

Zarządzenie Nr 51/2013
Starosty Jarocińskiego
z dnia 25 listopada 2013r.

w sprawie wprowadzenia i zatwierdzenia Planu ochrony informacji niejawnych,
Dokumentacji określającej poziom zagrożeń i właściwego doboru środków bezpieczeństwa
fizycznego dla systemu ochrony informacji niejawnych, Instrukcji określającej sposób i tryb
przetwarzania informacji niejawnych o klauzuli „POUFNE” i Instrukcji określającej sposób
i tryb przetwarzania informacji niejawnych o klauzuli „ZASTRZEŻONE” w Starostwie
Powiatowym w Jarocinie.

Na podstawie art. 15 ust. 1 pkt 5, art. 43 ust. 3, 4 i 5 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2010 r. poz. 182 nr 1228), § 3 Rozporządzenia Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych (Dz. U. z 2012 r. poz. 683), zarządzam co następuje:

§ 1. 1. Zatwierdzam i wprowadzam do stosowania Plan Ochrony Informacji Niejawnych w Starostwie Powiatowym w Jarocinie, stanowiący załącznik Nr 1 do zarządzenia.

2. Informacje zawarte w Planie związane z ochroną informacji niejawnych oraz sposobami ich ochrony, nie podlegają publikacji i są przeznaczone do użytku służbowego.

3. Plan przechowuje Pełnomocnik ds. ochrony informacji niejawnych.

§ 2. 1. Zatwierdzam wzór Dokumentacji określającą poziom zagrożeń dla systemu ochrony informacji niejawnych w Starostwie Powiatowym w Jarocinie, stanowiącą załącznik Nr 2 do zarządzenia.

2. Pełnomocnik ds. ochrony informacji niejawnych na podstawie wzoru dokumentacji o którym mowa w ust. 1, określi poziom zagrożeń dla systemu ochrony informacji niejawnych w Starostwie Powiatowym w Jarocinie.

3. Poziom zagrożeń o której mowa w ust. 2 podlega zatwierdzeniu przez Starostę.

4. Dokumentacja o której mowa w ust. 3, zawierająca informacje związane z ochroną informacji niejawnych oraz sposobami ich ochrony, nie podlega publikacji i jest przeznaczona do użytku służbowego.

5. Dokumentacja podlega stałej aktualizacji i po jej dokonaniu podlega zatwierdzeniu.

6. Dokumentację określającą poziom zagrożeń przechowuje Pełnomocnik ds. ochrony informacji niejawnych.

§ 3. Zatwierdzam i wprowadzam do stosowania Instrukcję określającą sposób i tryb przetwarzania informacji niejawnych o klauzuli „POUFNE” w Starostwie Powiatowym w Jarocinie, stanowiącą załącznik Nr 3 do zarządzenia.

§ 4. Zatwierdzam i wprowadzam do stosowania Instrukcję określającą sposób i tryb przetwarzania informacji niejawnych o klauzuli „ZASTRZEŻONE” w Starostwie Powiatowym w Jarocinie, stanowiącą załącznik Nr 4 do zarządzenia.

§ 5. 1. Zobowiązuję pracowników Starostwa do wprowadzenia i stosowania ustaleń zawartych w dokumentach o których mowa w § 1, 3 i 4.

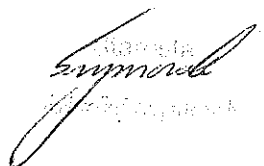
2. Nadzór nad realizacją postanowień niniejszego zarządzenia powierzam Pełnomocnikowi ds. ochrony informacji niejawnych.

§ 6

Traci moc Zarządzenie Nr 27/2008 Starosty Jarocińskiego z dnia 30 kwietnia 2008 roku w sprawie w sprawie wprowadzenia Planu Ochrony Informacji Niejawnych w Starostwie Powiatowym w Jarocinie.

§ 7

Zarządzenie wchodzi w życie z dniem podpisania.



Starosta
Jarocin

Sprawdzono pod względem
prawnym

RADCA PRAWNY

Tomasz Kuderski



Do użytku służbowego

Egz. Pojedynczy

ZATWIERDZAM

OIN.1410.1.2013.KR

Starosta
[Signature]
Jarocin Szymczak

PLAN OCHRONY INFORMACJI NIEJAWNYCH STAROSTWA POWIATOWEGO W JAROCINIE

**Pełnomocnik ds. Ochrony
Informacji Niejawnych**

[Signature]
Roman Król

**JAROCIN
2013**

Spis treści

L.p.	Nazwa jednostki redakcyjnej	Nr strony
Wstęp		3
Część I	Postanowienia ogólne	3
Część II	Przedmiot ochrony	6
Część III	Opis jednostki	6
	1. Charakterystyka jednostki	6
	2. Organizacja jednostki	7
	3. Organizacja ochrony informacji niejawnych	7
	4. Charakterystyka zatrudnienia i czas pracy	8
	5. Charakterystyka obiektu	9
	6. Ocena zagrożeń obiektu	11
Część IV	Strefy ochronne	12
	1. Strefa ochronna III – administracyjna	12
	2. Strefa ochronna II – bezpieczeństwa	13
	3. Strefa ochronna I – Kancelaria niejawna	13
	4. Organizacja pracy	14
Część V	Organizacja systemu dostępu do stref ochronnych	15
Część VI	Organizacja systemu ochrony fizycznej oraz opis zastosowanych rozwiązań organizacyjnych	16
Część VII	Procedury bezpieczeństwa dla strefy ochronnej I, strefy ochronnej II, strefy ochronnej III oraz specjalnej strefy ochronnej	17
Część VIII	Procedury zarządzania kluczami i kodami dostępu do pomieszczeń i urządzeń technicznych przeznaczonych do przechowywania i przetwarzania informacji niejawnych	18
Część IX	Bezpieczeństwo informacji niejawnych	19
	1. Poziom zagrożenia	19
	2. Dobór środków ochrony fizycznej	20
	3. Zabezpieczenie informacji niejawnych	20
	4. Zasady dostępu do informacji niejawnych	20
	5. Zakres udostępniania informacji niejawnych	22
	6. Ewidencja informacji niejawnych	22
	7. Nadzór w zakresie ochrony informacji niejawnych	22
Część VII	Procedury reagowania personelu jednostki organizacyjnej na zdarzenia i incydenty bezpieczeństwa oraz w przypadkach zagrożenia ujawnienia lub utraty informacji niejawnych	22
Część X	Plany awaryjne uwzględniające potrzebę ochrony informacji niejawnych działania w razie wystąpienia sytuacji szczególnych, w tym wprowadzenia stanów nadzwyczajnych, w celu zapobieżenia utracie poufności, integralności lub dostępności informacji niejawnych	24
Część X	Odpowiedzialność karna, dyscyplinarna i służbowa za naruszenie przepisów o ochronie informacji niejawnych	27
Część X	Ustalenia końcowe	27
Załączniki		

