

Zarządzenie Nr 83/21
Burmistrza Miasta Jędrzejowa
z dnia 03 marca 2021r.

w sprawie wprowadzenia Planu Ochrony Informacji Niejawnych w Urzędzie Miejskim w
Jędrzejowie

Na podstawie art. 18 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U.2019 poz.742) i przepisów wykonawczych:

- Rozporządzenie Prezesa Rady Ministrów z dnia 7 grudnia 2017 r. 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. 2017 poz. 2334),
- Rozporządzenie Prezesa Rady Ministrów z dnia 9 lipca 2020 r. w sprawie wzorów zaświadczeń stwierdzających odbycie szkolenia w zakresie ochrony informacji niejawnych oraz sposobu rozliczania kosztów przeprowadzenia szkolenia przez Agencję Bezpieczeństwa Wewnętrznego lub Służbę Kontrwywiadu Wojskowego (Dz.U. 2020 poz. 1256),
- Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie wzorów poświadczeń bezpieczeństwa (Dz.U.2015.220 t.j.),
- Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie wzoru decyzji o odmowie wydania poświadczenia bezpieczeństwa (Dz.U. 2010 nr 258 poz. 1753),
- Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie wzoru decyzji o cofnięciu poświadczenia bezpieczeństwa (Dz.U. 2010 nr 258 poz. 1754),
- Rozporządzenie Rady Ministrów z dnia 16 maja 2019 r. w sprawie wzorów kwestionariusza bezpieczeństwa przemysłowego, świadectwa bezpieczeństwa przemysłowego, decyzji o odmowie wydania świadectwa bezpieczeństwa przemysłowego oraz decyzji o cofnięciu świadectwa bezpieczeństwa przemysłowego (Dz. U. 2019 poz. 1103),
- Rozporządzenie Prezesa Rady Ministrów z dnia 27 kwietnia 2011 r. w sprawie przygotowania i przeprowadzania kontroli stanu zabezpieczenia informacji niejawnych (Dz.U. 2011 nr 93 poz. 541),
- Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie wzoru świadectwa akredytacji bezpieczeństwa systemu teleinformatycznego (Dz.U. 2011 nr 156 poz. 926),
- Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz.U. 2011 nr 159 poz. 948),
- Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie opłat za przeprowadzenie przez Agencję Bezpieczeństwa Wewnętrznego albo Służbę Kontrwywiadu Wojskowego czynności z zakresu bezpieczeństwa teleinformatycznego (Dz.U. 2011 nr 159 poz. 949),
- Rozporządzenie Prezesa Rady Ministrów z dnia 4 października 2011 r. w sprawie współdziałania Szefa Agencji Bezpieczeństwa Wewnętrznego i Szefa Służby Kontrwywiadu Wojskowego w zakresie wykonywania funkcji krajowej władzy bezpieczeństwa (Dz.U. 2011 nr 220 poz. 1302),
- Rozporządzenie Prezesa Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne (Dz.U. 2011 nr 271 poz. 1603),

- Rozporządzenie Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych (Dz.U. 2011 nr 276 poz. 1631 t.j.),
 - Rozporządzenie Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności (Dz.U. 2011 nr 288 poz. 1692),
 - Rozporządzenie Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych (Dz.U. 2012 poz. 683) oraz art. 33 ust. 2 ustawy z dnia 08 czerwca 1990r. o samorządzie gminy (Dz.U. 2020.713 t.j.)
- zarządzam co następuje:

§ 1.

W celu zapewnienia ochrony informacji niejawnych oraz przestrzegania przepisów o ochronie informacji niejawnych, wprowadzam do użytku służbowego Plan Ochrony Informacji Niejawnych w Urzędzie Miejskim w Jędrzejowie wraz z załącznikami, stanowiący załącznik do niniejszego zarządzenia.

§ 2.

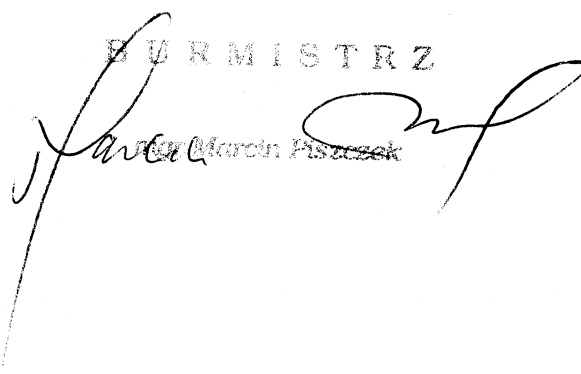
Wykonanie zarządzenia powierzam Pełnomocnikowi ds. Ochrony Informacji Niejawnych w Urzędzie Miejskim w Jędrzejowie.

§ 3.

Traci moc Zarządzenie Nr 9/08 Burmistrza Miasta Jędrzejowa z dnia 01 lutego 2008r. w sprawie wprowadzenia Planu Ochrony Informacji Niejawnych w Urzędzie Miejskim w Jędrzejowie z późniejszymi zmianami.

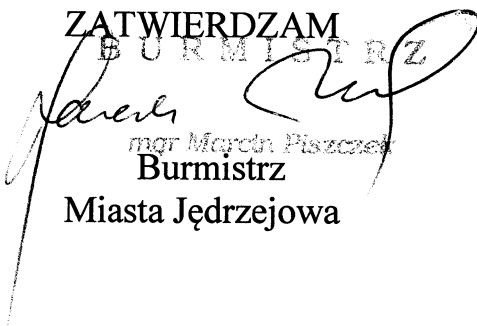
§ 4.

Zarządzenie wchodzi w życie po upływie 2 tygodni od podania go do wiadomości pracownikom.

BURMISTRZ

Marcin Piśczek

ZATWIERDZAM

BURMISTRZ


mgr Marek Piszczek

Burmistrz
Miasta Jędrzejowa

PLAN OCHRONY INFORMACJI NIEJAWNYCH W URZĘDZIE MIEJSKIM W JĘDRZEJOWIE

OPRACOWAŁ:
Wojciech Hatys
Pełnomocnik ds. Ochrony
Informacji Niejawnych

Jędrzejów marzec 2021r.



SPIS TREŚCI

I. Postanowienia ogólne	2
II. Akty prawne związane z ochroną informacji niejawnych	2
III. Określenie poziomu zagrożeń	4
IV. Przedmiot ochrony	11
V. Ewidencja informacji niejawnych	11
VI. Strefy ochronne	11
VII Kancelaria Materiałów Niejawnych	12
VIII. Postępowanie z przesyłkami	13
IX. Zakres udostępniania informacji niejawnych	14
X. Wykonywanie dokumentów niejawnych z wykorzystaniem sprzętu komputerowego	14
XI. Gromadzenie dokumentów zawierających informacje niejawne	16
XII. Oznaczenie, nadawanie, zmiana i znoszenie klauzuli niejawności materiałom niejawnym	16
XIII. Nadzór w zakresie ochrony informacji niejawnych	18
XIV. Odpowiedzialność karna za naruszenie przepisów o ochronie informacji niejawnych	18
XV. Archiwizowanie, gromadzenie i niszczenie materiałów niejawnych	20
XVI. Przechowywanie kluczy i pieczęci	21
XVII. Plany awaryjne uwzględniające potrzebę ochrony informacji niejawnych w razie wystąpienia sytuacji szczególnych, w tym wprowadzenia stanów nadzwyczajnych, w celu zapobieżenia utracie poufności, integralności lub dostępności informacji niejawnych	21
XVIII. Ustalenia końcowe	22
XIX. Zestawienie załączników do Planu Ochrony Informacji Niejawnych w Urzędzie Miejskim w Jędrzejowie	24

I. POSTANOWIENIA OGÓLNE

1. Plan ochrony informacji niejawnych w Urzędzie Miejskim w Jędrzejowie określa zasady i tryb postępowania z informacjami niejawnymi oraz zapewnia jednolity sposób postępowania z tymi informacjami.
2. Plan ochrony informacji niejawnych opracowany został na podstawie art. 15 ust.1 pkt 5 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. 2019 poz.742) oraz zawiera wymagane elementy, o których mowa w § 9 ust.1 i 2 rozporządzenia Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (Dz. U. poz. 683).
3. Definicje użyte w Planie ochrony informacji niejawnych:
 - 1) Ustawa - ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U.2019.0.742 t.j.);
 - 2) **Urząd** – Urząd Miejski w Jędrzejowie;
 - 3) **Burmistrz** – Burmistrz Miasta Jędrzejowa;
 - 4) **Sekretarz** – Sekretarz Gminy;
 - 5) **KMN** – Kancelaria Materiałów Niejawnych;
 - 6) **Kierownik** – Kierownik Kancelarii Materiałów Niejawnych;
 - 7) **Pełnomocnik Ochrony** - Pełnomocnik ds. Ochrony Informacji Niejawnych;
 - 8) **Plan OIN** - Plan Ochrony Informacji Niejawnych w Urzędzie Miejskim w Jędrzejowie

II. AKTY PRAWNE ZWIĄZANE Z OCHRONĄ INFORMACJI NIEJAWNYCH

1. Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U.2019 poz.742)
2. **Rozporządzenie** Prezesa Rady Ministrów z dnia 7 grudnia 2017 r. 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. 2017 poz. 2334)
3. **Rozporządzenie** Prezesa Rady Ministrów z dnia 9 lipca 2020 r. w sprawie wzorów zaświadczeń stwierdzających odbycie szkolenia w zakresie ochrony informacji niejawnych oraz sposobu rozliczania kosztów przeprowadzenia szkolenia przez Agencję Bezpieczeństwa Wewnętrznego lub Służbę Kontrwywiadu Wojskowego (Dz.U. 2020 poz. 1256)
4. **Rozporządzenie** Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie wzorów poświadczeń bezpieczeństwa (Dz.U.2015.220 t.j.)
5. **Rozporządzenie** Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie wzoru decyzji o odmowie wydania poświadczenia bezpieczeństwa (Dz.U. 2010 nr 258 poz. 1753)
6. **Rozporządzenie** Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie wzoru decyzji o cofnięciu poświadczenia bezpieczeństwa (Dz.U. 2010 nr 258 poz. 1754)
7. **Rozporządzenie** Rady Ministrów z dnia 16 maja 2019 r. w sprawie wzorów kwestionariusza bezpieczeństwa przemysłowego, świadectwa bezpieczeństwa przemysłowego, decyzji o odmowie wydania świadectwa bezpieczeństwa przemysłowego oraz decyzji o cofnięciu świadectwa bezpieczeństwa przemysłowego (Dz. U. 2019 poz. 1103)
8. **Rozporządzenie** Prezesa Rady Ministrów z dnia 27 kwietnia 2011 r. w sprawie przygotowania i przeprowadzania kontroli stanu zabezpieczenia informacji niejawnych (Dz.U. 2011 nr 93 poz. 541)
9. **Rozporządzenie** Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie wzoru świadectwa akredytacji bezpieczeństwa systemu teleinformatycznego (Dz.U. 2011 nr 156 poz. 926)

10. **Rozporządzenie** Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz.U. 2011 nr 159 poz. 948)
11. **Rozporządzenie** Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie opłat za przeprowadzenie przez Agencję Bezpieczeństwa Wewnętrznego albo Służbę Kontrwywiadu Wojskowego czynności z zakresu bezpieczeństwa teleinformatycznego (Dz.U. 2011 nr 159 poz. 949)
12. **Rozporządzenie** Prezesa Rady Ministrów z dnia 4 października 2011 r. w sprawie współdziałania Szefa Agencji Bezpieczeństwa Wewnętrznego i Szefa Służby Kontrwywiadu Wojskowego w zakresie wykonywania funkcji krajowej władzy bezpieczeństwa (Dz.U. 2011 nr 220 poz. 1302)
13. **Rozporządzenie** Prezesa Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne (Dz.U. 2011 nr 271 poz. 1603)
14. **Rozporządzenie** Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych (Dz.U. 2011 nr 276 poz. 1631t.j.)
15. **Rozporządzenie** Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności (Dz.U. 2011 nr 288 poz. 1692)
16. **Rozporządzenie** Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych (Dz.U. 2012 poz. 683)

III. OKREŚLENIE POZIOMU ZAGROŻEŃ

1. Określenie poziomu zagrożeń w Urzędzie Miejskim w Jędrzejowie

Niski	Średni	Wysoki
7-16	17-32	Powyżej

Lp.	CZYNNIK	OCENA ISTOTNOŚCI CZYNNIKA			UZASADNIENIE
		BARDZO ISTOTNY (8pkt)	ISTOTNY (4 pkt)	MAŁO ISTOTNY (1pkt)	
1	2	3	4	5	6
1	Klauzula tajności przetwarzanych informacji niejawnych			X	W Urzędzie w Jędrzejowie występuje tylko jedna klauzula tajności przetwarzanych informacji niejawnych. Są to informacje niejawne oznaczone klauzulą „zastrzeżone”. Należy przyjąć, że czynnik ten jest mało istotny.
2	Liczba materiałów niejawnych			X	Rocznie w Urzędzie przetwarza się około 167000 szt. wszystkich dokumentów. Natomiast dokumentów niejawnych o klauzuli „zastrzeżone” przetwarzanych jest 5 szt. Stanowi to 0,00003% przetwarzanych materiałów. Należy przyjąć, że czynnik ten jest mało istotny.
3	Postać informacji niejawnych				W Urzędzie dokumenty niejawne nie są przetwarzane w systemie teleinformatycznym. należy przyjąć, że czynnik ten jest mało istotny
4	Liczba osób			X	W Urzędzie Miejskim zatrudnionych jest 75 osób. Natomiast przetwarzaniem dokumentów niejawnych zajmuje się 10 osób. Stanowi to 7,5% zatrudnionych osób. Należy przyjąć, że czynnik ten jest mało istotny.
5	Lokalizacja		X		Pomieszczenie Kancelarii Materiałów Niejawnych gdzie przechowywane są dokumenty niejawne, usytuowane jest w

					budynku Miejsko-Gminnej Biblioteki Publicznej, na pierwszym piętrze. Budynek biblioteki usytuowany jest w sąsiedztwie budynku Urzędu Miejskiego. Na działce, na której usytuowane są te budynki, usytuowane są również dwa budynki bloków mieszkalnych i ogólnodostępny parking samochodowy. Całą działka jest ogrodzona lecz ogólnie dostępna. W bezpośrednim sąsiedztwie znajduje się budynek szkolny wraz z halą sportową.
6	Dostęp osób do budynków		X		Budynek Urzędu Miejskiego i budynek biblioteki są obiektami publicznymi. Wewnątrz budynków mogą swobodnie się poruszać osoby nie będące pracownikami (interesanci)
7	Inne czynniki			X	Należy przyjąć, że wystąpienie czynników typu działania obcych służb specjalnych, sabotaż, zamach, terrorystyczny, kradzież, pożar, działania sił przyrody jest mało prawdopodobne i tym samym czynnik ten jest mało istotny
Suma punktów		13			

