

**ZARZĄDZENIE NR 242/14
BURMISTRZA MYSZYŃCA**

z dnia 20 października 2014 r.

w sprawie wprowadzenia „Planu Ochrony Informacji Niejawnych w Urzędzie Miejskim w Myszyńcu” i „Instrukcji dotyczącej sposobu i trybu przetwarzania informacji niejawnych o klauzuli „zastrzeżone” w Urzędzie Miejskim w Myszyńcu oraz zakresu i warunków stosowania środków bezpieczeństwa fizycznego w celu ich ochrony”

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2013 r., poz. 594 z późn. zm.) oraz art. 14 ust. 1 i art. 43 ust. 5 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228) zarządzam, co następuje:

§ 1.

W celu zapewnienia ochrony informacji niejawnych wprowadza się „Plan Ochrony Informacji Niejawnych w Urzędzie Miejskim w Myszyńcu” w brzmieniu załącznika nr 1 do niniejszego zarządzenia.

§ 2.

Wprowadza się „Instrukcję dotyczącą sposobu i trybu przetwarzania informacji niejawnych o klauzuli „zastrzeżone” w Urzędzie Miejskim w Myszyńcu oraz zakresu i warunków stosowania środków bezpieczeństwa fizycznego w celu ich ochrony” stanowiącą załącznik nr 2 do niniejszego zarządzenia.

§ 3.

Traci moc „Plan Ochrony Informacji Niejawnych w Urzędzie Miejskim w Myszyńcu” zatwierdzony przez Burmistrza Myszyńca w dniu 14.07.2008 r.

§ 4.

Wykonanie zarządzenia powierza się Pełnomocnikowi ds. Ochrony Informacji Niejawnych.

§ 5.

Zarządzenie wchodzi w życie z dniem podpisania.

Burmistrz Myszyńca

Bogdan Glinka

PLAN OCHRONY INFORMACJI NIEJAWNYCH

W URZĘDZIE MIEJSKIM W MYSZYŃCU

Opracowany przez Pełnomocnika ds. Ochrony Informacji Niejawnych na podstawie postanowień art. 15 ust. 1 pkt 5 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2010 r. Nr 182, poz. 1228).

I. Definicje w rozumieniu Planu Ochrony Informacji Niejawnych

W rozumieniu Planu Ochrony Informacji Niejawnych:

1. jednostką organizacyjną – jest Urząd Miejski w Myszyńcu;
2. rękojmnią zachowania tajemnicy – jest 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 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;
5. przetwarzaniem informacji niejawnych – są wszelkie informacje wykonywane w odniesieniu do informacji niejawnych i na tych informacjach, w szczególności ich wytwarzanie, modyfikowanie, kopiowanie, klasyfikowanie, gromadzenie, przechowywanie, przekazywanie lub udostępnianie;
6. dokumentacją bezpieczeństwa systemu teleinformatycznego – jest dokument szczególnych wymagań bezpieczeństwa oraz dokument procedur bezpiecznej eksploatacji systemu teleinformatycznego, opracowane zgodnie z zasadami określonymi w ustawie;
7. akredytacją bezpieczeństwa teleinformatycznego – jest dopuszczenie systemu teleinformatycznego do przetwarzania informacji niejawnych;
8. urzędem – jest Urząd Miejski w Myszyńcu;
9. kierownik jednostki organizacyjnej – jest Burmistrz Myszyńca;
10. pełnomocnikiem ochrony – jest Pełnomocnik ds. ochrony informacji niejawnych w Urzędzie Miejskim w Myszyńcu;
11. ryzykiem – jest kombinacja prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji;
12. szacowaniem ryzyka – jest całościowy proces analizy i oceny ryzyka;
13. zarządzaniem ryzykiem – są skoordynowane działania w zakresie zarządzania bezpieczeństwem informacji, z uwzględnieniem ryzyka;
14. zatrudnieniem – jest również odpowiednio powołanie, mianowanie lub wyznaczenie.

II. Podstawowe zasady ochrony informacji niejawnych

Warunkiem skutecznego funkcjonowania systemu ochrony informacji niejawnych jest stosowanie następujących zasad:

1. zasada ograniczonego dostępu – informacje niejawne mogą być udostępniane wyłącznie osobie dającej rękojmię zachowania tajemnicy i tylko w zakresie niezbędnym do wykonywania przez nią pracy na zajmowanym stanowisku (tzw. zasada „need-to-know”). Stosowanie tej zasady ma zapewnić, że dostęp do informacji niejawnych jest determinowany zakresem obowiązków danego pracownika, co ogranicza do minimum liczbę osób, które zapoznają się z poszczególnymi informacjami;

2. zasada udostępniania informacji niejawnych wyłącznie osobom gwarantującym ich ochronę przed nieuprawnionym ujawnieniem - warunkiem wykonywania obowiązków związanych z dostępem do informacji niejawnych jest uzyskanie odpowiedniego poświadczenia bezpieczeństwa (z wyjątkami określonymi w ustawie) oraz odbycie przeszkolenia w zakresie ochrony informacji niejawnych. Ma to zapewnić, że dostęp do informacji niejawnych uzyskują wyłącznie osoby dające rękojmię zachowania tajemnicy i znające zasady postępowania oraz odpowiedzialności karnej, dyscyplinarnej i służbowej za naruszenie przepisów w zakresie ochrony informacji;

