

67

Zarządzenie nr 13/2013

**Starosty Grudziądzkiego
z dnia 26 sierpnia 2013 r.**

**w sprawie wprowadzenia i zatwierdzenia „Planu Ochrony Informacji
Niejawnych w Starostwie Powiatowym w Grudziądzu”**

Na podstawie art. 15 ust. 1 pkt 5 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2010 r. Nr 182, poz.1228) i § 9 Rozporządzenia Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych (Dz. U. z 2012, poz.683) zarządzam co następuje:

§ 1

Zatwierdzam i wprowadzam do stosowania „Plan Ochrony Informacji Niejawnych w Starostwie Powiatowym w Grudziądzu”, stanowiący załącznik Nr 1 do niniejszego zarządzenia.

§ 2

Zatwierdzam dokumentację określającą poziom zagrożeń dla systemu ochrony informacji niejawnych w Starostwie Powiatowym w Grudziądzu, stanowiącą załącznik Nr 2 do niniejszego zarządzenia.

§ 3

Nadzór nad realizacją postanowień niniejszego zarządzenia powierzam Pełnomocnikowi ds. Ochrony Informacji Niejawnych w Starostwie Powiatowym w Grudziądzu.

§ 4

Traci moc: „Plan Ochrony Informacji Niejawnych w Starostwie Powiatowym w Grudziądzu” wprowadzony w 2011 roku.

§ 5

Zarządzenie wchodzi w życie z dniem podpisania.


STAROSTA
Marek Szczepanowski

Nr 13/2013 z dnia 26 sierpnia 2013 r.

STAROSTWO POWIATOWE W GRUDZIĄDZU

ZATWIERDZAM

STAROSTA

Marek Szczepanowski

**PLAN OCHRONY
INFORMACJI NIEJAWNYCH
W STAROSTWIE POWIATOWYM
W GRUDZIĄDZU**

OPRACOWAŁ:

PEŁNOMOCNIK
ds. Ochrony Informacji Niejawnych

Piotr Jankowski
mgr Piotr Jankowski

Grudziądz - sierpień 2013 r.

Spis treści:

1. Podstawy prawne ochrony informacji niejawnych.
2. Definicje związane z Ochroną Informacji Niejawnych.
3. Przedmiot ochrony i klasyfikacja informacji niejawnych.
4. Ocena zagrożeń zewnętrznych i wewnętrznych
5. Opis stref ochronnych.
6. Ochrona fizyczna
7. Zasady wykonywania i przetwarzania dokumentów niejawnych.
8. Dostęp do informacji niejawnych
9. Wykonywanie dokumentów zawierających informacje niejawne za pomocą komputera.
10. Postępowanie z przesyłkami zawierającymi informacje niejawne
11. Nadzór w zakresie ochrony informacji niejawnych
12. Odpowiedzialność karna, dyscyplinarna lub służbowa za naruszenie przepisów o ochronie informacji niejawnych.
13. Gospodarka kluczami i pieczęciami.
14. Ochrona informacji niejawnych w razie wystąpienia sytuacji szczególnych, w tym wprowadzenia stanów nadzwyczajnych.

1. Podstawy prawne Ochrony Informacji Niejawnych.

Plan Ochrony Informacji Niejawnych w Starostwie Powiatowym w Grudziądzu określa zasady i tryb postępowania z informacjami niejawnymi oraz zapewnia jednolity sposób postępowania z tymi informacjami w Urzędzie.

Plan Ochrony Informacji Niejawnych w Starostwie Powiatowym w Grudziądzu przygotowany został zgodnie z ustawą z dnia 5 sierpnia 2010r. o ochronie informacji niejawnych (Dz. U. 2010.182.1228) oraz § 9 rozporządzenia Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (Dz. U. z 2012 r. poz. 683).

2. Definicje związane z Ochroną Informacji Niejawnych.

a/ rękojmnią zachowania tajemnicy – jest zdolność osoby do spełnienia ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem, stwierdzona w wyniku przeprowadzenia postępowania sprawdzającego,

b/ dokumentem – jest każda utrwalona informacja niejawna,

c/ materiałem – jest dokument lub przedmiot albo dowolna ich część, chronione jako informacja niejawna, a zwłaszcza urządzenie, wyposażenie lub broń wyprodukowane albo będące w trakcie produkcji, a także składnik użyty do ich wytworzenia,

d/ systemem teleinformatycznym – jest system w rozumieniu art. 48 ust.1 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych,

e/ akredytacją bezpieczeństwa teleinformatycznego – jest dopuszczenie systemu teleinformatycznego do wytwarzania, przetwarzania informacji niejawnych,

f/ przetwarzaniem informacji niejawnych - są wszelkie operacje wykonywane w odniesieniu do informacji niejawnych i na tych informacjach, w szczególności ich wytwarzanie, modyfikowanie, kopiowanie, klasyfikowanie, gromadzenie, przechowywanie, przekazywanie lub udostępnianie,

g/ dokumentacją bezpieczeństwa systemu – są Szczególne wymagania bezpieczeństwa oraz Procedury bezpiecznej eksploatacji danego systemu teleinformatycznego, sporządzone zgodnie z zasadami, określonymi w ustawie z dnia 5 sierpnia 2010r. o ochronie informacji niejawnych,

h/ ryzykiem – jest kombinacja prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji,

i/ **szacowaniem ryzyka** – jest całościowy proces analizy i oceny ryzyka,

j/ **zarządzaniem ryzykiem** – są skoordynowane działania w zakresie zarządzani

3. Przedmiot ochrony i klasyfikacja informacji niejawnych.

1. Przedmiotem ochrony w Starostwie Powiatowym w Grudziądzu, zwanym dalej „Urzędem”, są:
 - a) informacje niejawne oznaczone klauzulą „poufne” – występujące w zakresie działania Urzędu,
 - b) informacje niejawne oznaczone klauzulą „zastrzeżone” – występujące w zakresie działania Urzędu.
2. Informacjom niejawnym nadaje się klauzulę „zastrzeżone”, jeżeli nie nadano im wyższej klauzuli tajności, a ich nieuprawnione ujawnienie może mieć szkodliwy wpływ na wykonywanie zadań przez Urząd.
3. Klauzulę tajności nadaje Starosta lub osoba uprawniona do podpisania dokumentu lub oznaczenia innego niż dokument materiału.
4. Do ujednolicenia kwalifikowania informacji wymagających nadania klauzuli tajności oraz ustawowej ochrony danych ustala się wykaz informacji, którym może lub powinna być nadana klauzula tajności. Wykaz ten wymaga aktualizowania w systemach półrocznych.
5. Informacje niejawne oznaczone klauzulą tajności podlegają ochronie do czasu zniesienia klauzuli tajności.

Informacjom niejawnym nadaje się następujące klauzule:

- 1) Informacjom niejawnym nadaje się klauzulę „**poufne**”, jeżeli ich nieuprawnione ujawnienie spowoduje szkodę dla Rzeczypospolitej Polskiej przez to, że:
 - Utrudni prowadzenie bieżącej polityki zagranicznej Rzeczypospolitej Polskiej;
 - Utrudni realizację przedsięwzięć obronnych lub negatywnie wpłynie na zdolność bojową Sił Zbrojnych Rzeczypospolitej Polskiej;
 - Zakłóci porządek publiczny lub zagrazi bezpieczeństwu obywateli;
 - Utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za ochronę bezpieczeństwa lub podstawowych interesów Rzeczypospolitej Polskiej;
 - Utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za ochronę porządku publicznego, bezpieczeństwa obywateli lub ściganie sprawców przestępstw i przestępstw skarbowych oraz organom wymiaru sprawiedliwości;
 - Zagrazi stabilności systemu finansowego Rzeczypospolitej Polskiej;

- Wpływie niekorzystnie na funkcjonowanie gospodarki narodowej.

2) Informacjom niejawnym nadaje się klauzulę „zastrzeżone”, jeżeli są to informacje, którym nie nadano wyższej klauzuli tajności, a ich nieuprawnione ujawnienie może mieć szkodliwy wpływ na wykonywanie przez organy władzy publicznej lub inne jednostki organizacyjne zadań z zakresu obrony narodowej, polityki zagranicznej, bezpieczeństwa publicznego, przestrzegania praw i wolności obywateli, wymiaru sprawiedliwości albo wykonywania przez nią pracy na zajmowanym stanowisku albo wykonywania czynności zleconych.

4. Ocena zagrożeń zewnętrznych i wewnętrznych.

1. Zagrożeniami zewnętrznymi dla Starostwa Powiatowego w Grudziądzu są:

- 1) możliwość napadu przez elementy obcych służb specjalnych,
- 2) możliwość zorganizowania zamachu terrorystycznego,
- 3) możliwość napadu przez pojedyncze osoby wykorzystujące nadarzającą się okazję z powodu nieprawidłowości w ochronie urzędu,
- 4) kradzież lub zniszczenie materiałów,
- 5) wystąpienie zdarzeń kryzysowych lub klęski żywiołowej,
- 6) zakłócenia w komunikacji i zasilaniu.

2. Zagrożeniami wewnętrznymi dla Starostwa Powiatowego w Grudziądzu są:

- 1) próba wejścia osoby nieuprawnionej do pomieszczenia „Kancelarii”
- 2) próby powielania, kserowania dokumentów służbowych dla celów prywatnych,
- 3) nieuprawniony dostęp do informacji o wyższej klauzuli tajności nie wynikającym z posiadanych uprawnień,
- 4) próby wglądu w dokumenty niejawne przez osoby nieuprawnione,
- 5) zaniedbania personelu,
- 6) awarie sprzętu.

5. Opis stref ochronnych.

Obiekt jednostki organizacyjnej czyli Starostwa Powiatowego w Grudziądzu to trzykondygnacyjny samodzielnie stojący budynek, w którym znajdują się pomieszczenia Starostwa Powiatowego w Grudziądzu, obiekt położony jest w centrum miasta. Przed i za budynkiem Urzędu znajdują się dwa ogólnie dostępne parkingi przylegające bezpośrednio do budynku. Dostęp do budynku jest monitorowany przez system kamer.

Strefę ochronną I stanowi wydzielone pomieszczenie nr 29 na drugim piętrze, w którym jest zorganizowana „Kancelaria dokumentów niejawnych”. Nie przyjmuje się tu żadnych interesantów i nie ma tu stanowisk pracy dla urzędników. W pomieszczeniu tym jest również zorganizowane stanowisko TI do opracowywania dokumentów systemem komputerowym.

Wszystkie osoby nie związane z pionem ochrony oraz z systemem TI są rejestrowane w „Rejestrze osób przebywających w strefie ochronnej”.

Wejście do „Kancelarii dokumentów niejawnych” zabezpieczone jest kratą zamykaną na 2 kłódki oraz drzwiami w wykonaniu antywłamaniowym. Ściany trwałe, niepalne, okno zabezpieczone kratą i roletą zabezpieczającą przed wglądem. Korytarz jest zabezpieczany po godzinach pracy przez pracownika ochrony, który zamyka metalową kratę chroniącą dostęp do pomieszczeń służbowych.

Obiekt jest chroniony przed dostępem osób nieuprawnionych w sposób określony w instrukcji ochrony posiadanej przez agencję ochroniarską „ALFA”. Wyszpecyfikowane są wszystkie newralgiczne miejsca i punkty w ochronie obiektu. Opisana jest organizacja i sposób ochrony obiektu przez służbę ochrony. Podane są zasady i sposób kontroli ruchu osobowego.

Do instrukcji ochrony dołączone są:

zasady zdawania, przechowywania i wydawania kluczy oraz ich duplikatów, umożliwiających dostęp do pomieszczeń służbowych i takie same zasady dotyczące

Kancelarię dokumentów niejawnych otwiera i zamyka oraz plombuje kierownik kancelarii.

W przypadku nieobecności kierownika kancelarii, a kiedy wystąpi konieczność opracowania dokumentu niejawnego, procedura odbywa się w następujący sposób. Drzwi do pomieszczenia za pomocą klucza zapasowego otwiera pełnomocnik OIN wraz z osobą uprawnioną i wykonuje potrzebne czynności sporządzając na oddzielnej kartce notatkę. Po zakończeniu pracy wykonawca z pełnomocnikiem OIN, zabezpieczają dokumenty i zamykają pomieszczenie.

75

Klucze użytku bieżącego do pokoju z systemem TI są przechowywane w zaplombowanym woreczku u kierownika kancelarii, w kancelarii kadr (pokój nr 22).

Komplet kluczy zapasowych znajduje się w kasie kluczy zapasowych przechowywanych w pomieszczeniu ochrony budynku Starostwa Powiatowego.

6. Ochrona fizyczna.

1. Dokumenty lub materiały niejawne oznaczone klauzulą „**poufne**” wytworzone w Urzędzie oraz wpływające do Starostwa Powiatowego należy przechowywać w Kancelarii dokumentów niejawnych. Dokumenty lub materiały niejawne o klauzuli „poufne” muszą zostać zabezpieczone przez Kierownika kancelarii zgodnie z przepisami ustawy o ochronie informacji niejawnych, w szafie metalowej klasy A posiadającej odpowiednie zamknięcie oraz zaplombowanej pieczęcią.