WZÓR



Do użytku służbowego
Po wypełnieniu

ZATWIERDZAM

OIN.1410. .2013.

Dokumentacja
określająca poziom zagrożeń i właściwego
doboru środków bezpieczeństwa fizycznego
dla systemu ochrony informacji niejawnych
Starostwa Powiatowego w Jarocinie

Pełnomocnik ds. Ochrony
Informacji Niejawnych

JAROCIN
2013

Spis treści

Wstęp

Rozdział 1 PODSTAWOWE KRYTERIA I SPOSÓB OKREŚLANIA POZIOMU ZAGROŻEŃ

I. Wstęp

II. Objaśnienia

TABELA DO OKREŚLENIA POZIOMU ZAGROŻEŃ TABELA OCENY ISTOTNOŚCI CZYNNIKÓW ZAGROŻEŃ

TABELA DO OKREŚLENIA POZIOMU ZAGROŻEŃ

Rozdział 2 METODYKA DOBORU ŚRODKÓW BEZPIECZEŃSTWA FIZYCZNEGO

Część I. Instrukcja

Część II. Podstawowe wymagania bezpieczeństwa fizycznego

Część III. Klasyfikacja środków bezpieczeństwa fizycznego

Część IV. Punktacja zastosowanych środków bezpieczeństwa fizycznego

Podsumowanie

Wstęp

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 oraz dokonanie oceny zastosowanych środków bezpieczeństwa i ich zgodności z wymaganiami określonymi w rozporządzeniu dla systemu ochrony informacji niejawnych w Starostwie Powiatowym w Jarocinie.

Analizą objęto obiekt będący własnością powiatu jarocińskiego, zlokalizowany pod adresem: Al. Niepodległości 10-12, 63-200 Jarocin, w którym znajduje się pomieszczenie Kancelarii Niejawnej stanowiące głównym miejscem przetwarzania informacji niejawnych w Starostwie i będąca miejscem przechowywania dokumentów i materiałów oznaczonych klauzulą „POUFNE” oraz „ZASTRZEŻONE”.

Dokumentacja składa się z dwóch rozdziałów powiązany ze sobą. W pierwszym określa się poziom zagrożeń dla informacji niejawnych przetwarzanych w Starostwie, a w drugim dokonuje się oceny zastosowanych środków bezpieczeństwa. Prawidłowo przeprowadzona analiza zagrożeń i zastosowanych środków bezpieczeństwa wskazuje wszystkie istotne czynniki mogące mieć wpływ na bezpieczeństwo informacji niejawnych w Starostwie.

System środków bezpieczeństwa fizycznego obejmuje stosowanie rozwiązań organizacyjnych, wyposażenia i urządzeń służących ochronie informacji niejawnych oraz elektronicznych systemów pomocniczych wspomagających ochronę informacji niejawnych. W zależności od poziomu zagrożeń określonego w wyniku przeprowadzenia analizy stosuje się odpowiednią kombinację środków bezpieczeństwa fizycznego wskazaną w dokumentacji.

Dokumentacja po dokonanej analizie i zatwierdzeniu przez Starostę Jarocińskiego jest dokumentacją do użytku służbowego i podlega ochronie. Dokumentację przechowuje Pełnomocnik ds. ochrony informacji niejawnej.

Definicje użyte w dokumentacji:

- 1) **personel bezpieczeństwa** – osoby przeszkolone, nadzorowane, a w razie konieczności posiadające odpowiednie uprawnienie do dostępu do informacji niejawnych, wykonujące czynności związane z fizyczną ochroną informacji niejawnych, w tym kontrolę dostępu do pomieszczeń lub obszarów, w których są przetwarzane informacje niejawne, nadzór nad systemem dozoru wizyjnego, a także reagowanie na alarmy lub sygnały awaryjne;
- 2) **bariery fizyczne** – środki chroniące granice miejsca, w którym są przetwarzane informacje niejawne, w szczególności ogrodzenia, ściany, bramy, drzwi i okna;
- 3) **szafy i zamki** – stosowane do przechowywania informacji niejawnych lub zabezpieczające te informacje przed nieuprawnionym dostępem;
- 4) **system kontroli dostępu** – obejmujący elektroniczny system pomocniczy lub rozwiązanie organizacyjne, stosowany w celu zagwarantowania uzyskiwania dostępu do pomieszczenia lub obszaru, w którym są przetwarzane informacje niejawne, wyłącznie przez osoby posiadające odpowiednie uprawnienia;
- 5) **system sygnalizacji włamania i napadu** – elektroniczny system pomocniczy stosowany w celu realizacji procedur ochrony informacji niejawnych oraz podwyższenia poziomu bezpieczeństwa, który zapewniają bariery fizyczne, a w pomieszczeniach i budynkach zastępujący lub wspierający personel bezpieczeństwa;
- 6) **system dozoru wizyjnego** – elektroniczny system pomocniczy stosowany w celu bieżącego monitorowania ochronnego lub sprawdzania incydentów bezpieczeństwa i sygnałów alarmowych przez personel bezpieczeństwa;
- 7) **system kontroli osób i przedmiotów** – obejmujący 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.