3. zasada podporządkowania środków ochrony klauzuli informacji – w oparciu o przepisy ustawy oraz wydanych do niej aktów wykonawczych – środki ochrony fizycznej i zasady bezpieczeństwa obiegu dokumentów, muszą być adekwatne do klauzuli tajności wytwarzanych, przetwarzanych, przekazywanych i przechowywanych informacji. Dzięki temu dokumenty i materiały zawierające informacje niejawne tej samej wagi są we wszystkich instytucjach chronione w podobny sposób;

4. zasady dostosowania zakresu środków ochrony fizycznej do uwarunkowań i specyfiki danej instytucji – zgodnie z ustawą zakres stosowania środków ochrony fizycznej musi jednocześnie odpowiadać klauzuli tajności i ilości informacji niejawnych oraz poziomowi dostępu do takich informacji zatrudnionych osób oraz uwzględniać wskazania służb ochrony państwa dotyczące w szczególności ochrony przed zagrożeniami ze strony obcych służb specjalnych. Zasada ta uzupełnia poprzednią, stwarzając możliwość dostosowania zakresu i rodzaju środków ochrony do faktycznie występujących zagrożeń, w oparciu o fachową ocenę uprawnionych funkcjonariuszy służb ochrony państwa;

5. zasada kontroli wytwórcy nad sposobem ochrony informacji – osoba, która jest upoważniona do podpisania dokumentu lub oznaczenia innego niż dokument materiału (wytwórca), ma prawo do przyznania klauzuli tajności, która jednoznacznie określa środki ochrony danej informacji. Bez zgody tej osoby lub jej przełożonego klauzula tajności nie może być obniżona ani zniesiona. Celem takiego rozwiązania jest zapewnienie jednolitego sposobu ochrony informacji niejawnych przez wszystkich odbiorców dokumentu lub materiału, zgodnie z dokonaną przez wytwórcę oceną zakresu szkód, które mogłyby za sobą pociągnąć jego nieuprawnione ujawnienie;

6. zakaz zaniżania lub zawyżania klauzuli tajności – celem tej zasady jest stosowanie środków ochrony adekwatnych do wagi danej informacji, a w konsekwencji uniknięcie ponoszenia zbędnych kosztów związanych z zawyżaniem klauzuli tajności oraz koncentracja środków na ochronie informacji wymagających specjalnych środków bezpieczeństwa.

III. Ocena zagrożeń zewnętrznych i wewnętrznych

1. Zagrożeniami zewnętrznymi dla Urzędu Miejskiego w Myszyńcu są:

- ü możliwość napadu przez zorganizowane grupy przestępcze i terrorystyczne, działające w sposób profesjonalny, przemyślany i zorganizowany;

- ü możliwość napadu przez pojedynczych przestępców, przypadkowe osoby, które mogą wykorzystać m.in. nieprawidłowości w ochronie mienia urzędu;

- ü symptomy mogące świadczyć o przygotowaniu napadu lub włamania do budynku;

- ü wzmożone zainteresowanie osób postronnych obiektami, pomieszczeniami urzędu przejawiające m.in. przez podejmowanie prób uzyskania informacji o obiekcie lub jego pomieszczeniach;

- ü nawiązywanie rozmów przez osoby postronne z pracownikami urzędu,

- ü podszywanie się pod byłych pracowników urzędu i przejawianie zainteresowania tym, co się po latach zmieniło;

- obserwacja sposobu działania systemu ochronnego, sekretariatu, itp.
- rozpoznawanie systemu technicznych zabezpieczeń, w tym stosowania urządzeń alarmowych;
- celowe uszkodzanie urządzeń alarmowych, linii telefonicznych, oświetlenia, itp.

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

- systematyczną, skrupulatną i wnikliwą kontrolę systemu ochrony przez osoby odpowiedzialne za jego organizację;
- pracownicy pionu ochrony w czasie godzin pracy powinni zwracać szczególną uwagę na możliwość zaistnienia ewentualnych zagrożeń;
- stosować zasadę niedopuszczania osób niepowołanych do penetracji strefy administracyjnej;
- wykonywanie prac remontowych, porządkowych itp. w strefie administracyjnej, wyłącznie pod nadzorem osób odpowiedzialnych.

2. Zagrożeniami wewnętrznymi dla urzędu są:

- próby wyniesienia dokumentów lub materiałów przez pracowników urzędu;
- próby powielania, kserowania dokumentów służbowych dla celów prywatnych;
- próby wglądu w dokumenty niejawne przez osoby nieuprawnione;

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

- zwracanie szczególnej uwagi na osoby, które mogą być zainteresowane zaborem dokumentów;
- prowadzenie szczególnego nadzoru by nie dokonywano prób kserowania, kopiowania dokumentów bez uprzedniej zgody przełożonego;
- w trakcie prowadzonych szkoleń należy uwrażliwić pracowników na możliwość prób kontaktu grup zorganizowanych z pracownikami urzędu mającymi dostęp do dokumentów niejawnych;
- przestrzeganie zasady udostępniania informacji niejawnych (dostęp do informacji niejawnych mogą mieć tylko pracownicy posiadający poświadczenie bezpieczeństwa lub upoważnienie do dostępu do informacji niejawnych o klauzuli „zastrzeżone” wydane przez Burmistrza)

IV. Przedmiot ochrony

Przedmiotem ochrony w Urzędzie Miejskim w Myszyńcu są:

- informacje niejawne oznaczone klauzulą „zastrzeżone” wymienione w załączniku nr 1 do planu ochrony;
- pomieszczenie, w którym są przechowywane i opracowywane materiały niejawne.

