”, który odpowiada za zapewnienie przestrzegania przepisów o ochronie informacji niejawnych.

3. Do zadań pełnomocnika ochrony należy:

- 1) zapewnienie ochrony informacji niejawnych;
- 2) zapewnienie ochrony systemów teleinformatycznych;
- 3) zarządzaniem ryzykiem bezpieczeństwa informacji niejawnych;
- 4) kontrola ochrony informacji niejawnych w szczególności okresowa (co najmniej raz na trzy lata), kontrola ewidencji, materiałów i obiegu dokumentów;
- 5) opracowanie i aktualizowanie planu ochrony informacji niejawnych, w tym w razie wprowadzenia stanu nadzwyczajnego, i nadzorowanie jego realizacji;
- 6) prowadzenie szkoleń w zakresie ochrony informacji niejawnych;
- 7) prowadzenie zwykłych postępowań sprawdzających;
- 8) prowadzenie aktualnego wykazu osób zatrudnionych w jednostce organizacyjnej które posiadają uprawnienia do dostępu do informacji niejawnych oraz osób którym odmówiono wydania poświadczenia bezpieczeństwa lub je cofnięto.

Zadania, o których mowa w ust. 1 do 8, pełnomocnik realizuje przy pomocy wyodrębnionej i podległej mu komórki organizacyjnej do spraw ochrony informacji niejawnych, zwanej dalej „pionem ochrony”.

1. W przypadku stwierdzenia naruszenia w jednostce organizacyjnej przepisów o ochronie informacji niejawnych pełnomocnik ochrony zawiadamia o tym kierownika jednostki organizacyjnej i podejmuje niezwłocznie działania zmierzające do wyjaśnienia okoliczności tego naruszenia oraz ograniczenia jego negatywnych skutków.
2. W przypadku stwierdzenia naruszenia przepisów o ochronie informacji niejawnych o klauzuli „poufne”, pełnomocnik ochrony zawiadamia niezwłocznie ABW.

V. EWIDENCJA INFORMACJI NIEJAWNYCH PODLEGAJĄCEJ OCHRONIE

1 Informacje niejawne oznaczone klauzulą „poufne ”podlegają ewidencjonowaniu w komórce ochronnej Urzędu.

2. Informacje niejawne oznaczone klauzulą „zastrzeżone” podlegają ewidencjonowaniu w sekretariacie Urzędu.

3. Dokumenty i materiały zawierające informacje niejawne podlegają ewidencjonowaniu w dzienniku ewidencyjnym. W dzienniku ewidencyjnym podlegają wszystkie dokumenty, zarówno otrzymywane jak też bez względu na to, w której komórce organizacyjnej dokument został sporządzony i wykonany w Urzędzie.

4. Nośniki informacji niejawnych należy ewidencjonować w rejestrze wydanych przedmiotów

VI. ZABEZPIECZENIE INFORMACJI NIEJAWNYCH

1. Informacje niejawne oznaczone klauzulą „poufne” wymagają przechowywania i zabezpieczenia w komórce ochronnej w szafie pancernej z zamkami o skomplikowanym mechanizmie.
2. Szafa pancerna, w której przechowywane są dokumenty zawierające informacje niejawne, podlega codziennemu po zakończeniu pracy zamknięciu i oplombowaniu.
3. Klucze do szafy pancernej kierownik komórki ochronnej zabezpiecza poprzez zabieranie ich ze sobą, wobec faktu, iż w Urzędzie nie ma portierów dyżurujących w układzie całodobowym.
4. Duplikaty kluczy do szafy pancernej, podlegają deponowaniu u pełnomocnika ds. ochrony informacji niejawnych
5. Klucze do szafy pancernej, podlegają przekazaniu do przechowywania w pojemniku lub w woreczku każdorazowo zaplombowane przez kierownika komórki ochronnej.
6. Klucze do szafy pancernej oraz duplikaty tych kluczy, wymagają pokwitowania ich pobrania przez kierownika komórki ochronnej oraz przez pełnomocnika ochrony. Pokwitowania przyjęcia kluczy na swój stan, dokonać należy w książce ewidencji kluczy, prowadzonej w komórce ochronnej.
7. Informacje niejawne oznaczone klauzulą „zastrzeżone” znajdujące się w poszczególnych wydziałach Urzędu muszą być przechowywane w meblach biurowych zamykanych na klucz.

VII. SZKOLENIE W ZAKRESIE OCHRONY INFORMACJI NIEJAWNYCH

1. Szkolenie w zakresie ochrony informacji niejawnych przeprowadza się w celu zapoznania się z:
 - 1) przepisami dotyczącymi ochrony informacji niejawnych oraz odpowiedzialności karnej, dyscyplinarnej i służbowej za ich naruszenie, w szczególności za nieuprawnione ujawnienie informacji niejawnych;
 - 2) zasadami ochrony informacji niejawnych w zakresie niezbędnym do wykonania pracy lub pełnienia służby, z uwzględnieniem zasad zarządzania ryzykiem bezpieczeństwa informacji niejawnych, w szczególności szacowaniem ryzyka;
 - 3) sposobami ochrony informacji niejawnych oraz postępowania w sytuacjach zagrożenia dla takich informacji lub w przypadku ich ujawnienia;
 - 4) szkolenie przeprowadza ABW – dla pełnomocników ochrony i ich zastępców;
 - 5) szkolenie dla pozostałych osób zatrudnionych, pełniących służbę lub wykonujących czynności w jednostce organizacyjnej organizuje pełnomocnik ochrony;
 - 6) szkolenie przeprowadza się nie rzadziej niż raz na 5 lat. Można odstąpić od przeprowadzenia szkolenia, jeżeli osoba podejmująca pracę przedstawi pełnomocnikowi ochrony aktualne zaświadczenie o odbyciu szkolenia.
2. Szkolenie, o którym mowa wyżej kończy się wydaniem zaświadczenia. Odbierając zaświadczenie, osobna przeszkolona składa pisemne oświadczenie o zapoznaniu się z przepisami o ochronie informacji niejawnych.

VIII. BEZPIECZEŃSTWO OSOBOWE

1. Dopuszczenie do pracy na stanowiskach związanych z dostępem do informacji niejawnych o klauzuli „poufne” może nastąpić po uzyskaniu poświadczenia oraz odbyciu szkolenia w zakresie ochrony informacji niejawnych.
2. Dopuszczenie do pracy na stanowiskach związanych z dostępem do informacji

niejawnych o klauzuli „zastrzeżone” może nastąpić po pisemnym upoważnieniu przez kierownika jednostki organizacyjnej, jeżeli nie posiada ona poświadczenia bezpieczeństwa oraz odbyciu szkolenia w zakresie ochrony informacji niejawnych.