2. Dobór środków bezpieczeństwa dla pokoju nr 7b - znajdującego się w budynku Urzędu Miejskiego

Środek bezpieczeństwa	Punktacja
Kategoria K1: szafy do przechowywania informacji niejawnych	
Środek bezpieczeństwa K1S1 – konstrukcja szafy	
Szafa typ 1 charakteryzuje się następującymi cechami: Szafa metalowa, z dwoma ryglami, zamykana na klucz ale charakteryzuje się umiarkowaną odpornością na nieuprawnione próby otwarcia. jest zabezpieczona zamkiem typu 1.	1
Środek bezpieczeństwa K1S2 – zamek do szafy	
Zamek typu 1 charakteryzuje się umiarkowaną odpornością na nieuprawnione próby otwarcia i może być wykorzystywany wyłącznie w szafach typu 1.	1
Liczba punktów za kategorię K1 stanowiąca iloczyn liczby punktów za oba powyższe środki bezpieczeństwa ($K1 = K1S1 \times K1S2$)	1
Kategoria K2: Pomieszczenia	
Środek bezpieczeństwa K2S1 – konstrukcja pomieszczenia	
Konstrukcja pomieszczenia charakteryzuje się następującymi cechami: Jest to pokój biurowy wykonany z cegły lekkiej. Drzwi z zewnątrz obite blachą, spełniają wymagania klasy 1 określone w Polskiej Normie PN-EN1627. Drzwi po zamknięciu są plombowane. Po przeciągnięciu sznurka, który przymocowany jest do futryny drzwi, przykleja się na nim plastelinę i wykonuje w niej odcisk pieczęci (referentki). Okno w pokoju posiada kraty metalowe, co spełnia wymagania klasy 1 określonej w Polskiej Normie PN-NE1627	1
Środek bezpieczeństwa K2S2 – zamek do drzwi pomieszczenia	
Zamek do drzwi typu łucznik spełniający wymagania klasy 3 określone w Polskiej Normie PN-NE12209	1
Liczba punktów za kategorię K2 stanowiąca iloczyn liczby punktów za oba powyższe środki bezpieczeństwa ($K2 = K2S1 \times K2S2$)	1
Kategoria K3: Budynki	
Budynek jest lekką konstrukcją przeznaczony do ochrony zawartości i osób znajdujących się wewnątrz, tylko przed działaniami czynników zewnętrznych	1
Kategoria K4: Kontrola dostępu	
Środek bezpieczeństwa K4S1 – system kontroli dostępu	
System kontroli dostępu oparty na zamkniętych drzwiach pokoju, do którego można uzyskać dostęp za pomocą kluczy wydanych uprawnionym osobom. (Procedury dostępu do kluczy, określony są Zarządzeniem Nr 15 Burmistrza Miasta Jędrzejowa z dn. 22 stycznia 2015r.)	1
Środek bezpieczeństwa K4S2 – kontrola osób nieposiadających stałego upoważnienia (interesantów) do wejścia na obszar jednostki organizacyjnej	
Interesanci mogą swobodnie wchodzić do budynku Urzędu i nie podlegają żadnej kontroli wejścia i wyjścia.	0
Liczba punktów za kategorię K4 stanowiąca iloczyn liczby punktów za oba powyższe środki bezpieczeństwa ($K4 = K4S1 \times K4S2$)	1

Środek bezpieczeństwa	Punktacja
Kategoria K5: Personel bezpieczeństwa i systemy sygnalizacji napadu i włamania	
Środek bezpieczeństwa K5S1 – personel bezpieczeństwa	
W budynku urzędu nie występuje personel bezpieczeństwa, który dozorował by budynek Urzędu i teren wokół w godzinach nocnych	0
Środek bezpieczeństwa K5S2 – systemy sygnalizacji napadu i włamania	
System sygnalizacji napadu i włamania charakteryzuje się następującymi cechami: Jest to centrala alarmowa CA-64 i obejmuje między innymi ochronę wejścia do budynku Urzędu, sygnalizuje poruszanie się w chronionym obszarze. Dodatkowo łączem telefonicznym powiadamiany jest oficer dyżurny Policji o włamaniu do budynku Urzędu.	1
Liczba punktów za kategorię K5 stanowiąca sumę liczby punktów za oba powyższe środki bezpieczeństwa ($K5 = K5S1 + K5S2$)	1
Kategoria K6: Granice	
Środek bezpieczeństwa K6S1 – ogrodzenie	
Brak ogrodzenia, które w minimalny sposób zabezpieczało by teren przed jakimiś osobami. Teren przed budynkiem Urzędu jest ogólnie dostępny.	0
Środek bezpieczeństwa K6S2 – kontrola w punktach dostępu	
Brak kontroli w punktach dostępu	0
Środek bezpieczeństwa K6S3 – system kontroli osób i przedmiotów przy wejściu/wyjściu	
Brak kontroli systemu osób i przedmiotów przy wejściu/wyjściu	0
Środek bezpieczeństwa K6S4 – system wykrywania naruszenia ogrodzenia	
Brak kontroli systemu wykrywania naruszenia ogrodzenia	0
Środek bezpieczeństwa K6S5 – oświetlenie chronionego obszaru	
Teren przed wejściem do budynku Urzędu, jest oświetlony trzema lampami, co może stanowić czynnik odstrasżający potencjalnych intruzów	1
Środek bezpieczeństwa K6S6 – system dozoru wizyjnego	
System dozoru wizyjnego (monitoring), jest to system składający się z dwóch kamer i rejestratora IPOX PX-NVR1682H. Jedna z kamer umieszczona jest na ścianie frontowej, przed wejściem do budynku Urzędu, a druga na parterze budynku, na korytarzu. Pierwsza kamera IPOX PX-DIP2026-P/W rejestruje osoby przebywające przed budynkiem i wchodzące do budynku, natomiast druga kamera IPOX PX-T2IP20386-E rejestruje osoby, które weszły do budynku Urzędu	1
Liczba punktów za kategorię K6 stanowiąca sumę liczby punktów za powyższe środki bezpieczeństwa ($K6 = K6S1 + K6S2 + K6S3 + K6S4 + K6S5 + K6S6$)	2
Ogólna liczba punktów stanowiąca sumę wszystkich punktów za wszystkie kategorie: PUNKTY K1 + K2 + K3 + K4 + K6	7

3. *Dobór środków bezpieczeństwa dla kancelarii materiałów niejawnymieszczącej się w budynku Biblioteki Miejsko-Gminnej*

Środek bezpieczeństwa	Punktacja
Kategoria K1: szafy do przechowywania informacji niejawnych	
Środek bezpieczeństwa K1S1 – konstrukcja szafy	
Szafa typ 2, spełnia co najmniej wymagania klasy odporności na włamanie S1, określone w Polskiej Normie PN-NE 14450, jest zabezpieczona zamkiem typu 2 z kategorii K1S2	2
Środek bezpieczeństwa K1S2 – zamek do szafy	
Zamek typu 2 charakteryzuje się odpornością na sprawne działania osoby nieuprawnionej, posługującej się zwykłymi, powszechnie dostępnymi środkami. Zamek spełnia co najmniej wymagania Klasy A, określone w Polskiej Normie PN-EN 1300	2
Liczba punktów za kategorię K1 stanowiąca iloczyn liczby punktów za oba powyższe środki bezpieczeństwa ($K1 = K1S1 \times K1S2$)	4
Kategoria K2: Pomieszczenia	
Środek bezpieczeństwa K2S1 – konstrukcja pomieszczenia	
Konstrukcja pomieszczenia charakteryzuje się następującymi cechami: Jest to pokój biurowy wykonany z cegły lekkiej. Drzwi o zwiększonej odporności na włamanie określone w Polskiej Normie PN-EN1627. Drzwi po zamknięciu są plombowane. Po przeciągnięciu sznurka, który przymocowany jest do futryny drzwi, przykleja się na nim plastelinę i wykonuje w niej odcisk pieczęci (referentki). Okno w kancelarii zasłonięte rolokasetą i spełnia wymagania Klasy 1 określonej w Polskiej Normie PN-NE 1627	2
Środek bezpieczeństwa K2S2 – zamek do drzwi pomieszczenia	
Zamek wysokiego bezpieczeństwa, szyfrowy, tarczowy	2
Liczba punktów za kategorię K2 stanowiąca iloczyn liczby punktów za oba powyższe środki bezpieczeństwa ($K2 = K2S1 \times K2S2$)	4
Kategoria K3: Budynki	
Budynek jest lekką konstrukcją przeznaczony do ochrony zawartości i osób znajdujących się wewnątrz, tylko przed działaniami czynników zewnętrznych	1
Kategoria K4: Kontrola dostępu	
Środek bezpieczeństwa K4S1 – system kontroli dostępu	
System kontroli dostępu oparty na zamkniętych drzwiach pokoju, do którego można uzyskać dostęp za pomocą kluczy wydanych uprawnionym osobom. (Procedury dostępu do kluczy, określony są w planie ochrony informacji niejawnych)	1
Środek bezpieczeństwa K4S2 – kontrola osób wchodzących i przebywających w Kancelarii Materiałów niejawnych	
W kancelarii może przebywać kierownik kancelarii. Znajduje się w niej wydzielone miejsce (czytelnia), w której osoba upoważniona, w obecności kierownika kancelarii, może zapoznać się z dokumentami. Każdorazowe przebywanie osób w kancelarii odnotowywane jest w „rejestrze osób przebywających w kancelarii”.	1
Liczba punktów za kategorię K4 stanowiąca iloczyn liczby punktów za oba powyższe środki bezpieczeństwa ($K4 = K4S1 + K4S2$)	2

Środek bezpieczeństwa	Punktacja
<i>Kategoria K5: Personel bezpieczeństwa i systemy sygnalizacji napadu i włamania</i>	
Środek bezpieczeństwa K5S1 – personel bezpieczeństwa	
W budynku, w którym znajduje się KMN, nie występuje personel bezpieczeństwa, który dozorował by budynek urzędu i teren wokół w godzinach nocnych	0
Środek bezpieczeństwa K5S2 – systemy sygnalizacji napadu i włamania	
System sygnalizacji napadu i włamania charakteryzuje się następującymi cechami: Jest to centrala alarmowa SATEL i obejmuje ochronę wejścia do kancelarii, sygnalizuje poruszanie się w chronionym obszarze.	1
Liczba punktów za kategorię K5 stanowiąca sumę liczby punktów za oba powyższe środki bezpieczeństwa (K5 = K5S1 + K5S2)	1
<i>Kategoria K6: Granice</i>	
Środek bezpieczeństwa K6S1 – ogrodzenie	
Brak ogrodzenia, które w minimalny sposób zabezpieczało by teren przed jakimikolwiek osobami. Teren przed budynkiem Biblioteki Miejsko-Gminnej, w której znajduje się KMN, jest ogólnie dostępny.	0
Środek bezpieczeństwa K6S2 – kontrola w punktach dostępu	
Każdorazowe przebywanie osób w kancelarii odnotowywane jest w „rejestrze osób przebywających w kancelarii”.	1
Środek bezpieczeństwa K6S3 – system kontroli osób i przedmiotów przy wejściu/wyjściu	
Każdorazowe przebywanie osób w kancelarii odnotowywane jest w „rejestrze osób przebywających w kancelarii”.	1
Środek bezpieczeństwa K6S4 – system wykrywania naruszenia ogrodzenia	
Brak kontroli systemu wykrywania naruszenia ogrodzenia	0
Środek bezpieczeństwa K6S5 – oświetlenie chronionego obszaru	
Teren przed wejściem do budynku, w którym znajduje się kancelaria, jest oświetlony lampą ledową, co może stanowić czynnik odstrasżający potencjalnych intruzów	1
Środek bezpieczeństwa K6S6 – system dozoru wizyjnego	
Budynek, w którym znajduje się KMN, nie jest wyposażony w systemu dozoru wizyjnego (monitoring). Jednak kamera, która umieszczona jest na frontowej ścianie budynku Urzędu Miejskiego, w polu swojej obserwacji, obejmuje wejście do budynku biblioteki i rejestruje osoby wchodzące i wychodzące z tego budynku.	1
Liczba punktów za kategorię K6 stanowiąca sumę liczby punktów za powyższe środki bezpieczeństwa (K6 = K6S1 + K6S2 + K6S3 + K6S4 + K6S5 + K6S6)	4
Ogólna liczba punktów stanowiąca sumę wszystkich punktów za wszystkie kategorie: PUNKTY K1 + K2 + K3 + K4 + K5 + K6	16

Uzyskana wartość punktacji w kategoriach K1 + K2 + K3 oraz w kategoriach K4 + K5 + K6 dla poziomu zagrożeń w stopniu niskim wyniosła 16 pkt (minimum 2 pkt), co oznacza, że dobrane przez Pełnomocnika Ochrony środki zabezpieczeń fizycznych aż nadto są wystarczające do osiągnięcia minimalnego założonego poziomu ochrony informacji niejawnych o najwyższej w jednostce organizacyjnej klauzuli tajności „zastrzeżone”.

4. Ocena zagrożeń zewnętrznych i wewnętrznych

1. Zagrożenia zewnętrzne:

- 1) możliwość napadu przez zorganizowane grupy przestępcze i terrorystyczne, działające w sposób profesjonalny i zorganizowany;
- 2) możliwość napadu przez pojedynczych przestępców, możliwość napadu przez przypadkowe osoby wykorzystujące nadarzającą się okazję z powodu nieprawidłowości w ochronie mienia Urzędu;
- 3) Symptomy mogące świadczyć o przygotowaniu napadu lub włamania do budynku Urzędu:
 - a) wzmożone zainteresowanie osób postronnych obiektem, pomieszczeniami Urzędu,
 - b) podejmowanie prób uzyskania informacji o danym obiekcie, pomieszczeniu od pracowników podczas luźnych rozmów po „przypadkowym” spotkaniu,
 - c) nawiązanie rozmów przez osoby postronne z pracownikami,
 - d) podszywanie się pod byłych pracowników Urzędu i przejawianie zainteresowaniem tym co się po latach zmieniło,
 - e) interesowanie się osobami funkcyjnymi, w tym także ich przywarami oraz sposobem wykonywania obowiązków służbowych,
 - f) obserwacja sposobu działania systemu ochronnego, pracy sprzątaczk i itp.,
 - g) rozpoznawanie systemu technicznych zabezpieczeń, w tym stosowanych urządzeń alarmowych,
- 4) celowe uszkodzanie linii telefonicznych, oświetlenia itp.;
- 5) próby pozyskania do grup przestępczych pracowników Urzędu (dotyczy głównie osób mających problemy finansowe, towarzyskie, a także służbowe).