V. Ochrona fizyczna informacji niejawnych

Urząd jako instytucja, w której materiały zawierające informacje niejawne są wytwarzane, przetwarzane, przekazywane lub przechowywane, ma obowiązek stosowania środków ochrony fizycznej w celu uniemożliwienia osobom nie upoważnionym dostępu do takich informacji, a w szczególności przed:

- działaniem służb specjalnych,
- zamachem terrorystycznym lub sabotażem,
- kradzieżą lub zniszczeniem materiału,
- próbą wejścia osób nieuprawnionych,
- nieuprawnionym dostępem pracowników do materiałów oznaczonych wyższą klauzulą tajności

Zakres stosowania środków ochrony fizycznej musi odpowiadać klauzuli tajności i ilości informacji niejawnych, liczbie oraz poziomowi dostępu do takich informacji zatrudnionych osób.

W celu uniemożliwienia osobom nieuprawnionym dostępu do informacji niejawnych, podejmuje się następujące działania:

- wydziela się części obiektów, które poddane są szczególnej kontroli wejść i wyjść oraz kontroli przebywania, zwane dalej „strefami bezpieczeństwa”,

- wydziela się wokół stref bezpieczeństwa strefy administracyjne służące do kontroli osób lub pojazdów,

- dokumenty i materiały zawierające informacje niejawne o klauzuli „zastrzeżone” przechowuje się na stanowiskach pracy w meblach biurowych zamykanych na klucz,

- zapewnia się kontrolę stref bezpieczeństwa i stref administracyjnych przez przeszkolonych zgodnie z ustawą pracowników pionu ochrony,

- stosuje się wyposażenie i urządzenia służące ochronie informacji niejawnych, którym na podstawie odrębnych przepisów przyznano certyfikaty lub świadectwa kwalifikacyjne.

Pełnomocnik ochrony jest zobowiązany do bieżącego nadzoru nad stosowaniem środków ochrony fizycznej.

Burmistrz Myszyńca zatwierdza opracowaną przez pełnomocnika ochrony instrukcję sposobu i trybu przetwarzania informacji niejawnych o klauzuli „zastrzeżone” w podległych komórkach urzędu.

W urzędzie rozróżniamy jedną strefę bezpieczeństwa- strefę administracyjną. Służy ona do kontroli ruchu osób i pojazdów oraz zwiększenia skuteczności elektromagnetycznej. Jej granicę stanowi ogrodzenie terenu jednostki organizacyjnej (zewnątrzna ściana budynku) oraz granica strefy bezpieczeństwa. Wstęp do niej powinien być możliwy wyłącznie za zgodą osób upoważnionych przez kierownika jednostki organizacyjnej do przyjmowania interesantów. W strefie administracyjnej można wykonywać, przechowywać, wytwarzać dokumenty jawne lub dokumenty niejawne o klauzuli „zastrzeżone”.

VI. Ewidencja i zasady wykonywania dokumentów zawierających informacje niejawne

1. Informacje niejawne oznaczone klauzulą „zastrzeżone” podlegają ewidencjonowaniu w dzienniku korespondencji.

2. Każdy dokument niejawny przychodzący i wychodzący z urzędu podlega rejestracji w dzienniku korespondencji.

3. Numer ewidencyjny dokumentu niejawnego stanowiącego tajemnicę służbową o klauzuli „zastrzeżone” powinien być poprzedzony skrótem literowym „Z”.

4. Pełnomocnik ochrony ewidencjonuje wszystkie wykonane w urzędzie dokumenty, które zawierają informacje niejawne bez względu na to, w której komórce organizacyjnej dokument został sporządzony i wykonany.

5. Propozycje przyznania klauzuli tajności na wykonanym dokumencie przedstawia osoba sporządzająca dokument.

6. Klauzulę tajności na danym dokumencie przyznaje osoba, która jest upoważniona do podpisania dokumentu.

7. Dokumenty niejawne powinny być opisane i posiadać wszystkie wymagane oznaczenia zgodnie z Rozporządzeniem Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności (Dz. U. z 2011 r. Nr 288, poz. 1692),

8. Dokumenty zawierające informacje niejawne należy wykonać w takiej ilości egzemplarzy, jaka jest niezbędna dla załatwienia sprawy, a więc z wyeliminowaniem zbędnych egzemplarzy.

VII. Postępowanie sprawdzające

1. Zwykle postępowanie sprawdzające przeprowadza pełnomocnik ochrony na pisemne polecenie Burmistrza.

2. Każda osoba wobec której zostanie przeprowadzone postępowanie sprawdzające zobowiązana jest do:

- ü wypełnienie określonej przepisami ankiety bezpieczeństwa osobowego;
- ü wypełnienie ankiety w sposób dokładny i zgodny z prawdą.

3. Dopuszczenie do pracy albo zlecenie prac, związanych z dostępem danej osoby do informacji niejawnych o klauzuli „zastrzeżone” może nastąpić po:

- ü pisemnym upoważnieniu przez kierownika jednostki, jeżeli nie posiada on poświadczenia bezpieczeństwa;
- ü odbyciu szkolenia w zakresie ochrony informacji niejawnych.