2. W uzasadnionych przypadkach podyktowanych względami dłuższego okresu czasu, niezbędnego do wykonania zadań związanych z dostępem do informacji niejawnych, dokumenty lub materiały o klauzuli „poufne” mogą być wydawane poza pomieszczenie Kancelarii za zgodą Starosty.. Odbywa się to pod warunkiem, że odbiorca dokumentu lub materiału zapewni warunki ochrony tych dokumentów określone w ust. 1, tj. zapewni ich przechowanie w szafach metalowych klasy „A” z odpowiednim zamknięciem oraz możliwością zaplombowania.

3. Szafy metalowe, w których przechowuje się dokumenty o klauzuli „poufne” po zakończeniu pracy należy zamknąć, zaplombować pieczęcią i sprawdzić sposób ich zabezpieczenia.

4. Informacje niejawne oznaczone klauzulą „**zastrzeżone**” mogą być przechowywane w Kancelarii dokumentów niejawnych, lub na stanowiskach pracy, w meblach biurowych zamykanych na klucz. W przypadku przechowywania dokumentów lub materiałów „zastrzeżonych” poza pomieszczeniem Kancelarii dokumentów niejawnych, odnotowywane jest to w odpowiednich Dziennikach znajdujących się w posiadaniu Kierownika kancelarii. Pozwala to na ustalenie w każdym momencie, w jakim miejscu znajduje się w danej chwili materiał lub dokument zawierający informacje niejawne.

5. Budynek i znajdujące się w nim pomieszczenie Kancelarii dokumentów niejawnych podlegają ochronie. Poza godzinami służbowymi i w dniach wolnych od pracy budynek jest ochraniały przez profesjonalną służbę ochrony.

6. Pomieszczenia Kancelarii dokumentów niejawnych po zakończeniu pracy zostają zamknięte na dwa zamki zamontowane w drzwiach obitych blachą i zabezpieczone kratą metalową zamykaną na dwie kłódki oraz zaplombowane.

7. Zasady wykonywania i przetwarzania dokumentów niejawnych.

7.1 Dokumenty o klauzuli „poufne”.

7.1.1 Wymagania dotyczące dokumentów i materiałów oznaczonych klauzulą „POUFNE”:

1. System obiegu dokumentów ma zapewnić możliwość ustalenia w każdych okolicznościach, gdzie znajduje się materiał lub dokument zawierający IN.
2. Materiał lub dokument zawierający IN może być przekazywany poza Urząd wyłącznie za pośrednictwem „Kancelarii dokumentów niejawnych”.
3. Dostęp do IN może nastąpić pod warunkiem posiadania odpowiedniego PB oraz po odbyciu szkolenia w zakresie ochrony IN.
4. Dostęp do IN może być przyznawany tylko w zakresie niezbędnym do wykonywania obowiązków na zajmowanym stanowisku.

7.1.2 Minimalne warunki dotyczące przetwarzania informacji niejawnych oznaczonych klauzulą „POUFNE”:

1. Zakres stosowania środków bezpieczeństwa fizycznego określa POIN.
2. Na terenie Urzędu obowiązuje zakaz stosowania sprzętu teleinformatycznego do wytwarzania IN oznaczonych klauzulą „POUFNE”. Ww. sprzęt, w szczególności komputery wraz z urządzeniami peryferyjnymi (tj.: drukarka, skaner) może być wykorzystany do wytwarzania oprawy graficznej dokumentu lub materiału. Treść IN musi zostać naniesiona przy użyciu technik innych niż cyfrowe (np.: odręcznie lub przy użyciu maszyny do pisania nieposiadającej pamięci wewnętrznej).
3. IN oznaczone klauzulą „POUFNE” w Urzędzie powinny być przetwarzane w Kancelarii dokumentów niejawnych.
4. Kancelarią kieruje Kierownik kancelarii dokumentów niejawnych. Przekazywanie obowiązków na stanowisku kierownika następuje na podstawie protokołu zdawczo – odbiorczego, w obecności PO lub jego zastępcy, osoby zdającej i osoby przyjmującej obowiązki.
5. Przy udostępnianiu IN w dowolnej postaci obowiązuje zasada wiedzy niezbędnej przy spełnieniu warunku „bezpieczeństwo osobowe”.

- 79
6. Dokumenty udostępniane są na podstawie dekretacji odręcznej na dokumencie.
 7. Dekretacji może dokonać Starosta lub inna osoba przez niego upoważniona.
 8. O zakresie udostępnienia decydują osoby, o których mowa w pkt. 7.
 9. IN oznaczone klauzulą „POUFNE” w UM są ewidencjonowane i przechowywane w Kancelarii dokumentów niejawnych.
 10. Zasady tworzenia i gromadzenia akt w Starostwie Powiatowym określa Rozporządzenie Prezesa Rady Ministrów z dnia 18.01.2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz.U. z 2011 r. poz. 14 nr 67).
 11. IN przechowuje się w szafie metalowej. Szczegółowe wymagania określa POIN.
 12. Po zakończeniu pracy Kierownik kancelarii zamyka i zabezpiecza urządzenia do przechowywania IN oraz zabezpiecza pomieszczenia Kancelarii.
 13. Zasady dotyczące zarządzaniem kluczami i kodami do KT oraz kluczami i kodami zapasowymi do KT określa POIN.

7.1.3 Zasady przekazywania materiałów i dokumentów niejawnych oznaczonych klauzulą „POUFNE”:

1. Zasady i tryb nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających IN reguluje Rozporządzenie Prezesa Rady Ministrów z dnia 07.12.2011 r. w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne (Dz.U. z 2011 r. poz. 271 nr 1603).
2. Przewóz materiałów zawierających IN o klauzuli „poufne” w celu nadania za pośrednictwem Poczty Specjalnej realizuje Kierownik kancelarii dokumentów niejawnych wykorzystując do tego celu samochód służbowy..
3. Podczas przewożenia obowiązuje zasada optymalnej drogi, przez którą należy rozumieć drogę najkrótszą, ale możliwie najbezpieczniejszą, dającą możliwość dostarczenia materiału w najkrótszym czasie.
4. Podczas przewożenia lub przenoszenia materiałów niejawnych oznaczonych klauzulą „POUFNE” należy zachować wszelkie środki ostrożności, aby nie doprowadzić do kradzieży, utraty lub zniszczenia materiału.

W szczególności zabrania się:

- pozostawiania materiału bez nadzoru,
- przekazywania go osobom postronnym,

- 87
- wyjmowania z teczki (lub innego opakowania) na trasie przejazdu.

7.1.4 Sposoby i miejsca wytwarzania, kopiowania i skanowania dokumentów niejawnych oznaczonych klauzulą „POUFNE”:

1. Dokumenty oznaczone klauzulą „POUFNE” mogą być wytwarzane w UM wyłącznie poprzez kreślenie, pismo odręczne, wypełnianie formularzy lub przy użyciu mechanicznej maszyny do pisania.
2. Zabrania się przetwarzania IN oznaczonych klauzulą „POUFNE” w systemach teleinformatycznych (na komputerach) ze względu na brak stosownej akredytacji bezpieczeństwa teleinformatycznego.
3. Dokumenty, o których mowa w pkt. 1 należy sporządzać w ściśle określonej liczbie egzemplarzy i rozsyłać do adresatów na podstawie rozdzielnika pozostającego w aktach (w przypadku małej liczby adresatów rozdzielnik umieszczany jest na dokumencie).
4. Liczbę wykonanych egzemplarzy oraz zasięg ich obiegu ogranicza się do minimum niezbędnego do realizacji zadań służbowych, w miarę możliwości wykorzystując inne możliwości załatwienia sprawy.
5. Wytworzone dokumenty wykonawca techniczny ewidencjonuje w Dzienniku Ewidencji prowadzonym w Kancelarii dokumentów niejawnych oraz oznacza w sposób określony w Rozporządzeniu Prezesa Rady Ministrów z dnia 22.12.2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności (Dz.U. z 2011 r. poz. 288 nr 1692).
6. Na wykonanie kopii wymaga się uzyskania zgody osoby, która jest upoważniona do podpisania dokumentu lub oznaczenia innego niż dokument materiału.
7. Wszystkie kopie podlegają ewidencji w Dzienniku Ewidencji prowadzonym w Kancelarii.
8. Kopie wykonuje się na maszynie do pisania nieposiadającej pamięci kopiowanych stron.
9. Zabrania się skanowania oraz skanowania w celu sporządzenia kopii dokumentów niejawnych przy użyciu komputerów.

7.2 Dokumenty o klauzuli „zastrzeżone”.

7.2.1 Wymagania dotyczące dokumentów i materiałów oznaczonych klauzulą „ZASTRZEŻONE”:

1. System obiegu dokumentów ma zapewnić możliwość ustalenia w każdych okolicznościach, gdzie znajduje się materiał lub dokument zawierający IN.
2. Materiał lub dokument zawierający IN może być przekazywany poza Urząd za pośrednictwem Kancelarii dokumentów niejawnych.
3. Dostęp do IN oznaczonej klauzulą „ZASTRZEŻONE” może nastąpić pod warunkiem posiadania stosownego upoważnienia lub PB oraz po odbyciu szkolenia w zakresie ochrony IN.
4. Dostęp do IN może być przyznawany tylko w zakresie niezbędnym do wykonywania obowiązków na zajmowanym stanowisku.

7.2.2 Minimalne warunki dotyczące przetwarzania informacji niejawnych oznaczonych klauzulą „ZASTRZEŻONE”:

1. Zakres stosowania środków bezpieczeństwa fizycznego określa POIN.
2. Ewidencję materiałów zawierających IN oznaczonych klauzulą „ZASTRZEŻONE” prowadzi Kancelaria dokumentów niejawnych.
3. Pracownik, który pokwitował odbiór dokumentu z Kancelarii staje się jego dysponentem i jest za niego odpowiedzialny.
4. Na terenie Urzędu możliwe jest przetwarzanie IN oznaczonych klauzulą „ZASTRZEŻONE” przy użyciu sprzętu teleinformatycznego. Tryb i zasady korzystania ze sprzętu teleinformatycznego na potrzeby przetwarzania IN regulują SWB i PBE.
5. IN oznaczone klauzulą „ZASTRZEŻONE” w Urzędzie mogą być, z zastrzeżeniem pkt. 4, przetwarzane we wszystkich pomieszczeniach pod warunkiem zastosowania środków bezpieczeństwa wykluczających możliwość podglądu z zewnątrz lub możliwość wglądu w treść IN spowodowanym wejściem osób nieuprawnionych do tego pomieszczenia.
6. Pracą Kancelarii dokumentów niejawnych kieruje Kierownik kancelarii. Przekazywanie obowiązków na stanowisku Kierownika kancelarii następuje na podstawie protokołu zdawczo – odbiorczego, w obecności PO, osoby zdającej i osoby przyjmującej obowiązki.

7. Obowiązki Kierownika kancelarii określa Rozporządzenie Rady Ministrów z dnia 07.12.2011 r. w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych (Dz.U. z 2011 poz. 276 nr 1631).
8. Przy udostępnianiu IN w dowolnej postaci obowiązuje zasada wiedzy niezbędnej przy spełnieniu warunku „bezpieczeństwo osobowe”.
9. Dokumenty udostępniane są na podstawie dekretacji odręcznej na dokumencie.
10. Dekretacji może dokonać starosta lub inna osoba przez niego upoważniona.
11. O zakresie udostępnienia decydują ww. osoby.
12. W uzasadnionych przypadkach dyspozycja dotycząca udostępnienie IN może zostać wyrażonego na odrębnym dokumencie. Zasady, o których mowa w pkt. 9 i 10, mają odpowiednio zastosowanie.
13. Kierownik kancelarii odmawia udostępnienia lub wydania materiału osobie nieuprawnionej.

7.2.3 Miejsca ewidencji, gromadzenia i przechowywania materiałów i dokumentów niejawnych oznaczonych klauzulą „ZASTRZEŻONE”

1. IN oznaczone klauzulą „ZASTRZEŻONE” w Urzędzie są ewidencjonowane i przechowywane w Kancelarii dokumentów niejawnych.
2. W uzasadnionych przypadkach przechowywanie możliwe jest poza Kancelarią pod warunkiem zapewnienia minimalnych środków bezpieczeństwa.
3. Przed końcem pracy Urzędu IN są zwracane do miejsca składowania.
4. Zasady tworzenia i gromadzenia akt w Urzędzie określa Rozporządzenie Prezesa Rady Ministrów z dnia 18.01.2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz.U. z 2011 r. poz. 14 nr 67).
5. IN oznaczone klauzulą „ZASTRZEŻONE” przechowuje się w szafie zamykanej na klucz. Szczegółowe wymagania określa POIN.
6. Po zakończeniu pracy dysponent zamyka i zabezpiecza urządzenia do przechowywania IN oraz zabezpiecza pomieszczenia.
7. Zasady dotyczące zarządzaniem kluczami i kodami do drzwi i zamków, w których przechowywane są IN określa POIN.