2. Wnioski:

W związku z przedstawionymi kierunkami zagrożeń zewnętrznych należy wykonywać następujące czynności:

- 1) systematyczną, skrupulatną i wnikliwą kontrolę systemu ochrony przez osoby odpowiedzialne za jego organizację;
- 2) pracownicy w czasie dnia pracy powinni zwracać szczególną uwagę na możliwość zaistnienia ewentualnych zagrożeń;
- 3) stosować zasadę niedopuszczania osób niepowołanych do przebywania w pomieszczeniu do przetwarzania informacji niejawnych o klauzuli „Zastrzeżone”;
- 4) wykonywać prace porządkowe, remontowe itp. w pomieszczeniu do przetwarzania informacji niejawnych o klauzuli „Zastrzeżone” wyłącznie pod nadzorem wyznaczonego pracownika.

3. Zagrożenia wewnętrzne:

- 1) próby zaboru dokumentów lub mienia przez pracowników Urzędu;
- 2) próby powielania, kserowania dokumentów służbowych dla celów prywatnych;
- 3) rozpoznanie organizacji pracy Urzędu celem łatwiejszej pracy grup przestępczych na terenie Urzędu;
- 4) próby wglądu w dokumenty niejawne przez osoby nieuprawnione;
- 5) spożywanie alkoholu – przesłanka do wykroczeń dyscyplinarnych i przestępstw.

4. Wnioski:

W związku z przedstawionymi kierunkami zagrożeń należy:

- 1) zwracać szczególną uwagę na osoby, które mogą być zainteresowane dokumentami;
- 2) prowadzić nadzór nad wykonywaniem kopii dokumentów;
- 3) uwrażliwić pracowników w trakcie prowadzonych szkoleń na możliwość prób kontaktu grup przestępczych z pracownikami, którzy mają dostęp do dokumentów szczególnie ważnych;
- 4) bezwzględnie stosować zasady, że do informacji niejawnych mogą mieć dostęp tylko pracownicy posiadający poświadczenie bezpieczeństwa lub właściwe upoważnienie wydane przez Burmistrza;
- 5) zwracać szczególną uwagę na osoby, których zachowanie wskazuje na spożywanie alkoholu

IV. PRZEDMIOT OCHRONY

1. Informacje niejawne oznaczone klauzulą „Zastrzeżone”.
2. Pomieszczenia, w których są opracowywane i przechowywane materiały niejawne.

V. EWIDENCJA INFORMACJI NIEJAWNYCH

1. Dokumenty niejawne są ewidencjonowane na zasadach określonych przez Burmistrza, opisane w Planie OIN.
2. Ewidencjonowaniu podlegają wszystkie dokumenty oznaczone klauzulą „Zastrzeżone”.
3. Dokumenty niejawne wytworzone i wpływające do Urzędu, ewidencjonowane są w „Dzienniku ewidencji”.
4. Każdy dokument niejawny przychodzący lub wychodzący z Urzędu, ewidencjonuje się w odrębnej pozycji dziennika ewidencji.
5. Numer ewidencyjny każdego dokumentu opracowanego w Urzędzie, stanowiącego o klauzuli „Zastrzeżone” powinien być poprzedzony skrótem literowym „Z” (duże zet).
6. Sposób właściwego opisanie dokumentu niejawnego, został przedstawiony w Planie OIN.
7. Prowadzi się również „Rejestr dzienników”, służący do ewidencjonowania ksiązek, dzienników ewidencyjnych i rejestrów.

VI. STREFY OCHRONNE

1. Opis pierwszej strefy ochronnej, zwanej dalej „Strefą administracyjną”.
Pierwsza strefa ochronna, zwana na potrzeby niniejszego plany strefą administracyjną, obejmuje pokój nr 7b, który znajduje się na parterze budynku Urzędu. W pokoju tym są wytwarzane, przetwarzane i przechowywane dokumenty niejawne oznaczone klauzulą „Zastrzeżone”. Dostęp do pokoju mają tylko pracownicy Urzędu, posiadający poświadczenie bezpieczeństwa, lub upoważnienie do dostępu do informacji niejawnych. W pokoju mogą przebywać osoby nie posiadające poświadczenia lub upoważnienia do dostępu do informacji niejawnych (sprzątaczką) ale tylko w obecności osoby stale w nim pracującej. Osoba przebywająca w strefie administracyjnej powinna być wpisana w „Książkę przebywania osób w strefie”.
2. Opis drugiej strefy ochronnej, zwanej „Strefą bezpieczeństwa”.
Druga strefa, obejmuje wydzieloną część budynku, zabezpieczoną przed dostępem osób nieuprawnionych, poprzez kontrolę wejścia i wyjścia oraz kontrolę przebywania.

W strefie tej znajduje się KMN. Dostęp do tej strefy posiadają wyłącznie pracownicy pionu ochrony (Pełnomocnik Ochrony, Kierownik oraz Burmistrz).

Natomiast w uzasadnionym pełnieniu obowiązków służbowych okolicznościach, w strefie tej mogą przebywać osoby (goście);

- posiadający stosowne upoważnienie oraz poświadczenie bezpieczeństwa i zaświadczenie o szkoleniu na temat ochrony informacji niejawnych kontrolerzy badający funkcjonowanie ochrony informacji niejawnych,
- posiadający poświadczenie bezpieczeństwa oraz stosowne upoważnienie od kierownika jednostki organizacyjnej pracownicy, mający wykonać czynności zlecone. Kontrolę ewidencjonowania i przebywania gości w strefie bezpieczeństwa, prowadzi wprowadzający gości kierownik KMN lub Burmistrz.

Drzwi do strefy bezpieczeństwa, są stale zamknięte. By je otworzyć trzeba mieć klucze i znać kod dostępu. Otwarte mogą być wyłącznie przez kierownika KMN lub Burmistrza, który klucze od kancelarii, pobierze od kierownika KMN (pobranie kluczy jest każdorazowo ewidencjonowane).

VII KANCELARIA MATERIAŁÓW NIEJAWNYCH

1. W Urzędzie funkcjonuje Kancelarii Materiałów Niejawnych, która została utworzona na potrzeby jednostki w celu właściwego przechowywania i ewidencjonowania materiałów niejawnych oznaczonych klauzulą „Zastrzeżone”. Znajduje się ona na pierwszym piętrze budynku Biblioteki Miejsko-Gminnej.
2. Organizacja pracy kancelarii, zapewnia możliwość ustalenia w każdych okolicznościach, gdzie znajduje się materiał o klauzuli „Zastrzeżone” oraz kto z tym materiałem się zapoznał.
3. W kancelarii funkcjonuje jeden system antynapadowy. Wejście do kancelarii jest poprzedzone strefą ochronną, zwaną strefą bezpieczeństwa, stanowiącą filtr dostępu do kancelarii materiałów niejawnych.
4. Dostęp do tej strefy posiadają wyłącznie pracownicy pionu ochrony (Pełnomocnik Ochrony i kierownika KMN) oraz Burmistrz. Natomiast w uzasadnionym pełnieniu obowiązków służbowych okolicznościach, w strefie tej mogą przebywać osoby (goście);
 - posiadający stosowne upoważnienie oraz poświadczenie bezpieczeństwa i zaświadczenie o szkoleniu na temat ochrony informacji niejawnych kontrolerzy badający funkcjonowanie ochrony informacji niejawnych,
 - posiadający poświadczenie bezpieczeństwa oraz stosowne upoważnienie od Burmistrza, mający wykonać czynności zlecone.
5. Kontrolę ewidencjonowania i przebywania gości w strefie bezpieczeństwa, prowadzi wprowadzający gości kierownik KMN lub Burmistrz.
6. Ewidencja prowadzona jest w formie książki, z podaniem imienia nazwiska osoby wchodzącej, celu pobytu, daty, godziny wejścia i wyjścia.
7. Drzwi do strefy bezpieczeństwa, są stale zamknięte. By je otworzyć trzeba mieć klucze i znać kod dostępu. Otwarte mogą być wyłącznie przez kierownika KMN lub Burmistrza, który klucze od kancelarii, pobierze od kierownika KMN (pobranie kluczy jest każdorazowo ewidencjonowane).
8. Klucze od kancelarii materiałów niejawnych przechowywane są przez kierownika KMN w plombowanym referentką woreczku.
9. Kierownik KMN prowadzi ewidencję zdawania i pobierania plombowanego woreczka z kluczami – odnotowując dokładną godzinę oraz datę pobrania i zwrotu woreczka.
10. Nad prawidłowością prowadzenia ewidencji czuwa Pełnomocnik Ochrony jako osoba zobowiązana do kontroli środków ochrony fizycznej.

11. Kierownik KMN sprząta pomieszczenie kancelarii oraz strefę bezpieczeństwa osobiście.
12. W przypadku zmiany na stanowisku kierownika KMN sporządza się protokół zdawczo-odbiorczy.
13. Protokół o którym mowa w pkt. 12 sporządza się w obecności pracownika zdającego obowiązki, osoby przejmującej obowiązki oraz Pełnomocnika Ochrony. Protokół sporządza się w dwóch egzemplarzach. Pierwszy egz. przechowywany jest w KMN, drugi u Pełnomocnika Ochrony.
14. W przypadku czasowej nieobecności pracownika kancelarii przejmuje upoważniony pracownik pionu ochrony. W razie ich barku kancelarię przejmuje protokolarnie inny pracownik wyznaczony przez Burmistrza na wniosek Pełnomocnika Ochrony.

VIII. POSTĘPOWNIA Z PRZESYŁKAMI

1. Pracownik sekretariatu urzędu, przyjmuje przesyłki za pokwitowaniem i odciska na nich pieczęć oraz datę wpływu do urzędu i przekazuje ją kierownikowi KMN.
2. Przyjmując przesyłkę, sprawdza się;
 - a) prawidłowość adresu,
 - b) całość opakowania,
 - c) zgodność odcisku pieczęci na opakowaniu z nazwą jednostki organizacyjnej nadawcy.
3. W przypadku stwierdzenia uszkodzenia przesyłki lub śladów jej otwierania, osoba przyjmująca wzywa kierownika KMN, który sporządza wraz z doręczającym, protokół uszkodzenia. Jeden egz. protokołu przekazuje się nadawcy, drugi Pełnomocnikowi Ochrony. W przypadku gdy w obiegu przesyłek pośredniczy przewoźnik – kolejny egz. protokołu przekazuje się jemu.
4. Po przejęciu przez kierownika przesyłki od pracownika sekretariatu, sprawdza on, czy zawartość przesyłki odpowiada wyszczególnionym na niej numerom ewidencyjnym i ustala, czy liczba załączników i stron jest zgodna z liczbą oznaczoną na poszczególnych dokumentach.
5. Kierownik odnotowuje fakt sporządzenia protokołu, o których mowa w pkt. 3, w dzienniku ewidencji dokumentów, w rubryce „informacje uzupełniające/uwagi”.
6. Po przejęciu przesyłki przez kierownika i i wykonaniu czynności opisanych w pkt 4, przekazuje on przesyłkę Burmistrzowi w celu naniesienia imiennej dekretacji konkretnemu pracownikowi. Po zadekretowaniu korespondencji do konkretnej osoby, kierownik przekazuje przesyłkę za pokwitowaniem, tej osobie.
7. W kancelarii materiałów niejawnych nie otwiera się przesyłek oznaczonych „do rąk własnych”. W odpowiednim dzienniku lub rejestrze wpisuje się nadawcę, numer i datę wpływu dokumentu. W rubryce „informacje uzupełniające/uwagi” odnotowuje się, że przesyłka była oznaczona „do rąk własnych”.
8. Na opakowaniu przesyłki, wpisuje się datę wpływu, pozycję i numer, pod którym zarejestrowano przesyłkę i po wykonaniu powyższych czynności przekazuje się za pokwitowaniem- bezpośrednio adresatowi, a w razie jego nieobecności – osobie przez niego upoważnionej do odbioru.
10. Zatrzymanie przez adresata przesyłki, adresowanej „do rąk własnych” kierownik odnotowuje ten fakt w rubryce „informacje uzupełniające/uwagi”.
11. W przypadku zwrotu do kancelarii przesyłki adresowanej „do rąk własnych”, kierownik uzupełnia dane dotyczące przesyłki w odpowiednim dzienniku lub rejestrze.

12. Jeżeli adresat podjął decyzję o przechowaniu przesyłki „do rąk własnych” w kancelarii w stanie zamkniętym, kierownik KMN dokonuje czynności, o których mowa w pkt. 11 przy udziale adresata. Przesyłka w takim przypadku przechowywana w formie zabezpieczonego pakietu, a fakt ten odnotowuje się w rubryce „informacje uzupełniające/uwagi”.
13. Przesyłki pilne, doręcza się adresatom bezzwłocznie. Przy kwitowaniu odbioru tych przesyłek, odnotowuje się godzinę doręczenia.
14. Otrzymałą i wysłaną przesyłkę bądź wytworzony dokument, rejestruje się odpowiednio w kolejności wytwarzania lub otrzymania.
15. Wszelkich adnotacji w dzienniku ewidencji, dokonuje się atramentem lub tuszem. Zmian dokonuje się kolorem czerwonym, umieszczając datę czytelny podpis dokonującego zmiany.
16. Zabrania się wycierania i zmiany adnotacji.
17. Dokumenty, materiały oraz zbiory dokumentów dotyczące spraw ostatecznie zakończonych przechowuje się w kancelarii do czasu zniesienia okresu ochronnego. Po upływie tego okresu, znosi się klauzulę tajności i dokumenty przekazuje się do archiwum zakładowego.

IX. ZAKRES UDOSTĘPNIANIA INFORMACJI NIEJAWNYCH

1. Udostępnianie informacji niejawnych oznaczonych klauzulą „Zastrzeżone”, odbywa się na zasadach określonych w ustawie, tj. osobom posiadającym odpowiednie poświadczenie bezpieczeństwa lub upoważnienie, zaświadczenie o przeszkoleniu oraz dekretagę przełożonego.