4. Postępowanie sprawdzające ma na celu ustalenie, czy osoba sprawdzana daje rękojmię zachowania tajemnicy.

5. Zwykle postępowanie sprawdzające obejmuje:

- ü sprawdzenie, w niezbędnym zakresie, w ewidencjach, rejestrach i kartotekach, w szczególności w Krajowym Rejestrze Karnym, danych zawartych w wypełnionej i podpisanej przez osobę sprawdzaną ankiecie, a także sprawdzenie innych informacji uzyskanych w toku postępowania sprawdzającego, w zakresie niezbędnym do ustalenia, czy osoba daje rękojmię zachowania tajemnicy;
- ü sprawdzenie w ewidencjach, kartotekach, niedostępnych powszechnie, danych zawartych w ankiecie oraz innych informacji uzyskanych w toku postępowania sprawdzającego, w zakresie niezbędnym do ustalenia, czy osoba sprawdzana daje rękojmię zachowania tajemnicy.

6. Jeżeli w toku zwykłego postępowania sprawdzającego wystąpią wątpliwości nie pozwalające na ustalenie, czy osoba sprawdzana daje rękojmię zachowania tajemnicy, organ prowadzący postępowanie sprawdzające zapewnia osobie sprawdzanej w trakcie wysłuchania możliwość osobistego ustosunkowania się do informacji wywołujących te wątpliwości. Osoba ta może stawić się na wysłuchanie ze swoim pełnomocnikiem. Z przebiegu wysłuchania sporządza się protokół, który podpisuje osoba prowadząca wysłuchanie, osoba wysłuchana oraz pełnomocnik, jeżeli w nim uczestniczył. Organ prowadzący to postępowanie odstępuje od przeprowadzenia tej czynności jeżeli:

- ü jej przeprowadzenie wiązałoby się z ujawnieniem informacji niejawnych,
- ü postępowanie sprawdzające doprowadziło do niebudzącego wątpliwości ustalenia, że osoba sprawdzana nie daje rękojmi zachowania tajemnicy.

7. Postępowanie sprawdzające kończy się:

- ü wydaniem upoważnienia do dostępu do informacji niejawnych oznaczonych klauzulą „zastrzeżone”
- ü odmową wydania upoważnienia do dostępu do informacji niejawnych oznaczonych klauzulą „zastrzeżone”,
- ü umorzeniem.

9. Organ prowadzący postępowanie sprawdzające odmawia wydania upoważnienia do dostępu do informacji niejawnych oznaczonych klauzulą „zastrzeżone”, jeżeli osoba sprawdzana została skazana prawomocnym wyrokiem na karę pozbawienia wolności za przestępstwo umyślne ścigane z oskarżenia publicznego, także popełnione za granicą, lub umyślne przestępstwo skarbowe, jeżeli czyn, za który nastąpiło skazanie, wywołuje wątpliwości podlegające sprawdzeniu.

10. Osoba uprawniona do obsady stanowiska jest obowiązana, niezwłocznie po otrzymaniu zawiadomienia o odmowie wydania upoważnienia do dostępu do informacji niejawnych oznaczonych klauzulą „zastrzeżone” uniemożliwić dostęp do tych informacji osobie, której odmowa dotyczy.

VIII. Kontrola ochrony informacji niejawnych

Celem kontroli jest sprawdzenie i ocena stanu przestrzegania przepisów o ochronie informacji niejawnych, w tym:

- ü zapewnienie zgodnego z obowiązującym przepisami postępowania z dokumentami niejawnymi przez pracowników urzędu,

- ü eliminowanie stwierdzonych niedociągnięć i nieprawidłowości w zakresie wytwarzania, przechowywania i obiegu dokumentów niejawnych,

- ü ustalenie przyczyn ujawnionych naruszeń zasad ochrony informacji niejawnych, formułowanie wniosków i zaleceń w sprawie systemu ochrony informacji niejawnych,

- ü wyrabianie u pracowników urzędu właściwych nawyków w postępowaniu z dokumentami niejawnymi.

IX. Szkolenie w zakresie ochrony informacji niejawnych

Szkolenie w zakresie informacji niejawnych przeprowadza się w celu zapoznania pracowników urzędu z :

- ü przepisami dotyczącymi ochrony informacji niejawnych oraz odpowiedzialności karnej, dyscyplinarnej oraz służbowej za ich naruszenie, w szczególności za nieuprawnione ujawnienie informacji niejawnych,

- ü zasadami ochrony informacji niejawnych w zakresie niezbędnym do wykonywania pracy, z uwzględnieniem zasad zarządzania ryzykiem,

- ü sposobami ochrony informacji niejawnych oraz postępowania w sytuacjach zagrożenia dla takich informacji lub w przypadku ich ujawnienia.

Szkolenie przeprowadza pełnomocnik ochrony dla osób zatrudnionych i wykonujących czynności zlecone w urzędzie.

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.

Szkolenie kończy się wydaniem zaświadczenia. Odbierając zaświadczenie, osoba przeszkolona składa pisemne oświadczenie o zapoznaniu się z przepisami o ochronie informacji niejawnych.

X. Wykonywanie dokumentów zawierających informacje niejawne za pomocą komputera – bezpieczeństwo teleinformatyczne

1. Burmistrz udziela akredytacji bezpieczeństwa teleinformatycznego dla systemu teleinformatycznego przeznaczonego do przetwarzania informacji niejawnych o klauzuli „zastrzeżone” przez zatwierdzenie dokumentacji bezpieczeństwa systemu teleinformatycznego.

2. Dokument szczególnych wymagań bezpieczeństwa systemu teleinformatycznego powinien zawierać wyniki procesu szacowania ryzyka dla bezpieczeństwa informacji niejawnych przetwarzanych w systemie teleinformatycznym oraz określać przyjęte w ramach zarządzania ryzykiem sposoby osiągania i utrzymania odpowiedniego poziomu bezpieczeństwa systemu, a także opisywać aspekty jego budowy, zasady działania i eksploatacji, które mają związek z bezpieczeństwem systemu lub wpływają na jego bezpieczeństwo.