7.2.4 Zasady przekazywania materiałów i dokumentów niejawnych oznaczonych klauzulą „ZASTRZEŻONE”

- 87
1. Zasady i tryb nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających IN reguluje Rozporządzenie Prezesa Rady Ministrów z dnia 07.12.2011 r. w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne (Dz.U. z 2011 r. poz. 271 nr 1603).
 2. Wydanie materiałów zawierających IN poza Kancelarię dokumentów niejawnych odbywa się za pokwitowaniem w stosownej ewidencji. W uzasadnionych przypadkach dopuszcza się pokwitowania odbioru w innej formie o ile umożliwi ono zlokalizowanie wydanego materiału w razie niezwrócenia tego materiału przez odbiorcę.
 3. Przekazywanie materiałów zawierających IN oznaczonych klauzulą „ZASTRZEŻONE” poza Urząd realizowane jest za pismem poleconym, za zwrotnym potwierdzeniem odbioru, za pośrednictwem jednostek zewnętrznych, realizujących na rzecz Starostwa Powiatowego usługi dostarczania przesyłek na podstawie odrębnych umów.
 4. Podczas przewożenia lub przenoszenia materiałów niejawnych oznaczonych klauzulą „ZASTRZEŻONE” należy zachować wszelkie środki ostrożności, aby nie doprowadzić do kradzieży, utraty lub zniszczenia materiału. W szczególności zabrania się:
 - . pozostawiać materiału bez nadzoru,
 - . przekazywać go osobom postronnym,
 - . wyjmować z teczki (lub innego opakowania) na trasie przejazdu,

7.2.5 Sposoby i miejsca wytwarzania, kopiowania i skanowania dokumentów niejawnych oznaczonych klauzulą „ZASTRZEŻONE”

1. Dokumenty zawierające IN należy sporządzać w ściśle określonej liczbie egzemplarzy i rozsyłać do adresatów na podstawie rozdzielnika pozostającego w aktach (w przypadku małej liczby adresatów rozdzielnik umieszczany jest na dokumencie).
2. Liczbę wykonanych egzemplarzy oraz zasięg ich obiegu ogranicza się do minimum niezbędnego do realizacji zadań służbowych, w miarę możliwości wykorzystując inne możliwości załatwienia sprawy.
3. Wytworzone dokumenty wykonawca techniczny ewidencjonuje w Dzienniku Ewidencji prowadzonym w Kancelarii dokumentów niejawnych oraz oznacza w sposób określony w Rozporządzeniu Prezesa Rady Ministrów z dnia 22.12.2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności (Dz.U. z 2011 r. poz. 288 nr 1692).
4. Na wykonanie kopii wymaga się uzyskania zgody osoby, która jest upoważniona do podpisania dokumentu lub oznaczenia innego niż dokument materiału.

5. Wszystkie kopie podlegają ewidencji w Dzienniku Ewidencji prowadzonym w Kancelarii dokumentów niejawnych.
6. Kopie wykonuje się na maszynach kserograficznych nieposiadających pamięci kopiowanych stron.
7. Zabrania się skanowania oraz skanowania w celu sporządzenia kopii dokumentów niejawnych przy użyciu komputerów.

7.2.6 Zasady i sposoby niszczenia materiałów i dokumentów niejawnych oznaczonych klauzulą „ZASTRZEŻONE”

1. Dokumenty oznaczone klauzulą „ZASTRZEŻONE” podlegają niszczeniu komisijnemu.
2. Zezwolenie na zniszczenie materiałów niejawnych zakwalifikowanych przez komisję do zniszczenia wydaje Starosta.
3. Fizyczne zniszczenie dokumentów następuje poprzez pocięcie w niszczarce posiadającej odpowiedni certyfikat bezpieczeństwa.
4. Na okoliczność zniszczenia sporządzany jest protokół zniszczenia dokumentów.
5. Protokół zniszczenia dokumentów stanowi podstawę dla Kierownika kancelarii do zdjęcia z ewidencji wyszczególnionych w nim dokumentów, poprzez naniesienie w rubryce „Uwagi” odpowiedniego rejestru ewidencyjnego adnotacji o treści „Protokół zniszczenia znak: ... z dnia: ...” oraz uwierzytelnienie adnotacji wpisaniem daty i podpisem.

8. Dostęp do informacji niejawnych.

Informacje niejawne oznaczone klauzulą „poufne” lub „zastrzeżone” mogą być udostępnione wyłącznie osobom zatrudnionym w Urzędzie uprawnionym do dostępu do informacji niejawnych i tylko w zakresie powierzonych im do realizacji zadań.

1. Informacje niejawne oznaczone klauzulą „poufne” mogą być udostępnione osobom posiadającym ważne poświadczenie bezpieczeństwa uprawniające do dostępu do informacji niejawnych oznaczonych klauzulą „poufne” lub wyższej klauzuli tajności.

Informacje niejawne oznaczone klauzulą „zastrzeżone” mogą być udostępnione osobom posiadającym ważne poświadczenie bezpieczeństwa uprawniające do dostępu do informacji niejawnych wyższej klauzuli tajności.

97

Uzyskanie uprawnień do dostępu do informacji niejawnych oznaczonych klauzulą „poufne” może nastąpić po:

- 1) uzyskaniu poświadczenia bezpieczeństwa uprawniającego do dostępu do informacji niejawnych oznaczonych klauzulą „poufne” lub wyższa („tajne” albo „ściśle tajne”),
- 2) odbyciu szkolenia w zakresie ochrony informacji niejawnych zorganizowanego przez pełnomocnika ochrony informacji niejawnych Urzędu, potwierdzonego zaświadczeniem wg wzoru określonego w załącznikach do Rozporządzenia Prezesa Rady Ministrów z 28.12.2010 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. Nr 258, poz. 1751);
- 3) złożeniu oświadczenia potwierdzającego zapoznanie się z przepisami i zasadami ochrony informacji niejawnych na szkoleniu zorganizowanym przez pełnomocnika ochrony informacji niejawnych.

2. Uzyskanie uprawnień do dostępu do informacji niejawnych oznaczonych klauzulą „zastrzeżone” może nastąpić po:

- 1) uzyskaniu upoważnienia do dostępu do informacji niejawnych o klauzuli „zastrzeżone” udzielone przez Starostę,
- 2) odbyciu szkolenia w zakresie ochrony informacji niejawnych zorganizowanego przez pełnomocnika ochrony informacji niejawnych Urzędu, potwierdzonego zaświadczeniem wg wzoru określonego w załącznikach do rozporządzenia Prezesa Rady Ministrów z 28.12.2010 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. Nr 258, poz. 1751),
- 3) złożeniu oświadczenia potwierdzającego zapoznanie się z przepisami i zasadami ochrony informacji niejawnych na szkoleniu zorganizowanym przez pełnomocnika ochrony informacji niejawnych.

3. Upoważnienie do dostępu do informacji niejawnych o klauzuli „zastrzeżone” udzielone przez Starostę może być:

- 1) bezterminowe – ważne do odwołania; może być cofnięte w każdym czasie,
- 2) terminowe – udzielone na określony czas lub uprawniające do dostępu do informacji zawartych w dokumencie wskazanym w upoważnieniu,
- 3) okresowe – udzielone na czas realizacji czynności zleconych.

4. Upoważnienie nie ma mocy obowiązującej w innej jednostce organizacyjnej; zachowuje ważność jedynie w Starostwie Powiatowym.
5. Szkolenie w zakresie informacji niejawnych organizuje i przeprowadza pełnomocnik ochrony informacji niejawnych się nie rzadziej niż raz na 5 lat.
6. Odmowa przystąpienia osoby do szkoleń, o których mowa w ust. 1–2, oraz odmowa złożenia oświadczenia o zapoznaniu się z przepisami i z zasadami ochrony informacji niejawnych powoduje niemożliwość udostępnienia informacji niejawnych.
7. Informacje niejawne mogą być udostępniane wyłącznie osobom dającym rękojmię zachowania tajemnicy i tylko w zakresie niezbędnym do wykonywania przez nią pracy lub pełnienia służby na zajmowanym stanowisku albo wykonywania czynności zleconych.
8. Decyzja Starosty lub innej upoważnionej osoby dotycząca udostępnienia informacji niejawnej pracownikowi Urzędu powinna być w każdym przypadku określona w deklaracji imiennej, wyrażonej bezpośrednio na dokumencie.
9. Zakres informacji udostępnianych pracownikom powinien pokrywać się z tematyką spraw realizowanych przez konkretnego pracownika.
10. W sytuacjach innych, niż określone w ust. 1, decyzja Starosty lub innej upoważnionej osoby powinna zostać naniesiona z określeniem konkretnej osoby (lub osób) w deklaracji imiennej na danym dokumencie.
11. Prowadzący dziennik ewidencji dokumentów niejawnych odmawia udostępnienia informacji niejawnej osobom innym niż wskazane w deklaracji dokumentów.
12. Każda z osób, której dokument zawierający informacje niejawne został udostępniony, obowiązana jest:
- 1) fakt ten odnotować na tym dokumencie,
 - 2) określić sposób załatwienia sprawy, wskazując dokument załatwiający i kończący sprawę.
13. Pobieranie i zwrot dokumentów do prowadzącego dziennik ewidencji dokumentów niejawnych powinien zostać potwierdzony, przez pobierającego i zwracającego dokument po wykorzystaniu, czytelnym podpisem i datą w odpowiednich kolumnach (rubrykach) dziennika ewidencji dokumentów niejawnych.

9. Wykonywanie dokumentów zawierających informacje niejawne za pomocą komputera.

1. Bezpieczeństwo teleinformatyczne zapewnia się, chroniąc informacje niejawne przetwarzane w systemach teleinformatycznych przed utratą właściwości gwarantujących to bezpieczeństwo, w szczególności przed utratą poufności oraz utratą kontroli nad dostępem do informacji niejawnych, ich podglądem lub podsłuchem.
2. Bezpieczne dla informacji niejawnych wykorzystywanie systemów teleinformatycznych (komputerów), w których mają być wytwarzane, przetwarzane i przechowywane informacje niejawne, może mieć miejsce po spełnieniu wymagań określonych w rozdziale 9 „Bezpieczeństwo teleinformatyczne” ustawy z 5.8.2010 r. o ochronie informacji niejawnych (Dz.U. Nr 182, poz. 1228 ze zm.).
3. Bezpieczeństwo teleinformatyczne zapewnia się wykonując dokumenty o klauzuli „zastrzeżone” z wykorzystaniem systemu teleinformatycznego zainstalowanego w Kancelarii dokumentów niejawnych, kryptonim „ZAMEK”. System teleinformatyczny zainstalowany w Starostwie Powiatowym nie umożliwia wykonywania dokumentów o klauzuli „poufne”.
5. Bezpieczeństwo teleinformatyczne wymagane jest przed rozpoczęciem oraz w trakcie przetwarzania informacji niejawnych w systemie teleinformatycznym.
6. Systemy teleinformatyczne, w których mają być przetwarzane informacje niejawne, podlegają akredytacji bezpieczeństwa teleinformatycznego (art. 48 ust. 1 ustawy o ochronie informacji niejawnych).
7. Starosta Grudziądzki udziela akredytacji bezpieczeństwa teleinformatycznego dla systemu teleinformatycznego przeznaczonego do przetwarzania informacji niejawnych o klauzuli „zastrzeżone” – przez zatwierdzenie dokumentacji bezpieczeństwa systemu teleinformatycznego (art. 48 ust. 9 ustawy o ochronie informacji niejawnych).
6. Dokument szczególnych wymagań bezpieczeństwa systemu teleinformatycznego powinien zawierać w szczególności wyniki procesu szacowania ryzyka dla bezpieczeństwa informacji niejawnych przetwarzanych w systemie teleinformatycznym oraz określać przyjęte w ramach zarządzania ryzykiem, sposoby osiągania i utrzymywania odpowiedniego poziomu bezpieczeństwa systemu (art. 49 ust. 1 ustawy o ochronie informacji niejawnych).

10. Postępowanie z przesyłkami zawierającymi informacje niejawne.

1. Kierownik kancelarii dokumentów niejawnych przyjmuje z Sekretariatu Urzędu w celu zarejestrowania wszystkie przesyłki lub dokumenty przychodzące do Starostwa Powiatowego, oznaczone klauzulą tajności „zastrzeżone” lub „poufne” za pokwitowaniem i odciska na nich pieczęć oraz datę wpływu.

2. Przyjmując przesyłkę, sprawdza się:

- prawidłowość adresu,
- całość pieczęci i opakowania,
- zgodność odcisku pieczęci na opakowaniu z nazwą jednostki nadawcy.