Rozdział 1

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 podsumować. 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

Lp.	CZYNNIK	OCENA ISTOTNOŚCI CZYNNIKA				UZASADNIENIE	WSKAZÓWKI
		BARDZO ISTOTNY (8 pkt)	ISTOTNY (4 pkt)	MAŁO ISTOTNY (1 pkt)	6		
1	2	3	4	5	7		
1	Klauzula tajności przetwarzanych informacji niejawnych					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					Przy ocenie istotności czynnika należy brać pod uwagę wszystkie materiały niejawne zarejestrowane w urzędzeniach 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					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					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					Na wzrost oceny istotności tego czynnika ma wpływ np. to, że budynek użytkowany jest wspólnie z 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.	

Lp.	CZYNNIK	OCENA ISTOTNOŚCI CZYNNIKA				UZASADNIENIE	WSKAZÓWKI
		BARDZO ISTOTNY (8 pkt)	ISTOTNY (4 pkt)	MAŁO ISTOTNY (1 pkt)			
1	2	3	4	5	6	7	
6	Dostęp osób do budynku						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*)						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) lub szkody górnicze.
Suma punktów						POZIOM	

*) Jeśli kierownik jednostki organizacyjnej uzna, że w jego jednostce występują inne niż wymienione w wierszach 1-6 tabeli czynniki mające wpływ na zagrożenie ujawnieniem lub utratą informacji niejawnych, powinien je określić, stanowisko uzasadnić (informacje zamieszcza się w rubryce "Uzasadnienie"), a następnie dokonać oceny istotności tych czynników. Ocenie podlegają wszystkie inne czynniki łącznie. Oznacza to, że jeśli w jednostce występuje tylko jeden z wymienionych czynników, należy go ocenić jako "bardzo istotny", "istotny" lub "mało istotny" dla zagrożenia ujawnieniem lub utratą informacji niejawnych. Jeśli w jednostce występują dwa lub więcej czynników z tej grupy, należy oszacować je łącznie i ocenić wpływ tych czynników na ocenę zagrożenia ujawnieniem lub utratą informacji niejawnych. W sytuacji gdy np. jeden z "innych" czynników został oceniony jako "bardzo istotny", a drugi jako "mało istotny", należy wskazać ocenę o najwyższym znaczeniu (w tym przypadku ocena istotności "Innych czynników" zostałaaby wskazana na poziomie "bardzo istotnym"). W sytuacji gdy kierownik jednostki organizacyjnej uzna, że w jego jednostce czynniki wymienione w tabeli są nieistotne lub ich występowanie jest mało realne (np. zagrożenie ze strony obcych służb specjalnych) czynnik 7 powinien zostać oceniony jako "mało istotny".

TABELA DO OKREŚLENIA POZIOMU ZAGROŻENIA

POZIOM ZAGROŻENIA		
NISKI	ŚREDNI	WYSOKI
1 pkt - 16 pkt	17 pkt - 32 pkt	powyżej 32 pkt

Rozdział 2

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 bezpieczeństwa 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 kategorii 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
ŚCIŚLE TAJNE			
Obowiązkowo: kategorie K1+K2+K3*	10	11	13
Obowiązkowo: kategorie K4+K5**	6	7	7
Dodatkowo: kategoria K6	4	5	5
Łącznie suma punktów	20	23	25
TAJNE			
Obowiązkowo: kategorie K1+K2+K3	8	9	10
Obowiązkowo: kategorie K4+K5***	4	5	5
Dodatkowo: kategoria K6	4	5	5
Łącznie suma punktów	16	19	20
POUFNE			
Obowiązkowo: kategorie K1+K2+K3	6	8	9
Obowiązkowo: kategorie K4+K5	2	3	3
Dodatkowo: kategoria K6	3	3	4
Łącznie suma punktów	11	14	16
ZASTRZEŻONE			
Obowiązkowo: kategorie K1+K2+K3	2	2	2
Dodatkowo: kategoria K4, K5 lub K6	-	1	2
Łącznie suma punktów	2	3	4

* tylko jedna z wartości może być równa 0.

** żadna z wartości nie może być mniejsza od 2.

*** żadna z wartości nie może być równa 0.

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, niewyposazony 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 szyfowym i spełnia co najmniej wymagania klasy B określone w Polskiej Normie PN-EN 1300. Rozróżnia się: 1) zamek mechaniczny szyfowy co najmniej trzytarczowy, o cichym przesuwie, posiadający min. 100 podziałek na pokrętle i skali nastawień, przy której w przypadku każdej tarczy zamek trzytarczowy nie otworzy się, jeżeli pokrętko jest przekręcone więcej niż o 1 kreskę podziałki po obu stronach właściwej kreski podziałki, a w przypadku zamka czterotarczowego wartość ta wynosi 1,25. Zamek powinien być odporny na manipulację przez eksperta, również przy użyciu specjalistycznych narzędzi, przez okres 20 roboczych godzin. Zamek powinien być zabezpieczony przed działaniem destrukcyjnym, w tym przed przewierceniem i przeswietenieniem (atakami) radiologicznym (promieniomie 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 szyfowy spełnia te same wymagania co zamek mechaniczny szyfowy oraz nie generuje sygnałów, które mogą być wykorzystane do otwarcia zamka przez okres 20 roboczych godzin.
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 szyfowym i spełnia co najmniej wymagania klasy B określone w Polskiej Normie PN-EN 1300. Rozróżnia się: 1) zamek mechaniczny szyfowy co najmniej trzytarczowy, o cichym przesuwie, posiadający min. 100 podziałek na pokrętle i skali nastawień, przy której w przypadku każdej tarczy zamek trzytarczowy nie otworzy się, jeżeli pokrętko jest przekręcone więcej niż o 1 kreskę podziałki po obu stronach właściwej kreski podziałki, a w przypadku zamka czterotarczowego 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 szyfowy spełnia te same wymagania co zamek mechaniczny szyfowy oraz nie generuje sygnałów, które mogą być wykorzystane do otwarcia