3. Kierownik jednostki organizacyjnej wyznacza:

ü pracownika lub pracowników pionu ochrony pełniących funkcję inspektora bezpieczeństwa teleinformatycznego, odpowiedzialnych za weryfikację i bieżącą kontrolę zgodności funkcjonowania systemu teleinformatycznego ze szczególnymi wymaganiami bezpieczeństwa oraz przestrzegania procedur bezpiecznej eksploatacji;

ü osobę lub zespół osób, niepełniących funkcji inspektora bezpieczeństwa teleinformatycznego, odpowiedzialnych za funkcjonowanie systemu teleinformatycznego oraz za przestrzeganie zasad i wymagań bezpieczeństwa przewidzianych dla systemu teleinformatycznego, zwanego „administratorem systemu”

4. Pracownicy, którzy do opracowania i wykonania dokumentów zawierających informacje niejawne o klauzuli „zastrzeżone”, wykorzystują urządzenia komputerowe, zobowiązani 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.

XI. Okresy ochronne dla informacji niejawnych

1. Informacje niejawne podlegają ochronie do czasu zniesienia lub zmiany klauzuli tajności. Osoba, która jest uprawniona do podpisania lub oznaczenia dokumentu albo materiału, może określić datę lub zdarzenie, po których nastąpi zniesienie lub zmiana klauzuli tajności.

2. Kierownik jednostki przeprowadza, nie rzadziej niż raz na 5 lat, przegląd materiałów w celu ustalenia, czy spełniają ustawowe przesłanki ochrony.

3. Po zniesieniu lub zmianie klauzuli tajności podejmuje się czynności polegające na naniesieniu odpowiednich zmian w oznaczeniu materiału i poinformowaniu o nich odbiorców. Odbiorcy materiału którzy przekazali go kolejnym odbiorcom są odpowiedzialni za poinformowanie ich o zniesieniu lub zmianie klauzuli tajności.

4. Odbiorca materiału, w przypadku stwierdzenia zawyżenia lub zaniżenia klauzuli tajności, może zwrócić się do osoby, która ją nadała bądź do przełożonego tej osoby z wnioskiem o dokonanie zmiany.

XII. Nadzór w zakresie ochrony informacji niejawnych

Za ochronę informacji niejawnych w Urzędzie Miejskim odpowiada Burmistrz Myszyńca.

Burmistrzowi bezpośrednio podlega Pełnomocnik ds. ochrony informacji niejawnych w urzędzie, który odpowiada za zapewnienie przestrzegania przepisów o ochronie informacji niejawnych.

XIII. Odpowiedzialność karna, dyscyplinarna i służbowa za naruszenie przepisów o ochronie informacji niejawnych

1. Odpowiedzialności karnej podlega ten tylko, kto popełnił czyn zabroniony pod groźbą kary, przez ustawę obowiązującą w czasie jego popełnienia (art. 1 § 1 K.k.)

2. Zakres odpowiedzialności karnej osób, które dopuściły się przestępstwa lub czynu zabronionego przeciwko ochronie informacji niejawnych został określony przepisami art. 266 § 2 ustawy z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. z 2002 r. Nr 171, poz. 1397)

XIV. Archiwizowanie, gromadzenie i niszczenie informacji niejawnych

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

2. Dokumentacja wytwarzana i gromadzona dzieli się na:

- ü materiały archiwalne – wchodzące do państwowego zasobu archiwalnego,
- ü dokumentację niearchiwalną – inną dokumentację, nie stanowiącą materiałów archiwalnych

3. Rzeczową klasyfikację i kwalifikację dokumentacji ze względu na okres jej przechowywania, wytwarzania i gromadzenia zawiera jednolity rzeczowy wykaz akt.

4. Jednolity rzeczowy wykaz akt stanowi podstawę do gromadzenia dokumentacji w akta sprawy.

5. Dokumentacja niearchiwalna podlega brakowaniu po upływie okresu przechowywania, który jest określony w jednolitym rzeczowym wykazie akt.

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

7. Brakowanie dokumentacji niearchiwalnej następuje na wniosek Burmistrza na podstawie zgody Archiwum Państwowego w Warszawie Oddział w Puławsku.

8. Do wniosku, o zgodę na brakowanie dokumentacji niearchiwalnej, dołącza się:

- ü protokół oceny dokumentacji niejawniej,
- ü spis dokumentacji niejawniej przeznaczonej na makulaturę lub zniszczenie, albo spis dokumentacji technicznej niearchiwalnej przeznaczonej na makulaturę lub zniszczenie, którego wzór stanowi załącznik nr 5 do wyżej cytowanego rozporządzenia.

9. Protokół oraz spis dokumentacji sporządza komisja powołana przez Burmistrza, w której skład wchodzi: Sekretarz, osoba prowadząca archiwum zakładowe, przedstawiciel komórki organizacyjnej, z której dokumentacja niearchiwalna podlega brakowaniu oraz pełnomocnik ochrony.

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

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

12. Uporządkowanie dokumentów niearchiwalnych polega na podziale akt według jednolitego rzeczowego wykazu akt i prawidłowym ułożeniu ich wewnątrz teczek, opisaniu, nadaniu właściwego układu, sporządzeniu ewidencji oraz technicznym zabezpieczeniu.