X. WYKONYWANIE DOKUMENTÓW NIEJAWNYCH Z WYKORZYSTANIEM SPRZĘTU KOMPUTEROWEGO.

1. Bezpieczeństwo teleinformatyczne zapewnia się, chroniąc informacje przetwarzane w systemach i sieciach teleinformatycznych przed utratą właściwości gwarantujących to bezpieczeństwo, w szczególności przed utratą poufności, dostępności i integralności.
2. Bezpieczeństwo teleinformatyczne zapewnia się, przed rozpoczęciem oraz w trakcie przetwarzania informacji niejawnych w systemie lub sieci teleinformatycznej.
3. Za właściwą organizację bezpieczeństwa teleinformatycznego odpowiada Burmistrz, który w szczególności;
 - 1) zapewnia opracowanie dokumentacji bezpieczeństwa teleinformatycznego,
 - 2) realizuje ochronę fizyczną, elektromagnetyczną systemu sieci,
 - 3) zapewnia niezawodność transmisji oraz kontrolę dostępu do urządzeń systemu lub sieci teleinformatycznej,
 - 4) dokonuje analizy stanu bezpieczeństwa teleinformatycznego oraz zapewnia usunięcie stwierdzonych nieprawidłowości,
 - 5) zapewnia przeszkolenie z zakresu bezpieczeństwa teleinformatycznego dla osób uprawnionych do pracy w systemie lub sieci teleinformatycznej.
4. Ochrona fizyczna systemu lub sieci teleinformatycznej polega na;
 - 1) umieszczenie urządzeń systemu lub sieci teleinformatycznej w strefie ochronnej zwanej również „strefą kontrolowanego dostępu” w zależności od;
 - a) klauzuli tajności,
 - b) ilości,
 - c) zagrożeń poufności, integralności lub dostępności -informacji niejawnych,
 - 2) zastosowaniu środków zapewniających ochronę fizyczną, w szczególności przed;

- a) nieuprawnionym dostępem,
 - b) podglądem,
 - c) podsłuchem.
5. Ochrona elektromagnetyczna systemu lub sieci teleinformatycznej polega na niedopuszczeniu do utraty poufności i dostępności informacji niejawnych przetwarzanych w urządzeniach teleinformatycznych.
- Utrata poufności następuje w szczególności na skutek wykorzystania elektromagnetycznej emisji ujawniającej, pochodzącej z tych urządzeń.
 - Utrata dostępności następuje w szczególności na skutek zakłócania pracy urządzeń teleinformatycznych, za pomocą impulsów elektromagnetycznych o dużej mocy.
6. Ochronę elektromagnetyczną systemu lub sieci teleinformatycznej zapewnia się w szczególności przez umieszczenie urządzeń teleinformatycznych, połączeń linii w strefach kontrolowanego dostępu spełniających wymagania w zakresie tłumienności elektromagnetycznej, odpowiednio do wyników szacowanego ryzyka dla informacji niejawnych, lub zastosowania odpowiednich urządzeń teleinformatycznych, połączeń i linii o obniżonym poziomie emisji lub ich ekranowanie z jednoczesnym filtrowaniem zewnętrznych linii zasilających i sygnałowych.
7. W celu zapewnienia kontroli dostępu do systemu lub sieci teleinformatycznej;
- 1) Burmistrz lub osoba przez niego upoważniona, ustala warunki i sposób przydzielania uprawnień osobom uprawnionym do pracy w systemie lub sieci teleinformatycznej;
 - 2) administrator systemów określi warunki oraz sposób przydzielania tym osobom kont oraz mechanizmów kontroli dostępu, a także zapewnia ich właściwe wykorzystanie.
8. System lub sieć teleinformatyczną wyposaża się w mechanizm kontroli dostępu, odpowiednie do klauzuli tajności informacji niejawnych w nich przetwarzanych.
9. System i sieci teleinformatyczne, w których mają być wytwarzane, przetwarzane, przechowywane lub przekazywane informacje niejawne o klauzuli „zastrzeżone”, podlegają akredytacji kierownika jednostki organizacyjnej, przez zatwierdzenie dokumentacji bezpieczeństwa systemu teleinformatycznego.
9. W ciągu 30 dni od udzielenia akredytacji bezpieczeństwa teleinformatycznego, o której mowa w pkt. 9, Burmistrz przekazuje ABW dokumentację bezpieczeństwa teleinformatycznego.
10. ABW w ciągu 30 dni od otrzymania dokumentacji może przedstawić Burmistrzowi, który udzielił akredytacji, przeprowadzenie dodatkowych czynności związanych z bezpieczeństwem informacji niejawnych. Burmistrz w terminie 30 dni od otrzymania zaleceń, informuje ABW o ich realizacji. W szczególnie uzasadnionych przypadkach ABW może nakazać wstrzymanie przetwarzania informacji niejawnej w systemie teleinformatycznym posiadającym akredytację bezpieczeństwa teleinformatycznego.
11. Dokument szczególnych wymagań bezpieczeństwa systemu teleinformatycznego powinien zawierać w szczególności wyniki procesu szacowania ryzyka dla bezpieczeństwa informacji niejawnych, przetwarzanych w systemie teleinformatycznym oraz określić przyjęte w ramach zarządzania ryzykiem sposoby osiągania i utrzymywania odpowiedniego poziomu bezpieczeństwa systemu, a także opisywać aspekty jego budowy, zasady działania i eksploatacji, które mają związek z bezpieczeństwem systemu lub wpływają na jego bezpieczeństwo. Przebieg i wyniki procesu szacowania ryzyka mogą zostać przedstawione w odrębnym dokumencie szczególnych wymagań bezpieczeństwa.
12. Dokument szczególnych wymagań bezpieczeństwa, opracowuje się na etapie projektowania, w razie potrzeby konsultuje z ABW, bieżąco uzupełnia na etapie wdrażania i modyfikuje na etapie eksploatacji przed dokonaniem zmian w systemie teleinformatycznym.

13. Dokument procedur bezpiecznej eksploatacji opracowuje się na etapie wdrażania oraz modyfikuje na etapie eksploatacji przed dokonaniem zmian w systemie teleinformatycznym.
14. Podstawą dokonywania wszystkich zmian w systemie teleinformatycznym jest przeprowadzenie procesu szacowania ryzyka dla bezpieczeństwa informacji niejawnych przetwarzanych w tym systemie.
15. Burmistrz wyznacza:
 - 1) Pracownika pionu ochrony pełniącego funkcję inspektora bezpieczeństwa teleinformatycznego, odpowiedzialnego za weryfikację i bieżącą kontrolę zgodności funkcjonowania systemu teleinformatycznego ze szczególnymi wymaganiami bezpieczeństwa oraz przestrzegania procedur bezpiecznej eksploatacji.
 - 2) Administratora systemu – osobę odpowiedzialną za funkcjonowanie systemu teleinformatycznego oraz przestrzegania zasad i wymagań bezpieczeństwa, przewidzianych dla systemu teleinformatycznego, który wchodzi w skład pionu ochrony.
16. Funkcję administratora systemu oraz inspektora bezpieczeństwa teleinformatycznego mogą pełnić osoby, posiadające poświadczenie bezpieczeństwa odpowiednie do klauzuli informacji wytwarzanych, przetwarzanych, przechowywanych lub przekazywanych w systemie lub sieciach teleinformatycznych, po odbyciu specjalistycznych szkoleń z zakresu bezpieczeństwa teleinformatycznego prowadzonych przez służby ochrony państwa.

XI. GROMADZENIE DOKUMENTÓW ZAWIERAJĄCYCH INFORMACJE NIEJAWNE

1. Dokumenty zawierające informacje niejawne powinny być przechowywane zgodnie z rzeczowym podziałem akt.
2. Dokumenty niejawne o klauzuli „Zastrzeżone” są przechowywane w KMN lub na stanowiskach pracy w meblach biurowych, zamykanych na klucz.
3. Dokumenty ostatecznie załatwione wymagają wszycia w teczkę pism, po zakończeniu roku kalendarzowego, klauzule niejawności teczek określa się według dokumentu, na którym naniesiona jest klauzula tajności.

XII OZNACZANIE, NADAWANIE, ZMIANA I ZNOSZENIE KLAUZULI NIEJAWNOŚCI MATERIAŁOM NIEJAWNYM

1. Klauzulę tajności nadaje osoba, która jest uprawniona do podpisania dokumentu lub oznaczenia innego niż dokument materiału.
2. Informacje niejawne podlegają ochronie w sposób określony w ustawie o ochronie informacji niejawnych do czasu zniesienia lub zmiany klauzuli tajności.
3. Osoba wymieniona w pkt.1 może określić datę lub wydarzenie, po którym nastąpi zniesienie klauzuli tajności.
4. Zniesienie klauzuli tajności jest możliwe wyłącznie po wyrażeniu zgody przez osobę, o której mowa w pkt. 1 albo jej przełożonego w przypadku ustania ustawowych przesłanek ochrony.
5. Należy nie rzadziej niż raz na 5 lat dokonać przeglądu materiałów niejawnych celem ustalenia czy spełniają ustawowe przesłanki ochrony.
6. Po zniesieniu lub zmianie klauzuli tajności, podejmuje się czynności polegające na naniesieniu odpowiednich zmian w oznaczeniu materiału i poinformowaniu o nich odbiorców.
7. Poszczególne części materiału mogą być oznaczone różnymi klauzulami tajności.

8. Oznaczenie materiału klauzulą tajności polega na umieszczeniu na nim klauzuli tajności, którą nanosi się w sposób wyraźny i w pełnym jej brzmieniu.
9. W Urzędzie występuje tylko jedna klauzula tajności, oznaczona dużą literą „Z” – „Zastrzeżone”.
10. Materiały zawierające informacje niejawne utrwalone na piśmie, oznaczają się w następujący sposób:
 - 1) na każdej stronie umieszcza się:
 - a) na środku, jako pierwszy element w nagłówku strony, klauzulę tajności;
 - b) numer egzemplarza, a w przypadku gdy dokument wykonano w jednym egzemplarzu, napis „egz. pojedynczy”;
 - c) sygnaturę literowo-cyfrową, na którą składają się: literowe oznaczenie jednostki lub komórki organizacyjnej, symbol oznaczenia klauzuli tajności, numer, pod którym ten dokument został zarejestrowany, i rok, w którym dokonano rejestracji, a także, w zależności od potrzeb, inne oznaczenia ułatwiające ustalenie miejsca wykonania dokumentu w jednostce lub komórce organizacyjnej lub też jego przynależność do określonej sprawy;
 - d) numer strony oraz liczbę stron całego dokumentu;
 - e) na środku, jako ostatni element w stopce strony, klauzulę tajności;
 - 2) na pierwszej stronie umieszcza się również:
 - a) nazwę jednostki lub komórki organizacyjnej,
 - b) nazwę miejscowości i datę podpisania dokumentu,
 - c) w przypadku dokumentu, któremu nadano bieg korespondencyjny, imię i nazwisko lub nazwę stanowiska adresata; w przypadku wielu adresatów dokumentu, któremu nadano bieg korespondencyjny, dopuszcza się możliwość umieszczenia jedynie adnotacji „adresaci według rozdzielnika”;
 - 3) na ostatniej stronie pod treścią umieszcza się również:
 - a) liczbę załączników,
 - b) liczbę stron lub innych jednostek miary wszystkich załączników lub informację określającą rodzaj załączonego materiału i jego odpowiednią jednostkę miary,
 - c) klauzule tajności załączników wraz z numerami, pod jakimi zostały zarejestrowane, oraz liczbę stron każdego załącznika lub informację określającą rodzaj załączonego materiału i jego odpowiednią jednostkę miary,
 - d) w przypadku gdy adresatowi wysyła się inną liczbę załączników niż pozostawia w aktach, dodatkowo napis „tylko adresat” — jeżeli załączniki mają być przekazane adresatowi bez pozostawiania ich w aktach, lub napis „do zwrotu” — jeżeli załączniki mają zostać zwrócone nadawcy,
 - e) stanowisko oraz imię i nazwisko lub inne oznaczenie wskazujące osobę uprawnioną do jego podpisania,
 - f) liczbę wykonanych egzemplarzy,
 - g) adresatów poszczególnych egzemplarzy dokumentu albo adnotację „adresaci według rozdzielnika”,
 - h) dyspozycję „ad acta” w przypadku egzemplarza pozostającego w aktach nadawcy,
 - i) imię i nazwisko lub inne oznaczenie wskazujące wykonawcę.
11. Na dokumencie nieelektronicznym stanowiącym załącznik na pierwszej stronie umieszcza się dodatkowo informację: „Załącznik nr ... do dokumentu nr ... z dnia ...”.
12. Jeżeli wraz z dokumentem przesyła się załącznik zawierający informacje niejawne, to:
 - 1) dokument oznacza się klauzulą tajności nie niższą niż najwyższa klauzula tajności załączników;

- 2) na dokumencie — jeżeli po trwałym odłączeniu załączników dokument jest jawny albo jego klauzula tajności jest inna niż określona zgodnie z pkt 1 — na każdej stronie pod numerem egzemplarza umieszcza się adnotację o jawności albo klauzuli tajności dokumentu po odłączeniu załączników.
14. Dokumenty elektroniczne oraz dokumenty nieelektroniczne wytworzone w wyniku kopiowania lub tłumaczenia oznacza się zgodnie z Rozporządzeniem Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności:
15. Wytworzenie dokumentu w wyniku kopiowania lub tłumaczenia dokumentu nieelektronicznego odnotowuje się na ostatniej stronie dokumentu kopiowanego lub tłumaczonego przez umieszczenie informacji o:
 - 1) nazwie jednostki lub komórki organizacyjnej, w której wytworzono dokument;
 - 2) liczbie egzemplarzy dokumentu wytworzonego;
 - 3) dacie wytworzenia dokumentu;
 - 4) numerze, pod jakim wytworzony dokument został zarejestrowany.
16. Informacje, o których mowa w pkt. 15 ust. 1—3, umieszcza się przed wytworzeniem dokumentu w wyniku kopiowania lub tłumaczenia, natomiast numer, pod jakim został on zarejestrowany, umieszcza się po wytworzeniu.
17. Zgody na zniesienie lub zmianę klauzuli tajności udziela się w odrębnym dokumencie podlegającym rejestracji lub przez oznaczenie w postaci umieszczenia informacji:
 - 1) na dokumencie — w przypadku dokumentu nieelektronicznego;
 - 2) w metryce dokumentu — w przypadku dokumentu elektronicznego.
18. Oznaczenia zniesienia klauzuli tajności na dokumencie nieelektronicznym utrwalonym w formie pisma dokonuje się następująco:
 - 1) skreśla się wszystkie dotychczasowe oznaczenia znoszonej klauzuli tajności;
 - 2) nad pierwszym w kolejności skreślonym oznaczeniem klauzuli tajności umieszcza się napis „Zniesiono klauzulę tajności” oraz datę, podpis, imię i nazwisko lub inne oznaczenie wskazujące osobę dokonującą tych adnotacji oraz wskazuje się podstawę dokonania czynności.
19. Skreśleń i adnotacji, o których mowa w pkt. 18, ust. 1 i 2 dokonują: kierownik KMN.
20. Skreśleń i adnotacji, o których mowa w pkt. 18, ust. 1 i 2 dokonuje się kolorem czerwonym, w sposób czytelny. Wycieranie, wywabianie lub zamazywanie klauzul tajności i dokonanych zmian jest niedozwolone.