	zamka przez okres 20 roboczych godzin.
Typ 2 2 pkt	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) zapewnienia wysoką odporność na próby wymuszenia otwarcia oraz otwarcia z wykorzystaniem wielu różnych zaawansowanych narzędzi ręcznych i zasilanych prądem; 2) zapewnienia 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) zapewnienia wysoką odporność na działania osoby nieuprawnionej próbującej uzyskać dostęp siłą lub za pomocą różnorodnych narzędzi ręcznych; 2) zapewnienia 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.
Typ 2 2 pkt	Konstrukcja pomieszczenia charakteryzuje się następującymi cechami: 1) zapewnienia względna odporność na działania osoby nieuprawnionej próbującej uzyskać dostęp siłą lub za pomocą ograniczonej liczby narzędzi ręcznych; 2) zapewnienia 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 sklejek oraz płyty gipsowej 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 spełniają co 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 zamków oraz standard zabezpieczenia okien powinien być odpowiednio wyższy, adekwatnie do poziomu zagrożenia.

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.
Typ 3 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 największy jego element zewnętrzny.

Typ/ Punktacja	Funkcje lub cechy
Typ 4 5 pkt	Budynek charakteryzuje się wytrzymałą konstrukcją i następującymi cechami: 1) zapewnienia wysokiego poziomu odporności na próby włamania; 2) ścian, podłoga i strop są wykonane ze zbrojonego betonu lub podobnego materiału; 3) drzwi są wykonane ze stali wzmocnionej lub drewna pokrytego blachą stalową; 4) rama, mocowanie i szyby okien zapewniają zabezpieczenie przed fizycznym włamaniem, a ich powierzchnia jest jak najmniej szkodliwa.
Typ 3 3 pkt	Budynek charakteryzuje się następującymi cechami: 1) zapewnienia średniego poziomu 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 (rynną, drabiną, 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) zapewnienia średniego poziomu 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 itd.).
------------------------	--

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) sygnali 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 umożliwia odbycie 2 lub 3 patroli w nocy i przeprowadzenie 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 2 pkt	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 ogrodenia; 2) strażnicy nie mają uprawnień dostępu do danego obiektu lub budynku, ale w przypadku podejrzenia włamania zareagują poprzez wezwanie osoby posiadającej klucze.

Środek bezpieczeństwa KSS2 – 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) poruszenie się w chronionym obszarze (pułapkowo – 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 przebywała 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) poruszenie się w chronionym obszarze (pułapkowo – 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) poruszenie 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) poruszenie 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 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 dozoru 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.
Typ 1 1 pkt	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 zdecydowanie włamywacz/intruzy.

Środek bezpieczeństwa K6S2 – Kontrola w punktach dostępu

Typ/ Punktacja	Funkcje lub cechy
TAK=1 pkt NIE=0 pkt	Bramy i wejścia są zbudowane zgodnie z tym samym standardem bezpieczeństwa co ogrodzenie oraz zapewniona jest kontrola dostępu. 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
TAK=1 pkt NIE=0 pkt	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.

Środek bezpieczeństwa K6S4 – System wykrywania naruszenia ogrodzenia

Typ/ Punktacja	Funkcje lub cechy
TAK=1 pkt NIE=0 pkt	System: 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. 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
TAK=1 pkt NIE=0 pkt	Oświetlenie jest czynnikiem odstraszającym potencjalnych intruzów, jak również zapewniającym widoczność wymaganą, aby można było skutecznie – bezpośrednio (personel bezpieczeństwa) lub pośrednio (dozór wizyjny) – kontrolować obszar. 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
TAK=1 pkt NIE=0 pkt	System z obowiązkową rejestracją w rozdzielczości nie mniejszej niż 400 linii telewizyjnych i przechowywaniem zarejestrowanego zapisu przez czas nie krótszy niż 30 dni.