3. Pełnomocnik ochrony przeprowadza zwykle postępowanie sprawdzające na pisemne polecenie kierownika jednostki organizacyjnej.
4. ABW przeprowadza poszerzone postępowanie sprawdzające na pisemny wniosek kierownika jednostki organizacyjnej.
5. Postępowanie sprawdzające ma na celu ustalenie, czy osoba daje rękojmię zachowania tajemnicy.
6. Wszystkie czynności przeprowadzone w toku postępowań sprawdzających muszą być rzetelnie udokumentowane i powinny być zakończone przed upływem 3 miesięcy od dnia złożenia do pełnomocnika ochrony ankiety, lub złożenia wniosku o przeprowadzenie postępowania sprawdzającego wraz z wypełnioną ankietą.
7. Przeprowadzenie postępowania sprawdzającego wymaga pisemnej zgody osoby, której ma dotyczyć.
8. Ankieta po wypełnieniu stanowi tajemnicę prawnie chronioną i podlega ochronie dla informacji niejawnych o klauzuli „zastrzeżone” w przypadku zwykłego postępowania sprawdzającego.
9. Akta zakończonych postępowań sprawdzających prowadzonych przez pełnomocnika ochrony, związanych z dostępem do informacji niejawnych oznaczonych klauzulą „zastrzeżone” przechowuje pełnomocnik ochrony w szafie pancерnej, zamykanej i plombowanej na klucz.
10. Zwykle postępowanie sprawdzające obejmuje: sprawdzenie, w niezbędnym zakresie, w ewidencjach, rejestrach, kartotekach, w szczególności w Krajowym Rejestrze Karnym, danych zawartych w wypełnionej i podpisanej przez osobę ankietę, a także sprawdzenie innych informacji uzyskanych w toku postępowania sprawdzającego, w zakresie niezbędnym do ustalenia, czy osoba sprawdzana daje rękojmię zachowania tajemnicy.
11. Jeżeli jest to konieczne w wyniku uzyskanych informacji, zwykle postępowanie sprawdzające obejmuje rozmowę z osobą sprawdzaną.
12. Postępowanie sprawdzające kończy się wydaniem poświadczenia bezpieczeństwa lub odmową wydania poświadczenia bezpieczeństwa.
13. Poświadczenie bezpieczeństwa wydaje się na okres 10 lat do dostępu do informacji niejawnych o klauzuli „poufne”.
14. Na pisemny wniosek kierownika jednostki organizacyjnej lub osoby uprawnionej do obsady stanowiska, złożony co najmniej 6 miesięcy przed upływem terminu ważności poświadczenia bezpieczeństwa przeprowadza się kolejne postępowanie sprawdzające. Kolejne postępowanie sprawdzające powinno być zakończone przed upływem terminu ważności poświadczenia bezpieczeństwa.
15. Od wydanej przez pełnomocnika ochrony decyzji o odmowie wydania poświadczenia bezpieczeństwa, w wyniku zwykłego postępowania sprawdzającego, osobie sprawdzanej służy odwołanie do Szefa ABW. Odwołanie do Szefa ABW składa się za pośrednictwem pełnomocnika ochrony, który przeprowadził postępowanie sprawdzające.

IX. KOMÓRKA OCHRONNA I ŚRODKI BEZPIECZEŃSTWA FIZYCZNEGO

1. Kierownik jednostki organizacyjnej w której są przetwarzane informacje niejawne o klauzuli „poufne” tworzy komórkę, zwaną dalej „komórką ochronną” informacji niejawnych i zatrudnia jej kierownika.
2. Komórka ochronna stanowi wyodrębnioną komórkę organizacyjną, w zakresie ochrony informacji niejawnych podległą pełnomocnikowi ochrony, obsługiwana przez pracowników pionu ochrony, odpowiedzialną za właściwe rejestrowanie, przechowywanie, obieg i wydawanie materiałów uprawnionym osobom.
3. W komórce ochronnej Urzędu gromadzeniu podlegają dokumenty oznaczone klauzulami „poufne” i „zastrzeżone”.
4. Do podstawowych zadań kierownika komórki ochronnej należy:
 - 1) bezpośredni nadzór nad obiegiem dokumentów;
 - 2) udostępnienie lub wydawanie dokumentów osobom do tego uprawnionym;
 - 3) kontrola przestrzegania właściwego oznaczenia i rejestrowania dokumentów;
 - 4) prowadzenie bieżącej kontroli postępowania z dokumentami;
 - 5) wykonywanie poleceń pełnomocnika ochrony;
 - 6) prowadzenie dziennika ewidencji, rejestry dzienników, wydanych przedmiotów, książek ewidencyjnych i teczek.
5. Organizacja pracy komórki ochronnej zapewnia możliwość ustalenia w każdych okolicznościach, gdzie znajduje się materiał o klauzuli „poufne” lub „zastrzeżone” pozostający w dyspozycji jednostki organizacyjnej.
6. Komórka ochronna, odmawia udostępnienia lub wydania materiału osobie nieuprawnionej.
7. W komórce ochronnej oraz w wydziałach w których są przetwarzane informacje niejawne stosuje się środki bezpieczeństwa fizycznego odpowiednie do poziomu zagrożeń w celu uniemożliwienia osobom nieuprawnionym dostępu do takich informacji, w szczególności przed:
 - 1) zamachem terrorystycznym lub sabotażem;
 - 2) kradzieżą lub zniszczeniem materiału;
 - 3) próbą wejścia osób nieuprawnionych do pomieszczeń, w których są przetwarzane informacje niejawne;
 - 4) nieuprawnionym dostępem do informacji o wyższej klauzuli tajności niewynikającym z posiadanych uprawnień.

X. BEZPIECZEŃSTWO TELEINFORMATYCZNE

1. Systemy teleinformatyczne, w których mają być przetwarzane informacje niejawne, podlegają akredytacji bezpieczeństwa teleinformatycznego.
2. Akredytacji udziela się na czas określony, nie dłużej niż 5 lat.
3. Kierownik jednostki organizacyjnej udziela akredytacji bezpieczeństwa teleinformatycznego dla systemu teleinformatycznego przeznaczonego do przetwarzania informacji niejawnych o klauzuli „zastrzeżone” przez zatwierdzenie dokumentacji bezpieczeństwa systemu teleinformatycznego.
4. Wymagania szczegółowe w tym zakresie ustala inspektor bezpieczeństwa teleinformatycznego, zwany dalej „administratorem systemu” odpowiedzialny za weryfikację i bieżącą kontrolę zgodności funkcjonowania systemu teleinformatycznego ze szczególnymi wymaganiami bezpieczeństwa oraz przestrzegania procedur bezpiecznej eksploatacji.