XIII. NADZÓR W ZAKRESIE OCHRONY INFORMACJI NIEJAWNYCH

1. Za ochronę informacji niejawnych odpowiada Burmistrz.
2. Za przestrzeganie w jednostce przepisów o ochronie informacji niejawnych odpowiada Pełnomocnik Ochrony powoływany przez Burmistrza.

XIV. ODPOWIEDZIALNOŚĆ KARNA ZA NARUSZENIE PRZEPISÓW O OCHRONIE INFORMACJI NIEJAWNYCH

1. Zakres odpowiedzialności karnej osób, które dopuściły się przestępstwa lub czynu zabronionego przeciwko ochronie informacji niejawnych, został określony przepisami kodeksu karnego.

Przestępstwa przeciwko ochronie informacji

Art. 266.

- § 1. Kto, wbrew przepisom ustawy lub przyjętemu na siebie zobowiązaniu, ujawnia lub wykorzystuje informację, z którą zapoznał się w związku z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną, gospodarczą lub naukową, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
- § 2. Funkcjonariusz publiczny, który ujawnia osobie nieuprawnionej informację niejawną o klauzuli „zastrzeżone” lub „poufne” lub informację, którą uzyskał w związku z wykonywaniem czynności służbowych, a której ujawnienie może narazić na szkodę prawnie chroniony interes, podlega karze pozbawienia wolności do lat 3.

Przestępstwo nieuprawnionego uzyskania informacji

Art. 267.

- § 1. Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
- § 3. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem.
- § 4. Tej samej karze podlega, kto informację uzyskaną w sposób określony w § 1–3 ujawnia innej osobie.

Przestępstwo niszczenia informacji

art. 268.

- § 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
- § 2. Jeżeli czyn określony w § 1 dotyczy zapisu na informatycznym nośniku danych, sprawca podlega karze pozbawienia wolności do lat 3.

Art. 268a.

- § 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności do lat 3.
- § 2. Kto, dopuszczając się czynu określonego w § 1, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

przestępstwo sabotażu komputerowego

Art. 269.

- § 1. Kto niszczy, uszkadza, usuwa lub zmienia dane informatyczne o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego albo zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.
- § 2. Tej samej karze podlega, kto dopuszcza się czynu określonego w § 1, niszcząc albo wymieniając informatyczny nośnik danych lub niszcząc albo uszkadzając urządzenie służące do automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych.

XV. ARCHIWIZOWANIE, GROMADZENIE I NISZCZENIE MATERIAŁÓW NIEJAWNYCH

1. Archiwizowanie materiałów niejawnych odbywa się z zachowaniem zasad określonych w rozporządzeniu Ministra Kultury w sprawie postępowania z dokumentacją, zasad jej klasyfikowania i kwalifikowania oraz zasad i trybu przekazywania materiałów archiwalnych do archiwów państwowych (Dz. U. Nr 167 poz.1375).
2. Zasady postępowania z dokumentacją w komórkach wykonujących zadania w zakresie obronności i bezpieczeństwa państwa zostały określone w rozporządzeniu Prezesa Rady ministrów (Dz. U. 2010 Nr 34 poz.181).
3. Dokumentacja wytwarzana i gromadzona dzieli się na:
 - 1) materiały archiwalne – wchodzące do państwowego zasobu archiwalnego,
 - 2) dokumentację niearchiwalną – inną dokumentację, niestanowiącą materiałów archiwalnych.
4. Dokumentacja niearchiwalna, podlega brakowaniu po upływie okresu przechowywania określonego we właściwym wykazie akt.
5. Brakowanie dokumentacji niearchiwalnej polega na ocenie jej przydatności do celów praktycznych, wydzieleniu dokumentacji nieprzydatnej i przekazaniu jej na makulaturę.
6. Brakowanie dokumentacji niearchiwalnej następuje na podstawie zgody.
7. Zgodę, o której mowa, wyraża dyrektor miejscowo właściwego archiwum państwowego.
8. Wniosek o wyrażenie zgody na brakowanie dokumentacji niearchiwalnej należy złożyć dyrektorowi miejscowo właściwego archiwum państwowego.
9. Urząd przechowuje w archiwum zakładowym dokumenty brakowania, o których mowa wraz z dowodami przekazania nieprzydatnej dokumentacji niearchiwalnej na makulaturę bądź protokołami jej zniszczenia.
10. Uporządkowanie materiałów archiwalnych polega na podziale rzeczowym teczek i prawidłowym ułożeniu materiałów wewnątrz teczek, ich opisaniu, nadaniu właściwego układu, sporządzeniu ewidencji oraz technicznym zabezpieczeniu.
11. 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 być opatrzone kolejną numeracją.
12. 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 danej 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 najwcześniejszych i najpóźniejszych materiału archiwalnego w teczce;
 - 5) sygnatury teczki, to jest numeru spisu zdawczo-odbiorczego i numeru pozycji teczki w spisie zdawczo odbiorczym;
 - 6) symboli kwalifikacyjnego materiałów archiwalnych (kategoria A), liczby stron w teczce.
13. Czynności związane z brakowaniem materiałów niearchiwalnych, wobec których archiwum państwowe wyraziło zgodę jest dokumentowane, przez sporządzenie protokołu komisyjnego zniszczenia dokumentów niearchiwalnych.
14. Protokół komisyjnego zniszczenia materiałów niearchiwalnych sporządzany jest w dwóch egzemplarzach, z czego jeden egzemplarz należy przesłać do właściwego archiwum państwowego.

XVI. PRZECHOWYWANIE KLUCZY I PICZĘCI

1. Pieczęcie, którymi posługuje się kierownik KMN przechowywane są w szafach metalowych w kancelarii.
2. Szafy metalowe w kancelarii po zamknięciu powinny być dodatkowo plombowane pieczęciami do plasteliny (referentką).
3. Klucze do szaf metalowych po zakończeniu pracy należy złożyć w pomieszczeniu kancelarii, w miejscu niewidocznym.
4. Po zakończeniu pracy kierownik kancelarii zamyka i plombuje pieczęciami do plasteliny drzwi wejściowe do kancelarii.
5. Klucze do drzwi wejściowych należy umieścić w woreczku i zasnurować. Na troki przykleić plastelinę i wykonać w niej odcisk pieczęcią do plasteliny.
6. Woreczek z kluczami należy złożyć w budynku urzędu, w pokoju nr 31, w stalowej szkatułce, na której po zamknięciu należy wykonać odcisk pieczęcią do plasteliny. Tak zabezpieczoną szkatułkę umieszcza się w szafie biurowej. Klucze od tej szafy i klucze od szkatułki należy schować do woreczka na klucze, zasnurować, na troki przykleić plastelinę i wykonać na niej odcisk pieczęcią do plasteliny. Tak przygotowany woreczek oddać za pokwitowaniem do pokoju Nr 2.
7. Pieczęć do plasteliny kierownik KMN posiada stale przy sobie i odpowiada za nią.
8. Zapasowy komplet kluczy do KMN, umieszczony w woreczku na klucze, zdeponowany jest u Pełnomocnika Ochrony.
9. Kierownik kancelarii po przybyciu do pracy, codziennie sprawdza czy nie została naruszona pieczęć na woreczku na klucze oraz powinien sprawdzić stan pieczęci na drzwiach wejściowych do kancelarii materiałów niejawnych.

XVII. PLANY AWARYJNE UWZGLĘDNIAJĄCE POTRZEBĘ OCHRONY INFORMACJI NIEJAWNYCH W RAZIE WYSTĄPIENIA SYTUACJI SZCZEGÓLNYCH, W TYM WPROWADZENIA STANÓW NADZWYCZAJNYCH, W CELU ZAPOBIEŻENIA UTRACIE POUFNOŚCI, INTEGRALNOŚCI LUB DOSTĘPNOŚCI INFORMACJI NIEJAWNYCH

1. W sytuacjach szczególnych zagrożeń, jeżeli zwykłe środki konstytucyjne są niewystarczające, może zostać wprowadzony odpowiedni stan nadzwyczajny: stan wojenny, stan wyjątkowy lub stan klęski żywiołowej.
2. Działania podjęte w celu ochrony materiałów niejawnych będących w posiadaniu jednostki organizacyjnej muszą odpowiadać stopniowi zagrożenia podstawowych interesów Rzeczypospolitej Polskiej w zakresie obronności, bezpieczeństwa, stosunków gospodarczych i międzynarodowych państwa.
3. W przypadku wprowadzenia stanu wojennego lub stanu wyjątkowego wzmacnia się ochronę budynku Urzędu, w tym pomieszczenia kancelarii materiałów niejawnych. Wzmocnienie ochrony w przypadku stanu wojennego ma na celu zabezpieczenie budynku przed grupami dywersyjnymi i sabotażowymi oraz przed ewentualnymi demonstrantami czy też uczestnikami starć z siłami porządkowymi w przypadku wprowadzenia stanu wyjątkowego. W analogiczny sposób postępuje się w przypadku wystąpienia zdarzeń kryzysowych, gdy jest to konieczne.

Działania jakie zostaną podjęte obejmują m.in.:

- 1) wprowadzenie kontroli interesantów w oparciu o imienne przepustki;
- 2) wzmocnienie ochrony obiektu funkcjonariuszami Straży Miejskiej lub pracownikami firmy ochroniarskiej;

- 3) przeniesienie kancelarii materiałów niejawnych do zapasowego miejsca pracy.
4. W przypadku bezpośredniego zagrożenia przeprowadza się ewakuację materiałów niejawnych. W przypadku nagłego zagrożenia, decyzję o zniszczeniu materiałów niejawnych podejmuje Burmistrz, a w przypadku jego nieobecności Pełnomocnik Ochrony. Bezpośrednie zagrożenie może wynikać z działań wojennych, w wyniku których materiały niejawne mogą dostać się w ręce agresora.
5. Ewakuacja akt powinna obejmować: zapakowanie materiałów do worków ewakuacyjnych (będących na wyposażeniu kancelarii materiałów niejawnych), przemieszczenie worków na środek transportu i przewiezienie do wyznaczonego przez Burmistrza miejsca ewakuacji.
6. Nadzór i ochronę transportu do miejsca ewakuacji dokumentów zapewniają pracownicy pionu ochrony.
7. Opis postępowania w sytuacjach kryzysowych i analiza ryzyka wystąpienia sytuacji kryzysowych.

Za sytuacje kryzysowe w zakresie informacji niejawnych przyjmuje się zdarzenia:

Lp.	Rodzaje sytuacji kryzysowej	Poziom ryzyka (skala 1-5)	Sposób postępowania z dokumentami
1	Zanik napięcia	3	P
2	Awaria systemu alarmowego	3	P
3	Pożar	3	E
4	Zagrożenia Atmosferyczne	2	E
5	Zagrożenia chemiczne	1	E
6	Zagrożenia atakiem terroru	1	Z
7	Sabotaż	2	E
8	Włamanie	2	Z
9	Napad	1	Z
10	Kradzież	2	-
11	Zniszczenie dokumentu	2	-
12	Wtargnięcie lub okupacja budynku	2	Z
13	Działania obcych służb specjalnych	1	E

gdzie 1 - oznacza najmniejsze ryzyko wystąpienia danej sytuacji, a 5 największe ryzyko, „P” - pozostawić, „E” - ewakuować, „Z” - zniszczyć.

W każdym ww. przypadku Pełnomocnik Ochrony powinien podjąć działania prowadzące do wyjaśnienia przyczyn tejże sytuacji oraz usunięcia jej skutków. W sytuacji kiedy ewakuacja staje się konieczna, ewakuacji podlegają wszystkie dokumenty niejawne przechowywane w Urzędzie. Niszczenie materiałów dokonywane jest za pomocą odpowiedniej niszczarki dokumentów lub ich spalanie. Protokół zniszczenia materiałów niejawnych winien zawierać opis okoliczności, w jakich dokonano zniszczenia, gdzie, kiedy, na czyje polecenie i w jaki sposób oraz spis zniszczonych materiałów.

XVIII. USTALENIA KOŃCOWE

1. Z planem ochrony zapoznają się:
 - 1) Burmistrz Miasta
 - 2) Kierownik Kancelarii Materiałów Niejawnych
 - 3) Wszystkie osoby, które pracując w Urzędzie i mają do czynienia z informacjami niejawnymi.

2. W przypadku wystąpienia wątpliwości, a także potrzeby przybliżenia zasad dotyczących realizacji zadań związanych z ochroną informacji niejawnych, sporządzania i wykonywania dokumentów zawierających informacje „Zastrzeżone”, pracownicy Urzędu mogą w każdym czasie zwracać się o wyjaśnienie czy też instruktaż do:
 - 1) Pełnomocnika ds. Ochrony Informacji Niejawnych;
 - 2) Kierownika Kancelarii Materiałów Niejawnych.
3. Integralną częścią planu ochrony informacji niejawnych stanowią załączniki w ilości 9 szt., wyspecyfikowane w dołączonym do Planu Ochrony zestawieniu załączników.

