ZARZĄDZENIE NR 36/2026
BURMISTRZA KAMIENIA KRAJEŃSKIEGO

z dnia 31 marca 2026 r.

w sprawie wprowadzenia Planu Ochrony Informacji Niejawnych w Urzędzie Miejskim w Kamieniu Krajeńskim

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2025 r. poz. 1153 ze zm.) i art. 43 ust. 5 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2025 r. poz. 1209) zarządza się, co następuje:

§ 1. Wprowadzić w Urzędzie Miejskim w Kamieniu Krajeńskim Plan Ochrony Informacji Niejawnych, stanowiący załącznik do niniejszego zarządzenia.

§ 2. Zobowiązać pracowników Urzędu Miejskiego w Kamieniu Krajeńskim do stosowania ustaleń zawartych w planie, o którym mowa w § 1.

§ 3. Powierzyć nadzór nad wykonaniem zarządzenia Pełnomocnikowi ds. Ochrony Informacji Niejawnych.

§ 4. Traci moc zarządzenie nr 68/2012 Burmistrza Kamienia Krajeńskiego z dnia 12 listopada 2012 r. w sprawie wprowadzenia Planu Ochrony Informacji Niejawnych w Urzędzie Miejskim w Kamieniu Krajeńskim.

§ 5. Zarządzenie wchodzi w życie z dniem podpisania.

Burmistrz Kamienia Krajeńskiego

Natalia Marciniak

Załącznik do
Zarządzenia nr 36/2026
Burmistrza Kamienia Krajeńskiego
z dnia 31 marca 2026 r.

URZĄD MIEJSKI W KAMIENIU KRAJEŃSKIM

PLAN OCHRONY INFORMACJI NIEJAWNYCH W URZĘDZIE MIEJSKIM W KAMIENIU KRAJEŃSKIM

Sporządził: Pełnomocnik ds. ochrony informacji niejawnych

2026 -03- 31
…… *(data)*

Pełnomocnik do spraw ochrony informacji niejawnych
Kamil Sieg
…… *(podpis)*

Zatwierdził: Burmistrz Kamienia Krajeńskiego

2026 -03- 31
…… *(data)*

BURMISTRZ
Natalia Marciniak
…… *(podpis)*

Kamień Krajeński 2026 r.

POSTANOWIENIA OGÓLNE

1. Podstawy prawne ochrony informacji niejawnych

- Ustawa z dnia 5 sierpnia 2010 r. **o ochronie informacji niejawnych** (Dz. U. z 2025 r. poz. 1209):
- Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2025 r. poz. 1691)
- 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. poz. 2334);
- Rozporządzenie Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. **w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzuli tajności** (Dz. U. z 2011 r. nr 288, poz. 1692);
- Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie wzoru świadectwa akredytacji bezpieczeństwa systemu teleinformatycznego (Dz. U. z 2011 r. nr 156, poz. 926);
- Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. **w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego** (Dz. U. z 2011 r. 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. poz. 1236);
- Rozporządzenie Prezesa Rady Ministrów z dnia 27 kwietnia 2011 r. w sprawie przygotowania i przeprowadzania kontroli stanu zabezpieczenia informacji niejawnych (Dz. U. z 2011 r. nr 93, poz. 541);
- Rozporządzenie Rady Ministrów z dnia 29 maja 2012 r. **w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych** (Dz. U. poz. 683 z późn, zm.);
- 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. poz. 1256).
- Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie wzorów poświadczeń bezpieczeństwa (t.j. Dz. U. z 2015 poz. 220);
- Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie wzoru decyzji o odmowie wydania poświadczenia bezpieczeństwa (Dz. U. z 2010 r. nr 258, poz. 1753);
- Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie wzoru decyzji o cofnięciu poświadczenia bezpieczeństwa (Dz. U. z 2010 r. 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. poz. 1103)

- Rozporządzenie Prezesa Rady Ministrów z dnia 13 stycznia 2021 r. w sprawie wysokości i trybu zwrotu zryczałtowanych kosztów ponoszonych przez Agencję Bezpieczeństwa Wewnętrznego albo Służbę Kontrwywiadu Wojskowego za przeprowadzenie sprawdzenia przedsiębiorcy oraz postępowań sprawdzających (Dz. U. poz. 84);
- 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 r. nr 220, poz. 1302);
- Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (t.j. Dz. U. z 2025 r. poz. 383 z późn. zm.);
- 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. z 2017 r. poz. 1558);
- Rozporządzenie Prezesa Rady Ministrów z dnia 7 grudnia 2011 r. **w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne** (Dz. U. z 2011 r. nr 271, poz. 1603);
- Rozporządzenie Ministra Sprawiedliwości z dnia 9 września 2017 r. w sprawie sposobu postępowania z protokołami przesłuchań i innymi dokumentami lub przedmiotami, na które rozciąga się obowiązek zachowania w tajemnicy informacji niejawnych albo zachowania tajemnicy związanej z wykonywaniem zawodu lub funkcji (Dz. U. poz. 1733).

2. Wprowadzenie

Przedmiotem ochrony w Urzędzie Miejskim w Kamieniu Krajeńskim są informacje niejawne o klauzuli „zastrzeżone".

Na podstawie art. 15 ust. 1 pkt 5 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (t.j. Dz. U. z 2025 r. poz. 1209), do obowiązków pełnomocnika ochrony informacji niejawnych należy opracowanie i aktualizowanie, wymagającego akceptacji kierownika jednostki organizacyjnej, planu ochrony informacji w jednostce organizacyjnej oraz nadzorowanie jego realizacji w razie wprowadzenia stanu nadzwyczajnego.