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

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

- ü nazwy jednostki organizacyjnej i komórki organizacyjnej, w której materiały powstały,
- ü znaku akt, tj. symbolu literowego komórki organizacyjnej oraz symbolu klasyfikacyjnego z jednolitego rzeczowego wykazu akt obowiązującego w danej jednostce organizacyjnej,
- ü tytułu teczki, tj. nazwy hasła klasyfikacyjnego według jednolitego rzeczowego wykazu akt obowiązującego w danej jednostce organizacyjnej, oraz informacji o rodzaju materiałów archiwalnych znajdujących się w teczce,
- ü rocznych dat końcowych, tj. dat najwcześniejszego i najpóźniejszego materiału archiwalnego w teczce,

- ü sygnatury akt, tj. numer spisu zdawczo-odbiorczego łamany przez pozycję tego spisu,
- ü kategorii archiwalną,
- ü liczby stron w teczce

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

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

XV. Przechowywanie pieczęci

Pieczęci, którymi posługuje się Pełnomocnik ds. ochrony informacji niejawnych przechowywane są w meblach biurowych zamykanych na klucz.

XVI. Ustalenia końcowe

1. Pełnomocnik ochrony zapoznaje pracowników z ustaleniami Planu Ochrony Informacji Niejawnych w urzędzie oraz zapewnia przestrzeganie jego postanowień.

2. Pełnomocnik ochrony wprowadza zasadę zapoznania z planem ochrony wszystkie osoby, które podejmują pracę w komórkach organizacyjnych.

3. W przypadku wystąpienia wątpliwości, także potrzeby przybliżenia zasad dotyczących realizacji zadań związanych z ochroną informacji niejawnych, sporządzania i wykonywania dokumentów zawierających informacje niejawne, pracownicy urzędu mogą, w każdym czasie, zwracać się o wyjaśnienia i instruktaż do pełnomocnika ochrony.

4. Integralną część planu stanowią załączniki w ilości 4, wymienione w załączonym do planu ochrony zestawieniu.

Zestawienie załączników do Planu Ochrony Informacji Niejawnych w Urzędzie Miejskim w Myszyńcu **Załącznik nr 1**

Wykaz informacji niejawnych oznaczonych klauzulą „zastrzeżone”

Załącznik nr 2

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

Załącznik nr 3

Wzór wniosku o wydanie upoważnienia do dostępu do informacji niejawnych oznaczonych klauzulą „zastrzeżone” w Urzędzie Miejskim w Myszyńcu

Załącznik nr 4

Wzór upoważnienia dostępu do informacji niejawnych oznaczonych klauzulą „zastrzeżone” w Urzędzie Miejskim w Myszyńcu

Burmistrz Myszyńca

Bogdan Glinka

Wykaz informacji niejawnych oznaczonych klauzulą „zastrzeżone”

Lp.	Rodzaj informacji
1.	Zestawienie zadań w zakresie zabezpieczania potrzeb sił zbrojnych w warunkach zewnętrznego zagrożenia bezpieczeństwa państwa i w czasie wojny
2.	Plan operacyjny funkcjonowania Gminy Myszyniec w warunkach zewnętrznego zagrożenia bezpieczeństwa państwa i w czasie wojny
3.	Dokumentacja dotycząca świadczeń rzeczowych i osobistych przewidzianych do realizacji na terenie Gminy Myszyniec
4.	Wnioski o nadanie medalu za długoletnie pożycie małżeńskie

Burmistrz Myszyńca

Bogdan Glinka

Wykaz stanowisk i funkcji oraz rodzajów prac zleconych, z którymi może łączyć się dostęp do informacji niejawnych oznaczonych klauzulą „zastrzeżone”

Lp.	Stanowisko - Funkcja
1.	Burmistrz Myszyńca
2.	Sekretarz Gminy
3.	Kierownik Urzędu Stanu Cywilnego
4.	Z-ca Kierownika Urzędu Stanu Cywilnego
5.	Skarbnik Gminy
6.	Z-ca Skarbnika Gminy
7.	Stanowisko pracy ds. księgowości budżetowej
8.	Stanowisko pracy ds. płac
9.	Stanowisko pracy ds. księgowości podatkowej
10.	Stanowisko pracy ds. wymiaru podatków i opłat
11.	Kierownik Referatu Inwestycji, Planowania Przestrzennego, Gospodarki Komunalnej
12.	Stanowisko pracy ds. gospodarki komunalnej i ochrony środowiska
13.	Stanowisko pracy ds. gospodarki przestrzennej
14.	Stanowisko pracy ds. gospodarki mieniem komunalnym
15.	Stanowisko pracy ds. inwestycji
16.	Stanowisko pracy ds. inwestycji w ochronie środowiska
17.	Stanowisko pracy ds. drogownictwa
18.	Stanowisko pracy ds. organizacyjnych, kadrowych i obsługi rady
19.	Stanowisko pracy ds. kancelaryjno-technicznych
20.	Stanowisko pracy ds. ewidencji ludności
21.	Stanowisko pracy ds. dowodów osobistych
22.	Stanowisko pracy ds. ewidencji działalności gospodarczej
23.	Stanowisko pracy ds. obronnych, przeciwpożarowych, profilaktyki i uzależnień
24.	Stanowisko pracy ds. pozyskiwania środków, realizacji projektów i współpracy z organizacjami pozarządowymi
25.	Stanowisko pracy ds. oświaty i obsługi przedsiębiorców
26.	Stanowisko pracy ds. społecznych
27.	Informatyk