**ZESTAWIENIE ZAŁĄCZNIKÓW
DO PLANU OCHRONY INFORMACJI NIEJAWNYCH
W URZĘDZIE MIEJSKIM W JĘDRZEJOWIE**

Nr załącznika	Czego dotyczy załącznik	Strona, na której znajduje się załącznik
1.	2.	3.
1	Wykaz stanowisk i funkcji, z którymi może łączyć się dostęp do informacji niejawnych oznaczonych klauzulą „Zastrzeżone” występujących w Urzędzie Miejskim w Jędrzejowie	24
2	Wykaz informacji niejawnych oznaczonych klauzulą „Zastrzeżone” mogące występować w zakresie działania Urzędu Miejskiego w Jędrzejowie	25
3	Przykłady oznaczenia materiałów o klauzuli tajności „Zastrzeżone”	od 26 do 32
4	Szczegółowa instrukcja dotycząca sposobu i trybu przetwarzania informacji niejawnych oznaczonych klauzulą „Zastrzeżone” oraz zakresu i warunków stosowania środków bezpieczeństwa fizycznego w celu ich ochrony w Urzędzie Miejskim w Jędrzejowie	od 33 do 40
5	Instrukcja alarmowa w przypadku zgłoszenia o podłożeniu lub znalezieniu ładunku wybuchowego w Urzędzie Miejskim w Jędrzejowie	od 41 do 42
6	Instrukcja postępowania w przypadku otrzymania przesyłki niewiadomego pochodzenia	43
7	Wzór upoważnienia uprawniającego do dostępu do informacji niejawnych oznaczonych klauzulą „Zastrzeżone” dla pracownika zatrudnionego w Urzędzie Miejskim w Jędrzejowie.	44
8	Protokół otwarcia szafy, sejfów w Kancelarii Materiałów Niejawnych	45
9	Pion Ochrony Informacji Niejawnych w Urzędzie Miejskim w Jędrzejowie	46

**WYKAZ STANOWISK I FUNKCJI, Z KTÓRYMI MOŻE SIĘ ŁĄCZYĆ DOSTĘP DO
INFORMACJI NIEJAWNYCH OZNACZONYCH KLAUZULĄ „ZASTRZEŻONE”
WYSTĘPUJĄCYCH W URZĘDZIE MIEJSKIM W JĘDRZEJOWIE**

1. **Burmistrz**– zadania z zakresu spraw obronnych oraz nadzór nad ochroną materiałów i dokumentów niejawnych oznaczonych klauzulą „Zastrzeżone”, wytwarzanych i przechowywanych w Urzędzie Miejskim w Jędrzejowie.
2. **Sekretarz Gminy**–zakres obowiązków wynikający z upoważnień wydanych przez Burmistrza Miasta, a dotyczących spraw obronnych, ochrony dokumentów niejawnych oznaczonych klauzulą „Zastrzeżone”, wytwarzanych i przechowywanych w Urzędzie Miejskim w Jędrzejowie.
3. **Pełnomocnik ds. Ochrony Informacji Niejawnych**– cały zakres obowiązków wynikający z ustawy o ochronie informacji niejawnych i aktów wykonawczych do tej ustawy, dotyczących ochrony informacji niejawnych oznaczonych klauzulą „Zastrzeżone”, wytwarzanych, przekazywanych i przechowywanych w Urzędzie Miejskim.
4. **Kierownik Kancelarii Materiałów Niejawnych** – cały zakres obowiązków wynikających z ustawy o ochronie informacji niejawnych i aktów wykonawczych do tej ustawy, dotyczących ochrony informacji niejawnych oznaczonych klauzulą „Zastrzeżone”, wytwarzanych, przekazywanych i przechowywanych w Urzędzie Miejskim.
5. **Wieloosobowe Stanowisko ds. Zarządzania Kryzysowego, Obrony Cywilnej i Spraw Wojskowych**– zadania z zakresu planowania i opracowania wniosków w zakresie świadczeń osobistych i rzeczowych na potrzeby obrony cywilnej, nadzór nad wykonaniem świadczeń osobistych i rzeczowych na rzecz sił zbrojnych oraz organizowanie i przygotowanie do działań systemu wykrywania i alarmowania formacji obrony cywilnej.
6. **Inspektor Bezpieczeństwa Teleinformatycznego**– odpowiedzialny za weryfikację i bieżącą kontrolę zgodności funkcjonowania systemu teleinformatycznego ze szczególnymi wymaganiami bezpieczeństwa oraz przestrzegania procedur bezpiecznej eksploatacji.
7. **Administrator Systemu Teleinformatycznego**– odpowiedzialny za funkcjonowanie systemu teleinformatycznego oraz za przestrzeganie zasad i wymagań bezpieczeństwa, przewidzianych dla systemu teleinformatycznego.
8. **Obsługa sekretariatu urzędu** – zadania z zakresu przyjmowania w sekretariacie Urzędu Miejskiego, korespondencji niejawnej oznaczonej klauzulą „Zastrzeżone”.

**WYKAZ INFORMACJI OZNACZONYCH KLAUZULĄ „ZASTRZEŻONE” MOGĄCYCH
WYSTĘPOWAĆ W ZAKRESIE DZIAŁANIA URZĘDU MIEJSKIEGO W JĘDRZEJOWIE**

1. Dokumentacja Akcji Kurierskiej.
2. Korespondencja związana z Akcją Kurierską.
3. Sprawozdania związana z Akcją Kurierską.
4. Plan Obrony Cywilnej.
5. Plan Operacyjny Funkcjonowania Miasta i Gminy Jędrzejów w Warunkach Zagrożenia Bezpieczeństwa Państwa i w Czasie Pokoju.
6. Regulamin Organizacyjny Urzędu Miejskiego na Czas Wojny.
7. Plan Zapewnienia Warunków Funkcjonowania Burmistrza Miasta i Gminy Jędrzejów oraz Urzędu Miejskiego w Dotychczasowym Miejsu Pracy (DPM).
8. Dokumentacja Stałego Dyżuru.
9. Tabela Sygnałowa „ZEFIR”.
10. Wzory do planowania operacyjnego.
11. Wzory dokumentów związanych z Akcją Kurierską.
12. Raport Zniszczenia Dokumentacji Urzędowej Wycofanej z Obiegu.
13. Dziennik Ewidencyjny.
14. Rejestr Wydanych Przedmiotów

**PRZYKŁADY
OZNACZENIA MATERIAŁÓW O KLAUZULI TAJNOŚCI
„ZASTRZEŻONE”**

PRZYKŁAD 1 - Pismo bez załączników - pierwsza strona

Zastrzeżone

.....
(nazwa jednostki lub komórki organizacyjnej)

Jędrzejów 10 stycznia 2021r.

POIN 5223.Z-11-2021

Egz. Nr 1
lub „Egz. pojedynczy”

**Imię i nazwisko
nazwa stanowiska
albo
„adresaci według rozdzielnika”**

Treść pisma
.....
.....
.....
.....

Objaśnienie:

- 1) na środku, jako pierwszy element w nagłówku strony, klauzulę tajności;
- 2) nazwę jednostki lub komórki organizacyjnej;
- 3) nazwę miejscowości i datę podpisania dokumentu;
- 4) sygnaturę literową oznaczenia jednostki lub komórki organizacyjnej, symbol klasyfikacji z jednolitego rzeczowego wykazu akt, symbol oznaczenia klauzuli tajności „Zastrzeżone”, numer, pod którym ten dokument został zarejestrowany i rok w którym dokonano rejestracji;
- 5) Numer egzemplarza, a w przypadku gdy dokument wykonano w jednym egzemplarzu, napis „egz. pojedynczy”;
- 6) Stanowisko oraz imię i nazwisko lub inne oznaczenie wskazujące osobę uprawnioną do podpisania;
- 7) w przypadku dokumentu, któremu nadano bieg korespondencyjny, imię i nazwisko lub nazwę stanowiska adresata; w przypadku wielu adresatów dokumentu, któremu nadano bieg korespondencyjny, dopuszcza się możliwość umieszczenia jedynie adnotacji „adresaci według rozdzielnika”;
- 8) numer strony oraz liczbę stron całego dokumentu;
- 9) na środku, jako ostatni element w stopce strony, klauzule tajności.

kolejna strona pisma

Zastrzeżone

POIN 5223.Z-11-2021

Egz. Nr 1
(lub „Egz. pojedynczy”

c.d. pisma

2/3

Zastrzeżone

Zastrzeżone

Egz. Nr 1
lub „egz. pojedynczy”

c.d. pisma

stanowisko oraz imię i nazwisko
osoby uprawnionej do podpisania

Wykonał: Jan Kowalski

Zastrzeżone

3/3

PRZKŁAD 2 - Pismo z załącznikami - ostatnia strona

POIN 5223.Z-11-2021

Egz. Nr 1
lub „Egz. pojedynczy”

Treść pisma

stanowisko oraz imię i nazwisko
osoby uprawnionej do podpisania

Załączników: 3, na 6 stronach.

Zał. Nr 1 – „zastrzeżone”, POIN 5223.Z-8-2021, na 2 stronach,
Zał. Nr 2 – „zastrzeżone”, POIN 5223.Z-9-2021, na 3 stronach, - „do zwrotu”,
Zał. Nr 3 – „zastrzeżone”, POIN 5223.Z-10-2021, na 1 stronie, - „tylko adresat”

Wykonano w 2 egz.

Egz. Nr 1 - adresat

Egz. Nr 2 – a/a

Lub

„adresaci według rozdzielnika”

Wykonał Jan Kowalski

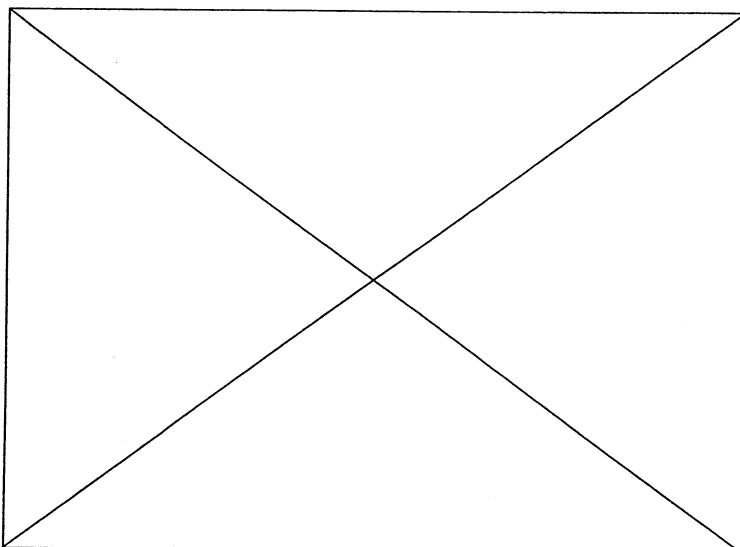
Zastrzeżone

3/3

Objaśnienia:

- 1) na środku, jako pierwszy element w nagłówku strony, klauzulę tajności;
- 2) nazwę jednostki lub komórki organizacyjnej;
- 3) nazwę miejscowości i datę podpisania dokumentu;
- 4) sygnaturę literową oznaczenia jednostki lub komórki organizacyjnej, symbol klasyfikacji z jednolitego rzeczowego wykazu akt, symbol oznaczenia klauzuli tajności „Zastrzeżone”, numer, pod którym ten dokument został zarejestrowany i rok w którym dokonano rejestracji;
- 5) numer egzemplarza, a w przypadku gdy dokument wykonano w jednym egzemplarzu, napis „egz. pojedynczy”;
- 6) stanowisko oraz imię i nazwisko lub inne oznaczenie wskazujące osobę uprawnioną do podpisania;
- 7) liczbę załączników;
- 8) liczbę stron lub innych jednostek miary wszystkich załączników;
- 9) w przypadku, gdy adresatowi wysyła się inną liczbę załączników, niż pozostawia w aktach, dodatkowo napis „tylko adresat” – jeżeli załączniki mają być przekazane adresatowi bez pozostawienia ich w aktach, lub napis „do zwrotu” – jeżeli załączniki mają zostać zwrócone nadawcy;
- 10) liczbę wykonanych egzemplarzy;
- 11) adresatów poszczególnych egzemplarzy dokumentu albo adnotację „adresaci według rozdzielnika”
- 12) imię i nazwisko wykonawcy;
- 13) numer strony oraz liczbę stron całego dokumentu;
- 14) na środku, jako ostatni element w stopce strony, klauzulę tajności.

PRZKŁAD 2 – zasady pakowania



Na kopercie wewnętrznej w miejscach sklejenia koperty odciska się pieczęć „do pakietów”. Dodatkowo w miejscach sklejenia koperty nakleja się przezroczystą taśmę samoprzylepną

Zastrzeżone

POIN 5223.Z-11-2021

Dyrektor Wydziału
Bezpieczeństwa
i Zarządzania Kryzysowego
Urzędu Wojewódzkiego
w Kielcach

Pakował: Jan Kowalski
Podpis osoby pakującej

Koperta wewnętrzna:

- 1) klauzula tajności i ewentualne dodatkowe oznaczenie,
- 2) określenie adresata,
- 3) imię, nazwisko i podpis osoby pakującej,
- 4) numer, pod którym dokument został zarejestrowany,

Nazwa jednostki organizacyjnej nadawcy

WPN – 1/7/01

Dyrektor Wydziału
Bezpieczeństwa
i Zarządzania Kryzysowego
Urzędu Wojewódzkiego
w Kielcach
aleja IX Wieków Kielc 3
25-516 Kielce

Koperta zewnętrzna:

- 1) nazwa jednostki organizacyjnej adresata,
- 2) adres siedziby adresata,
- 3) numer wykazu i pozycji w wykazie przesyłek nadanych.

SZCZEGÓŁOWA INSTRUKCJA OKREŚLAJĄCA SPOSÓB I TRYB PRZETWARZANIA INFORMACJI NIEJAWNYCH OZNACZONYCH KLAUZULĄ „ZASTRZEŻONE”

Rozdział I

§ 1.

Instrukcja określająca sposób i tryb przetwarzania informacji niejawnych o klauzuli „Zastrzeżone” – zwana dalej Instrukcją – określa zasady i sposób postępowania z informacjami niejawnymi oznaczonymi klauzulą „Zastrzeżone” oraz zasady ochrony tych informacji w Urzędzie Miejskim w Jędrzejowie (dalej Urząd).

§ 2.

Instrukcja dotyczy wszystkich pracowników Urzędu bez względu na zajmowane przez nich stanowiska, jeśli wiążą się one z dostępem do informacji niejawnych oznaczonych klauzulą „Zastrzeżone”.

Rozdział II

KLASYFIKOWANIE INFORMACJI NIEJAWNYCH

§ 3.

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

§ 4.

Klauzulę tajności nadaje osoba, która jest uprawniona do podpisania dokumentu lub oznaczenia innego niż dokument materiału. Osoba ta może określić datę lub wydarzenie, po których nastąpi zniesienie lub zmiana klauzuli tajności.

§ 5.

Zniesienie lub zmiana klauzuli tajności są możliwe wyłącznie po wyrażeniu pisemnej zgody przez osobę, o której mowa w § 4, albo jej przełożonego – w przypadku ustania lub zmiany ustawowych przesłanek ochrony. Po zniesieniu lub zmianie klauzuli tajności podejmuje się czynności polegające na naniesieniu odpowiednich zmian w oznaczeniu dokumentu i poinformowaniu o tym jego odbiorców.

§ 6.