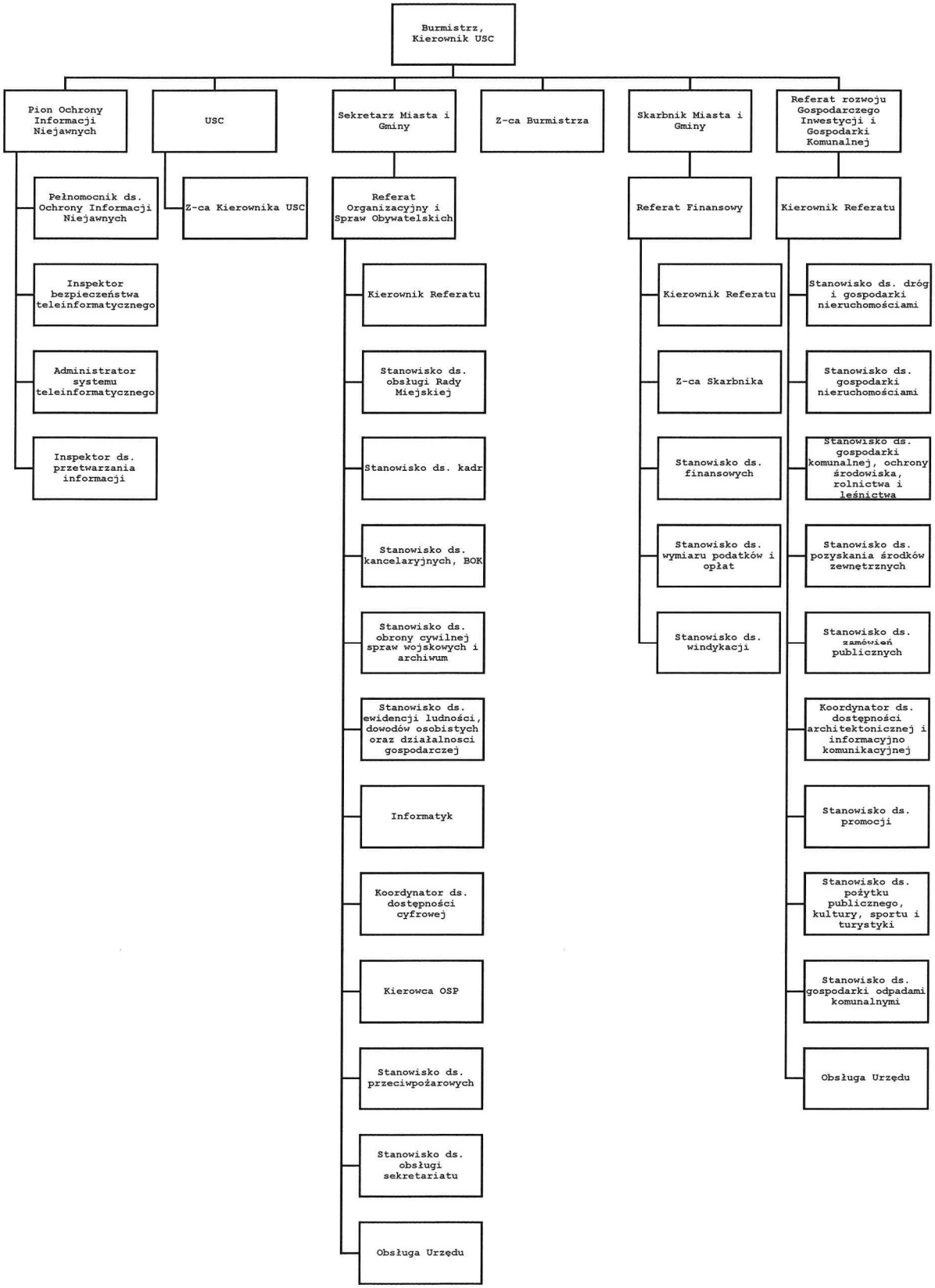
Plan ochrony informacji niejawnych jest dokumentem określającym sposób i tryb przetwarzania informacji niejawnych w podległych komórkach organizacyjnych oraz stosowanie odpowiednich środków bezpieczeństwa fizycznego w celu zapewnienia poufności, integralności i dostępności tych informacji.

Zgodnie z § 9 ust. 1 Rozporządzenia Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (Dz. U. po. 683 z późn. zm.), kierownik jednostki organizacyjnej zobowiązany jest do zatwierdzenia planu ochrony informacji niejawnych, który powinien zostać opracowany w ciągu trzech lat od dnia wejścia w życie rozporządzenia, tj. 4 lipca 2012 r.

Zakres odpowiedzialności karnej osób, które dopuściły się przestępstwa lub czynu zabronionego przeciwko ochronie informacji niejawnych został określony przepisami Kodeksu Karnego w art. 266 ustawy z dnia 6 czerwca 1997 r. Kodeks Karny (t.j. Dz. U. z 2025 r. poz. 383 z późn. zm)) i brzmi: **„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."**

Wobec pracowników, którzy nie przestrzegają wymagań związanych z ochroną informacji niejawnych, dopuszczają się uchybień w zakresie niewłaściwego zabezpieczenia dokumentów, stwarzając warunki do ujawnienia tajemnicy osobom nieuprawnionym, mogą być zastosowane sankcje służbowe i dyscyplinarne.

W Urzędzie Miejskim w Kamieniu Krajeńskim wyodrębniono pion ochrony informacji niejawnych, zwany dalej „pionem ochrony".



Rys. 1. Schemat organizacyjny Urzędu Miejskiego w Kamieniu Krajeńskim

Zgodnie z Regulaminem Organizacyjnym Urzędu do zadań Pionu ochrony informacji niejawnych należy wykonywanie czynności określonych w przepisach ustawy o ochronie informacji niejawnych oraz w przepisach wykonawczych do tej ustawy, a w szczególności:

a) zapewnienie ochrony informacji niejawnych;
b) ochrona systemów i sieci teleinformatycznych;
c) zapewnienie ochrony fizycznej Urzędu;
d) kontrola ochrony informacji niejawnych oraz przestrzegania przepisów o ochronie tych informacji;
e) okresowa kontrola ewidencji, materiałów i obiegu dokumentów;
f) opracowanie planu ochrony Urzędu i nadzorowanie jego realizacji;
g) szkolenie pracowników w zakresie ochrony informacji niejawnych.