5. Administratorem systemu, może być osoba , która posiada odpowiednie poświadczenie bezpieczeństwa, zaświadczenie o odbytym przeszkoleniu w zakresie ochrony informacji niejawnych i po odbyciu specjalistycznych szkoleń z zakresu bezpieczeństwa teleinformatycznego prowadzonych przez ABW.

XI. WYKONYWANIE DOKUMENTÓW ZAWIERAJĄCYCH INFORMACJE NIEJAWNE ZA POMOCĄ KOMPUTERA

Pracownicy, którzy do opracowania dokumentów zawierających informacje niejawne oznaczone klauzulą „poufne” lub „zastrzeżone” wykorzystują urządzenia komputerowe, **OBOWIAZANI** są zabezpieczyć 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. Pracownicy, którzy sami korzystają z komputera, a więc gdy komputer związany jest z określonym stanowiskiem pracy, dokonują codziennego uruchamiania i wyłączenia komputera za pomocą hasła. Takie hasło stanowi „klucz” do uruchomienia komputera.
2. W przypadku zachowania tekstu zawierającego informacje niejawne, wykonane za pomocą komputera nie stosować jego rejestrowania na dysku twardym, a więc w stałej pamięci komputera, natomiast zastosować dyskietkę lub płytę CD, którą po zakończeniu pracy, można i trzeba wyjąć z komputera.
3. Dyskietka (płyta CD), na której została zarejestrowana informacja niejawna o klauzuli „poufne”, „zastrzeżone”, a więc podlegająca ochronie i która może być potrzebna do późniejszego wykorzystania wymagają przekazania do komórki ochronnej lub do sekretariatu Urzędu w celu:
 - a) zarejestrowania jako nośnika informacji podlegającej ochronie;
 - b) dyskietki (płyty CD) muszą być przechowywane z pozostałymi dokumentami o tej samej klauzuli w meblach biurowych, zamykanych na klucz w poszczególnych wydziałach Urzędu.
4. W przypadku wykonania dokumentów przy wykorzystania komputera gdy nie zachodzi potrzeba zachowania tekstu dokumentu na elektronicznym nośniku magnetycznym, a więc w przypadku wykorzystania komputera jedynie jako maszyna do pisania, nie wprowadzać zapisu do pamięci komputera, zarówno do pamięci stałej, jak też na dyskietkę, płytę CD, a więc doprowadzić do wykasowania tekstu z chwilą niezbędnej ilości egzemplarzy danego dokumentu w sposób uniemożliwiający jego powtórne odtworzenie czy odczytanie przez osoby nieuprawnione.
5. Fizyczne zniszczenie dyskietki, płyty, dokonywać komisyjnie, w obecności i przy udziale kierownika komórki ochronnej i informatyka doprowadzając tym samym do zmian w zapisach w odniesieniu do dyskietek i płyt CD.
6. Zmiana użytkownika komputera nie może nastąpić bez wiedzy pracownika wcześniej pracującego na tym komputerze, a więc może nastąpić dopiero w przypadku oczyszczenia pamięci stałej komputera i uzyskania zapewnienia pracownika, że komputer nie posiada w swojej pamięci informacji podlegającej ochronie.

XII. ODPOWIEDZIALNOŚĆ ZA DOKUMENTY ZAWIERAJĄCE INFORMACJE NIEJAWNE OZNACZONE KLAUZULĄ „POUFNE”, „ZASTRZEŻONE”.

1. Odpowiedzialność za dokumenty zawierające informacje niejawne, ponosi każda osoba, której dokument zawierający te informacje został przekazany lub udostępniony.
2. Odpowiedzialność osoby, której dokument powierzony został zawierający informacje podlegającej ochronie polega na:

- a) stworzeniu warunków do ochrony dokumentów przed nieuprawnionym dostępem;
 - b) zabezpieczeniu dokumentów przez cały okres niezbędny do realizacji zadań związanych z dostępem do informacji zawartych w treści posiadanych dokumentów;
 - c) nie udostępnieniu dokumentów innym osobom bez wyrażonej zgody, imiennej dekretacji dokonanej przez kierownika jednostki organizacyjnej.
3. Odpowiedzialność za prawidłową ewidencję dokumentów ponosi kierownik komórki ochronnej i pracownik sekretariatu Urzędu.

XIII. GROMADZENIE DOKUMENTÓW ZAWIERAJĄCYCH INFORMACJE NIEJAWNE

1. Dokumenty zawierające informacje niejawne oznaczone klauzulą „poufne”, „zastrzeżone”, podlegają gromadzeniu w teczkach akt oznaczonych właściwą klauzulą tajności. Dokumenty spraw ostatecznie załatwionych przechowuje się 2 lata.
2. Dokumenty zawierające informacje niejawne muszą być przechowywane w szafie pancерnej, oznaczone klauzulą „poufne”, natomiast oznaczone klauzulą „zastrzeżone” w meblach biurowych.
3. Akta spraw zakończonych podlegają ochronie do czasu zniesienia lub zmiany klauzuli tajności. Zniesienie lub zmiana klauzuli tajności są możliwe wyłącznie po wyrażeniu pisemnej zgody przez osobę, która jest uprawniona do podpisania dokumentu.
4. Kierownik jednostki organizacyjnej przeprowadza nie rzadziej niż raz na 5 lat przegląd materiałów w celu ustalenia, czy spełniają ustawowe przesłanki ochrony.

XIV. ODPOWIEDZIALNOŚĆ KARNA, DYSCYPLINARNA I SŁUŻBOWA ZA NARUSZENIE PRZEPISÓW O OCHRONIE INFORMACJI NIEJAWNYCH

1. Odpowiedzialność karną osób, które dopuściły się przestępstwa lub czynu zabronionego przeciwko ochronie informacji niejawnych, określają przepisy Kodeksu Karnego, w art. od 265 do 269 (ustawy z dnia 6 czerwca 1997 roku, Kodeks Karny, Dz. U. z 1997r roku Nr 88, poz.553 z późn. zm.).
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.
3. Nie przestrzeganie zasad i nie realizowanie bądź niewłaściwe realizowanie określonych w Planie Ochrony zadań związanych z ochroną informacji niejawnych, występujących w działalności Urzędu, powodować może zastosowanie sankcji jak w pkt. 2.