3. Przesyłki zawierające dokumenty lub materiały niejawne, przychodzące do Starostwa Powiatowego pakowane są zawsze w 2 kopertach. Zewnętrzna koperta nie posiada znamion informujących o zawartości w przesyłce informacji niejawnej. Pracownik Sekretariatu Urzędu otwierając kopertę zewnętrzną natrafia na kopertę wewnętrzną, na której widnieją oznaczenia nadające klauzulę tajności, bez otwierania koperty wewnętrznej przekazuje przesyłkę Kierownikowi kancelarii dokumentów niejawnych w celu jej rejestracji.

4. 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 Informacji Niejawnych, a w przypadku gdy w obiegu przesyłek pośredniczył przewoźnik – kolejny egzemplarz protokołu przekazuje się także jemu.

5. Kierownik kancelarii dokumentów niejawnych po zarejestrowaniu przesyłki przekazuje ją adresatowi, który w jego obecności otwiera przesyłkę. Po otwarciu ustala się, czy liczba załączników i stron jest zgodna z liczbą oznaczoną na poszczególnych dokumentach.

6. W przypadku stwierdzenia nieprawidłowości Kierownik kancelarii dokumentów niejawnych sporządza w dwóch egzemplarzach protokół z otwarcia przesyłki zawierający opis nieprawidłowości, jeden egzemplarz przekazuje do nadawcy.

7. Kierownik kancelarii dokumentów niejawnych odnotowuje fakt sporządzenia protokołu w odpowiednim dzienniku lub rejestrze w rubryce „Informacje uzupełniające/Uwagi”.

8. Kierownik kancelarii dokumentów niejawnych nie otwiera 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”.

9. Na opakowaniu przesyłki wpisuje się datę wpływu, pozycję i numer, pod którym zarejestrowano przesyłkę. Przesyłkę przekazuje się – za pokwitowaniem – bezpośrednio adresatowi, a w razie jego nieobecności – osobie przez niego upoważnionej do odbioru, pod warunkiem posiadania przez te osoby odpowiednich uprawnień do dostępu do informacji niejawnych.

10. Zatrzymanie przez adresata dokumentu, adresowanego „do rąk własnych”, odnotowuje się w rubryce „Informacje uzupełniające/Uwagi”.

11. W przypadku zwrotu do Kierownika kancelarii dokumentów niejawnych przesyłki adresowanej „do rąk własnych” celem jej przechowywania, uzupełnia się dane dotyczące przesyłki w odpowiednim dzienniku lub rejestrze.

12. Adresat może podjąć decyzję o przechowywaniu przesyłki „do rąk własnych” w kancelarii dokumentów niejawnych w stanie zamkniętym. Przesyłka jest w takim przypadku zaplombowana przez adresata, a fakt ten odnotowuje się w rubryce „Informacje uzupełniające/Uwagi”.

13. Przesyłki pilne, telegramy i szyfrogramy doręcza się adresatom bezzwłocznie. Przy kwitowaniu odbioru tych przesyłek odnotowuje się godzinę doręczenia.

14. Otrzymałą i wysyłąną przesyłkę bądź wytworzony dokument rejestruje się odpowiednio w kolejności wytworzenia lub otrzymania.

11. Nadzór w zakresie ochrony informacji niejawnych.

1. Kadra kierownicza i kierownicy komórek organizacyjnych Urzędu, przełożeni pracowników, a także pełnomocnik ochrony informacji niejawnych, z tytułu pełnionej funkcji:

1) zapoznają podległych pracowników z ustaleniami planu ochrony informacji niejawnych w Urzędzie,

2) zapewniają bieżące przestrzeganie postanowień planu ochrony informacji niejawnych.

2. Pełnomocnik ochrony informacji niejawnych organizuje i powtarza nie rzadziej niż raz na 5 lat szkolenia w zakresie ochrony informacji niejawnych. Szkolenie powinno kończyć się wydaniem stosownego zaświadczenia i oświadczenia od przeszkolonych.

3. W przypadku wystąpienia wątpliwości dotyczących zasad dotyczących realizacji zadań związanych z informacjami niejawnymi pracownicy Urzędu mogą i powinni w każdym czasie zwracać się o wyjaśnienia czy instruktaż roboczy do:

- 1) pełnomocnika ochrony informacji niejawnych,
- 2) kierownika Kancelarii dokumentów niejawnych.

4. Integralną część planu ochrony stanowią załączniki określone w „Zestawieniu załączników”.

12. Odpowiedzialność karna, dyscyplinarna lub służbowa za naruszenie przepisów o ochronie informacji niejawnych.

1. Pełnomocnik ochrony informacji niejawnych w Starostwie Powiatowym, realizując zadania określone ustawą z dnia 5.8.2010 r. o ochronie informacji niejawnych (Dz.U. Nr 182, poz. 1228 ze zm.) i związanymi z ustawą przepisami wykonawczymi:

- 1) sprawuje nadzór nad realizacją i przestrzeganiem przepisów, w tym także ustaleń określonych w niniejszym planie ochrony informacji niejawnych,
- 2) sprawuje nadzór i kontrolę w zakresie ochrony informacji niejawnych, a także odpowiada za przestrzeganie przepisów o ochronie informacji niejawnych w odniesieniu do wszystkich komórek organizacyjnych Urzędu.

2. Odpowiedzialność karną osób, które dopuściły się przestępstwa lub czynu zabronionego przeciwko ochronie informacji niejawnych, określają przepisy Kodeksu Karnego.

3. W stosunku do pracowników, którzy nie przestrzegają wymagań związanych z ochroną informacji niejawnych i nierzetelnie wykonują swoje obowiązki, dopuszczają się uchybień w zakresie zabezpieczania dokumentów i informacji podlegających ochronie, stwarzając warunki do ujawnienia tajemnicy osobom nieuprawnionym, mogą zostać zastosowane sankcje dyscyplinarne i służbowe.

13. Gospodarka kluczami i pieczęciami.

Ustala się zasady gospodarki kluczami i pieczęciami:

- Szafa metalowa w pomieszczeniu Kancelarii dokumentów niejawnych po zamknięciu musi być dodatkowo plombowana pieczęcią - referentką.

- Po zakończeniu pracy Kierownik kancelarii zamyka i plombuje pieczęcią - referentką drzwi wejściowe.
- Klucz od drzwi wejściowych należy umieścić w pojemniku lub woreczku, dodatkowo zabezpieczając pieczęcią referentką, następnie tak przygotowany pojemnik lub woreczek należy przechowywać w szafie metalowej w kancelarii kadr (pokój nr 22),
- Tworzy się zapasowy komplet kluczy od pomieszczeń i szafy Kancelarii dokumentów niejawnych. Zapasowy komplet kluczy umieszczony jest w zamkniętym, plombowanym woreczku na klucze.
- Komplet kluczy zapasowych złożony jest w szafce na klucze zapasowe od pomieszczeń Starostwa Powiatowego na dyżurce Służby Ochrony.

14. Ochrona informacji niejawnych w razie wystąpienia sytuacji szczególnych, w tym wprowadzenia stanów nadzwyczajnych.

1) Konieczność podjęcia działań zmierzających do zabezpieczenia materiałów zawierających informacje niejawne stanowiące tajemnicę państwową może mieć miejsce w przypadkach:

- Spodziewanego zagrożenia państwa.
- Wprowadzenia stanu nadzwyczajnego.
- Wybuchu konfliktu zbrojnego mającego bezpośredni związek z Państwem Polskim.
- Zagrożeń wewnętrznych spowodowanych klęskami żywiołowymi.

2) Zabezpieczeniu podlegają:

a) w pierwszej kolejności zabezpieczeniu podlegają:

- materiały z ostatnich 10 lat
- materiały mające bezpośredni związek z funkcjonowaniem urzędu w warunkach zagrożenia
- materiały mające bezpośredni związek ze sprawami obronnymi i zabezpieczeniem potrzeb Sił Zbrojnych

- 705
- b) w drugiej kolejności gdy czas i warunki na to pozwalają – pozostałe materiały niejawne.
- 3) Priorytet w zakresie zabezpieczenia materiałów zawierających informacje niejawne mają materiały dotyczące:
- zapasowych miejsc pracy kierownictwa i wydziałów urzędu;
 - funkcjonowaniu urzędu w warunkach „W” i w warunkach zagrożenia;
 - zabezpieczenia potrzeb Sił Zbrojnych i jednostek zmilitaryzowanych – służb specjalnych /Policja, Straż Pożarna/.
- 4) Zabezpieczenia materiałów, o których mowa w niniejszym planie – dokonuje się poprzez ich ewakuowanie z pomieszczenia Kancelarii Dokumentów Niejawnych do KM Państwowej Straży Pożarnej w Grudziądzu ul. Piłsudskiego 25/27.
- 5) Decyzję w sprawie zabezpieczenia – ewakuacji materiałów podejmuje Pełnomocnik do Spraw Ochrony Informacji Niejawnych.
- 6) W przypadkach uzasadnionych pod nieobecność Pełnomocnika do Spraw Ochrony Informacji Niejawnych decyzję podejmuje Starosta lub Sekretarz Powiatu.
- 7) W przypadku konieczności zabezpieczenia materiałów w godzinach pozasłużbowych osoba podejmująca decyzję o konieczności zabezpieczenia materiałów poleca ściągnięcie kierownika Kancelarii Dokumentów Niejawnych przy użyciu wszelkich możliwych środków.
- 8) Zapewnia się niezbędny środek transportu oraz pracowników w ilości niezbędnej do zapakowania i przemieszczenia materiałów wymagających zabezpieczenia.
- 9) Zabezpieczenia – ewakuacji materiałów dokonuje się w obecności Kierownika Kancelarii Dokumentów Niejawnych, a w przypadku jego nieobecności zabezpieczenia materiałów dokonuje komisja wyznaczona przez osobę zarządzającą zabezpieczeniem materiałów niejawnych.

10) Komisja, dokonująca otwarcia Kancelarii Dokumentów Niejawnych i realizująca czynności związane z zabezpieczeniem części lub całości materiałów znajdujących się w kancelarii sporządza protokół z którego musi wynikać:

- zasadność otwarcia kancelarii pod nieobecność jej kierownika,
- określenie rodzaju i ilości materiałów poddanych zabezpieczeniu – ewakuacji,
- określenie materiałów, które pozostały w kancelarii , a więc tych materiałów, które nie zostały objęte zabezpieczeniem,
- określenie sposobu zabezpieczenia materiałów w nowym miejscu ich przechowywania,
- określenie sposobu zabezpieczenia materiałów, które pozostały w Kancelarii Dokumentów Niejawnych.

11) Komisja wymieniona przystępując do otwarcia kancelarii a więc wykonująca polecenie zarządzającego dokonanie zabezpieczenia materiałów wykorzystuje klucze pozostawione przez kierownika kancelarii u dyżurnego portiera w urzędzie.

12) Komisja, w przypadku pozostawienia w kancelarii części materiałów, które nie podlegały zabezpieczeniu lub te których nie zdołano zabezpieczyć obowiązana jest zamknąć i zaplombować pomieszczenie Kancelarii Dokumentów Niejawnych. Spełnienie lub nie spełnienie tego obowiązku Komisja obowiązkowo umieszcza w treści sporządzanego przez siebie protokołu dotyczącego zarówno otwarcia kancelarii jak też i zabezpieczenia materiałów.

ZATWIERDZAM:

STAROSTA
Marek Szczepanowski

**Dokumentacja określająca poziom zagrożeń
dla systemu ochrony informacji niejawnych
Starostwa Powiatowego w Grudziądzu**

OPRACOWAŁ:
PEŁNOMOCNIK
ds. Ochrony Informacji Niejawnych

[Signature]
mgr Piotr Jankowski

Grudziądz 2013 r.

Niniejsza dokumentacja opracowana została na podstawie § 3 Rozporządzenia Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych (Dz.U.2012.683).

Celem opracowania jest określenie poziomu zagrożeń dla systemu ochrony informacji niejawnych w Starostwie Powiatowym w Grudziądzu oraz dokonanie oceny zastosowanych środków bezpieczeństwa w przedmiotowym systemie pod kątem wymagań określonych w ww. rozporządzeniu. Analizą objęto obiekt, zlokalizowany pod adresem: ul. Małomłyńska 1, 86-300 Grudziądz, w którym zlokalizowana jest Kancelaria Dokumentów Niejawnych będąca głównym miejscem przetwarzania informacji niejawnych w Urzędzie i będąca jednocześnie jedynym miejscem przechowywania dokumentów i materiałów oznaczonych klauzulami „POUFNE”.