W ramach Pionu ochrony informacji niejawnych wyodrębniono stanowiska Pełnomocnika ds. Ochrony Informacji Niejawnych, Administratora systemu teleinformatycznego oraz Inspektora bezpieczeństwa teleinformatycznego, którzy posiadają następujące zadania:

h) do zadań Pełnomocnika ds. Ochrony Informacji Niejawnych należy realizacja zadań wynikających z ustawy z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych;
i) do zadań Administratora systemu teleinformatycznego należy:
    - opracowanie szczególnych wymagań bezpieczeństwa i procedur bezpiecznej eksploatacji;
    - prowadzenie dokumentacji dotyczącej bezpieczeństwa teleinformatycznego;
    - współpraca z Pełnomocnikiem ds. Ochrony Informacji Niejawnych, Inspektorem bezpieczeństwa teleinformatycznego oraz stanowiskami pracy w Urzędzie w zakresie nadzoru nad ochroną systemu teleinformatycznego;
    - kontrola poprawności haseł dostępu do systemu, częstotliwości ich zmiany oraz przechowywania ich kopii;
    - nadzór nad wprowadzeniem zaleceń Służb Ochrony Państwa dotyczących bezpieczeństwa teleinformatycznego;
    - przestrzeganie przepisów zawartych w ustawach z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych i z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.
j) do zadań Inspektora bezpieczeństwa teleinformatycznego należy:
    - uczestniczenie w opracowaniu szczególnych wymagań bezpieczeństwa i procedur bezpiecznej eksploatacji;
    - prowadzenie dokumentacji dotyczącej bezpieczeństwa teleinformatycznego;
    - współpraca z Pełnomocnikiem ds. Ochrony Informacji Niejawnych oraz stanowiskami pracy w Urzędzie w zakresie kontroli, szkoleń i ochrony;
    - prowadzenie rejestru haseł zabezpieczających system teleinformatyczny;
    - przestrzeganie przepisów zawartych w ustawach z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych i z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, w tym przeprowadzanie okresowej kontroli systemów teleinformatycznych na poszczególnych stanowiskach pracy w Urzędzie.

3. Definicje

W niniejszym Planie używane są następujące pojęcia:

a) **Akredytacja bezpieczeństwa teleinformatycznego** – to dopuszczenie systemu lub sieci teleinformatycznej do wytwarzania, przetwarzania, przechowywania lub przekazywania informacji niejawnych, na zasadach określonych w ustawie;
b) **Burmistrz** – to Burmistrz Kamienia Krajeńskiego;
c) **Dokument** – to każda utrwalona informacja niejawna;
d) **Informacje niejawne** – to informacje, których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne, niezależnie od formy i sposobu ich wyrażania, a także w trakcie ich opracowywania;
e) **Informacje niejawne o klauzuli „zastrzeżone"** – to informacje, których nieuprawnione ujawnienie może mieć szkodliwy wpływ na wykonanie przez organy władzy publicznej lub inne jednostki organizacyjne zadań w zakresie obrony narodowej, polityki zagranicznej, bezpieczeństwa publicznego, przestrzegania praw i wolności obywateli, wymiaru sprawiedliwości albo interesów ekonomicznych Rzeczypospolitej Polskiej;
f) **Materiał** – to dokument lub przedmiot albo dowolna ich część, chronione jako informacja niejawna, a zwłaszcza urządzenie, wyposażenie lub broń wyprodukowane albo będące w trakcie produkcji, a także składnik użyty do ich wytworzenia;
g) **Pełnomocnik** – to Pełnomocnik Ochrony Informacji Niejawnych;
h) **Przetwarzanie informacji niejawnych** – to wszelkie operacje wykonywane w odniesieniu do informacji niejawnych i na tych informacjach, w szczególności ich wytwarzanie, modyfikowanie, kopiowanie, klasyfikowanie, gromadzenie, przechowywanie, przekazywanie lub udostępnianie;
i) **Rękojmia zachowania tajemnicy** – to zdolność osoby do spełnienia ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem, stwierdzona w wyniku przeprowadzenia postępowania sprawdzającego;
j) **Strefa ochronna** – to obszar np. wydzielona część budynku lub cały budynek, a także pomieszczenie wyposażone lub zabezpieczone w odpowiednie środki bezpieczeństwa fizycznego, adekwatne do klauzuli przetwarzanych informacji, w których można przetwarzać informacje niejawne;
k) **System informatyczny** – to system teleinformatyczny w rozumieniu art. 2 pkt 3 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną;
l) **Urząd** – to Urząd Miejski w Kamieniu Kajeńskim.

4. Klasyfikacja informacji niejawnych

1. Informacją niejawną w rozumieniu przepisów ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych jest informacja, której nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne.

2. Informacjom niejawnym mogą być nadane klauzule:
   a) ściśle tajne;
   b) tajne;
   c) poufne;
   d) zastrzeżone.

3. Wprowadza się następujące oznaczenia klauzul tajności dla informacji niejawnych przetwarzanych w Urzędzie Miejskim w Kamieniu Krajeńskim: **„Z"** – dla klauzuli **„zastrzeżone".**

4. Klauzule tajności nadaje osoba, która jest uprawniona do podpisania dokumentu lub oznaczenia innego niż dokument materiału. Poszczególne części materiału mogą być oznaczone różnymi klauzulami tajności.

5. Dokumenty niejawne wytworzone w Urzędzie powinny być oznaczone w sposób określony w Rozporządzeniu Prezesa Rady Ministrów z dnia 2 grudnia 2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności.