XV. POSTĘPOWANIE Z MATERIAŁAMI ZAWIERAJĄCYMI INFORMACJE NIEJAWNE W RAZIE WPROWADZENIA STANU NADZWYCZAJNEGO

Konieczność podjęcia działań zmierzających do zabezpieczenia materiałów (dokumentów) zawierających informacje niejawne o klauzuli „poufne” lub „zastrzeżone”, może mieć miejsce w przypadkach:

1. spodziewanego zagrożenia państwa;
2. wprowadzenia stanu nadzwyczajnego;

3. zagrożeń wewnętrznych spowodowanych klęskami żywiołowymi.

1. Zabezpieczeniu podlegają:

1. wszystkie dokumenty przechowywane w komórce ochronnej i w poszczególnych wydziałach Urzędu;
 - a) w pierwszej kolejności należy zabezpieczyć dokumenty mające bezpośredni związek z funkcjonowaniem Urzędu i materiały mające związek ze sprawami obronnymi;
 - b) w drugiej kolejności pozostałe dokumenty m. in.: plan akcji kurierskiej, plan obrony cywilnej, Plan Operacyjny funkcjonowania Starostwa Powiatowego w warunkach zewnętrznego zagrożenia bezpieczeństwa państwa i w czasie wojny.
2. Zabezpieczenie dokumentów wymienionych w pkt.1, jest niezbędne dla zapewnienia realizacji zadań jednostki organizacyjnej na rzecz Sił Zbrojnych, Urzędu jak też i mieszkańców.
3. Zabezpieczenie dokumentów, dokonuje się poprzez dodatkowe zabezpieczenie (opłombowanie szaf i drzwi), względnie ewakuowanie z pomieszczenia ochrony do innych pomieszczeń lub innego budynku..
4. Materiały niejawne po ewakuacji należy odpowiednio zabezpieczyć przez zamknięcie i opłombowanie pomieszczeń, a także jeżeli jest to możliwe, należy zabezpieczyć całodobowy nadzór nad tymi pomieszczeniami.
5. Kierownicy wydziałów i pracownicy samodzielnych stanowisk bezpośrednio odpowiadają za zabezpieczenie, ewakuację dokumentów zawierających informacje niejawne w swoich wydziałach i na stanowiskach pracy.
6. Decyzje w sprawie zabezpieczenia, ewakuacji dokumentów podejmuje pełnomocnik ochrony lub upoważniony pracownik pionu ochrony.
7. W przypadkach uzasadnionych, pod nieobecność pełnomocnika ochrony lub upoważnionego pracownika pionu ochrony, decyzje podejmuje kierownik jednostki organizacyjnej lub jego zastępca.
8. Miejsce zabezpieczenia materiałów podlegających ochronie, ustala osoba podejmująca decyzje o ewakuacji.
9. W przypadku gdy zabezpieczenie dokumentów w budynku Urzędu lub w innym budynku poza urzędem jest niemożliwe, należy przystąpić do likwidacji dokumentów informacji niejawnych.
10. Decyzje w sprawie likwidacji dokumentów niejawnych podejmuje pełnomocnik ochrony. W przypadku jego nieobecności decyzje podejmuje kierownik jednostki organizacyjnej lub jego zastępca. Likwidację dokumentów należy przeprowadzić wg załączonego wzoru załącznik Nr 1.
11. W skład komisji likwidacyjnej mogą wejść tylko te osoby, które posiadają aktualne poświadczenie bezpieczeństwa lub posiadają pisemne upoważnienie wydane przez kierownika jednostki organizacyjnej, jeżeli nie posiada ona poświadczenia bezpieczeństwa upoważniające do dostępu do informacji niejawnych oznaczonych klauzulą „poufne”, „zastrzeżone. Komisja likwidacyjna może przystąpić do likwidacji dokumentów niejawnych, jeżeli będą w niej uczestniczyły co najmniej dwie osoby.
12. W celu wykonania zadań związanych z zabezpieczeniem materiałów będących przedmiotem zabezpieczenia, konieczne jest:
 1. wydanie stosownego polecenia kierownikowi ochrony oraz kierownikom wydziałów, a także pracownikom samodzielnych stanowisk;

2. zapewnienie niezbędnego środka transportu oraz pracowników w ilości niezbędnej do zapakowania i przeniesienia materiałów wymagających zabezpieczenia;
3. zabezpieczenie ewakuacji dokumentów dokonuje komisja wyznaczona przez osobę zarządzającą zabezpieczeniem materiałów;
4. komisja dokonuje otwarcia komórki ochronnej i realizuje czynności związane z zabezpieczeniem całości materiałów i sporządza protokół, z którego musi wynikać:
 - a) określeniu rodzaju i ilości dokumentów poddanych zabezpieczeniu, ewakuacji;
 - b) określenie sposobu zabezpieczenia dokumentów w nowym miejscu ich przechowywania; materiałów;
 - c) określenie sposobu zabezpieczenia dokumentów, które pozostały w komórce ochronnej;
5. komisja przystępując do otwarcia komórki ochronnej, a więc wykonując polecenie zarządzającego dokonuje zabezpieczenia materiałów, wykorzystując:
 - klucze zapasowe do komórki ochronnej, zdeponowane u pełnomocnika ochrony;
6. w przypadku pozostawienia w komórce ochronnej części materiałów, które nie podlegały zabezpieczeniu, lub których nie zdołano zabezpieczyć, komisja obowiązana jest zamknąć i zaplombować pomieszczenie komórki ochronnej.
Spełnienie lub nie spełnienie tej czynności, komisja obowiązkowo uwzględni treści sporządzonego protokołu otwarcia komórki ochronnej jak też i zabezpieczenia materiałów. Wzór protokołu stanowi załącznik Nr 2.

13. W celu odpowiedniego wykonania zadań związanych z zabezpieczeniem materiałów (dokumentów), kierownicy wydziałów oraz inspektorzy samodzielnych stanowisk pracy obowiązani są:

1. dokonać prawidłowego zabezpieczenia w swoich wydziałach i na stanowiskach pracy, materiałów zawierających informacje niejawne o klauzuli „zastrzeżone”;
2. wykonać polecenia oraz współpracować z pionem ochrony w zakresie zabezpieczenia, ewakuacji oraz likwidacji materiałów niejawnych oznaczonych klauzulą „zastrzeżone”
3. opracować względnie uaktualnić materiały informacji niejawnych, mogące wystąpić w działalności urzędu oraz pozostałe dokumenty przechowywane w komórce ochronnej, jeżeli wyniknie taka potrzeba.