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)	
Środek bezpieczeństwa K1S2 - Zamek do szafy	
Liczba punktów za środek bezpieczeństwa (K1S2 = 4, 3, 2 lub 1 pkt)	
Liczba punktów za kategorię K1 stanowiącą iloczyn liczby punktów za oba powyższe środki bezpieczeństwa ($K1=K1S1 \times K1S2$)	
KATEGORIA K2: Pomieszczenia	
Środek bezpieczeństwa K2S1 - Konstrukcja pomieszczenia	
Liczba punktów za środek bezpieczeństwa (K2S1 = 4, 3, 2 lub 1 pkt)	
Środek bezpieczeństwa K2S2 - Zamek do drzwi pomieszczenia	
Liczba punktów za środek bezpieczeństwa (K2S2 = 4, 3, 2 lub 1 pkt)	
Liczba punktów za kategorię K2 stanowiącą iloczyn liczby punktów za oba powyższe środki bezpieczeństwa ($K2=K2S1 \times K2S2$)	
KATEGORIA K3: Budynki	
Liczba punktów za kategorię ($K3 = 5, 3, 2$ lub 1 pkt)	
KATEGORIA K4: Kontrola dostępu	
Środek bezpieczeństwa K4S1 - Systemy kontroli dostępu	
Liczba punktów za środek bezpieczeństwa (K4S1 = 4, 3, 2 lub 1 pkt)	
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)	
Liczba punktów za kategorię K4 stanowiącą sumę liczby punktów za oba powyższe środki bezpieczeństwa ($K4=K4S1+K4S2$)	
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)	
Środek bezpieczeństwa K5S2 - Systemy sygnalizacji napadu i włamania	
Liczba punktów za środek bezpieczeństwa (K5S2 = 4, 3, 2 lub 1 pkt)	
Liczba punktów za kategorię K5 stanowiącą sumę liczby punktów za oba powyższe środki bezpieczeństwa ($K5=K5S1+K5S2$)	
KATEGORIA K6: Granice	
Środek bezpieczeństwa K6S1 – Ogrodzenie	
Liczba punktów za środek bezpieczeństwa (K6S1 = 4, 3, 2 lub 1 pkt)	
Środek bezpieczeństwa K6S2 - Kontrola w punktach dostępu	
Liczba punktów za środek bezpieczeństwa (K6S2 = 1 lub 0 pkt)	
Środek bezpieczeństwa K6S3 - System kontroli osób i przedmiotów przy wejściu/wyjściu	
Liczba punktów za środek bezpieczeństwa (K6S3 = 1 lub 0 pkt)	
Środek bezpieczeństwa K6S4 - System wykrywania naruszenia ogrodzenia	
Liczba punktów za środek bezpieczeństwa (K6S4 = 1 lub 0 pkt)	
Środek bezpieczeństwa K6S5 - Oświetlenie chronionego obszaru	
Liczba punktów za środek bezpieczeństwa (K6S5 = 1 lub 0 pkt)	
Środek bezpieczeństwa K6S6 - System dozoru wizyjnego granic	
Liczba punktów za środek bezpieczeństwa (K6S6 = 1 lub 0 pkt)	
Liczba punktów za kategorię K6 stanowiącą sumę liczby punktów za powyższe środki bezpieczeństwa ($K6=K6S1+K6S2+K6S3+K6S4+K6S5+K6S6$)	
Ogólna liczba punktów stanowiąca sumę punktów za wszystkie kategorie	
PUNKTY=K1+K2+K3+K4+K5+K6	

PODSUMOWANIE

Objaśnienia

Analizę poziom zagrożeń i dobór środków bezpieczeństwa fizycznego rozpatruje się w zakresie przetwarzania informacji niejawnych o najwyższej klauzuli. Nie zwalnia to kierownika jednostki organizacyjne od obowiązku zabezpieczenia pozostałych materiałów niejawnych niższych klauzul jeśli są przetwarzane w innych obiektach lub pomieszczeniach nie objętych tą analizą. Dla nich sporządza się odrębną analizę.

Analizę zagrożeń przeprowadza się w wartości punktowej. Suma z kolumn „Oceny istotności czynnika” z „Tabeli oceny istotnych czynników zagrożeń” wskazuje poziom zagrożenia. Poziom zagrożeń w zależności od skali (punktacyjnej) określa „Tabela do określenia poziomu zagrożeń”.

Dalszym krokiem jest dobór środków bezpieczeństwa fizycznego i/lub weryfikacji istniejących już środków który przeprowadza się w dwóch etapach.

Pierwszy etap przeprowadza się poprzez dokonanie analizy doboru środków bezpieczeństwa fizycznego lub weryfikacji już istniejących z wymogami określonymi w tabelach "Klasyfikacji środków bezpieczeństwa fizycznego" i przypisanie im wartości liczbowych. Wartości liczbowe nanosi się do tabeli „Punktacja zastosowanych środków bezpieczeństwa fizycznego” z której uzyskujemy wynik dla poszczególnych kategorii.

Kolejny etap oparty jest na porównaniu wyników punktowych dla poszczególnych grup kategorii wynikających z tabeli „Punktacja zastosowanych środków bezpieczeństwa fizycznego” do tabeli "Podstawowe wymagania bezpieczeństwa fizycznego". W tabeli "Podstawowe wymagania bezpieczeństwa fizycznego" określono minimalną łączną sumę 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 rozporządzenia. W przypadku niespełnienia minimalnych wymagań należy dokonać doboru adekwatnych środków bezpieczeństwa fizycznego w konkretnym przypadku, który 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”). Jeśli 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.

W przypadku kiedy liczba punktów uzyskanych po zastosowaniu środka należącego do grup kategorii oznaczonych jako „obowiązkowo” i „dodatkowe” jest mniejsza od minimalnej łącznej sumy punktów wymaganych do osiągnięcia założonego poziomu ochrony informacji niejawnych, należy zastosować środki bezpieczeństwa fizycznego, które zagwarantują osiągnięcia minimalnego poziomu ochrony.

Ostatnim krokiem jest zatwierdzenie przez kierownika poziomu zagrożeń oraz zastosowanych środków bezpieczeństwa fizycznego wg. poniższego wzoru.

WZÓR

Jarocin, dnia

Do użytku służbowego

Po wypełnieniu

ZATWIERDZAM

Ocena
poziomu zagrożeń do zastosowanych środków bezpieczeństwa fizycznego
w Starostwie Powiatowym w Jarocinie

I. Klauzule tajności przetwarzanych informacji niejawnych			
Najwyższa klauzula tajności		Pozostałe klauzule tajności	
II. Poziom zagrożeń nieuprawnionego ujawnienia lub utraty informacji niejawnych			
Liczba pkt z „Oceny istotności czynników zagrożeń”		Poziom zagrożeń wynikający z „Tabeli do określania poziomu zagrożeń”	
III. Zabezpieczenie informacji niejawnych i dobór środków bezpieczeństwa fizycznego			
Obowiązująca norma*		Starostwo	Uwagi
Najwyższa klauzula tajności informacji przetwarzanych w jednostce organizacyjnej	Poziom zagrożeń	Punktacja zastosowanych środków bezpieczeństwa fizycznego	
POUFNE			
Obowiązkowo: kategorie K1+K2+K3			
Obowiązkowo: kategorie K4+K5			
Dodatkowo: kategoria K6			
Łącznie suma punktów			
ZASTRZEŻONE			
Obowiązkowo: kategorie K1+K2+K3			
Dodatkowo: kategoria K4, K5 lub K6			
Łącznie suma punktów			
IV. Ocena prawidłowego zabezpieczenie informacji niejawnych i doboru odpowiednich środków bezpieczeństwa fizycznego			
Klauzula tajności	Norma	Uwagi	
Obowiązkowo: kategorie K1+K2+K3			
Obowiązkowo: kategorie K4+K5			
Dodatkowo: kategoria K6			
Klauzula tajności	Norma	Uwagi	
Obowiązkowo: kategorie K1+K2+K3			
Dodatkowo: kategoria K4, K5 lub K6			
V. Podsumowanie			