6. Sposób właściwego opisania dokumentu niejawnego został przedstawiony w załączniku do Planu Ochrony Informacji Niejawnych.

7. Zniesienie lub zmiana klauzul tajności są możliwe po wyrażeniu pisemnej zgody osoby, która nadała klauzulę. Osoba ta może określić datę lub wydarzenie, po których nastąpi zniesienie klauzuli tajności. Czynność ta może zostać dokonana wyłącznie w przypadku ustania lub zmiany ustawowych przesłanek informacji.

8. Zawyżanie lub zaniżanie klauzuli tajności jest niedopuszczalne.

9. Odbiorca materiału w przypadku stwierdzenia zawyżenia lub zaniżenia klauzuli tajności może zwrócić się do osoby, która jego nadała albo do przełożonego tej osoby z wnioskiem o dokonanie stosowanej zmiany.

10. Należy nie rzadziej niż na 3 lata dokonać przeglądu materiałów celem ustalenia, czy spełniają ustawowe przesłanki ochrony.

ŚRODKI BEZPIECZEŃSTWA

1. Przedmiot ochrony

1. Przedmiotem ochrony w Urzędzie Miejskim w Kamieniu Krajeńskim są:
a) informacje niejawne oznaczone klauzulą „zastrzeżone";
b) budynek Urzędu
c) pomieszczenie, w którym są przechowywane i opracowywane materiały niejawne tzw. kancelaria materiałów niejawnych;
d) wydzielone stanowisko komputerowe, przetwarzające informacje w systemie IT.

2. Analiza zagrożeń dla informacji niejawnych
a) Informacje niejawne muszą być chronione odpowiednio do nadanej klauzuli tajności. W tym celu należy zastosować środki bezpieczeństwa wskazane w ustawie i wydanych na jej podstawie przepisach wykonawczych.
b) W celu zapewniania właściwej ochrony informacji niejawnych przeprowadzono analizę zagrożeń dla informacji niejawnych w Urzędzie:

- **Zagrożenia zewnętrzne:**

a) Możliwość napadu przez zorganizowane grupy przestępcze i terrorystyczne, działające w sposób profesjonalny, przemyślany i zorganizowany;
b) Możliwość napadu przez pojedynczych przestępców, możliwość napadu przez przypadkowe osoby wykorzystujące nadarzającą się okazję z powodu nieprawidłowości w ochronie mienia Urzędu.

Symptomy mogące świadczyć o przygotowaniu napadu lub włamania do budynku Urzędu:
a) wzmożone zainteresowanie osób postronnych obiektem, pomieszczeniami Urzędu objawiające się m.in.: podejmowaniem prób pozyskania informacji o danym obiekcie, pomieszczeniu od pracownikówa. podczas luźnych rozmów po „przypadkowym" spotkaniu;
b) nawiązanie rozmów przez osoby postronne z pracownikami;
c) podszywanie się pod byłych pracowników Urzędu i przejawianie zainteresowania tym, co się po latach zmieniło;
d) interesowanie się osobami funkcyjnymi, w tym także ich przywarami oraz sposobem wykonywania obowiązków służbowych;
e) obserwacja sposobu działania systemu ochronnego, sekretariatu, sprzątaczki, itp.,
f) rozpoznawanie systemu technicznych zabezpieczeń, w tym stosowanych urządzeń alarmowych;
g) celowe uszkadzanie urządzeń alarmowych, linii telefonicznych, oświetlenia, itp.;
h) próby pozyskania do grup przestępczych pracowników Urzędu (dotyczy głównie osób mogących mieć problemy finansowe, towarzyskie, a także służbowe).

W związku z przedstawionymi kierunkami zagrożeń należy wykonywać następujące czynności uprzedzające ewentualne możliwości zaistnienia zagrożeń:
a) systematyczną, skrupulatną i wnikliwą kontrolę systemu ochrony przez osoby odpowiedzialne za jego organizację,
b) pracownicy pionu ochrony w czasie dnia pracy powinny zwracać szczególną uwagę na możliwość zaistnienia ewentualnych zagrożeń,

c) stosować zasadę niedopuszczenia osób niepowołanych do penetracji strefy ochrony, wykonywania prac porządkowych, remontowych, itp. w strefie ochrony wyłącznie pod nadzorem osób odpowiedzialnych.

- **Zagrożenia zewnętrzne:**

a) próby zaboru dokumentów lub mienia przez pracowników Urzędu,
b) próby powielania, kserowania dokumentów służbowych dla celów prywatnych,
c) byli pracownicy Urzędu zwolnieni dyscyplinarnie,
d) rozpoznanie organizacji pracy Urzędu celem łatwiejszej pracy grup przestępczych na ternie Urzędu,
e) próby wglądu w dokumenty niejawne przez osoby nieuprawnione,
f) spożywanie alkoholu – przesłanka do wykroczeń dyscyplinarnych i przestępstw.

W związku z przedstawionymi kierunkami zagrożeń należy wykonywać następujące czynności uprzedzające ewentualne możliwości zaistnienia zagrożeń:
a) zwracanie szczególnej uwagi na osoby, które mogą być zainteresowane zaborem dokumentu,
b) prowadzenie szczególnego nadzoru, by nie dokonywano prób kserowania, kopiowania bez zgody przełożonego,
c) uwrażliwianie pracowników w trakcie prowadzonych szkoleń na możliwość kontaktu grup przestępczych z pracownikami, którzy maja dostęp do dokumentów szczególnie ważnych,
d) zastosowanie zasady, że do informacji niejawnych mogą mieć dostęp tylko pracownicy posiadający poświadczenie bezpieczeństwa lub właściwe, upoważnienie wydane przez Burmistrza,
e) wprowadzenie szczególnej uwagi na osoby, których zachowanie wskazuje na nadmiernie spożywanie alkoholu.