14. Realizacja postanowień dotyczy:

1. przygotowanie materiałów już posiadających do ewentualnego zabezpieczenia;
2. bieżącego gromadzenia materiałów, z myślą o wymogach związanych z ewentualnością ich zabezpieczenia.

Czynności wymienione w pkt 1 i 2 powierza się kierownikowi komórki ochronnej oraz kierownikom wydziałów, a także pracownikom samodzielnych stanowisk.

15. W zależności od istniejących zagrożeń, pion ochrony winien zapewnić współpracę w zakresie zabezpieczenia, ewakuacji materiałów niejawnych z Policją, Strażą Miejską, Strażą Pożarną.

W Z Ó R

Załącznik nr 1
wprowadzenie stanu nadzwyczajnego

PROTOKÓŁ

Poufne/Zastrzeżone

zniszczenia dokumentów informacji niejawnych Starostwa Powiatowego w Nowym Dworze Gdańskim, w związku z wprowadzeniem stanu nadzwyczajnego.

Na podstawie decyzji z dnia
(wpisać osobę wydającą decyzje)

Komisja w składzie:

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

dokonała zniszczenia n/w dokumentów:

L.p.	Numer rejestracyjny	Stopień tajności	Nazwa dokumentu	Ilość		Kat. archiwalna	Uwagi
				Egz.	Ark.		
1.	2	3	4	5	6	7	8

Wszystkie dokumenty wyszczególnione od poz. do poz., po odnotowaniu w rejestrach ewidencyjnych, zniszczono dnia w obecności

Wykonano w 1 egz.

Egz. Nr 1 – a/a

Wyk. i druk.

Nr

Podpisy komisji:

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

Nowy Dwór Gdański, dnia

W Z Ó R

Załącznik nr 2
wprowadzenie stanu nadzwyczajnego

Poufne/Zastrzeżone
Egz. Nr

PROTOKÓŁ

Spisany na okoliczność otwarcia zabezpieczenia i ewakuacji dokumentów informacji
niejawnych z pomieszczenia komórki ochronnej Starostwa Powiatowego w Nowym Dworze
Gdańskim w związku z wprowadzeniem stanu nadzwyczajnego.

Komisja w składzie:

1.
2.
3.

Na podstawie decyzji z dnia
(wpisać osobę wydającą decyzję)

Komisja postanowiła dokonać otwarcia komórki ochronnej i zabezpieczyć n/w dokumenty:

1.

Lp.	Numer ewidencji dokumentu	Stopień tajności	Nazwa dokumentu	Ilość		Kat. Arch.	Uwagi
				egz.	ark.		
1	2	3	4	5	6	7	8

Wszystkie dokumenty od poz. 1, do poz. zostały zapakowane do worka
zaplombowanego i ewakuowano do
(wymienić pomieszczenie- budynek)

2. Dokumenty wyszczególnione od poz. do poz. pozostały w komórce
ochronnej w szafie pancernej zaplombowanej.

3.
(określić sposób zabezpieczenia dokumentów w nowym miejscu i ich przechowywania)
.....
.....
.....

Wykonano w 2 egz.

Podpisy komisji:

Egz. Nr 1 – a/a

Egz. Nr 2 – pełnomocnik ochrony

Wyk. i druk. -

Nr

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

Nowy Dwór Gdański, dnia

XVI. POSTANOWIENIA KOŃCOWE

1. Kierownicy wydziałów, inspektorzy oraz przełożeni pracowników a także kierownik komórki ochronnej i pełnomocnik ochrony:
 - a) zapoznają podległych pracowników z ustaleniami Planu Ochrony informacji niejawnych w Urzędzie;
 - b) zapewnią bieżące przestrzeganie postanowień Planu Ochrony informacji niejawnych, mogących występować w działalności kierowanej komórki organizacyjnej.
2. Osoby, wymienione w pkt. XVI.1, mają obowiązek zapoznania z Planem Ochrony informacji niejawnych wszystkie osoby, podejmujące pracę w Urzędzie.
3. W przypadku wystąpienia wątpliwości, a także przybliżenia zasad dotyczących realizacji zadań związanych z ochroną informacji niejawnych, sporządzenia i wykonania dokumentów, pracownicy Urzędu mogą zwrócić się o wyjaśnienia czy też instruktaż do:
 - a) pełnomocnika ds. ochrony informacji niejawnych;
 - b) kierownika komórki ochronnej.
4. W sprawach nie ujętych w niniejszym planie zastosowanie mają przepisy ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2010 r. Nr 182, poz. 1228) i Rozporządzenia Rady Ministrów z dnia 1 czerwca 2010 r. w sprawie organizacji i funkcjonowania kancelarii tajnych (Dz. U. z 2010 r. Nr 114, poz. 765).

Otrzymują:

1. Kierownicy wydziałów.
2. Pracownicy samodzielnych stanowisk.

Opracował:
Pełnomocnik ochrony
R. Orzechowski

Zatwierdził:

STAROSTA

...inż. Zbigniew Piórkowski

Nowy Dwór Gdański, dnia 3 marca 2011 roku.

INSTRUKCJA

dotyczącą sposobu i trybu przetwarzania informacji niejawnych o klauzuli „zastrzeżone” w Starostwie Powiatowym w Nowym Dworze Gdańskim oraz zakres i warunki stosowania środków bezpieczeństwa fizycznego w celu ich ochrony.

Rozdział 1

Postanowienia ogólne

§ 1

Niniejsza instrukcja, jest dokumentem wewnętrznym wydanym przez Starostę Nowodworskiego i ma zastosowanie do przetwarzania informacji niejawnych o klauzuli „zastrzeżone” z zabezpieczeniem ochrony tych informacji.

§ 2

Instrukcja została opracowana zgodnie z Art. 43.5. ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2010 r. Nr 182, poz. 1228).