PODSTAWOWE KRYTERIA I SPOSÓB OKREŚLANIA POZIOMU ZAGROŻEŃ

I. Wstęp

W celu prawidłowego zabezpieczenia informacji niejawnych, w tym doboru odpowiednich środków bezpieczeństwa fizycznego, należy określić poziom zagrożeń nieuprawnionym ujawnieniem lub utratą informacji niejawnych. Określenie poziomu zagrożeń jest indywidualną oceną znaczenia czynników, o których mowa w § 3 ust. 6 rozporządzenia, mogących mieć wpływ na bezpieczeństwo informacji niejawnych w konkretnej jednostce organizacyjnej. Z uwagi na specyfikę, zakres i różnorodność zadań realizowanych przez podmioty podlegające przepisom ustawy, ocena przedstawionych czynników leży w sferze odpowiedzialności kierownika jednostki organizacyjnej, w której informacje niejawne są przetwarzane. Każdy z wymienionych czynników powinien zostać poddany wnikliwej analizie pod kątem jego znaczenia dla zagrożenia ujawnieniem lub utratą informacji niejawnych. Ocena poziomu zagrożeń uwzględniająca klauzule tajności przetwarzanych informacji będzie determinowała stosowanie odpowiednich środków bezpieczeństwa fizycznego, o których mowa w tabeli II "Podstawowe wymagania bezpieczeństwa fizycznego" załącznika nr 2 "Metodyka doboru środków bezpieczeństwa fizycznego".

Przy określaniu poziomu zagrożeń oceniane jest znaczenie czynnika dla bezpieczeństwa informacji niejawnych w konkretnej jednostce organizacyjnej, a nie sam czynnik jako taki.

II. Objasnienia

1. Poziom zagrożeń ustala się na podstawie wyboru "Oceny istotności czynnika" mającego wpływ na ujawnienie lub utratę informacji niejawnych w jednostce organizacyjnej. Z uzasadnienia oceny (sporządzonej według wskazań przedstawionych w "Tabeli oceny istotności czynników zagrożeń") powinno wynikać, jakie znaczenie dla jednostki organizacyjnej ma konkretny czynnik (czy jest bardzo istotny, czy mało istotny), a nie to, w jaki sposób czy za pomocą, jakich środków bezpieczeństwa fizycznego zabezpieczono informacje niejawne. Wynik analizy dokonanej w konkretnej jednostce organizacyjnej ma znaczenie dla określenia poziomu zagrożeń w zależności od tego, czy wskazane w "Tabeli oceny istotności czynników zagrożeń" czynniki bierze się pod uwagę jako: "bardzo istotne", "istotne" albo "mało istotne" dla zagrożenia ujawnieniem lub utratą informacji niejawnych.
2. W kolumnie 2 "Tabeli oceny istotności czynników zagrożeń" wskazano czynniki mające lub mogące mieć wpływ na bezpieczeństwo informacji niejawnych.
3. Każdy z czynników podlega indywidualnej ocenie pod kątem znaczenia dla zagrożenia ujawnieniem lub utratą informacji niejawnych w konkretnej jednostce organizacyjnej, tj. powinien zostać oceniony jako czynnik, który ma: "bardzo istotne znaczenie", "istotne znaczenie" lub "małe znaczenie". Wybór należy uzasadnić. Wyjątek stanowi czynnik 1, "Klauzula przetwarzanych informacji", gdzie wskazano, że dla informacji o klauzuli "ściśle tajne" czynnik ten ma "bardzo istotne znaczenie" (w rubryce "Uzasadnienie" należy wpisać, że w jednostce są przetwarzane informacje o tej klauzuli tajności).
4. Wartości punktowe przypisano odpowiednio "ocenie istotności" (a nie czynnikom jako takim), tj. czynnik oceniony jako "bardzo istotny" - 8 pkt, "istotny" - 4 pkt, "mało istotny" - 1 pkt. Liczba punktów nie podlega modyfikacji.
5. W celu dokonania oceny czynnika należy kierować się "Wskazaniami", przedstawionymi w kolumnie 7. Informacje tu przedstawione wskażą mierniki ocen.
6. Liczbę punktów z kolumn 3-5 ("Ocena istotności czynnika") należy zsumować. Uzyskany wynik wskaże poziom zagrożenia, zgodnie ze skalą określoną w "Tabeli do określania poziomu zagrożeń":
 - do 16 pkt - poziom niski,
 - od 17 do 32 pkt - poziom średni,
 - powyżej 32 pkt - poziom wysoki.

TABELA OCENY ISTOTNOŚCI CZYNNIKÓW ZAGROŻEŃ

L.p.	CZYNNIK	OCENA ISTOTNOŚCI CZYNNIKA			UZASADNIENIE	WSKAZÓWKI
		BARDZO ISTOTNY (8 pkt)	ISTOTNY (4 pkt)	MAŁO ISTOTNY (1 pkt)		
1	2	3	4	5	6	7
1	Klauzula tajności przetwarzanych informacji niejawnych		4		Mała liczba IN oznaczonych klauzulą „POUFNE”	Analizie podlegają wszystkie klauzule tajności wszystkich przetwarzanych informacji niejawnych. Przy ocenie istotności czynnika stosuje się zasadę: im wyższe klauzule tajności przetwarzanych informacji, tym czynnik ma istotniejsze znaczenie. Dla informacji niejawnych o klauzuli "ściśle tajne" wartość oceny jest stała i wynosi 8 pkt (czynnik ma "bardzo istotne" znaczenie). W przypadku nowo organizowanej jednostki organizacyjnej należy przyjąć wartości szacunkowe
2	Liczba materiałów niejawnych			1	Stosunkowo mała liczba dokumentów zawierających IN	Przy ocenie istotności czynnika należy brać pod uwagę wszystkie materiały niejawne zarejestrowane w urządzeniach ewidencyjnych, pozostające w faktycznej dyspozycji jednostki organizacyjnej. W uzasadnieniu należy odnieść się do przybliżonej ogólnej liczby wszystkich materiałów, stosując zasadę: im więcej informacji niejawnych o najwyższych klauzulach

						tajności, tym czynnik ma istotniejsze znaczenie. W przypadku nowo organizowanej jednostki organizacyjnej należy przyjąć wartości szacunkowe.
3.	Postać informacji niejawnych			1	Dokumenty oznaczane klauzulą „POUFNE” wytwarzane są ręcznie lub przy użyciu mechanicznej maszyny do pisania. Dokumenty „ZASTRZEŻONE” przetwarzane są na BSK.	Przy ocenie należy brać pod uwagę ogólną liczbę przetwarzanych informacji niejawnych, stosując zasadę, że im więcej informacji przetwarzanych w systemach teleinformatycznych (w stosunku do ogólnej liczby materiałów) tym czynnik jest bardziej istotny. W przypadku nowo organizowanej jednostki organizacyjnej należy przyjąć wartości szacunkowe.
4.	Liczba osób			1	Mała liczba pracowników upoważnionych do dostępu do IN w stosunku do wszystkich zatrudnionych	Przy ocenie istotności tego czynnika należy uwzględnić pracowników jednostki organizacyjnej mających lub mogących mieć dostęp do informacji niejawnych, tj. osoby zajmujące stanowiska, wykonujące zadania lub prace zlecone związane z dostępem do takich informacji, a także posiadane przez nich uprawnienia oraz uzasadnioną potrzebę dostępu do informacji niejawnych. Im więcej osób (w stosunku do liczby zatrudnionych) tym czynnik jest bardziej istotny. W przypadku nowo organizowanej jednostki organizacyjnej należy przyjąć wartości szacunkowe.
5.	Lokalizacja		4		Obiekt Starostwa Powiatowego jest użytkowany	Na wzrost oceny istotności tego czynnika ma wpływ np. to, że budynek użytkowany jest wspólnie z

					również przez obce jednostki organizacyjne. Budynek przy ul. Małomłyńskiej nie graniczy z budynkami obcymi.	innymi podmiotami lub budynek jest w zabudowie zwartej (np. budynek, którego ściany przylegają do innego budynku). Na wzrost oceny istotności czynnika ma wpływ także najbliższe sąsiedztwo np.: obiekty przedstawicielstw i podmiotów zagranicznych, hotele, obiekty sportowe i hale widowiskowe, ogólnodostępne parkingi, garaże, zakłady przemysłowe i instalacje stanowiące zagrożenie dla życia lub zdrowia.
6.	Dostęp osób do budynku		4		Obiekt Starostwa Powiatowego jest zamknięty i strzeżony w nocy. W godzinach urzędowania powszechnie dostępny.	Na wzrost oceny istotności tego czynnika ma wpływ możliwość swobodnego poruszania się po budynku osób niebędących pracownikami jednostki organizacyjnej, np. gości, interesantów (w obiektach użyteczności publicznej).
7.	Inne czynniki			1	Brak zdefiniowanych zagrożeń	Poziom zagrożeń powinien uwzględniać inne czynniki wynikające ze specyfiki jednostki organizacyjnej, niewykazane powyżej, a mogące mieć wpływ na ochronę informacji niejawnych, np.: działanie obcych służb specjalnych, sabotaż, zamach terrorystyczny, kradzież lub inna działalność przestępcza, pożar, działanie sił przyrody (np. obszar zagrożony powodzią).
Suma punktów		16			Poziom niski	

TABELA DO OKREŚLANIA POZIOMU ZAGROŻEŃ

POZIOM ZAGROŻEŃ		
NISKI	ŚREDNI	WYSOKI
7 pkt – 16 pkt	17 pkt – 32 pkt	powyżej 32 pkt

METODYKA DOBORU ŚRODKÓW BEZPIECZEŃSTWA FIZYCZNEGO

Część I. Instrukcja:

1. Proces doboru środków bezpieczeństwa fizycznego powinien zapewniać elastyczność ich stosowania w zależności od określonego poziomu zagrożeń. W § 4 - 8 rozporządzenia ustalone zostały podstawowe wymagania doboru środków bezpieczeństwa fizycznego.
2. Poniżej przedstawiono metody wyboru najbardziej odpowiednich i ekonomicznych kombinacji środków bezpieczeństwa fizycznego.
3. W częściach II - IV przedstawiono opcje zapewniające wielopoziomową ochronę informacji niejawnych oraz spełniające wymagania określone w § 4 - 8 rozporządzenia.
4. Środki bezpieczeństwa fizycznego określone w części III "Klasyfikacja środków bezpieczeństwa fizycznego" zostały podzielone na 6 kategorii, z których każda dotyczy określonego aspektu bezpieczeństwa fizycznego. Aby ułatwić odczytywanie informacji, wykaz środków został sporządzony w formie tabeli z przypisanymi im wartościami liczbowymi.
5. Pierwszym etapem procesu doboru środków bezpieczeństwa fizycznego jest odczytanie z tabeli w części II "Podstawowe wymagania fizycznego" minimalnej łącznej sumy punktów wymaganych do osiągnięcia założonego poziomu ochrony informacji w wyniku zastosowania odpowiednich kombinacji środków bezpieczeństwa fizycznego. Liczba wymaganych do uzyskania punktów zależy od najwyższej klauzuli tajności informacji niejawnych przetwarzanych w danej lokalizacji oraz poziomu zagrożeń, określonego wcześniej zgodnie z przepisem § 3 rozporządzenia.
6. Drugim etapem jest odczytanie z tej samej tabeli w części II, odpowiadającej założonemu poziomowi ochrony informacji, minimalnej liczby punktów koniecznych do uzyskania w każdej z grup obejmującej kategorię wymaganych do zastosowania środków bezpieczeństwa fizycznego (oznaczonej "obowiązkowo").
7. Trzecim etapem jest dokonanie wyboru określonych środków bezpieczeństwa fizycznego, przy którym należy posługiwać się tabelą z części III "Klasyfikacja środków bezpieczeństwa fizycznego". W tej tabeli należy odczytać liczbę punktów odpowiadającą wybranemu środkowi bezpieczeństwa i wpisać ją w odpowiednie miejsce w tabeli w części IV "Punktacja zastosowanych środków bezpieczeństwa fizycznego". Niezastosowanie danego środka jest jednoznaczne z przyznaniem za niego liczby punktów "0". Przy dokonywaniu wyboru konieczne jest uwzględnienie wymagań określonych w rozporządzeniu, jak też w samej tabeli z części III "Klasyfikacja środków bezpieczeństwa fizycznego". Dobór adekwatnych środków bezpieczeństwa fizycznego w konkretnym przypadku musi zapewnić uzyskanie zarówno minimalnej łącznej sumy punktów wymaganych do osiągnięcia założonego poziomu ochrony informacji niejawnych (w zależności od najwyższej klauzuli tajności informacji przetwarzanych w danej lokalizacji oraz poziomu zagrożeń), jak również uzyskanie minimalnej liczby punktów odpowiadających każdej z grup kategorii środków bezpieczeństwa fizycznego (oznaczonych jako "obowiązkowo"). W przypadku gdy liczba punktów uzyskanych po zastosowaniu środka należącego do grup kategorii oznaczonych jako "obowiązkowo" jest mniejsza od minimalnej łącznej sumy punktów wymaganych do osiągnięcia założonego poziomu ochrony informacji niejawnych, należy zastosować środki z kategorii oznaczonych "dodatkowo" zapewniające uzyskanie minimalnej łącznej sumy punktów.
8. Za zastosowanie produktów, które posiadają ważne certyfikaty wydane przed wejściem w życie niniejszego rozporządzenia, przyznaje się liczbę punktów odpowiednio do spełnianych przez nie wymagań określonych w tabeli z części III "Klasyfikacja środków bezpieczeństwa fizycznego".
9. Przykładowe rozwiązanie dla średniego poziomu zagrożeń i najwyższej klauzuli informacji niejawnych "tajne" zawarte jest w części V.
10. Spis norm użytych w metodyce:
 - PN-EN 1627 - Okna, drzwi, żaluzje. Odporność na włamanie. Wymagania i klasyfikacja.