2. Dostęp do informacji niejawnych

1. Zgodnie z zasadą ograniczonego dostępu informacje niejawne mogą być udostępnione wyłącznie osobie dającej rękojmię zachowania tajemnicy i tylko w zakresie niezbędnym do wykonywania przez nią pracy na zajmowanym stanowisku (tzw. Zasada „need-to-know").

2. Informacje niejawne, którym nadano klauzulę tajności „zastrzeżone", mogą być udostępnione wyłącznie:
a) osobie uprawnionej (zgodnie z przepisami ustawy dotyczącymi dostępu do określonej klauzuli);
b) w warunkach uniemożliwiających ich nieuprawnione ujawnienie.

3. Dostęp do informacji niejawnych o klauzuli **„zastrzeżone"** może uzyskać pracownik Urzędu, który uzyskał poświadczenie bezpieczeństwa oraz odbył szkolenie w zakresie ochrony informacji niejawnych. Jeżeli pracownik nie posiada poświadczenia bezpieczeństwa może on uzyskać dostęp do informacji niejawnych wyłącznie po otrzymaniu pisemnego upoważnienia przez Burmistrza oraz odbyciu szkolenia z zakresu informacji niejawnych.

4. Na pisemne polecenie Burmistrza Pełnomocnik przeprowadza zwykłe postępowanie sprawdzające wobec pracowników jednostki, którzy w związku z wykonywaną pracą

powinny mieć dostęp do ewentualnych informacji niejawnych oznaczonych klauzulą „poufne".

5. Pełnomocnik ochrony organizuje szkolenie dla osób zatrudnionych w jednostce organizacyjnej, pełniących w niej służbę lub wykonujących czynności zlecone w jednostce organizacyjnej.

6. Dopuszczenie do pracy związanej z dostępem do informacji niejawnych może nastąpić po odbyciu szkolenia w zakresie ochrony informacji niejawnych. Bez znajomości zasad, procedur, ani podstaw prawnych systemu ochrony informacji niejawnych nie jest możliwy dostęp do informacji niejawnych.

3. Strefa ochronna

1. Budynek Urzędu Miejskiego w Kamieniu Krajeńskim zlokalizowany jest przy ul. Plac Odrodzenia 3 w Kamieniu Krajeńskim.

2. Budynek Urzędu użytkowany jest wspólnie z innymi podmiotami:
a) Bank Spółdzielczy w Więcborku;
b) Biuro PZU SA;
c) Miejsko-Gminny Ośrodek Pomocy Społecznej;
d) Miejsko-Gminny Zakład Usług Oświatowych;
e) Biuro Gminnej Spółki Wodnej.

3. W związku z powyższym w Urzędzie została wyznaczona strefa ochronna w postaci kancelarii materiałów niejawnych. Kancelaria materiałów niejawnych stanowi wydzielone pomieszczenia na pierwszym piętrze Urzędu, do którego **wstęp możliwy jest wyłącznie** przez biuro inspektora ds. obrony cywilnej spraw wojskowych i archiwum.

4. Po zakończeniu pracy w budynku dostęp na 1 piętro zabezpieczane jest kratami antywłamaniowymi oraz uruchamiany jest system alarmowy.

5. W pomieszczeniu kancelarii nie ma okien. Drzwi do pomieszczenia kancelarii zabezpieczone są systemem elektromagnetycznym. Do wyznaczonej strefy prowadzona jest kontrola wejścia, wyjścia oraz przebywania w strefie (system kontroli osób).

6. W kancelarii materiałów niejawnych znajduje się szafa metalowa, w której należy przechowywać informacje niejawne oznaczone klauzulą „zastrzeżone".

7. Informacje niejawne oznaczone klauzulą „zastrzeżone" można przechowywać na stanowiskach pracy, w meblach biurowych zamykanych na klucz, w nieznanym i niedostępnym powszechnie miejscu.

8. Każdorazowo, po zakończeniu godzin pracy, pracownik ma obowiązek zabezpieczenia posiadanych materiałów oznaczonych klauzulą „zastrzeżone" poprzez umieszczenie ich w zamykanych szafach meblowych oraz zamykanie pomieszczeń bądź przekazanie ich do kancelarii materiałów niejawnych.

9. Pracownicy przechowujący materiały niejawne w pomieszczeniach służbowych udający się na urlopy, szkolenia lub w podróże służbowe mają obowiązek poinformowania o tym fakcie Pełnomocnika.

10. Budynek i znajdujące się w nim pomieszczenia stanowiące siedzibę Urzędu podlegają ochronie. Ochrona fizyczna budynku i znajdujących się w nim pomieszczeń odbywa się poprzez system alarmowy oraz zabezpieczenia fizyczne w postaci kart antywłamaniowych.

11. Kody do instalacji alarmowej do budynku Urzędu mogą posiadać: Burmistrz Kamienia Krajeńskiego oraz upoważnieni pracownicy odpowiedzialni za otworzenie i zamknięcie budynku Urzędu.

4. Procedury bezpieczeństwa dla stref ochronnych

1. Bezpieczeństwo teleinformatyczne zapewnia się chroniąc informacje przetwarzane w systemach telcinformatycznych 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 teleinformatycznym.

3. Za właściwą organizację bezpieczeństwa teleinformatycznego odpowiada Burmistrz, który w szczególności:
   a) zapewnia opracowanie dokumentacji bezpieczeństwa systemu teleinformatycznego;
   b) realizuje ochronę fizyczną systemu teleinformatycznego;
   c) zapewnia niezawodność transmisji oraz kontrolę dostępu do urządzeń systemu teleinformatycznego;
   d) dokonuje analizy stanu bezpieczeństwa teleinformatycznego oraz zapewnia usunięcia stwierdzonych nieprawidłowości;
   e) zapewnia przeszkolenie z zakresu bezpieczeństwa teleinformatycznego dla osób uprawnionych do pracy w systemie lub sieci teleinformatycznej;
   f) zawiadamia właściwą służbę ochrony państwa o zaistniałym incydencie bezpieczeństwa teleinformatycznego dotyczącym informacji niejawnych oznaczonych co najmniej klauzulą „poufne".