§ 3

Określenia i skróty użyte w Instrukcji oznaczają:

1. komórka organizacyjna – oznacza wydział, samodzielne stanowisko w Starostwie Powiatowym;
2. „pełnomocnik ochrony” oznacza pełnomocnika ds. ochrony informacji niejawnych, kierujący zagadnieniami z zakresu ochrony informacji niejawnych;
3. „komórka ochrony” oznacza pracowników wchodzących w skład personelu ochrony informacji niejawnych Starostwa Powiatowego;
4. dokumentem – jest każda utrwalona informacja niejawna;
5. materiałem – jest dokument lub przedmiot albo dowolna ich część, chronione jako informacja niejawna;
6. przetwarzanie informacji niejawnych – są wszelkie operacje wykonane w odniesieniu do informacji niejawnych i na tych informacjach, w szczególności ich wytwarzanie, modyfikowanie, kopiowanie, klasyfikowanie, gromadzenie, przechowywanie, przekazywanie lub udostępnianie;

§ 4

1. Do wykonania prac stanowiące informacje niejawne o klauzuli „zastrzeżone” mogą być uprawnione wyłącznie osoby posiadające poświadczenia bezpieczeństwa lub pisemne upoważnienie wydane przez kierownika jednostki organizacyjnej, jeżeli nie

posiadają poświadczenie bezpieczeństwa oraz odbyciu szkolenia w zakresie informacji niejawnych.

2. nadzór nad ochroną informacji niejawnych o klauzuli „zastrzeżone” sprawują bezpośrednio kierownicy wydziałów;
3. pełnomocnik ochrony odpowiada za zapewnienie przestrzegania przepisów o ochronie informacji niejawnych oraz sprawuje ogólną koordynację i kontrolę w tym zakresie w komórkach organizacyjnych Urzędu;
4. zadania z zakresu koordynacji i kontroli ochrony informacji niejawnych pełnomocnik ochrony wykonuje przy pomocy pracowników pionu ochrony;;
5. szkolenie w zakresie ochrony informacji niejawnych przeprowadza pełnomocnik ochrony w stosunku do osób zatrudnionych w Starostwie Powiatowym.

§ 5

Kierownik komórki organizacyjnej przed rozwiązaniem stosunku pracy z pracownikiem posiadającym poświadczenie bezpieczeństwa upoważniające do dostępu do informacji niejawnych o klauzuli „zastrzeżone” przyjmuje protokółalnie całość dokumentacji posiadających klauzulę „zastrzeżone” i wyznacza pracownika, który ma prowadzić wspomnianą dokumentację. O powyższym fakcie niezwłocznie należy powiadomić pełnomocnika ochrony, który podejmuje działania określone w ustawie o ochronie informacji niejawnych.

Rozdział 2

Oznaczanie i sporządzanie dokumentów informacji niejawnych.

§ 6

1. Informacje niejawne o klauzuli „zastrzeżone” jest to wiadomość z którą pracownik zapoznał się w związku z pełnieniem swoich obowiązków w Starostwie, a które ujawnienie może mieć szkodliwy wpływ i narazić na szkodę interes Starostwa lub obywatela.
2. Pracownikowi mogą być udostępnione informacje niejawne, które wchodzą w zakres wykonywanych przez niego obowiązków;
3. Zgodę na udostępnienie informacji niejawnych może wyrazić na piśmie Starosta względnie upoważniona przez niego osoba, wyłącznie w odniesieniu do informacji wytwarzanych w Starostwie;
4. Klauzulę tajności przyznaje osoba, która jest upoważniona do podpisywania dokumentu;
5. Uprawnienie do przyznawania, zmiany i znoszenia klauzuli tajności przysługuje wyłącznie w zakresie posiadanego prawa dostępu do informacji niejawnych;
6. Osoba, o której mowa w ust. 4, ponosi odpowiedzialność za przyznanie klauzuli tajności i bez jej zgody albo zgody jej przełożonego klauzula nie może być zmieniona lub zniesiona;

§ 7

1. Pracownicy, którzy do opracowania dokumentów zawierających informacje niejawne o klauzuli „zastrzeżone” wykorzystują urządzenia komputerowe, obowiązani są zabezpieczyć

informacje podlegające ochronie przed ich nieuprawnionym ujawnieniem, a także przed dotarciem do tych informacji przez osoby, które nie powinny zapoznać się z treścią.

2. W przypadku zachowania tekstu zawierające informacje niejawnne, wykonane za pomocą komputera nie stosować jego rejestrowania na dysku twardym, a więc w stałej pamięci komputera, natomiast zastosować dyskietkę lub płytę CD, którą po zakończeniu pracy, można i trzeba wyjąć z komputera.

3. Dyskietka (płyta CD), na której została zarejestrowana informacja niejawnna o klauzuli „zastrzeżone”, a więc podlegająca ochronie, nakłada na pracowników obowiązek zarejestrowania dyskietki (płyty CD) w rejestrze wydanych przedmiotów i przechowywania jej z dokumentami informacjami niejawnnymi o klauzuli „zastrzeżone”.

§ 8

1. Materiałom w postaci dokumentów zawierających informacje niejawnne utrwalone w formie pisemnej, zwane dalej „pismem” oznaczone „Z” dla klauzuli „zastrzeżone” oznacza się w następujący sposób:

1) na każdej stronie pisma umieszcza się:

a) w prawym górnym rogu, w kolejności pionowej:

- klauzulę tajności,
- numer egzemplarza pisma, a w przypadku gdy pismo wykonano w jednym egzemplarzu – napis „Egz. pojedynczy”,

b) w lewym górnym rogu sygnaturę literowo-cyfrową, na którą składają się oddzielone myślnikami: literowe oznaczenie jednostki lub komórki organizacyjnej, oznaczenie klauzuli tajności, pod którym pismo zostało zarejestrowane w dzienniku ewidencji, łamany przez rok lub dwie ostatnie cyfry roku, w którym pismo zostało wykonane, a także w zależności od potrzeb, inne oznaczenia ułatwiające ustalenia miejsca jego wykonania w jednostce organizacyjnej lub też przynależność pisma do określonej sprawy,

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

2) na pierwszej stronie umieszcza się również:

a) w lewym górnym rogu nazwę jednostki lub komórki organizacyjnej,

b) w prawym górnym rogu:

- nazwę miejscowości i datę podpisania pisma,
- w przypadku pisma, któremu nadano bieg korespondencyjny pod numerem egzemplarza w kolejności pionowej: nazwę stanowiska adresata oraz imię i nazwisko, a w przypadku wielu adresatów umieszczeniu jednej adnotacji - „adresaci według rozdzielnika”;

3) na ostatniej stronie pisma umieszcza się również:

a) z lewej strony pod treścią:

- liczbę załączników oraz liczbę stron lub innych jednostek miary wszystkich załączników, jeżeli są dołączone do pisma,
- klauzule tajności załączników wraz z numerami, pod jakimi zostały zarejestrowane w odpowiedniej ewidencji,
- liczbę stron każdego załącznika,
- w przypadku, gdy adresatowi wysyła się inną liczbę załączników, niż pozostawia się w aktach, dodatkowo napis „tylko adresat” – jeżeli załączniki mają być przekazane adresatowi bez pozostawienia ich w aktach,

b) z prawej strony pod treścią pisma i adnotacją o załącznikach w kolejności pionowej: nazwa stanowiska oraz imię i nazwisko osoby uprawnionej do jego podpisania,

- c) w lewym dolnym rogu w kolejności pionowej:
- liczbę wykonanych egzemplarzy,
 - adresatów poszczególnych egzemplarzy pisma lub adnotację „adresaci wg rozdzielnika”
 - imię i nazwisko lub inne dane identyfikujące sporządzającego i wykonawcę.
2. W przypadku pisma, któremu nadano bieg korespondencyjny, na pierwszej stronie w prawym górnym rogu pod numerem egzemplarza można nanosić dodatkowe oznaczenia np. „odpis tylko za pisemną zgodą nadawcy”, „kopiowanie tylko za pisemną zgodą nadawcy”, „udzielenie tylko za pisemną zgodą nadawcy”.

§ 9

1. Dokumenty elektroniczne przetwarzane wyłącznie w systemie teleinformatycznym, podlegają ewidencji w elektronicznym rejestrze dokumentów, oznacza się w sposób określony w § 8.
2. Dokumenty elektroniczne, o których mowa w ust. 1, na każdej stronie w prawym górnym rogu pod klauzulą tajności zamiast oznaczenia numeru egzemplarza umieszcza się napis „Egz. elektroniczny”.

§ 10

1. Na pismach stanowiących załączniki, na pierwszej stronie w prawym górnym rogu, umieszcza się dodatkowo napis: „Załącznik nr ... do pisma nr ... z dnia ...”.
2. Jeżeli przy piśmie przewodnim przesyła się załączniki oznaczone klauzulami tajności, to:
- 1) klauzula pisma przewodniego lub dokumentu nie może być niższa niż klauzula załącznika;
 - 2) na piśmie przewodnim, jeżeli jego klauzula jest inna po odłączeniu załączników, zamieszcza się dyspozycję co do klauzuli tajności pisma po trwałym ich odłączeniu; na każdej stronie pod numerem egzemplarza zamieszcza się napis: „... (nazwa klauzuli tajności) po odłączeniu załączników” lub „Jawne po odłączeniu załączników”.
3. Przy rejestracji pisma przewodniego, o którym mowa w ust. 2 pkt 2, we właściwej ewidencji, w rubryce „Informacje uzupełniające/Uwagi” wpisuje się adnotacje o treści „... (nazwa klauzuli tajności) po odłączeniu załączników” lub „Jawne po odłączeniu załączników”.

§ 11

1. Na materiałach lub innych niż pismo klauzulę tajności i sygnaturę literowo-cyfrową umieszcza się przez ostemplowanie, nadrukowanie, wpisanie odręczne lub w inny widoczny sposób, bezpośrednio, a jeżeli to jest niemożliwe – na ich obudowie lub opakowaniu.
2. Utrwalenie informacji niejawnych w formie dźwięku, obrazu powinno być poprzedzone i kończyć się informacją o nadanej klauzuli tajności.
3. Na trwale oprawionych zbiorach dokumentów, rejestrach, książkach i broszurach klauzule tajności umieszcza się po prawej stronie na górze i dole zewnętrznych ścianek okładki oraz, jeżeli jest, na stronie tytułowej.

§ 12

Na pismach zawierających informacje niejawne, wobec których minął okres ochronny lub ustanowiony przez osoby nadającą klauzulę tajności:

- 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 tej adnotacji;
3) skreśleń i adnotacji, o których mowa w ust. 1-2, dokonuje się kolorem czerwonym, w sposób czytelny. Wycieranie, wywabianie lub zamazywanie klauzuli tajności i dokonanych zmian jest niedozwolone.

§ 13

1. Na zawierających informacje niejawne kopiach, odpisach i w wydrukach dokumentów elektronicznych przetwarzanych w systemie teleinformatycznym umieszcza się:
1) na wszystkich stronach w prawym górnym rogu napis: „Kopia” lub „Odpis”;
2) na pierwszej stronie dodatkowo numer, pod jakim zostały w dzienniku ewidencyjnym, numer wykonanego egzemplarza kopii, lub odpisu;
3) na ostatniej stronie dodatkowo napis „Za zgodność” i odcisk tuszowej pieczęci z nazwą jednostki lub komórki organizacyjnej w której sporządzono kopię lub odpis.
2. Zgodność z oryginałem kopii lub odpisu potwierdza podpisem kierownik jednostki lub komórki organizacyjnej lub inne osoby przez nich upoważnione. Podpis dokonuje się czytelnie imieniem i nazwiskiem.
3. Fakt sporządzenia kopii lub odpisu odnotowuje się na ostatniej stronie dokumentu, z którego sporządzono kopię lub wyciąg, przez odcisk pieczęci i umieszczenie adnotacji informującej o:
1) nazwie jednostki lub komórki organizacyjnej, w której sporządzono kopię, wyciąg;
2) liczbę egzemplarzy sporządzonych kopii lub odpisów;
3) dacie sporządzenia kopii lub odpisu;
4) numerze pod jakim kopia lub odpis zostały zarejestrowane w dzienniku ewidencyjnym.
4. Adnotacje, o których mowa ust. 3 pkt 1-3, wpisuje się przed wykonaniem kopii lub odpisu, natomiast numer, pod jakim zostały zarejestrowane w dzienniku ewidencyjnym, nanosi się dopiero po wykonaniu kopii lub odpisu.

§ 14

Oznaczenie pism, akt, informacji niejawnych po naniesieniu klauzuli tajności „zastrzeżone”, należy opisywać zgodnie z rzeczowym wykazem akt obowiązującym w Urzędzie, z jednoczesnym uwzględnieniem oznaczeń dokumentów zgodnie z § 8 niniejszej instrukcji

Rozdział 3

Ewidencja informacji niejawnych o klauzuli „zastrzeżone”.