* Obowiązujące wskazania z tabeli „Podstawowe wymagania bezpieczeństwa fizycznego”

** Spełnienie obowiązujących wskazań z tabeli „Podstawowe wymagania bezpieczeństwa fizycznego”

.....
(Podpis Pełnomocnika ds. oin)



ZATWIERDZAM
OIN.1410.1.2013.KR

[Signature]
Starosta
Jarocin

Instrukcja
dotycząca sposobu i trybu przetwarzania
informacji niejawnych o klauzuli „poufne”
W
Starostwie Powiatowym w Jarocinie

Pełnomocnik ds. Ochrony
Informacji Niejawnych

[Signature]
Roman Król

Wstęp

§ 1

Instrukcja określa zasady i sposób postępowania z informacjami niejawnymi oznaczonymi klauzulą „poufne” oraz zasady ochrony tych informacji w Starostwie Powiatowym w Jarocinie, zwanym dalej Starostwem.

§ 2

Instrukcja dotyczy wszystkich pracowników Starostwa bez względu na zajmowane przez nich stanowiska, jeśli łączą się one z dostępem do informacji niejawnych oznaczone klauzulą „poufne”.

Rozdział I

Przetwarzanie i dostęp do informacji niejawnych oznaczonych klauzulą „poufne”

§ 3

1. Starostwo przetwarza informacje niejawne o klauzuli „poufne”, zwane dalej dokumentami „poufnymi”.
2. Przez przetwarzanie informacji niejawnych o klauzuli „poufne” rozumie się wszelkie operacje wykonywane w odniesieniu do informacji niejawnych i na tych informacjach, w szczególności ich wytwarzanie, modyfikowanie, kopiowanie, klasyfikowanie, gromadzenie, przechowywanie, przekazywanie lub udostępnianie.
3. Informacjami niejawnymi o klauzuli „poufne” w Starostwie są informacje dotyczące m.in.:
 - 1) realizacji zadań obronnych związanych z bezpieczeństwem państwa,
 - 2) inne – zgodnie z decyzją osób uprawnionych do podpisywania dokumentów „poufnych”.

§ 4

1. Przetwarzanie dokumentów „poufnych” może odbywać się wyłącznie w warunkach zapewniających ochronę przed dostępem osób nieupoważnionych przy zastosowaniu środków ochrony fizycznej.
2. Nadzór nad przetwarzaniem dokumentów „poufnych” w Starostwie prowadzi Pion Ochrony.
3. W komórkach organizacyjnych Starostwa za przetwarzanie dokumentów „poufnych” odpowiadają ich kierownicy.
4. Pracownik Starostwa odpowiada za dokumenty „poufne” które przetwarza.

§ 5

1. Wszystkie dokumenty „poufne” wpływające, wytworzone i wychodzące w Starostwie są ewidencjonowane.
2. Ewidencje, wydawanie i rozliczenie pracownika z wydanych dokumentów „poufnych” prowadzi Kancelaria niejawna.

§ 6

1. Pracownik Pionu Ochrony – Kancelista odpowiedzialny za pracę Kancelarii niejawnej odpowiada za obieg, przechowywanie i ewidencję dokumentów „poufnych” w Starostwie.
2. W sytuacji długotrwałej nieobecności Kancelisty wyznacza się osobę zastępującą lub jego obowiązki może pełnić zastępczo Pełnomocnik ds. ochrony informacji niejawnych.
3. Pomieszczenie Kancelarii jest zabezpieczone w sposób gwarantujący niemożność niekontrolowanego dostępu osób nieuprawnionych. Klucze do Kancelarii przechowywane są zgodnie z Planem ochrony.
4. Przetwarzanie dokumentów „poufnych” w Starostwie odbywa się tylko w strefach ochronnych.
5. Przetwarzanie dokumentów „poufnych” poza strefami ochronnymi może odbywać się wyłącznie w warunkach zapewniających ochronę przed dostępem osób nieupoważnionych, przy zastosowaniu środków ochrony fizycznej określony w przepisach.

§ 7

1. Dostęp do dokumentów „poufnych” może mieć osoba posiadająca poświadczenie bezpieczeństwa upoważniające do dostępu do informacji niejawnych oznaczonych klauzulą „poufne” oraz po odbyciu szkolenia w zakresie ochrony informacji niejawnych.

2. Poświadczenie bezpieczeństwa upoważniające do dostępu do informacji niejawnych oznaczonych klauzulą „poufne” jest wydawane przez Pełnomocnika ds. ochrony informacji niejawnych po przeprowadzonym zwykłym postępowaniu sprawdzającym.
3. Pełnomocnik ds. ochrony informacji niejawnych organizuje szkolenie pracowników z zakresu ochrony informacji niejawnych.
4. Zwykłe postępowanie sprawdzające jest prowadzone w stosunku do pracowników, którzy będą mieli dostęp dokumentów „poufnych” na podstawie przepisów prawa lub wykonywania innych czynności wynikających z zakresu obowiązków lub poleceń przełożonych na zajmowanym stanowisku służbowym.
5. Materiał zawierający informacje niejawne oznaczony klauzulą „poufne” może wytwarzać wyłącznie osoba spełniająca warunki określone w ust. 1.
6. Aktualny wykaz osób, które posiadają uprawnienia do dostępu informacji niejawnych prowadzi Pełnomocnik ds. ochrony informacji niejawnych.