4. Burmistrz wyznacza:
   a) **Pełnomocnika ochrony informacji niejawnych,** który odpowiada za zapewnienie przestrzegania przepisów o ochronie informacji niejawnych m.in. poprzez zapewnienie ochrony systemów teleinformatycznych, w których są przetwarzane informacje niejawne oraz zarządzanie ryzykiem bezpieczeństwa informacji niejawnych, w szczególności szacowanie ryzyka;
   b) **Inspektora bezpieczeństwa teleinformatycznego,** tzn. pracownika pionu ochrony, odpowiedzialnego za weryfikację i bieżącą kontrolę zgodności funkcjonowania systemu teleinformatycznego ze szczególnymi wymaganiami bezpieczeństwa oraz przestrzegania procedur bieżącej eksploatacji;
   c) **Administratora systemu,** tzn. osobą niepełniącej funkcji inspektora bezpieczeństwa teleinformatycznego, odpowiedzialnego za funkcjonowanie systemu teleinformatycznego oraz za przestrzeganie zasad i wymagań bezpieczeństwa przewidzianych dla systemu teleinformatycznego.

5. Dokumentacja bezpieczeństwa systemu teleinformatycznego stanowi odrębne opracowanie.

6. Dokumentację bezpieczeństwa systemu teleinformatycznego:
   a) opracowuje się na etapie projektowania systemu;
   b) bieżąco uzupełnia na etapie wdrażania systemu;
   c) uaktualnia na etapie eksploatacji systemu.

7. Kierownik jednostki organizacyjnej udziela akredytacji bezpieczeństwa teleinformatycznego dla systemu teleinformatycznego przeznaczonego do przetwarzania informacji niejawnych o klauzuli „zastrzeżone" przez zatwierdzanie dokumentacji bezpieczeństwa systemu teleinformatycznego.

8. W ciągu 30 dni od udzielenia akredytacji bezpieczeństwa teleinformatycznego kierownik jednostki organizacyjnej przekazuje ABW dokumentację bezpieczeństwa systemu teleinformatycznego.

9. W ciągu 30 dni od otrzymania dokumentacji bezpieczeństwa systemu teleinformatycznego ABW może przedstawić kierownikowi jednostki organizacyjnej, który udzielił akredytacji bezpieczeństwa teleinformatycznego, zalecenia dotyczące konieczności przeprowadzenia dodatkowych czynności związanych z bezpieczeństwem informacji niejawnych.

10. Kierownik jednostki organizacyjnej w terminie 30 dni od otrzymania zalecenia informuje ABW o realizacji zaleceń. W szczególnie uzasadnionych przypadkach ABW może nakazać wstrzymanie przetwarzania informacji niejawnych w systemie teleinformatycznym posiadającym akredytację bezpieczeństwa teleinformatycznego.

5. Wykorzystanie urządzeń i sieci teleinformatycznej

1. System teleinformatyczny do przetwarzania informacji niejawnych mogą być wykonywane tylko materiały niejawne o klauzuli „zastrzeżone".

2. Stacja komputerowa, która znajduje się w kancelarii materiałów niejawnych nie jest połączona z systemami i sieciami teleinformatycznymi.

3. Niedopuszczalne jest wykonywanie innych pism nie zawierających klauzuli tajności.

4. Na stacji komputerowej może pracować osoba posiadająca aktualny dostęp do informacji niejawnych.

5. Po zakończeniu pracy w systemie inspektor ds. przetwarzania informacji sprawdza, czy informacje zostały właściwie zabezpieczone (zgodnie z Procedurami bezpiecznej eksploatacji).

6. Procedura zarządzania uprawnieniami do wejścia, wyjścia i przebywania w strefach ochronnych

1. Pracownik mający dostęp do kancelarii materiałów niejawnych powinien:

a) przed otwarciem drzwi sprawdzić stan zamków i zabezpieczenie drzwi;
b) sprawdzić stan zabezpieczeń szaf, sprzętu biurowego;
c) przestrzegać zasad zakazu wstępu osobom nieuprawnionym do kancelarii materiałów niejawnych.

2. Inspektor ds. przetwarzania informacji prowadzi rejestr wejść, wyjść i przebywania w kancelarii materiałów niejawnych.

3. Sprzątanie pomieszczeń, w których są przechowywane informacje niejawne powinno odbywać w obecności upoważnionego pracownika przed zakończeniem pracy.

7. Procedura zarządzania kluczami i kodami dostępu

1. Pomieszczenia, w których znajdują się informacje niejawne z klauzulą „zastrzeżone" po godzinach pracy powinno być zamykane, a klucze zabierane.

2. Komplet kluczy zapasowych należy złożyć do zdeponowania w szafie metalowej w jednym z pomieszczeń Urzędu.

3. Zabrania się wynoszenia kluczy do pomieszczeń poza teren Urzędu.

4. W razie utraty (zgubienia kluczy) do pomieszczenia kancelarii materiałów niejawnych należy niezwłocznie dokonać zmiany zamków.

PROCEDURY REAGOWANIA OSÓB ODPOWIEDZIALNYCH ZA OCHRONĘ INFORMACJI NIEJAWNYCH

1. Postępowanie z przesyłkami

1. Osobą upoważnioną do przejmowania korespondencji niejawnej wpływającej do Urzędu w formie listów czy paczek jest Pełnomocnik ochrony.

2. Listy lub paczki zawierające korespondencję niejawną mogą wpływać z zewnątrz jako przesyłki „polecone" poprzez sekretariat. Pracownik sekretariatu, po stwierdzeniu, że wewnątrz znajduje się druga koperta oznaczona klauzulą tajności, nie otwiera jej i nie rejestruje w swojej ewidencji, informując niezwłocznie Pełnomocnika ochrony o jej nadejściu.