Informacjom niejawnym, materiałom, a zwłaszcza dokumentom i ich zbiorom przyznaje się klauzulę tajności co najmniej równą najwyższej zaklasyfikowanej informacji lub najwyższej klauzuli w zbiorze.

§ 7.

Informacjami niejawnymi o klauzuli „Zastrzeżone” w Urzędzie są informacje wyszczególnione w załączniku Nr 2 do Planu Ochrony Informacji Niejawnych w Urzędzie Miejskim w Jędrzejowie.

Rozdział III

DOSTĘP DO INFORMACJI NIEJAWNYCH O KLAUZULI "ZASTRZEŻONE"

§ 8.

Dokumenty niejawne o klauzuli „Zastrzeżone” mogą być udostępniane wyłącznie osobom, które spełniają następujące warunki:

- 1) posiadają ważne poświadczenie bezpieczeństwa upoważniające do dostępu do informacji niejawnych o klauzuli co najmniej „Zastrzeżone” lub upoważnienie Burmistrza wystawione zgodnie z art. 21 ust. 4 ustawy o ochronie informacji niejawnych,
- 2) odbyli przeszkolenie w zakresie ochrony informacji niejawnych i posiadają aktualne zaświadczenie stwierdzające odbycie tego szkolenia (nie starsze niż 5 lat od daty wystawienia),
- 3) realizują zadania, które wymagają dostępu do określonej informacji zastrzeżonej.

§ 9.

Ewidencję poświadczeń bezpieczeństwa oraz upoważnień, o których mowa w § 8 pkt 1, prowadzi Pełnomocnik Ochrony. Pracownik, który posiada poświadczenie bezpieczeństwa wydane w innej jednostce organizacyjnej, obowiązany jest do przedłożenia oryginału Pełnomocnikowi Ochrony w ciągu 5 dni od chwili poinformowania go o tym fakcie.

§ 10.

Kierownicy wydziałów Urzędu zobowiązani, są do informowania Pełnomocnika Ochrony o konieczności wydania upoważnienia przez Burmistrza pracownikom, których zakres obowiązków wymaga dostępu do dokumentów niejawnych oznaczonych klauzulą „Zastrzeżone”.

Rozdział IV

OBIEG DOKUMENTÓW I MATERIAŁÓW OZNACZONYCH KLAUZULĄ „ZASTRZEŻONE”

§ 11.

Dokumenty niejawne oznaczone klauzulą „Zastrzeżone”, wpływające do sekretariatu Urzędu za pośrednictwem Poczty Polskiej lub przesyłek kurierskich, przekazywane są kierownikowi KMN, gdzie po zarejestrowaniu w „Dzienniku ewidencji”, polegającym na spisaniu danych z koperty bez jej otwierania, przekazywane są Burmistrzowi lub innemu wskazanemu na kopercie adresatowi.

§ 12.

Pracownik sekretariatu dokonujący odbioru przesyłki zobowiązany jest sprawdzić:

- 1) prawidłowość adresu,
- 2) całość pieczęci i opakowania,
- 3) zgodność odcisku pieczęci na opakowaniu z nazwą jednostki nadawcy,
- 4) zgodność numerów na przesyłce z numerami w wykazie przesyłek nadanych lub w książce doręczeń,
- 5) odcisnąć na przesyłce pieczęć oraz wpisać datę wpływu do Urzędu.

W przypadku stwierdzenia uszkodzenia przesyłki lub śladów jej otwierania osoba kwitująca odbiór przesyłki sporządza, wraz z doręczającym, protokół uszkodzenia. Jeden egzemplarz protokołu przekazuje się nadawcy, drugi – Pełnomocnikowi Ochrony, a w przypadku, gdy w obiegu przesyłek pośredniczył przewoźnik – kolejny egzemplarz protokołu przekazuje się także jemu.

§ 13.

Kierownik odnotowuje fakt sporządzenia protokołu, o których mowa w § 12, w dzienniku ewidencji dokumentów, w rubryce „informacje uzupełniające/uwagi”.

§ 14.

Po przejęciu przesyłki od pracownika sekretariatu i otwarciu jej kierownik KMN przeprowadza następujące czynności:

1) sprawdza, czy zawartość przesyłki odpowiada wyszczególnionym na niej numerom ewidencyjnym,

2) ustala, czy liczba załączników i stron jest zgodna z liczbą oznaczoną na poszczególnych dokumentach.

W razie stwierdzenia nieprawidłowości kierownik KMN sporządza w dwóch egzemplarzach protokół z otwarcia przesyłki, zawierający opis nieprawidłowości, jeden egzemplarz przekazując do nadawcy. Fakt sporządzenia protokołu odnotowuje się w „Dzienniku ewidencji”, w rubryce „Informacje uzupełniające/Uwagi”.

§ 15.

Po przejęciu przesyłki przez kierownika i wykonaniu czynności opisanych w § 12, 13 i 14, przekazuje on przesyłkę Burmistrzowi w celu naniesienia imiennej dekretacji konkretnemu pracownikowi. Po zadekretowaniu korespondencji do konkretnej osoby, kierownik przekazuje przesyłkę za pokwitowaniem, tej osobie.

§ 16.

Na opakowaniu przesyłki, wpisuje się datę wpływu, pozycję i numer, pod którym zarejestrowano przesyłkę.

§ 17.

W przypadku wpływu do Urzędu pisma niejawnego oznaczonego „do rąk własnych”, pracownik sekretariatu przekazuje dokument kierownikowi KMN, który w dzienniku ewidencji dokumentów wpisuje nadawcę, numer i datę wpływu dokumentu. W rubryce „informacje uzupełniające/uwagi” odnotowuje, że przesyłka była oznaczona „do rąk własnych” i przekazuje ją przesyłkę adresatowi.

§ 18.

Ostateczny odbiorca przekazanego dokumentu niejawnego jest zobowiązany uzupełnić brakujące wpisy w „Dzienniku ewidencji” przez podanie kierownikowi KMN danych niezbędnych do pełnej rejestracji dokumentu.

§ 19.

W przypadku wpływu do Urzędu pisma niejawnego oznaczonego klauzulą „Zastrzeżone” – z pominięciem sekretariatu Urzędu – lub w przypadku braku przez osoby odbierające korespondencję niejawną odpowiedniego upoważnienia bądź poświadczenia bezpieczeństwa, o otrzymaniu takiej korespondencji, należy niezwłocznie powiadomić Pełnomocnika Ochrony lub kierownika KMN.

§ 20.

Kierownik KMN odmawia udostępnienia dokumentów osobie niespełniającej warunków określonych w § 8 i powiadamia o tym fakcie ostatniego dekretującego, który wskazał taką osobę – w celu zmiany dekretacji. W przypadku odmowy lub braku możliwości zmiany dekretacji kierownik KMN powiadamia o tym fakcie Pełnomocnika Ochrony.

§ 21.

W razie konieczności przekazania dokumentu innemu pracownikowi należy zwrócić go do KMN. Kierownik KMN przekazuje go zgodnie z dekretacją na dokumencie po dokonaniu właściwych zapisów w „Dzienniku ewidencji”. Zabrania się przekazywania przez pracowników Urzędu bezpośrednio sobie dokumentów zastrzeżonych, z pominięciem KMN.

§ 22.

Każdy pracownik, który zapoznał się z treścią dokumentu zastrzeżonego, dokonuje stosownej adnotacji, stwierdzającej ten fakt bezpośrednio na dokumencie.

§ 23.

Za właściwe zabezpieczenie dokumentu zastrzeżonego przed nieuprawnionym dostępem odpowiada osoba, która pobrała go z KMN.

§ 24.

Burmistrz Miasta lub osoba przez niego wyznaczona, przed rozwiązaniem stosunku pracy z pracownikiem posiadającym poświadczenie bezpieczeństwa lub upoważnienie do dostępu do informacji niejawnych o klauzuli „Zastrzeżone” przejmuje od niego protokolarnie całość materiałów posiadających klauzulę „Zastrzeżone” i wyznacza pisemnie pracownika, który ma dalej prowadzić przejętą dokumentację. Protokół sporządza się w 2 egzemplarzach – dla odchodzącego pracownika oraz dla Urzędu. Egzemplarz Urzędu przekazywany jest do KMN. O powyższym fakcie należy powiadomić Pełnomocnika Ochrony.

§ 25.

Nowy pracownik przejmuje dokumenty zgodnie z protokołem zdawczo-odbiorczym. Podstawą przekazania przejętej dokumentacji jest dekreteacja sporządzona przez Burmistrza na tym protokole.

Rozdział V

WYTWARZANIE I WYSYŁANIE DOKUMENTÓW OZNACZONYCH KLAUZULĄ „ZASTRZEŻONE”

§ 26.

Informacje niejawne oznaczone klauzulą „Zastrzeżone”, wytworzone w Urzędzie w formie dokumentu pisanego, mogą być sporządzane odręcznie, na maszynie do pisania (bez pamięci) lub na komputerze, który uzyskał akredytację bezpieczeństwa teleinformatycznego zatwierdzoną przez Burmistrza.

§ 27.

Wytwarzanie i przetwarzanie dokumentów w postaci elektronicznej oznaczonych klauzulą „Zastrzeżone” jest dopuszczalne wyłącznie na bezpiecznym stanowisku komputerowym.

§ 28.

Dokumenty o klauzuli „Zastrzeżone” są sporządzane i wykonywane przez pracownika merytorycznie odpowiedzialnego za jego opracowanie. Praca z dokumentem zastrzeżonym, w tym sporządzanie i wykonanie może odbywać się w pokoju Nr7b, mieszczącym się na parterze budynku Urzędu Miejskiego.

§ 29.

Materiały niejawne o klauzuli „Zastrzeżone”, przesyłane w postaci listów, nadaje się jako listy polecone lub wartościowe, zapakowane w dwie nieprzezroczyste mocne koperty. Materiały niejawne o klauzuli „Zastrzeżone”, przesyłane w postaci paczek, nadaje się jako paczki z zadeklarowaną wartością, opakowane w dwie warstwy nieprzezroczystego mocnego papieru.

§ 30

Szczegółowe zasady pakowania, oznaczania kopert i paczek, adresowania i przesyłania dokumentów zastrzeżonych określa rozporządzenie Prezesa Rady Ministrów z dnia 7 grudnia 2011r. w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne (Dz. U. 2011 nr 271 poz. 1603)

W przypadku konieczności zorganizowania narady, w trakcie której ustnie będą omawiane informacje oznaczone klauzulą „Zastrzeżone”, uczestnicy spotkania muszą zostać niezwłocznie poinformowani o jego niejawnym charakterze.

W spotkaniu mogą uczestniczyć wyłącznie osoby spełniające warunki, o których mowa w § 8 Instrukcji, których zakres obowiązków obejmuje sprawy omawiane na spotkaniu.

Rozdział VI

REJESTROWANIE I OZNACZANIE DOKUMENTÓW OZNACZONYCH KLAUZULĄ „ZASTRZEŻONE”

§ 32.

Wszystkie dokumenty zawierające informacje „Zastrzeżone” podlegają niezwłocznemu ewidencjonowaniu w prowadzonym przez kierownika KMN „Dzienniku ewidencji”, którego wzór określony został w załączniku nr 2 do rozporządzenia Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych, (Dz. U. 2011 nr 276 poz. 1631). Dotyczy to zarówno dokumentów wytworzonych w Urzędzie, jak i otrzymanych z zewnątrz.

§ 33.

1) Materiały zawierające informacje niejawne utrwalone w formie pisemnej, zwane dalej „pismem”, oznacza się w sposób następujący:

na każdej stronie pisma umieszcza się:

- a) na środku jako pierwszy element w nagłówku strony, klauzulę tajności,
- b) sygnaturę literowo-cyfrową, na którą składają się: literowe oznaczenie jednostki lub komórki organizacyjnej, symbol oznaczenia klauzuli tajności i numer, pod którym pismo zostało zarejestrowane w Dzienniku ewidencji, łamany przez rok lub dwie ostatnie cyfry roku, w którym pismo zostało wykonane;
- c) numer strony łamany przez liczbę stron całego pisma,
- d) na środku jako ostatni element w stopce strony, klauzulę tajności;

2) na pierwszej stronie pisma umieszcza się również:

- a) nazwę jednostki lub komórki organizacyjnej,
- b) nazwę miejscowości i datę podpisania pisma,
- c) w przypadku pisma, któremu nadano bieg korespondencyjny, nazwę stanowiska adresata oraz imię i nazwisko; w przypadku wielu adresatów dokumentu, któremu nadano bieg korespondencyjny, dopuszcza się możliwość umieszczenia jedynie adnotacji „adresaci według rozdzielnika”;

3) na ostatniej stronie pisma pod treścią umieszcza się również:

- a) liczbę załączników,
- b) liczbę stron załączników, jeżeli są dołączone do pisma,
- c) klauzule tajności załączników wraz z numerami, pod jakimi zostały zarejestrowane w Dzienniku ewidencji oraz liczbę stron każdego załącznika lub informację określającą rodzaj załączonego materiału i jego odpowiednią jednostkę miary,
- d) w przypadku, gdy adresatowi wysyła się inną liczbę załączników, niż pozostawia w aktach, dodatkowo napis „tylko adresat” – jeżeli załączniki mają być przekazane adresatowi bez pozostawiania w aktach, napis „do zwrotu” – jeżeli załączniki mają zostać zwrócone osobie uprawnionej do jego podpisania,
- e) nazwa stanowiska oraz imię i nazwisko osoby uprawnionej do jego podpisania,

2. Jeżeli przy piśmie przewodnim przesyłane są załączniki oznaczone klauzulami tajności, to:
 - 1) klauzula pisma przewodniego lub dokumentu nie może być niższa niż klauzula załącznika o najwyższym stopniu tajności;
 - 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. W przypadku opisanym powyżej, przy rejestracji pisma przewodniego w „Dzienniku ewidencji”, w rubryce „Informacje uzupełniające/Uwagi” wpisuje się adnotację o treści „(nazwa klauzuli tajności) po odłączeniu załączników” lub „Jawne po odłączeniu załączników”.

§ 34.

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

- 1) udzielanie informacji, tylko za pisemną zgodą nadawcy,
- 2) kopiowanie tylko za pisemną zgodą nadawcy,
- 3) odpis tylko za pisemną zgodą nadawcy,
- 4) kopiowanie stron od ... do... tylko za pisemną zgodą nadawcy,
- 5) odpis od ... do ... tylko za pisemną zgodą nadawcy,
- 6) wypis (wyciąg) od ... do... tylko za pisemną zgodą nadawcy.

§ 35.