- PN-EN 14450 - Pomieszczenia i urządzenia do przechowywania wartości. Wymagania, klasyfikacja i metody badań odporności na włamanie. Pojemniki bezpieczne i szafy.
- PN-EN 1300 - Pomieszczenia i urządzenia do przechowywania wartości. Klasyfikacja zamków o wysokim stopniu zabezpieczenia z punktu widzenia odporności na nieuprawnione otwarcie.
- PN-EN 50131-1 - Systemy alarmowe. Systemy sygnalizacji włamania i napadu. Wymagania systemowe.
- PN-EN 50133-1 - Systemy alarmowe. Systemy kontroli dostępu. Część 1: Wymagania systemowe.
- PN-EN 12209 - Okucia budowlane. Zamki. Zamki mechaniczne wraz z zaczepami. Wymagania i metody badań.
- PN-EN 1143-1 - Pomieszczenia i urządzenia do przechowywania wartości. Wymagania, klasyfikacja i metody badań odporności na włamanie. Część 1: Szafy, szafy ATM, pomieszczenia i drzwi do pomieszczeń.

Część II. Podstawowe wymagania bezpieczeństwa fizycznego.

Najwyższa klauzula tajności informacji przetwarzanych w jednostce organizacyjnej	Poziom zagrożeń		
	Niski	Średni	Wysoki
POUFNE			
Obowiązkowo: kategorie K1+K2+K3	6	8	9
Obowiązkowo: kategorie K4+K5	2	3	3
Diodatkowo: kategoria K6	3	3	4
Łącznie suma punktów	<u>11</u>	14	16
ZASTRZEŻONE			
Obowiązkowo: kategorie K1+K2+K3	2	2	2
Dodatkowo: kategorie K4,K5 lub K6	-	1	2
Łącznie suma punktów	2	3	4

UWAGA!

Wymagania dla Starostwa Powiatowego zostały pogrubione i wyróżnione większą trzcionką. Suma punktów została dodatkowo podkreślona.

Część III. Klasyfikacja środków bezpieczeństwa fizycznego.

KATEGORIA K1: Szafy do przechowywania informacji niejawnych

Środek bezpieczeństwa K1S1 - Konstrukcja szafy

Typ / Punktacja	Funkcje lub cechy
Typ 4 4 pkt	Szafa: 1) spełnia co najmniej wymagania klasy odporności na włamanie 0 określone w Polskiej Normie PN-EN 1143-1; 2) jest zabezpieczona dwoma zamkami typu 3 lub 4 z Kategorii K1S2.
Typ 3 3 pkt	Szafa: 1) spełnia co najmniej wymagania klasy odporności na włamanie S2 określone w Polskiej Normie PN-EN 14450; 2) jest zabezpieczona zamkiem typu 3 lub 4 z Kategorii K1S2.
Typ 2 2 pkt	Szafa: 1) spełnia co najmniej wymagania klasy odporności na włamanie S1 określone w Polskiej Normie PN-EN 14450; 2) jest zabezpieczona zamkiem typu 2 lub 3 z Kategorii K1S2.
Typ 1 1 pkt	Szafa charakteryzuje się następującymi cechami: 1) jest to zamykany na klucz mebel biurowy, niewyposażony w żadne szczególne funkcje zabezpieczające, ale charakteryzujący się umiarkowaną odpornością na nieuprawnione próby otwarcia; 2) jest zabezpieczona zamkiem typu 1 lub 2 z Kategorii K1S2.

Środek bezpieczeństwa K1S2 - Zamek do szafy

Typ / Punktacja	Funkcje lub cechy
Typ 4 4 pkt	Zamek charakteryzuje się wysokim poziomem odporności na fachowe i profesjonalne działania osoby nieuprawnionej posługującej się wyjątkowo zaawansowanymi narzędziami i umiejętnościami, które nie są powszechnie dostępne. Zamek jest zamkiem szyfrowym i spełnia co najmniej wymagania klasy B określone w Polskiej Normie PN-EN 1300. Rozróżnia się: 1) zamek mechaniczny szyfrowy co najmniej trzyczłonowy, o cichym, przesuwie, posiadający min. 100 podziałek na pokrętle i skali nastawień, przy której w przypadku każdej tarczy zamek trzyczłonowy nie otworzy się, jeżeli pokrętło jest przekręcone więcej niż o 1 kreskę podziałki po obu stronach właściwej kreski podziałki, a w przypadku zanika czterotarczowego wartość ta

	wynosi 1,25. Zamek powinien być odporny na manipulację przez eksperta, również przy użyciu specjalistycznych narzędzi, przez okres 20 roboczogodzin. Zamek powinien być zabezpieczony przed działaniem destrukcyjnym, w tym przed przewierceniem i prześwietleniem (atakiem) radiologicznym (promieniowanie z radioaktywnego źródła nieprzekraczającego równowartości 10 curie, Co-60 z odległości 760 mm przez 20 godzin). Zmiana kombinacji powinna być blokowana i uaktywniana kluczem od tyłu obudowy zamka. Szafa powinna być wyposażona w dwa komplety kluczy od ustawiania szyfru; 2) zamek elektroniczny szyfrowy spełnia te same wymagania co zamek mechaniczny szyfrowy oraz nie generuje sygnałów, które mogą być wykorzystane do otwarcia zamka przez okres 20 roboczogodzin.
Typ 3 3 pkt	Zamek charakteryzuje się wysokim poziomem odporności na fachowe i profesjonalne działania osoby nieuprawnionej posługującej się wyjątkowo zaawansowanymi narzędziami i umiejętnościami, dostępnymi powszechnie dla profesjonalistów. Zamek jest zamkiem szyfrowym i spełnia co najmniej wymagania klasy B określone w Polskiej Normie PN-EN 1300. Rozróżnia się: 1) zamek mechaniczny szyfrowy co najmniej trzyczarkowy, o cichym przesuwie, posiadający min. 100 podziałek na pokrętło i skali nastawień, przy której w przypadku każdej tarczy zamek trzyczarkowy nie otworzy się, jeżeli pokrętło jest przekręcone więcej niż o 1 kreskę podziałki po obu stronach właściwej kreski podziałki, a w przypadku zamka czterotarowego wartość ta wynosi 1,25. Zmiana kombinacji powinna być blokowana i uaktywniana kluczem od tyłu obudowy zamka. Zamek powinien być zabezpieczony przed działaniem destrukcyjnym, w tym przed przewierceniem. Z szafą powinny być dostarczone dwa komplety kluczy do zmiany kodu; 2) zamek elektroniczny szyfrowy spełnia te same wymagania co zamek mechaniczny szyfrowy oraz nie generuje sygnałów, które mogą być wykorzystane do otwarcia zamka przez okres 20 roboczogodzin.
<u>Typ 2</u> <u>2 pkt</u>	Zamek 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.
Typ 1 1 pkt	Zamek charakteryzuje się umiarkowaną odpornością na nieuprawnione próby otwarcia i może być wykorzystywany wyłącznie w szafach typu 1. Zamek spełnia co najmniej wymagania kategorii 4 określone w Polskiej Normie PN-EN 12209.

KATEGORIA K2: Pomieszczenia

Kategoria K2 opisuje pomieszczenia, w których informacje niejawne przechowywane są w szafach opisanych w kategorii K1, i nie dotyczy pomieszczeń wzmocnionych, o których mowa w § 5 ust. 3 rozporządzenia.

O zaklasyfikowaniu pomieszczenia do danego typu decyduje najniższy element (ściana, podłoga, strop, drzwi, okna).

Środek bezpieczeństwa K2S1 - Konstrukcja pomieszczenia

Typ / Punktacja	Funkcje lub cechy
Typ 4 4 pkt	Konstrukcja pomieszczenia charakteryzuje się następującymi cechami: 1) zapewnia wysoką odporność na próby wymuszenia otwarcia oraz otwarcia z wykorzystaniem wielu różnych zaawansowanych narzędzi ręcznych i zasilanych prądem; 2) zapewnia wysoki poziom odporności na potajemne próby uzyskania nieuprawnionego dostępu; 3) zbudowane zostało ze zbrojonego betonu o grubości 15 cm lub materiału o podobnej wytrzymałości; 4) drzwi i okna spełniają co najmniej wymagania klasy 4 określone w Polskiej Normie PN-EN 1627; 5) drzwi są wyposażone w zamek typu 4 z Kategorii K2S2.
Typ 3 3 pkt	Konstrukcja pomieszczenia charakteryzuje się następującymi cechami: 1) zapewnia wysoką odporność na działania osoby nieuprawnionej próbującej uzyskać dostęp siłą lub za pomocą różnorodnych narzędzi ręcznych; 2) zapewnia wysoki poziom odporności na potajemne próby uzyskania nieuprawnionego dostępu; 3) zbudowane zostało z cegły lekkiej o grubości 25 cm lub materiału o podobnej wytrzymałości; 4) drzwi i okna spełniają co najmniej wymagania klasy 3 określone w Polskiej Normie PN-EN 1627; 5) drzwi są wyposażone w zamek typu 2 lub 3 z Kategorii K2S2.
<u>Typ 2</u> <u>2 pkt</u>	Konstrukcja pomieszczenia charakteryzuje się następującymi cechami: 1) zapewnia względną odporność na działania osoby nieuprawnionej próbującej uzyskać dostęp siłą lub za pomocą ograniczonej liczby narzędzi ręcznych; 2) zapewnia wysoki poziom odporności na potajemne próby uzyskania nieuprawnionego dostępu; 3) zbudowane zostało z cegły lekkiej o grubości 15 cm lub materiału o podobnej wytrzymałości albo ze sklejk i płyt gipsowych na ramie wspierającej; 4) drzwi i okna spełniają co najmniej wymagania klasy 2 określone w Polskiej Normie PN-EN 1627; 5) drzwi są wyposażone w zamek typu 1 lub 2 z Kategorii K2S2. Okna nie muszą spełniać powyższych wymagań, jeżeli: - dolna krawędź okna znajduje się na wysokości przynajmniej 5,5 m nad gruntem lub innym elementem budynku (np. balkonem lub balustradą), - nie znajdują się na ostatnim piętrze, - w pobliżu nie znajduje się żaden element (np. rynna, drabina, drzewo) ułatwiający potencjalny dostęp i penetrację

Typ 1 1 pkt	Konstrukcja pomieszczenia charakteryzuje się następującymi cechami: 1) jest to pomieszczenie lub pokój biurowy, który może zostać zamknięty (w przypadku pozostawienia bez nadzoru), zapewniający poziom bezpieczeństwa odpowiedni dla materiałów tam przechowywanych; 2) zbudowane zostało z cegły lekkiej, gipsokartonu, drewna, płyt pilśniowych lub innego materiału o podobnej wytrzymałości; 3) drzwi i okna spełniające najmniej wymagania klasy 1 określone w Polskiej Normie PN-EN 1627. Uwaga: Jeżeli wymagane jest, by takie pomieszczenie było zabezpieczone przed długotrwałymi potajemnymi próbami uzyskania dostępu (na przykład w nocy lub podczas weekendu), standard drzwi i ich zaników oraz standard zabezpieczenia okien powinien być odpowiednio wyższy, adekwatnie do poziomu zagrożeń.
------------------------	---

Środek bezpieczeństwa K2S2 - Zamek do drzwi pomieszczenia

Typ / Punktacja	Funkcje lub cechy
Typ 4 4 pkt	Zamek spełniający co najmniej wymagania klasy 7 określone w Polskiej Normie PN-EN 12209.
<u>Typ 3</u> 3 pkt	Zamek spełniający co najmniej wymagania klasy 5 określone w Polskiej Normie PN-EN 12209.
Typ 2 2 pkt	Zamek spełniający co najmniej wymagania klasy 4 określone w Polskiej Normie PN-EN 12209.
Typ 1 1 pkt	Zamek spełniający co najmniej wymagania klasy 3 określone w Polskiej Normie PN-EN 12209.

KATEGORIA K3: Budynki

O zaklasyfikowaniu budynku do danego typu decyduje najsłabszy jego element zewnętrzny.