Burmistrz Myszyńca

Bogdan Glinka

Myszyniec, dn

Urząd Miejski w Myszyńcu

Plac Wolności 60

07-430 Myszyniec

Pełnomocnik

**ds. ochrony informacji niejawnych
w Urzędzie Miejskim w Myszyńcu**

**Wniosek o wydanie upoważnienia
dostępu do informacji niejawnych oznaczonych klauzulą „zastrzeżone”
w Urzędzie Miejskim w Myszyńcu**

Na podstawie art. 21 ust. 4 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228) wnoszę o wydanie upoważnienia do dostępu do informacji niejawnych oznaczonych klauzulą „zastrzeżone” niżej wymienionemu pracownikowi * w związku z realizacją zadania:

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

(wpisać rodzaj zadania)

1.	Imię i nazwisko	
2.	Stanowisko służbowe	
3.	Numer PESEL	
4.	Imię ojca	
5.	Data i miejsce urodzenia	
6.	Adres zamieszkania lub pobytu	

Akceptuję

.....

.....

Pełnomocnik ds. ochrony
Burmistrza)

(podpis i pieczęć

informacji niejawnych

* dane niezbędne w związku z realizacją obowiązku wynikającego z art. 15 ust. 8 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2010 r. Nr 182, poz. 1228)

Burmistrz Myszyńca

Bogdan Glinka

.....

(pieczęć nagłówkowa)

UPOWAŻNIENIE
dostępu do informacji niejawnych oznaczonych klauzulą „zastrzeżone”
w Urzędzie Miejskim w Myszyńcu
Nr

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

Panią/Pana

(imię i nazwisko oraz data urodzenia)

do dostępu do informacji niejawnych oznaczonych klauzulą
„zastrzeżone”

na okres do

Z upoważnienia

Burmistrza Myszyńca

.....

(imienna pieczęć i podpis pełnomocnika ochrony)

Myszyniec, dn

Burmistrz Myszyńca

Bogdan Glinka

Załącznik Nr 2 do Zarządzenia Nr 242/14

Burmistrza Myszyńca

z dnia 20 października 2014 r.

Instrukcja dotycząca sposobu i trybu przetwarzania informacji niejawnych o klauzuli „zastrzeżone” w Urzędzie Miejskim w Myszyńcu oraz zakresu i warunków stosowania środków bezpieczeństwa fizycznego w celu ich ochrony opracowana przez Pełnomocnika ds. Ochrony Informacji Niejawnych

Instrukcja stanowi wewnętrzne uregulowania w odniesieniu do całokształtu zagadnień związanych z informacjami niejawnymi o klauzuli „zastrzeżone” i określa:

1. Wytwarzanie, przetwarzanie, klasyfikowanie i oznaczanie dokumentów niejawnych o klauzuli „zastrzeżone”.
2. Obieg, ewidencję i przechowywanie dokumentacji zawierającej informacje niejawne oznaczone klauzulą „zastrzeżone”.
3. Udostępnianie i ochrona dokumentów niejawnych o klauzuli „zastrzeżone”
4. Niszczenie materiałów zawierających informacje niejawne oznaczone klauzulą „zastrzeżone”

Rozdział 1.

Wytwarzanie, przetwarzanie, klasyfikowanie i oznaczanie dokumentów niejawnych o klauzuli „zastrzeżone”

§ 1.

1. Informacje niejawne mogą być wytwarzane, przetwarzane, przechowywane i udostępniane w warunkach uniemożliwiających ich nieuprawnione ujawnienie (dotyczy to również wersji roboczych dokumentów niejawnych), przy zastosowaniu środków ochrony fizycznej oraz zachowaniu zasad bezpieczeństwa teleinformatycznego.

2. Załatwianie spraw, sporządzanie wersji roboczych oraz wykonywanie czystopisów dokumentów zawierających informacje niejawne o klauzuli „zastrzeżone” odbywa się na wydzielonym stanowisku komputerowym przez uprawnionego pracownika, po uprzednim założeniu dla niego konta dostępu i przeszkoleniu w zakresie zasad pracy na wydzielonym stanowisku komputerowym.

§ 2.

1. Klasyfikowanie informacji niejawnej oznacza przyznanie tej informacji w sposób wyraźny, w pełnym brzmieniu klauzuli zdefiniowanej w ustawie z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228)

2. Klauzula nie może być zmieniona lub zniesiona bez zgody osoby odpowiedzialnej za przyznanie klauzuli tajności lub jej przełożonego.

3. Zawyżanie lub zaniżanie klauzuli tajności jest niedopuszczalne.

4. Sposób oznaczania materiałów niejawnych posiadających klauzulę „zastrzeżone” określa rozporządzenie Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności (Dz. U. Nr 288, poz. 1692)

Rozdział 2.

Obieg, ewidencja i przechowywanie dokumentacji zawierającej informacje niejawne oznaczone klauzulą „zastrzeżone”

§ 3.