§ 15

1. Dla wszystkich dokumentów informacji niejawnych oznaczonych klauzulą „zastrzeżone” zakłada się dziennik ewidencyjny.
2. Nośniki (dyskietki, płyty CD) informacji niejawnych o klauzuli „zastrzeżone” ewidencjonuje się w rejestrze wydanych przedmiotów.
3. Rejestr pism w dzienniku ewidencyjnym oraz rejestr wydanych przedmiotów prowadzi się sekretariacie starostwa przez pracownika tego sekretariatu.
4. Rejestry kancelaryjne mogą być prowadzone przez kilka lat. Numerację zapisów rozpoczyna się w każdym roku od nr 1.

5. Każdemu rejestrowi odpowiada teczka, oznaczona symbolem rejestru, przeznaczona do przechowywania akt.
6. Teczke zakłada się w zasadzie na każdy rok kalendarzowy oddzielnie. Dopuszcza się w przypadku małej ilości korespondencji, prowadzenie teczek przez okres dłuższy niż 1 rok.
7. Sprawy dotyczące informacji niejawnych oznaczone klauzulą tajności „zastrzeżone” należy przechowywać w teczkach oddzielnie.
8. Teczke należy zarejestrować w rejestrze dzienników, książek ewidencyjnych i teczek.
9. Teczke aktową w postaci dokumentu zawierającego informacje niejawne o klauzuli „zastrzeżone” należy opisywać w następujący sposób:

- 1) z lewej strony u góry symbol komórki organizacyjnej (pieczętka);
- 2) w prawym górnym rogu oznacza się kategorię archiwalną oraz po prawej stronie w widocznym miejscu umieszcza się klauzulę tajności „zastrzeżone”, na górze i dole zewnętrznej ścianki okładki;
- 3) na środku teczki, znak akt, tytuł teczki, hasło, według jednolitego rzeczowego wykazu akt i ewentualnie bliższe określenie zawartości teczki;
- 4) pod tytułem teczki w prawym górnym rogu:
 - Rozpoczęto
(data)
 - Zakończono
(data)
 - Teczka zawiera ark.
- 5) wewnątrz teczki należy dołączyć spis spraw (opis pism) wg wzoru:

OPIS PISM

znajdujących się w teczce

Lp.	Numer pisma		Nazwa zakładu lub jednostki organizacyjnej	Nr strony
	wychodzącego	wchodzącego		
1.				

- numerować strony dokumentu w prawym górnym rogu,
- na zakończenie teczki przesnuować i opieczetować całość akt.

10. Każdą sprawę załatwia się oddzielnym pismem bez łączenia jej z inną sprawą nie mającą z nią bezpośredniego związku. Znak sprawy jest stałą cechą rozpoznawczą sprawy, każde pismo dotyczące tej sprawy otrzymuje identyczny znak. Znak sprawy zawiera:

- a) symbol literowy komórki organizacyjnej;
- b) symbol liczbowy hasła wg jednolitego rzeczowego wykazu akt;
- c) liczbę kolejną pod którą sprawa została zarejestrowana w spisie spraw;
- d) cyfry ostatnie oznaczają rok w którym rozpoczęto sprawę,
(np.OSO-5211/Z-3/11, literka „Z”- oznacza zastrzeżone).

11. Na materiałach w postaci wykresów map i rysunków, klauzulę tajności umieszcza się pod legendą, blokiem tytułowym lub skalą oraz na stronach zewnętrznych w miejscach widocznych po złożeniu.

Rozdział 4

Przesyłki informacji niejawnych o klauzuli „zastrzeżone”.

§ 16

1. Materiały informacji niejawnych o klauzuli „zastrzeżone” nadane w postaci listów przekazuje się jako listy polecone lub wartościowe, w dwóch nieprzezroczystych mocnych kopertach, które oznacza się:

- 1) na wewnętrznej kopercie:
 - a) klauzule tajności i ewentualnie dodatkowe oznaczenie;
 - b) imienne określenie adresata;
 - c) imię i nazwisko i podpis osoby pakującej;
 - d) numer, pod którym dokument został zarejestrowany w dzienniku ewidencyjnym;
 - 2) na zewnętrznej kopercie:
 - a) nazwa jednostki organizacyjnej adresata;
 - b) adres siedziby adresata;
 - c) numer wykazu i pozycji w wykazie przesyłek nadanych;
 - d) nazwa jednostki organizacyjnej nadawcy.
2. Przewoźnik, „Poczta Polska” przyjmuje przesyłki na podstawie wykazu przesyłek nadanych, sporządzonego przez nadawcę. Przyjęcie przesyłki potwierdza się podpisem i pieczęcią przewoźnika.

Rozdział 5

Zabezpieczenie materiałów niejawnych o klauzuli „zastrzeżone”.

§ 17

1. Dokumenty informacji niejawnych o klauzuli „zastrzeżone”, znajdujące się w pomieszczeniach biurowych jednostki organizacyjnej muszą być przechowywane w meblach biurowych zamykanych na klucz.
2. Nie należy pozostawiać dokumentów informacji niejawnych opisanych klauzulą „zastrzeżone” w pomieszczeniu mogącym dostać się w niepowołane ręce osób trzecich, a także powodować utratę lub zniszczenie.
3. Odpowiedzialność za zabezpieczenie dokumentów informacji niejawne, ponosi kierownik wydziału, a także każda osoba, której dokument zawierający te informacje został przekazany.

Rozdział 6

Postanowienia końcowe

§ 18

1. Każdy pracownik prowadzący sprawy informacji niejawnych w Urzędzie, zobowiązany jest zapoznać się z niniejszą Instrukcją i stosować przepisy w niej zawarte na swoim stanowisku.
2. Nadużycie przez pracownika postanowień niniejszej Instrukcji może stanowić podstawę do pociągnięcia go do odpowiedzialności dyscyplinarnej, lub karnej, w trybie i na zasadach przewidzianych przepisami prawa.
3. W sprawach nie ujętych niniejszą Instrukcją, stosuje się przepisy zawarte w ustawie z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2010 r. Nr 182, poz. 1228) oraz rozporządzenie Prezesa Rady Ministrów z dnia 13 sierpnia 2010 r. w sprawie sposobu oznaczenia materiałów, umieszczenia na nich klauzul tajności (Dz. U. z 2010 r. Nr 159, poz. 1069).

Opracował:
Pełnomocnik ochrony
R. Orzechowski

Zatwierdził:

STAROSTA

.....
inż. Zbigniew Piórkowski