Wykonanie kopii, odpisów, wyciągów, wypisów i tłumaczeń dokumentu zastrzeżonego następuje wyłącznie na podstawie pisemnego polecenia Burmistrza, odnotowanego na tym dokumencie. Czynności te realizuje osoba wskazana w dekretacji.

§ 36.

Szczegółowe zasady oznaczania materiałów niejawnych, w tym zwłaszcza dokumentów elektronicznych, oraz sporządzania kopii, odpisów, wyciągów, wypisów, tłumaczeń, a także wydruków z dokumentów elektronicznych, jak również dokumentowania tych czynności, określa rozporządzenie Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności (Dz.U. 2011 nr 288 poz. 1692).

Rozdział VII

PRZECHOWYWANIE, NISZCZENIE I ARCHIWIZOWANIE DOKUMENTÓW OZNACZONYCH KLAUZULĄ „ZASTRZEŻONE”

§ 37.

Dokumenty oznaczone klauzulą „Zastrzeżone” podlegają obowiązkowej ochronie przed kradzieżą i nieuprawnionym ujawnieniem. Dokumenty zastrzeżone przechowuje się zamknięte w Kancelarii Materiałów Niejawnych.

§ 38.

Dokumenty zastrzeżone są gromadzone przez pracowników upoważnionych do dostępu do tych informacji w teczkach akt z klauzulą „Zastrzeżone”. Dokumentów niejawnych oznaczonych klauzulą „Zastrzeżone” nie wolno przechowywać razem z dokumentami jawnymi, chyba że stanowią integralną część dokumentacji. Wówczasteczka musi zostać wyraźnie oznaczona klauzulą „Zastrzeżone”.

§ 39.

W przypadku spraw ostatecznie zakończonych, gdy dokument jest nadal chroniony,teczka akt o klauzuli „Zastrzeżone” przechowywana jest w Kancelarii Materiałów Niejawnych, do chwili zniesienia klauzuli tajności. W przypadku zniesienia klauzuli tajności Kancelaria Materiałów Niejawnych przekazuje teczkę akt do archiwum zakładowego.

§ 40.

W celu zniszczenia materiałów niejawnych oznaczonych klauzulą „Zastrzeżone”, które nie podlegają trwałemu przechowywaniu i utraciły praktyczne znaczenie, powołuje się komisję złożoną z co najmniej dwóch pracowników spełniających warunki, o których mowa w § 8 Instrukcji. W skład komisji obligatoryjnie wchodzi Kierownik Kancelarii Materiałów Niejawnych lub Pełnomocnik Ochrony. Komisja sporządza protokoły oceny dokumentacji niearchiwalnej oraz spisy dokumentacji niearchiwalnej przeznaczonej do zniszczenia. W oparciu o przygotowaną dokumentację Burmistrz występuje z wnioskiem o udzielenie zgody na zniszczenie do dyrektora właściwego archiwum państwowego.

§ 41.

Fakt zniszczenia materiałów niejawnych dokumentuje się protokolarnie oraz odnotowuje się w rubryce „Uwagi” dziennika wymienionego w § 29 Instrukcji, z adnotacją o treści „Zniszczono na podstawie protokołu z dnia”. Protokół zniszczenia przechowuje się w Kancelarii Materiałów Niejawnych.

§ 42.

Informacje niejawne oznaczone klauzulą „Zastrzeżone”, utrwalone na papierze, niszczy się przez pocięcie w niszczarce, która zapewnia zniszczenie materiału w sposób uniemożliwiający odtworzenie jego treści.

§ 43.

Szczegółowe zasady brakowania dokumentów reguluje rozporządzenie Ministra Kultury i Dziedzictwa Narodowego z dnia 20 października 2015 r. w sprawie klasyfikowania i kwalifikowania dokumentacji, przekazywania materiałów archiwalnych do archiwów państwowych i brakowania dokumentacji niearchiwalnej (Dz. U. z 2015 r. poz. 1743 z późn. zm.).

§ 44.

Informacje niejawne oznaczone klauzulą „Zastrzeżone” zapisane w formie elektronicznej niszczy się przez fizyczne zniszczenie nośnika (płyty CD/DVD itp.)

Rozdział VIII

POSTĘPOWANIE W PRZYPADKU NARUSZENIA ZASAD OCHRONY LUB UJAWNIECIA INFORMACJI OZNACZONYCH KLAUZULĄ „ZASTRZEŻONE”

§ 45.

Pracownicy Urzędu mają obowiązek powiadomić Pełnomocnika Ochrony o każdym stwierdzonym fakcie:

- 1) naruszenia bezpieczeństwa informacji oznaczonych klauzulą „Zastrzeżone”, polegającym na zaniechaniu właściwego działania lub działaniu niezgodnym z przepisami o ochronie informacji niejawnych, mogących spowodować ujawnienie tych informacji,
- 2) ujawnienia informacji oznaczonych klauzulą „Zastrzeżone” poprzez utratę, zagubienie, kradzież dokumentu lub innego przedmiotu niejawnego albo udostępnienie go osobie nieuprawnionej.

§ 46.

Pełnomocnik Ochrony powiadamia o tym fakcie Burmistrza oraz podejmuje niezwłocznie działania zmierzające do:

- 1) wyjaśnienia okoliczności naruszenia przepisów i ustalenia winnych tych naruszeń,
- 2) określenia stopnia szkody jaka może ponieść Urząd lub jej pracownicy,
- 3) zminimalizowania skutków powstałych szkód,
- 4) podjęcie działań prewencyjnych.

§ 47.

Po zakończeniu postępowania wyjaśniającego, o którym mowa w § 46, Pełnomocnik Ochrony występuje do Burmistrza o wszczęcie przeciwko osobom winnym postępowania dyscyplinarnego.

§ 48.

W stosunku do osób posiadających aktualne Poświadczenie Bezpieczeństwa, które w sposób rażący naruszyły przepisy o ochronie informacji niejawnych, Pełnomocnik Ochrony przeprowadza kontrolne postępowanie sprawdzające, z pominięciem terminów określonych w art. 33 ust. 9 i 10 ustawy o ochronie informacji niejawnych.

§ 49.

W stosunku do osób posiadających pisemne upoważnienie do dostępu do informacji niejawnych o klauzuli „Zastrzeżone”, które w sposób rażący naruszyły przepisy o ochronie informacji niejawnych, Burmistrz wydaje decyzję o cofnięciu upoważnienia w trybie określonym w k.p.a.

§ 50.

Ponadto, zgodnie z postanowieniami zawartymi w § 100 Kodeksu Pracy „pracownik jest obowiązany m.in. do zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę oraz do przestrzegania tajemnicy określonej w odrębnych przepisach.

§ 51.

Za naruszenie przepisów wymienionych w § 48 Burmistrz ma prawo zastosować jedną z poniższych kar:

- 1) karę upomnienia,
- 2) karę nagany,
- 3) karę pieniężną.

POSTANOWIENIA KOŃCOWE

§ 52.

Każdy pracownik Urzędu mający na zajmowanym stanowisku dostęp do informacji niejawnych oznaczonych co najmniej klauzulą „Zastrzeżone” jest zobowiązany zapoznać się z niniejszą Instrukcją i stosować zawarte w niej przepisy. Fakt zapoznania należy potwierdzić podpisem. Osobą odpowiedzialną za zapoznanie pracowników jest Pełnomocnik Ochrony.

§ 53.

Każdy pracownik Urzędu jest zobowiązany niezwłocznie powiadomić bezpośredniego przełożonego oraz Pełnomocnika Ochrony o wszelkich nieprawidłowościach związanych z naruszaniem zapisów niniejszej Instrukcji.

**INSTRUKCJA ALARMOWA W PRZYPADKU ZGŁOSZENIA O PODŁOŻENIU LUB
ZNALEZIENIU ŁADUNKU WYBUCHOWEGO W URZĘDZIE MIEJSKIM W
JĘDRZEJOWIE**

I. Alarmowanie

1. Osoba, która przyjęła zgłoszenie o podłożeniu ładunku wybuchowego albo zauważyła w obiekcie przedmiot niewiadomego pochodzenia mogący być ładunkiem wybuchowym jest obowiązana o tym powiadomić:
 - 1) Burmistrza,
 - 2) Komendanta Powiatowego Policji,
 - 3) Komendanta Straży Miejskiej.
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.

II. Akcja poszukiwawcza ładunku wybuchowego po uzyskaniu informacji o jego podłożeniu

1. Do czasu przybycia Policji akcją kieruje Burmistrz, a w czasie jego nieobecności, Sekretarz lub osoba przez niego upoważniona.
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 pomieszczenia 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, świecące elementy elektroniczne itp.).
3. Pomieszczenia ogólnodostępne takie jak: korytarze, klatki schodowe, hale, toalety, piwnice, 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 tych przedmiotów lub zmiany w ich wyglądzie i usytuowaniu mogły nastąpić na skutek działania sprawcy podłożenia ładunku wybuchowego. W takiej sytuacji kierujący akcją wydaje decyzję ewakuacji osób z zagrożonego obiektu przed przybyciem Policji.
6. Miejscem ewakuacji, jest teren za halą sportową Liceum Ogólnokształcącego.
7. Należy zachować spokój i opanowanie, aby nie dopuścić do przejawów paniki.

III. 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 obiekt Burmistrzowi.

IV. 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.

INSTRUKACJA POSTĘPOWANIA W PRZYPADKU OTRZYMANIA PRZESYŁKI NIEWIADOMEGO POCHODZENIA

W przypadku otrzymania jakiegokolwiek przesyłki niewiadomego pochodzenia lub budzącej podejrzenie z jakiegokolwiek innego powodu;

- brak nadawcy,
- brak adresu nadawcy,
- przesyłka pochodzi od nadawcy lub miejsca, z którego się nie spodziewamy,
- inne podejrzenia,

NIE NALEŻY JEJ OTWIERAĆ!!!

NALEŻY:

- umieścić przesyłkę w grubym worku plastikowym, szczelnie zamknąć.
- worek należy umieścić w drugim plastikowym worku, szczelnie zamkniętym, zakleić taśmą lub plastrem.
- paczki nie należy przemieszczać, należy pozostawić ją na miejscu.

POWIADOMIĆ:

- Komendę Powiatową Policji, tel. 112, 47 804 62 05
 - Komendę Powiatową Państwowej Straży Pożarnej, tel. 112, 41 386 18 95
 - Komendę Straży Miejskiej 41 386 17 87, kom 888 630 134
- 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:

- nie naruszać zawartości - nie rozsypywać, nie przenosić, nie dotykać, nie wachać, nie powodować ruchu powietrza w pomieszczeniu (wyłączyć systemy wentylacyjne, zamknąć okna),
- całą zawartość umieścić w worku plastikowym, zamknąć go i zakleić taśmą lub plastrem,
- dokładnie umyć ręce,
- zaklejony worek umieścić w drugim worku, zamknąć go i zakleić.
- ponownie umyć ręce.

POWIADOMIĆ:

- Komendę Powiatową Policji, tel. 112, 47 804 62 05
- Komendę Powiatową Państwowej Straży Pożarnej, tel. 112, 41 386 18 95
- Komendę Straży Miejskiej 41 386 17 87, kom 888 630 134

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

**WZÓR UPOWAŻNIENIA UPRAWNIAJACEGO DO DOSTĘPU DO INFORMACJI
NIEJAWNYCH OZNACZONYCH KLAUZULĄ „ZASTRZEŻONE” DLA
PRACOWNIKA ZATRUDNIONEGO W URZĘDZIE MIEJSKIM W JĘDRZEJOWIE**

.....
(Nazwa jednostki organizacyjnej)

UPOWAŻNIENIE Nr

Na podstawie art. 21 ust. 1 pkt 1 ustawy z dnia 5 sierpnia 2010r. o ochroni informacji niejawnych (Dz. U. z 2019r. poz. 742)

u p o w a ż n i a m

Pana/nią/
(imię i nazwisko, data urodzenia)

w zakresie dostępu do informacji niejawnych oznaczonych klauzulą „zastrzeżone” – występujące na zajmowanym stanowisku służbowym.
Upoważnienie jest ważne do odwołania i może być cofnięte w każdym czasie.

.....
(miejscowość i data)

mp.

.....
(Podpis i imienna pieczęć kierownika
jednostki organizacyjnej)

Jędrzejów,

.....
(nazwa komórki organizacyjnej)

WYRAŻAM ZGODĘ NA OTWARCIE
POMIESZCZENI/SZAFY/SEJFU

.....
(czytelny podpis kierownika komórki organizacyjnej)

**PROTOKÓŁ
Z KOMISYJNEGO OTWARCIA/ZAMKNIĘCIA
POMIESZCZENIA/SZAFY/SEJFU*)**

Na polecenie w dniu
o godz. komisja w składzie:
1)
2)
3)
dokonała komisyjnego otwarcia pomieszczenia/szafy/sejfu* Nr będącego w
dyspozycji
(opis pomieszczenia/szafy/sejfu)
.....
i pobrano
.....
Powyższe
..... wydano
.....
(imię i nazwisko osoby pobierającej) (czytelny podpis)

Pomieszczenie/szafę/sejf *zamknięto i zaplombowano pieczęcią numerową
Nr Klucze przekazano

Podpisy członków komisji:
.....
.....

*) niepotrzebne skreślić

**PION OCHRONY INFORMACJI NIEJAWNYCH W URZĘDZIE MIEJSKIM W
JĘDRZEJOWIE**

1. Pionem Ochrony Informacji Niejawnych kieruje Pełnomocnik ds. Ochrony Informacji Niejawnych w Urzędzie Miejskim w Jędrzejowie.
2. Skład Pionu Ochrony:
 - 1) Pełnomocnik ds. Ochrony Informacji Niejawnych;
 - 2) Kierownik Kancelarii Materiałów Niejawnych;
 - 3) Administrator Systemu Teleinformatycznego;
 - 4) Inspektor Bezpieczeństwa Teleinformatycznego.
3. Do zadań Pionu Ochrony Informacji Niejawnych należy:
 - 1) zapewnienie ochrony informacji niejawnych w tym stosowanie środków bezpieczeństwa fizycznego;
 - 2) zapewnienie ochrony systemów teleinformatycznych;
 - 3) zarządzanie ryzykiem bezpieczeństwa informacji niejawnych, w szczególności szacowanie ryzyka;
 - 4) kontrola ochrony informacji niejawnych oraz przestrzegania przepisów o ochronie tych informacji;
 - 5) okresowe kontrole ewidencji, materiałów niejawnych i obiegu dokumentów, opracowanie i aktualizowanie planu ochrony informacji niejawnych w Urzędzie Miejskim;
 - 6) organizowanie szkoleń pracowników, w zakresie ochrony informacji niejawnych.