3. Przyjmując przesyłkę sprawdza się:
   a) prawidłowość oznaczenia nadawcy i adresata;
   b) całość pieczęci i opakowania;
   c) zgodność odcisku pieczęci na opakowaniu z nazwą jednostki organizacyjnej nadawcy.

4. Korespondencji niejawnej mylnie skierowanej nie ewidencjonuje się w kancelarii niejawnej, lecz przekazuje łącznie z poprzednim opakowaniem w nowej kopercie właściwemu adresatowi za zwrotnym potwierdzeniem odbioru.

5. Pisma zawierające informacje niejawne należy załatwić bez zbędnej zwłoki.

6. Dokumenty niejawne wpływające do Urzędu podlegają ewidencjonowaniu w dzienniku korespondencji.

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

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

9. Rejestracji pism dokonuje się atramentem lub tuszem w kolorze niebieskim lub czarnym.

10. W przypadku anulowania pozycji w dzienniku ewidencji podaje się powód anulowania, umieszczając datę, imię i nazwisko oraz podpis osoby dokonującej anulowania. Anulowanie pozycji w dzienniku dokonuje się kolorem czerwonym.

11. Zabrania się wycierania, zamazywania lub nadpisywania zapisów dokonanych w dzienniku ewidencji.

12. Wysyłanie pism niejawnych odbywa się w dwóch kopertach za pośrednictwem poczty, za zwrotnym potwierdzeniem odbioru.

13. Dopuszcza się osobiste doręczenie pism niejawnych za pośrednictwem książki doręczeń przesyłek.

14. W przypadku otrzymania jakiejkolwiek przesyłki niewiadomego pochodzenia lub budzącej podejrzenia z jakiegokolwiek innego powodu np.:
    a) braku nadawcy;
    b) braku adresu nadawcy;
    c) pochodzeniu przesyłki od nadawcy lub z miejsca, z którego nie spodziewamy się:
    d) innych podejrzeń:

Nie wolno otwierać tej przesyłki!

Należy:

- umieścić przesyłkę w grubym worku plastikowym i szczelnie go zamknąć;
- worek należy umieścić w drugim plastikowym worku, szczelnie zamkniętym, zakleić taśmą lub plastrem:
- nie przemieszczać paczki (należy pozostawić ja na miejscu);
- powiadomić:
  - Komendę Powiatową Policji – nr tel. 997;
  - Komendę Powiatową Państwowej Straży Pożarnej – nr tel. 998,

Które 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 – nic rozsypywać, nie przenosić, nie dotykać, nie wąchać, 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 – nr tel. 997;
  - Komendę Powiatową Straży Pożarnej – nr tel. 998;
  - Powiatową Stację Sanitarno-Epidemiologiczną (tel. 52 388 12 30; telefon alarmowy czynny od 15:00 – 7:00 oraz w dni wolne od pracy: 606 425 137);
  - Pogotowie Ratunkowe – nr tel. 999.

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

POSTĘPOWANIE W PRZYPADKU NARUSZENIA USTAWY O OCHRONIE INFORMACJI NIEJAWNYCH I PRZEPISÓW WYKONAWCZYCH DO USTAWY

1. Za ochronę informacji niejawnych w Urzędzie odpowiada Burmistrz.

2. Zadania określone ustawą o ochronie informacji niejawnych w imieniu Burmistrza wykonuje pełnomocnik ochrony poprzez:
   a) sprawowanie nadzoru nad realizacją zadań i przestrzeganiem przepisów określonych w Planie ochrony;
   b) sprawowanie kontroli w zakresie ochrony informacji niejawnych oraz przestrzegania związanych z upoważnieniem do dostępu do tych informacji, w odniesieniu do wszystkich komórek organizacyjnych Urzędu.

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

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

5. W przypadku naruszenia przepisów o ochronie informacji niejawnych oznaczonych klauzulą „poufne" lub wyższą pełnomocnik ochrony powiadamia Burmistrza oraz właściwe służby ochrony państwa.

PLANY AWARYJNE W RAZIE WYSTĄPIENIA SYTUACJI SZCZEGÓLNYCH

Instrukcja alarmowa w przypadku zgłoszenia o podłożeniu lub znalezieniu ładunku wybuchowego w budynku urzędu

1. **Alarmowanie:**

   Osoba, która przyjęła zgłoszenie o podłożeniu ładunku wybuchowego albo zauważyła w obiekcie przedmiot niewiadomego pochodzenia mogący być ładunkiem wybuchowym jest zobowiązana o tym powiadomić:
   a) **burmistrza,**
   b) **Komendanta Powiatowego Policji.**
   zawiadamiając policję należy podać treść rozmowy ze zgłaszającym o podłożeniu ładunku wybuchowego, zwłaszcza:
      - miejsce i opis zlokalizowanego przedmiotu, który może być ładunkiem wybuchowym,
      - numer telefonu, z którego prowadzona jest rozmowa i swoje stanowisko,
      - uzyskać od policji potwierdzenie przyjętego zawiadomienia.