1. Przesyłki zawierające informacje niejawne o znaczone klauzulą „zastrzeżone” dostarczane są do sekretariatu urzędu.
2. Przesyłka zawierająca informacje niejawne oznaczone klauzulą „zastrzeżone” powinna być opakowana w dwie koperty lub w dwa opakowania: zewnętrzne i wewnętrzne.
3. Pracownik sekretariatu przyjmujący przesyłkę zawierającą informacje oznaczone klauzulą „zastrzeżone” upoważniony jest tylko do otwarcia koperty lub opakowania zewnętrznego.
4. Po otwarciu przesyłki i stwierdzeniu, że koperta lub opakowanie wewnętrzne jest oznakowane klauzulą „zastrzeżone”, przesyła ją w stanie zamkniętym, wraz z kopertą lub opakowaniem zewnętrznym do Pełnomocnika ds. ochrony informacji niejawnych w urzędzie.
5. Dokumenty zastrzeżone wpływające do urzędu rejestrowane są przez pełnomocnika ochrony w dzienniku korespondencji dla informacji niejawnych o klauzuli „zastrzeżone”. Z chwilą zarejestrowania dokumentu, na każdym z dokumentów, na pieczęcie wpływu, umieszcza się numer ewidencyjny, pod którym dany dokument został zarejestrowany.
6. Następnie pełnomocnik ochrony dokonuje dekretacji na dokumencie i kieruje ten dokument do konkretnego pracownika, do załatwienia.
7. Po dekretacji, pracownik przyjmujący dokument zastrzeżony potwierdza jego odbiór w odpowiedniej rubryce dziennika korespondencji.
8. Pracownik załatwiający sprawę dokonuje na dokumencie adnotacji informującej o sposobie załatwienia sprawy, z jednoczesnym wpisaniem numeru pisma, pod którym odpowiedź, a więc pismo załatwiające sprawę, zarejestrowane zostało w dzienniku korespondencji.
9. Materiały niejawne oznaczone klauzulą „zastrzeżone” opakowane zgodnie z obowiązującymi w tym zakresie przepisami, przyjmuje się i wysyła za pośrednictwem sekretariatu, jako przesyłki polecone, ze zwrotnym potwierdzeniem odbioru.
10. Sposób pakowania, adresowania i przysyłania materiałów zawierających informacje niejawne oznaczone klauzulą „zastrzeżone” określa rozporządzenie Prezesa Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne (Dz. U. z 2011 r. Nr 271, poz. 1603).
11. Obowiązkowej ewidencji podlegają wszystkie dokumenty niejawne zarówno otrzymane jak i wykonane w urzędzie.

Rozdział 3.

Udostępnianie i ochrona dokumentów niejawnych o klauzuli „zastrzeżone”

§ 4.

1. Materiały zawierające informacje niejawne o klauzuli „zastrzeżone” mogą być udostępniane tylko pracownikowi, który posiada poświadczenie bezpieczeństwa osobowego lub pisemne upoważnienie Burmistrza do dostępu do informacji niejawnych o klauzuli „zastrzeżone”.
2. Materiały zawierające informacje niejawne o klauzuli „zastrzeżone” mogą być udostępniane tylko temu pracownikowi, który wskazany został imienną dekretacją pełnomocnika ochrony.
3. W przypadku, kiedy zaistnieje uzasadniona potrzeba zapoznania z treścią dokumentu pracownika, który nie został wskazany imienną dekretacją, wymagane jest rozszerzenie pierwotnej dekretacji dokonanej na dokumencie.

4. Każdy pracownik, który zapoznał się z treścią dokumentu zastrzeżonego, dokonuje stosownej adnotacji i stwierdza ten fakt bezpośrednio na tym dokumencie.

§ 5.

1. Materiały zawierające informacje niejawne o klauzuli „zastrzeżone”, po załatwieniu spraw, wymagają gromadzenia w teczkach oraz oznaczenia symbolami zgodnie z jednolitym rzeczowym wykazem akt.

2. Materiały zawierające informacje niejawne o klauzuli „zastrzeżone”, gromadzone przez pracowników upoważnionych do dostępu do informacji niejawnych, podlegają codziennemu zabezpieczeniu na stanowiskach pracy, w meblach biurowych zamykanych na klucz.

3. Informacje niejawne podlegają ochronie w sposób określony w ustawie o ochronie informacji niejawnych. Osoba, która nadaje klauzulę tajności może określić datę lub wydarzenie, po którym nastąpi zniesienie lub zmiana klauzuli tajności. Po upływie tego okresu materiały zawierające informacje „zastrzeżone” mogą być przekazywane do Archiwum Zakładowego.

4. Po zniesieniu lub zmianie klauzuli tajności podejmuje się czynności polegające na naniesieniu odpowiednich zmian w oznaczeniu materiału i poinformowaniu o nich odbiorców. Odbiorcy materiału, którzy przekazali go kolejnym odbiorcom są odpowiedzialni za poinformowanie ich o zniesieniu lub zmianie klauzuli tajności.

Rozdział 4.

Niszczenie materiałów zawierających informacje niejawne oznaczone klauzulą „zastrzeżone”

§ 6.

1. Niszczenie wydruków próbnych czystopisów odbywa się przez pocięcie w niszczarce w sposób uniemożliwiający odtworzenie ich treści.

2. Materiały niejawne oznaczone klauzulą „zastrzeżone”, które utraciły praktyczne znaczenie i dla których minął okres przechowywania, winny być niszczone, po uprzedniej zgodzie Archiwum Państwowego w Pułtusk, w obecności dwóch pracowników spełniających wymogi opisane w § 4, w niszczarce, w sposób uniemożliwiający odtworzenie ich treści. Fakt zniszczenia należy odnotować w dzienniku ewidencyjnym.

3. Informacje niejawne oznaczone klauzulą „zastrzeżone” zapisane w formie elektronicznej niszczy się przez fizyczne zniszczenie nośnika.

Burmistrz Myszyńca

Bogdan Glinka