Typ / Punktacja	Funkcje lub cechy
Typ 4 4 pkt	Budynek charakteryzuje się wytrzymałą konstrukcją i następującymi cechami: 1) zapewnia wysoki poziom odporności na próby włamania; 2) ściany, podłoga i strop są wykonane ze zbrojonego betonu lub podobnego materiału; 3) drzwi są wykonane ze stali wzmacnianej lub drewna pokrytego blachą stalową; 4) rama, mocowanie i szyby okien zapewniają zabezpieczenie przed fizycznym włamaniem, a ich powierzchnia jest jak najmniej uszkodzona.
Typ 3 3 pkt	Budynek charakteryzuje się następującymi cechami: 1) zapewnia średni poziom odporności na próby włamania; 2) stanowi wytrzymałą konstrukcję, zazwyczaj z cegły lub pustaków, opartą na ścianach szczelinowych lub podobnej budowie; 3) okna i drzwi są wykonane w standardzie odpowiadającym standardowi budynku w zakresie odporności na włamanie. Okna nie muszą być zabezpieczone w powyższy sposób, jeżeli: - dolne krawędzie okien znajdują się na wysokości przynajmniej 5,5 m nad gruntem lub innym elementem budynku (np. balkonem lub balustradą), - nie można uzyskać do nich dostępu z dachu lub z wykorzystaniem znajdującego się w pobliżu elementu (rynna, drabina, drzewo) ułatwiającego potencjalny dostęp i penetrację. Uwaga: jako Typ 3 może również zostać sklasyfikowany budynek zbudowany z zastosowaniem nowoczesnych technologii budowlanych, z wykorzystaniem prefabrykowanych paneli lub ramy stalowej i szkła bądź podobnych materiałów.
Typ 2 2 pkt	Budynek charakteryzuje się następującymi cechami: 1) zapewnia średni poziom odporności na próby włamania; 2) stanowi lekką konstrukcję, zazwyczaj z pojedynczego rzędu cegieł lub lekkich bloczków, bądź jest to wytrzymałe pomieszczenie biurowe przystosowane do transportu; 3) okna i drzwi są wykonane w standardzie odpowiadającym standardowi budynku w zakresie odporności na włamanie. Okna nie muszą być zabezpieczone w powyższy sposób, jeżeli: - dolne krawędzie okien znajdują się na wysokości przynajmniej 5,5 m nad gruntem lub innym elementem budynku (np. balkonem lub balustradą), - nie można uzyskać do nich dostępu z dachu lub z wykorzystaniem znajdującego się w pobliżu elementu (np. rynna, drabina, drzewo) ułatwiającego potencjalny dostęp i penetrację.
Typ 1 1 pkt	Budynek jest lekką konstrukcją przeznaczoną do ochrony zawartości i osób znajdujących się wewnątrz tylko przed działaniem czynników zewnętrznych (deszcz, wiatr i t.d.)

KATEGORIA K4: Kontrola dostępu**Środek bezpieczeństwa K4S1 - Systemy kontroli dostępu**

Typ / Punktacja	Funkcje lub cechy
Typ 4 4 pkt	Elektroniczny automatyczny system kontroli dostępu o następujących cechach: 1) spełnia co najmniej wymagania systemu w klasie rozpoznania 3, a w klasie dostępu B - określone w normie PN-EN 50133-1; 2) jest to automatyczny system zapewniający właściwy stopień ochrony, wymagający jedynie minimalnego nadzoru przez personel bezpieczeństwa; 3) jest stosowany w połączeniu z barierą dostępu uniemożliwiającą powrót, działającą na zasadzie uniemożliwiającej otwarcie danego przejścia kontrolowanego, jeżeli wcześniej nie nastąpiło wyjście ze strefy, do której zamierza się wejść, bądź bez uprzedniego wejścia do poprzedzającej go strefy; 4) sygnały ostrzeżeń i alarmów z systemu przekazywane są do stacji monitoringu obsługiwanej przez personel bezpieczeństwa; 5) obejmuje wszystkie wejścia i wyjścia kontrolowanego pomieszczenia lub obszaru.
Typ 3 3 pkt	Elektroniczny automatyczny system kontroli dostępu o następujących cechach: 1) spełnia co najmniej wymagania systemu w klasie rozpoznania 3, a w klasie dostępu B - określone w normie PN-EN 50133-1; 2) wstęp kontrolowany jest przez odpowiednią barierę, która może wymagać bezpośredniego nadzoru przez personel bezpieczeństwa; 3) obejmuje wszystkie wejścia i wyjścia kontrolowanego pomieszczenia lub obszaru.
Typ 2 2 pkt	Dopuszcza się zastosowanie jednego z poniższych rozwiązań: 1. elektroniczny automatyczny system kontroli dostępu o następujących cechach: 1) spełnia co najmniej wymagania systemu w klasie rozpoznania 2, a w klasie dostępu B - określone w normie PN-EN 50133-1; 2) wstęp kontrolowany jest przez odpowiednią barierę, która może wymagać bezpośredniego nadzoru strażnika; 3) obejmuje wszystkie wejścia i wyjścia kontrolowanego obszaru; lub 2. system kontroli dostępu obejmujący wszystkie wejścia i wyjścia z kontrolowanego obszaru, wymagający: 1) obecności personelu bezpieczeństwa; 2) zastosowania fotografii lub systemu wstępu na podstawie unikalnych przepustek; w zależności od ustaleń związanych z przyznawaniem wstępu akceptowane mogą być również inne dokumenty identyfikacyjne, na przykład legitymacja służbowa.
Typ 1 1 pkt	System tego typu może być stosowany do zabezpieczania obszarów, w których przetwarzane są informacje niejawnie najwyższej o klauzuli "poufne". System kontroli dostępu oparty na zamkniętych drzwiach pomieszczenia lub obszaru, do którego można uzyskać dostęp za pomocą: 1. kodów - spełnia co najmniej wymagania systemu w klasie rozpoznania 1, a w klasie dostępu B - określone w normie PN-EN 50133-1; lub 2. kluczy wydawanych uprawnionym osobom.

Środek bezpieczeństwa K4S2 - Kontrola osób nieposiadających stałego upoważnienia do wejścia na obszar jednostki organizacyjnej (interesantów)

Typ / Punktacja	Funkcje lub cechy
Eskorta 3 pkt	Kontrolę interesantów organizuje się w następujący sposób: 1) wprowadzani interesanci przez cały czas swojej wizyty przebywają pod nadzorem osoby uprawnionej lub pracownika, z którym związana jest ich wizyta; 2) jeżeli interesanci muszą odwiedzić kilka różnych działów lub pracowników, powinni formalnie przechodzić spod nadzoru jednej osoby pod nadzór innej, z zapewnieniem wszelkiej dokumentacji dotyczącej takiej wizyty i zmiany towarzyszących osób uprawnionych; 3) interesanci są zobligowani do noszenia odpowiedniego identyfikatora odróżniającego ich od pracowników.
Przepustka 1 pkt	Kontrolę interesantów organizuje się w następujący sposób: 1) interesanci mogą uzyskać prawo wstępu na dany obszar bez konieczności nadzoru osoby uprawnionej; 2) interesanci są zobligowani do noszenia plakietki z przepustką, która ich identyfikuje jako osoby nieposiadające stałego upoważnienia do wejścia na obszar jednostki organizacyjnej, i tym samym odróżnia ich od pracowników. Uwaga: należy pamiętać, że system oparty na wydawaniu interesantom przepustek, jest skuteczny, jeżeli wszyscy pracownicy jednostki organizacyjnej również noszą identyfikatory.

KATEGORIA K5: Personel bezpieczeństwa i systemy sygnalizacji napadu i włamania
Środek bezpieczeństwa K5S1 - Personel bezpieczeństwa

Typ / Punktacja	Funkcje lub cechy
Typ 5 5 pkt	Personel bezpieczeństwa organizuje się w następujący sposób: 1) personel bezpieczeństwa składa się z osób zatrudnionych w jednostce organizacyjnej; 2) organizuje się częsty, wewnętrzny patrol kontrolujący wnętrze budynku po losowo wybranych trasach i przeprowadzany w nieregularnych odstępach czasu, jednak nie rzadziej niż co dwie godziny; 3) strażnicy mają przydzielone określone zadania do wykonania podczas patrolu.
Typ 4 4 pkt	Personel bezpieczeństwa organizuje się w następujący sposób: 1) personel bezpieczeństwa składa się z osób zatrudnionych w jednostce organizacyjnej; 2) organizuje się wewnętrzny patrol kontrolujący wnętrze budynku po losowo wybranych trasach i przeprowadzany w nieregularnych odstępach czasu nieprzekraczających 6 godzin, co umożliwi odbicie 2 lub 3 patroli w nocy i przeprowadzenie okresowych kontroli zabezpieczeń podczas weekendów lub dni wolnych od pracy.
Typ 3 3 pkt	Personel bezpieczeństwa organizuje się w następujący sposób: 1) zadania personelu bezpieczeństwa mogą wykonywać pracownicy firmy zewnętrznej; 2) patrol ograniczony jest do kontroli terenu i jego granic, podczas którego strażnicy sprawdzają zabezpieczenia budynków, ale nie mają do nich dostępu; 3) częstotliwość patroli powinna zależeć od środowiska operacyjnego i poziomu zagrożenia.
Typ 2 <u>2 pkt</u>	Personel bezpieczeństwa organizuje się w następujący sposób: 1) w jednostce organizacyjnej funkcjonują strażnicy "stacjonarni", którzy nie są zobowiązani do przeprowadzania patroli, ale są zatrudnieni do przebywania w pomieszczeniu kontroli zdarzeń lub w stróżówce oraz do sprawdzania podejrzanych zdarzeń i wzywania pomocy, gdy jest to wymagane; 2) zadania mogą wykonywać pracownicy firmy zewnętrznej.
Typ 1 1 pkt	Personel bezpieczeństwa organizuje się w następujący sposób: 1) w jednostce organizacyjnej funkcjonują strażnicy "sporadyczni", którzy są zatrudnieni do odwiedzania terenu nocą i podczas weekendów w celu przeprowadzenia podstawowej kontroli ogrodzenia; 2) strażnicy nie mają uprawnień dostępu do danego obiektu lub budynku, ale w przypadku podejrzenia włamania zareagują poprzez wezwanie osoby posiadającej klucze.

Środek bezpieczeństwa K5S2 - Systemy sygnalizacji napadu i włamania

Typ / Punktacja	Funkcje lub cechy
Typ 4 4 pkt	System, charakteryzuje się następującymi cechami: 1) spełnia wymagania systemu stopnia 4 określone w normie PN-EN 50131-1; 2) obejmuje ochroną cały obszar, w tym szafy służące do przechowywania informacji niejawnych i sygnalizuje co najmniej: a) otwarcie drzwi, okien i innych zamknięć chronionego obszaru, b) penetrację drzwi, okien i innych zamknięć chronionego obszaru bez ich otwierania, c) penetrację ścian, sufitów i podłóg, d) poruszanie się w chronionym obszarze (pułapkowe - nadzór nad wybranymi miejscami, w których występuje wysokie prawdopodobieństwo wykrycia), e) atak na szafy służące do przechowywania informacji niejawnych; 3) stosowany jest wraz z systemem dozoru wizyjnego z obowiązkową rejestracją w rozdzielczości nie mniejszej niż 400 linii telewizyjnych i przechowywaniem zarejestrowanego zapisu przez czas nie krótszy niż 30 dni, nie obejmującym pomieszczeń służących wyłącznie jako pomieszczenia przeznaczone do spotkań; 4) stan systemu sygnalizacji napadu i włamania oraz systemu dozoru wizyjnego, w tym generowane ostrzeżenia i alarmy, jest stale monitorowany przez personel bezpieczeństwa. Uwaga: 4 pkt przyznaje się również w przypadku obszarów, w których przez 24 godziny na dobę przebywają pracownicy.
Typ 3 3 pkt	System charakteryzuje się następującymi cechami: 1) spełnia co najmniej wymagania systemu stopnia 3 określone w normie PN-EN 50131-1; 2) obejmuje ochroną otwory wejściowe i wnętrze obszaru oraz sygnalizuje co najmniej: a) otwarcie drzwi, okien i innych zamknięć chronionego obszaru, b) penetrację drzwi, okien i innych zamknięć chronionego obszaru bez ich otwierania, c) poruszanie się w chronionym obszarze (pułapkowe - nadzór nad wybranymi miejscami, w których występuje wysokie prawdopodobieństwo wykrycia), d) atak na szafy służące do przechowywania informacji niejawnych; 3) stan systemu, w tym generowane ostrzeżenia i alarmy, jest stale monitorowany przez personel bezpieczeństwa. Uwaga: 3 pkt przyznaje się również w przypadku systemu wykonanego przed wejściem w życie rozporządzenia, zgodnie z wymaganiami systemu co najmniej klasy SA3 określonymi w Polskiej Normie PN-93/E-08390, pod warunkiem spełnienia wymagań w zakresie ochrony i nadzoru określonych w pkt 2 dla typu 4.
Typ 2 2 pkt	System charakteryzuje się następującymi cechami: 1) spełnia co najmniej wymagania systemu stopnia 2 określone w normie PN-EN 50131-1 i zapewnia identyfikację użytkowników włączających i wyłączających system lub jego część; 2) obejmuje ochroną miejsca, w których informacje niejawne są przechowywane oraz całą granicę obszaru (okna, drzwi i inne otwory) i sygnalizuje co najmniej:

	a) otwarcie drzwi, okien i innych zamknięć chronionego obszaru, b) poruszanie się w chronionym obszarze (pułapkowo - nadzór nad wybranymi miejscami, w których występuje wysokie prawdopodobieństwo wykrycia); 3) stan systemu, w tym generowane ostrzeżenia i alarmy, jest stale monitorowany przez personel bezpieczeństwa. Uwaga: 2 pkt przyznaje się również w przypadku systemu wykonanego przed wejściem w życie rozporządzenia, zgodnie z wymaganiami systemu co najmniej klasy SA3 określonymi w Polskiej Normie PN-93/E-08390, pod warunkiem spełnienia wymagań w zakresie ochrony i nadzoru określonych w pkt 2 dla typu 3
Typ 1 1 pkt	System charakteryzuje się następującymi cechami: 1) spełnia co najmniej wymagania systemu stopnia 1 określone w normie PN-EN 50131-1; 2) obejmuje ochroną miejsca, w których informacje niejawne są przechowywane i sygnalizuje co najmniej: a) otwarcie drzwi do chronionego obszaru, b) poruszanie się w chronionym obszarze (pułapkowo - nadzór nad wybranymi miejscami, w których występuje wysokie prawdopodobieństwo wykrycia). Uwaga: 1 pkt przyznaje się również w przypadku systemu wykonanego przed wejściem w życie rozporządzenia, zgodnie z wymaganiami systemu co najmniej klasy SA3 określonymi w Polskiej Normie PN-93/E-08390, pod warunkiem spełnienia wymagań w zakresie ochrony i nadzoru określonych w pkt 2 dla typu 2.