Rozdział II

Wpływ i przyjmowanie materiałów zawierających informacje niejawne oznaczone klauzulą „poufne”

§ 8

Przesyłki zawierające dokumenty „poufne” wpływają do Starostwa za pośrednictwem operatora pocztowego, przewoźnika lub są dostarczone przez nadawcę.

§ 9

1. Przesyłki zawierające dokumenty „poufne” wpływające do Starostwa dostarczane za pośrednictwem operatora pocztowego odbierają pracownicy biura obsługi lub sekretariatu Starostwa, którzy przekazują przesyłki do Kancelarii niejawnej.
2. Pracownik Starostwa, biura obsługi lub sekretariatu, po stwierdzeniu, że przesyłka zawiera dokumenty „poufne” (adnotacja „poufne” na wewnętrznej kopercie) nie otwiera wewnętrznej koperty lecz odciska na niej pieczęć wpływu Starostwa z datą i przekazuje do Kancelarii niejawnej.

§ 10

Przesyłki zawierające dokumenty „poufne” wpływające do Starostwa dostarczane przez przewoźnika lub nadawcę odbierają upoważnieni pracownicy Pionu Ochrony – Kancelarii niejawnej.

§ 11

Korespondencja zawierająca dokumenty „poufne” nie podlega wprowadzaniu i przechowywaniu w elektronicznym systemie obiegu dokumentów.

§ 12

1. W razie stwierdzenia uszkodzenia opakowania wewnętrznej przesyłki oznaczone klauzulą „poufne” lub śladów jej otwierania, osoba przyjmująca przesyłkę sporządza wraz z doręczycielem protokołów uszkodzenia w trzech egzemplarzach, z których pierwszy otrzymuje Pełnomocnik ds. ochrony informacji niejawnych, drugi wysyła się nadawcy, a trzeci pozostawia się w aktach doręczyciela.
2. W przypadku stwierdzenia nieprawidłowości w zawartości przesyłki zawierającej dokumenty „poufne” pracownik Kancelarii niejawnej lub przyjmujący przesyłkę sporządza w dwóch egzemplarzach protokołów z otwarcia przesyłki zawierający opis nieprawidłowości, jeden egzemplarz przekazuje do kancelarii nadawcy a drugi Kancelarii niejawnej. Fakt sporządzenia protokołu odnotowuje się w „Dzienniku ewidencji” w rubryce „Informacje uzupełniające/Uwagi”.

Rozdział III

Obieg, ewidencja, dekretacja i oznaczenie materiałów niejawnych oznaczonych klauzulą „poufne”

§ 13

1. Dokumenty „poufne” wpływające do Starostwa w postaci przesyłek przekazywane są bez zbędnej zwłoki do Kancelarii niejawnej.

2. Otrzymywaną albo wysyłaną przesyłkę bądź wytworzony dokument lub inny materiał o klauzuli „poufne” rejestruje się Kancelarii niejawnej w „Dzienniku ewidencji” odpowiednio w kolejności otrzymania, wysłania lub wytworzenia.
3. Zapisów w „Dzienniku ewidencji” dokonuje się atramentem lub tuszem w kolorze niebieskim lub czarnym. Zmian dokonuje się kolorem czerwonym, umieszczając datę, imię i nazwisko oraz podpis osoby dokonującej zmiany. Anulowania zapisu dokonuje się tak samo, z tym że należy podać powód anulowania zapisu.
4. Przekazywanie dokumentów „poufnych” bezpośrednio adresatowi z pominięciem Kancelarii niejawnej jest zabronione, nawet gdy są oznaczone napisem „Do rąk własnych”.
5. Kancelaria niejawna dokumenty „poufne” po zarejestrowaniu przekazuje do dekretacji, z zastrzeżeniem korespondencji imiennej, którą bez otwierania koperty przekazuje bezpośrednio adresatowi po zarejestrowaniu.
6. Dekretację dokumentów „poufnych” dokonuje Starosta, Pełnomocnik ds. ochrony informacji niejawnych lub adresat.
7. Wydawanie dokumentów „poufnych” adresatom lub osobom wskazanym w dekretacji odbywa się za pokwitowaniem w „dzienniku ewidencyjnym” lub na „karcie pokwitowania dokumentu”.
8. Dekretacji nie umieszcza się na planach i dokumentach stanowiących załączniki do planów.
9. Dekretowanie i wydawanie dokumentów „poufnych” osobie nieposiadającej ważnego poświadczenia bezpieczeństwa jest zabronione.
10. Pracownicy Starostwa pobierający dokumenty „poufne” do pracy nie udostępniają innym pracownikom dokumentu do zapoznania i pracy w przypadku, kiedy taki pracownik wcześniej nie potwierdził faktu zapoznania się w „dzienniku ewidencyjnym” lub na „karcie pokwitowania dokumentu”.

§ 14

1. Pracownicy przetwarzający informacje niejawne nanoszą na materiał informację określającą klauzulę tajności i zmianę lub zniesienie nadanej klauzuli, a także umieszczają dodatkowe dyspozycje.
2. Dokumenty „poufne” oznacza się klauzulą tajności w sposób wyraźny i w pełnym brzmieniu - „poufne”.
3. W przypadku gdy poszczególnym częściom materiału zostały nadane różne klauzule tajności bądź gdy niektóre z tych części są jawne, wyodrębnione części oddziela się oznaczeniem odpowiedniej klauzuli tajności wskazanej w pełnym brzmieniu lub określeniem „jawne”. Części materiału zawierające tekst lub obraz oddziela się przez odpowiednie ich oznaczenie przed rozpoczęciem i po zakończeniu tekstu lub obrazu.
4. Jeżeli poszczególnym częściom materiału zostały nadane różne klauzule tajności, materiał oznacza się klauzulą tajności co najmniej równą najwyższej klauzuli tajności, jaką nadano części materiału.
5. Kontrolę prawidłowości oznaczenia dokumentów „poufnych” przed zarejestrowaniem w „Dzienniku ewidencyjnym” przeprowadza Kancelista.
6. Klauzula nie może być zmieniona lub zniesiona bez zgody osoby odpowiedzialnej za przyznanie klauzuli tajności lub jej przełożonego.
7. Zawyżanie lub zaniżanie klauzuli tajności jest niedopuszczalne.
8. Sposób oznaczania dokumentów „poufnych”, określa 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).