2. Akcja poszukiwawcza ładunku wybuchowego po uzyskaniu informacji o jego podłożeniu:
   a) do czasu przybycia policji akcją kieruje Burmistrz, a w czasie jego nieobecności Zastępca Burmistrza, Sekretarz bądź Pełnomocnik ochrony.
   b) kierujący akcją zarządza, aby użytkownicy pomieszczeń dokonali sprawdzenia, czy w tych pomieszczeniach znajdują się:
      - przedmioty, rzeczy lub urządzenia, paczki, itp., których wcześniej nie było i nie wnieśli ich użytkownicy pomieszczeń,
      - ślady przemieszczania elementów wyposażenia pomieszczeń,
      - 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.).
   c) pomieszczenia ogólnodostępne takie jak: korytarze, klatka schodowa, toalety, piwnice, itp. oraz najbliższe otoczenie zewnętrzne obiektu powinny być sprawdzone przez wyznaczonych do tego pracowników.
   d) 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 umiejscowienie należy natychmiast powiadomić Burmistrza i policję.
   e) w przypadku, gdy użytkownicy pomieszczeń faktycznie stwierdzą obecność przedmiotów (rzeczy, urządzeń), których wcześniej nie było lub zmiany w wyglądzie i usytuowaniu przedmiotów stale znajdujących się w tych pomieszczeniach, należy domniemywać, że pojawienie się tych przedmiotów lub zmiany w ich wyglądzie i usytuowaniu mogły nastąpić na skutek działania sprawcy podłożenia ładunku wybuchowego. W takiej sytuacji kierujący akcją może wydać decyzję ewakuacji osób z zagrożonego obiektu przed przybyciem policji.
   f) **należy zachować spokój i opanowanie, aby nie dopuścić do przejawów paniki.**
   g) **Współpraca z policją w czasie akcji:**

- 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.
- Policjant lub dowódca grupy interwencyjnej przejmuje kierowanie akcja, a kierujący dotychczas akcją winien udzielić mu wszechstronnej pomocy.
- na wniosek policjanta kierującego akcją Burmistrz podejmuje decyzję o ewakuacji użytkowników i innych osób z obiektu, o ile wcześniej to nie nastąpiło.
- 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.
- Policjant kierujący akcją po zakończeniu działań przekazuje protokolarne obiekt Burmistrzowi.

Osobom przyjmującym zgłoszenie o podłożeniu ładunku wybuchowego oraz Burmistrzowi nie wolno lekceważyć żadnej informacji. Każdorazowo osoby te winny zawiadomić o tym policję, która z urzędu dokona sprawdzenia wiarygodności każdego zgłoszenia.

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

POSTANOWNIA KOŃCOWE

1. Kierownicy Referatów są zobowiązani do zapoznania pracowników Urzędu z postanowieniami Planu Ochrony Informacji Niejawnych.

2. Burmistrz oraz Pełnomocnik zapewniają bieżące przestrzeganie postanowień Planu Ochrony w zakresie ochrony informacji niejawnych, mogących występować na poszczególnych stanowiskach pracy.

3. W przypadku jakichkolwiek wątpliwości o wyjaśnienia należy zwracać się do Pełnomocnika Ochrony Informacji Niejawnych.

4. W sprawach nieuregulowanych w planie ochrony mają zastosowanie odpowiednie przepisy ustawy o ochronie informacji niejawnych oraz aktów wykonawczych wydanych na jaj podstawie.

Załącznik nr 1
do Planu Ochrony Informacji
Niejawnych
w Urzędzie Miejskim
w Kamieniu Krajeńskim

Pierwsza strona dokumentu zawierającego informacje niejawne o klauzuli „zastrzeżone"

ZASTRZEŻONE

Egz. Nr .../Egzemplarz pojedynczy

.....
.....
Nazwa jednostki lub komórki organizacyjnej

.....
Sygnatura literowo-cyfrowa

Kamień Krajeński, dnia .....
Miejscowość, data podpisania dokumentu

ADRESAT
.....
.....

TREŚĆ DOKUMENTU

Nr strony/liczba stron dokumentu

ZASTRZEŻONE

Kolejna strona dokumentu zawierającego informacje niejawne o klauzuli „zastrzeżone”

ZASTRZEŻONE

Egz. Nr …/Egzemplarz pojedynczy

.....

Sygnatura literowo-cyfrowa

DALSZA TREŚĆ DOKUMENTU

Nr strony/liczba stron dokumentu

ZASTRZEŻONE

Ostatnia strona dokumentu zawierającego informacje niejawne o klauzuli „zastrzeżone"

ZASTRZEŻONE

Egz. Nr .../Egzemplarz pojedynczy

.....

Sygnatura literowo-cyfrowa

DALSZA TREŚĆ DOKUMENTU

W przypadku gdy do pisma przewodniego dołączone są załączniki:

1. Liczba załączników:
2. Liczba stron lub innych jednostek miary wszystkich załączników lub informację określają rodzaj materiału i jego odpowiednią jednostkę miary;
3. Klauzule tajności załączników wraz z numerami, pod jakim zostały zarejestrowane oraz liczba stron każdego załącznika lub informacje określające rodzaj załączonego materiału i jego odpowiednią jednostkę miary;
4. 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, napis „do zwrotu" – jeżeli załączniki mają zostać zwrócone nadawcy.

.....
Nazwa stanowiska oraz imię i nazwisko
Osoby uprawnionej do jego podpisania

5. Liczba wykonanych egzemplarzy;
6. Adresaci poszczególnych egzemplarzy albo adnotacja „adresaci według rozdzielnika";
7. Dyspozycje „ad acta" w przypadku egzemplarza pozostawionego w aktach nadawcy;
8. Nazwisko osoby, która wykonała dokument.

Nr strony/liczba stron dokumentu

ZASTRZEŻONE

Uzasadnienie

do zarządzenia Nr 36/2026 Burmistrza Kamienia Krajeńskiego z dnia 31 marca 2026 r. w sprawie wprowadzenia Planu Ochrony Informacji Niejawnych w Urzędzie Miejskim w Kamieniu Krajeńskim

Jednostka organizacyjna, w której są przetwarzane informacje niejawne zobowiązana jest do opracowania oraz aktualizowania planu ochrony informacji niejawnych, a także nadzorowania jego realizacji w razie wprowadzenia stanu nadzwyczajnego. Powyższe należy do zadań pełnomocnika ochrony informacji niejawnych jednostki organizacyjnej, który realizuje swoje zadania przy pomocy wyodrębnionego pionu ochrony.