KATEGORIA K6: Granice**Środek bezpieczeństwa K6S1 – Ogrodzenie**

Typ / Punktacja	Funkcje lub cechy
Typ 4 4 pkt	Ogrodzenie charakteryzuje się następującymi cechami: 1) zapewnia wysoki poziom zabezpieczenia, maksymalnie utrudnia i opóźnia działania profesjonalnego i zdeterminowanego intruza/włamywacza, który dysponuje szeroką wiedzą i zaawansowanymi narzędziami; 2) projekt i konstrukcja ogrodzenia zapewniają wysoki poziom odporności na ataki dokonywane poprzez wspinanie się na ogrodzenie lub wyłamanie ogrodzenia; 3) minimalna wysokość wynosi 250 cm; 4) górna część jest zabezpieczona z obu stron przed wspinaniem się i przechodzeniem przez ogrodzenie; 5) zapewnia łatwe monitorowanie; 6) jest przeważnie wspomagane innymi systemami zabezpieczenia ogrodzenia, takimi jak system dozom wizyjnego, system wykrywania naruszenia ogrodzenia; 7) jeśli to możliwe, między budynkami a ogrodzeniem zachowana jest wolna przestrzeń o szerokości 25 m.
Typ 3 3 pkt	Ogrodzenie charakteryzuje się następującymi cechami: 1) zapewnia średni poziom zabezpieczenia, jest zaprojektowane w celu utrudnienia i opóźnienia działań dobrze przygotowanego intruza/włamywacza, który dysponuje ograniczoną liczbą narzędzi ręcznych; 2) projekt i konstrukcja ogrodzenia zapewniają odporność na próby wspinania się na ogrodzenie lub wyłamanie ogrodzenia; 3) minimalna wysokość wynosi 250 cm; 4) górna część jest zabezpieczona przed wspinaniem się i przechodzeniem przez ogrodzenie; 5) zapewnia łatwe monitorowanie; 6) jeśli to możliwe, między budynkami a ogrodzeniem zachowana jest wolna przestrzeń o szerokości 25 m.
Typ 2 2 pkt	Ogrodzenie charakteryzuje się następującymi cechami: 1) zabezpiecza przed włamaniem, zapewnia umiarkowany poziom odporności na próby wspinania się na ogrodzenie lub wyłamanie ogrodzenia przez nieprofesjonalnego włamywacza/intruza, niedysponującego określonymi umiejętnościami i posługującego się powszechnie dostępnymi, typowymi narzędziami; 2) minimalna wysokość wynosi 250 cm.
<u>Typ 1</u> <u>1 pkt</u>	Ogrodzenie jest zaprojektowane bez uwzględnienia żadnych szczególnych wymagań w zakresie bezpieczeństwa; takie ogrodzenie służy wyłącznie do wyznaczenia granic terenu i zapewnienia minimalnego zabezpieczenia przed osobami innymi niż zdeterminowany włamywacz/intruza.

Środek bezpieczeństwa K6S2 - Kontrola w punktach dostępu

Typ / Punktacja	Funkcje lub cechy
<u>Tak = 1 pkt</u>	Bramy i wejścia są zbudowane zgodnie z tym samym standardem bezpieczeństwa co ogrodzenie oraz zapewniona jest kontrola dostępu.
Nie = 0 pkt	Uwaga: skuteczność każdego ogrodzenia zależy w dużym stopniu od poziomu bezpieczeństwa zapewnionego przy punktach dostępu umieszczonych w ogrodzeniu.

Środek bezpieczeństwa K6S3 - System kontroli osób i przedmiotów przy wejściu/wyjściu

Typ / Punktacja	Funkcje lub cechy
<u>Tak = 1 pkt</u>	Elektroniczny system pomocniczy lub rozwiązanie organizacyjne polegające na zwracaniu się o dobrowolne poddanie się kontroli lub udostępnienie do kontroli rzeczy osobistych, a także przedmiotów wnoszonych lub wynoszonych - stosowany w celu zapobiegania próbom nieuprawnionego wnoszenia na chroniony obszar rzeczy zagrażających bezpieczeństwu informacji niejawnych lub nieuprawnionego wynoszenia informacji niejawnych z budynków lub obiektów.
Nie = 0 pkt	

Środek bezpieczeństwa K6S4 - System wykrywania naruszenia ogrodzenia

Typ / Punktacja	Funkcje lub cechy
Tak = 1 pkt	1) jest stosowany przy ogrodzeniu w celu zwiększenia poziomu bezpieczeństwa zapewnionego przez ogrodzenie; 2) jest instalowany w formie zamaskowanych urządzeń bądź też widocznego sprzętu, co działa jak czynnik odstraszający.
<u>Nie = 0 pkt</u>	Ponieważ może wywoływać fałszywe alarmy, to należy go stosować tylko w połączeniu z systemem weryfikacji alarmu, takim jak na przykład system dozoru wizyjnego.

Środek bezpieczeństwa K6S5 - Oświetlenie chronionego obszaru

Typ / Punktacja	Funkcje lub cechy
<u>Tak = 1 pkt</u>	Oświetlenie jest czynnikiem odstrasżającym potencjalnych intruzów, jak również zapewniającym widoczność wymaganą, aby można było skutecznie - bezpośrednio (personel bezpieczeństwa) lub pośrednio (dozór wizyjny) - kontrolować obszar.
Nie = 0 pkt	Charakteryzuje się następującymi cechami: 1) standard oświetlenia jest zgodny z minimalnymi wymaganiami określonymi dla systemu dozoru wizyjnego (jeżeli taki system zastosowano); 2) instalacja oświetlenia uwzględnia warunki terenu.

Środek bezpieczeństwa K6S6 - System dozoru wizyjnego granic

Typ / Punktacja	Funkcje lub cechy
<u>Tak = 1 pkt</u>	System z obowiązkową rejestracją w rozdzielczości nie mniejszej niż 400 linii telewizyjnych i przechowywaniem zarejestrowanego zapisu przez czas nie krótszy niż 30 dni.
Nie = 0 pkt	

Część IV. Punktacja zastosowanych środków bezpieczeństwa fizycznego

ŚRODEK BEZPIECZEŃSTWA	PKT
KATEGORIA K1: Szafy do przechowywania informacji niejawnych	
Środek bezpieczeństwa K1S1 - Konstrukcja szafy	
Liczba punktów za środek bezpieczeństwa (K1S1 = 4, 3, 2 lub 1 pkt)	3
Środek bezpieczeństwa K1S2 - Zamek do szafy	
Liczba punktów za środek bezpieczeństwa (K1S2 = 4, 3, 2 lub 1 pkt)	2
Liczba punktów za kategorię K1 stanowiąca iloczyn liczby punktów za oba powyższe środki bezpieczeństwa (K1=K1S1xK1S2)	5
KATEGORIA K2: Pomieszczenia	
Środek bezpieczeństwa K2S1 - Konstrukcja pomieszczenia	
Liczba punktów za środek bezpieczeństwa (K2S1 = 4, 3, 2 lub 1 pkt)	2
Środek bezpieczeństwa K2S2 - Zamek do drzwi pomieszczenia	
Liczba punktów za środek bezpieczeństwa (K2S2 = 4, 3, 2 lub 1 pkt)	3
Liczba punktów za kategorię K2 stanowiąca iloczyn liczby punktów za oba powyższe środki bezpieczeństwa (K2=K2S1xK2S2)	6
KATEGORIA K3: Budynki	
Liczba punktów za kategorię (K3 = 5, 3, 2 lub 1 pkt)	3
KATEGORIA K4: Kontrola dostępu	
Środek bezpieczeństwa K4S1 - Systemy kontroli dostępu	
Liczba punktów za środek bezpieczeństwa (K4S1 = 4, 3, 2 lub 1 pkt)	1
Środek bezpieczeństwa K4S2 - Kontrola osób nieposiadających stałego upoważnienia do wejścia na obszar jednostki organizacyjnej (interesantów)	
Liczba punktów za środek bezpieczeństwa (K4S2 = 3 lub 1 pkt)	0
Liczba punktów za kategorię K4 stanowiąca sumę liczby punktów za oba powyższe środki bezpieczeństwa (K4=K4S1+K4S2)	1
KATEGORIA K5: Personel bezpieczeństwa i systemy sygnalizacji napadu i włamania	
Środek bezpieczeństwa K5S1 - Personel bezpieczeństwa	
Liczba punktów za środek bezpieczeństwa (K5S1 = 5, 4, 3, 2 lub 1 pkt)	2

Środek bezpieczeństwa K5S2 - Systemy sygnalizacji napadu i włamania	
Liczba punktów za środek bezpieczeństwa (K5S2 = 4, 3, 2 lub 1 pkt)	0
Liczba punktów za kategorię K5 stanowiąca sumę liczby punktów za oba powyższe środki bezpieczeństwa (K5=K5S1+K5S2)	2
KATEGORIA K6: Granice	
Środek bezpieczeństwa K6S1 – Ogrodzenie	
Liczba punktów za środek bezpieczeństwa (K6S1 = 4, 3, 2 lub 1 pkt)	1
Środek bezpieczeństwa K6S2 - Kontrola w punktach dostępu	
Liczba punktów za środek bezpieczeństwa (K6S2 = 1 lub 0 pkt)	1
Środek bezpieczeństwa K6S3 - System kontroli osób i przedmiotów przy wejściu/wyjściu	
Liczba punktów za środek bezpieczeństwa (K6S3 = 1 lub 0 pkt)	1
Środek bezpieczeństwa K6S4 - System wykrywania naruszenia ogrodzenia	
Liczba punktów za środek bezpieczeństwa (K6S4 = 1 lub 0 pkt)	0
Środek bezpieczeństwa K6S5 - Oświetlenie chronionego obszaru	
Liczba punktów za środek bezpieczeństwa (K6S5 = 1 lub 0 pkt)	1
Środek bezpieczeństwa K6S6 - System dozoru wizyjnego granic	
Liczba punktów za środek bezpieczeństwa (K6S6 = 1 lub 0 pkt)	1
Liczba punktów za kategorię K6 stanowiąca sumę liczby punktów za powyższe środki bezpieczeństwa (K6=K6S1+K6S2+K6S3+K6S4+K6S5+K6S6)	5
Ogólna liczba punktów stanowiąca sumę punktów za wszystkie kategorie PUNKTY=K1+K2+K3+K4+K5+K6	22

Podsumowanie:

Dla zagrożeń na poziomie **11** punktów (zdefiniowany poziom zagrożeń Starostwa powiatowego w Grudziądzu) wymagania w zakresie stosowania środków bezpieczeństwa fizycznego określono następująco:

1. kategorie K1+K2+ K3 – minimum 6 punktów (kategorie obowiązkowe),
2. kategorie K4+K5 – minimum 2 punkty (kategorie obowiązkowe),
3. kategoria K6 – 3 punkty (kategoria dodatkowa - nieobowiązkowa).

Ogólna liczba punktów we wszystkich kategoriach tj.: od K1 do K6 przy stosowanych obecnie środkach bezpieczeństwa, dla Starostwa Powiatowego w Grudziądzu wynosi **22** punkty.

Suma punktów w kategoriach **K1+K2+ K3**, które są obowiązkowe, wynosi **14 pkt** i w całości wypełnia wymagania wynikające z Części II.

Suma punktów w kategoriach **K4 +K5**, które są obowiązkowe, wynosi **3 pkt** i w całości wypełnia wymagania wynikające z Części II.

W chwili obecnej zastosowane środki ochrony odpowiadają wymaganiom określonym w Rozporządzeniu Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych (Dz.U.2012.683).