Rozdział IV

Wysyłanie lub przekazywanie materiałów zawierających informacje niejawne oznaczone klauzulą „poufne”

§ 15

1. Przesyłki zawierające dokumenty „poufne” mogą być wysyłane za pomocą operatora pocztowego, przewoźnika lub dostarczane do adresata.

2. Przesyłka zawierająca dokumenty „poufne” powinna być opakowana w dwie koperty lub dwa opakowania: zewnętrzne i wewnętrzne.

§ 16

1. Dokumenty „poufne” wysyła się za pośrednictwem biura obsługi Starostwa, jako przesyłki pocztowe polecone, za zwrotnym potwierdzeniem odbioru i za potwierdzeniem wysyłki przez biuro obsługi w „Wykazie przesyłek nadanych”.
2. Przesyłki zawierające dokumenty „poufne” przekazuje się za pośrednictwem przewoźnika do adresata. Przewoźnik przyjmuje przesyłkę do przewozu i potwierdza przyjęcie w „Wykazie przesyłek nadanych”.
3. Przesyłki zawierające dokumenty „poufne” dostarczają adresatom wyznaczeni pracownicy Starostwa posiadający odpowiednie poświadczenie bezpieczeństwa, najkrótszą drogą, z wykorzystaniem teczki umożliwiającej właściwe zabezpieczenie przesyłki (szyfrowany zamek). Według tych zasad odbywa się również transport tych materiałów do podpisu między budynkami Starostwa. Do potwierdzeń dostarczenia dokumentów niejawnych adresatowi używa się „książki doręczeń przesyłek miejscowych”, „wykazu przesyłek nadanych” lub adresat pisemnie potwierdza odbiór.

§ 17

Przekazywanie dokumentów „poufnych” do przewozu lub przewożonych, osobie nieposiadającej ważnego poświadczenia bezpieczeństwa jest zabronione.

§ 18

Sposób pakowania, adresowania, przesyłania i przewożenia materiałów zawierających informacje niejawne oznaczone klauzulą „poufne” w postaci przesyłek i paczek określa rozporządzenie Prezesa Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne (Dz. U. z 2011 r. Nr 271, poz. 1603).

Rozdział V

Przechowywanie materiałów zawierających informacje niejawne oznaczone klauzulą „poufne”

§ 19

1. Wszystkie materiały zawierające informacje niejawne oznaczone klauzulą „poufne” przechowuje się w Kancelarii niejawnej w szafie metalowej.
2. Dokumenty „poufne” mogą zostać udostępnione tylko w przypadku zagwarantowania warunków zapewniających ochronę dokumentów przed dostępem osób nieupoważnionych przy zastosowaniu środków ochrony fizycznej.

§ 20

1. Dokumenty „poufne” niezbędne do wykonywania pracy z Kancelarii niejawnej pobiera pracownik, który potwierdza odbiór tych materiałów.
2. Dokumenty „poufne” w czasie godzin pracy mogą być przechowywane w pomieszczeniach biurowych, pod warunkiem ich zabezpieczenia przed dostępem osób nieupoważnionych.
3. Za właściwe zabezpieczenie dokumentów „poufnych” odpowiada osoba, która dokument taki wykonuje lub pobrała z Kancelarii niejawnej.
4. Po zakończeniu pracy dokumenty „poufne” zdaje się do Kancelarii niejawnej.

§ 21

Dokumenty „poufne” są przechowywane w Kancelarii niejawnej w teczkach akt o klauzuli „poufne” i oznakowanych zgodnie z jednolitym rzeczowym wykazem akt (rozporządzenie Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt (JRWA) oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych - Dz.U. Nr 14, poz. 67).

§ 22

1. Kancelaria niejawna przechowuje dokumenty „poufne” przechowuje się do czasu kiedy utracą praktyczne znaczenie dla potrzeb komórek Starostwa.

2. Dokumenty „poufne”, które utraciły praktyczne znaczenie, po przeglądzie materiałów w Kancelarii niejawnej, znosi się lub zmienia klauzulę tajności.
3. Dokumenty „poufne” którym zniesiono klauzulę i utraciły praktyczne znaczenie dla potrzeb komórek Starostwa oraz dla celów kontrolnych przekazuje się do archiwum zakładowego lub niszczy.

Rozdział VI

Niszczenie materiałów zawierających informacje niejawne oznaczone klauzulą „poufne”

§ 23

Dokumenty „poufne”, które nie podlegają trwałemu przechowywaniu i utraciły praktyczne znaczenie są brakowane zgodnie z obowiązującymi przepisami archiwalnymi. Dokumenty „poufne” wybrakowane niszczy wykonawca w obecności osoby odpowiedzialnej za ewidencję materiałów niejawnych, a fakt zniszczenia odnotowuje się w rubryce „Uwagi” „Dziennika ewidencyjnego”.

§ 24

Dokumenty „poufne” utrwalone na papierze niszczy się przez pocięcie w niszczarce, która zapewnia zniszczenie materiału w sposób uniemożliwiający odtworzenie jego treści.

Rozdział VII

Przepisy końcowe.

§ 25

Kierownicy komórek organizacyjnych Starostwa zapewniają i nadzorują stosowanie ustaleń zawartych w instrukcji.

§ 26

W przypadku stwierdzenia nieuprawnionego ujawnienia informacji niejawnych o klauzuli „poufne”, należy o tym fakcie natychmiast powiadomić przełożonego i Pełnomocnika ds. ochrony informacji niejawnych, zwanego dalej Pełnomocnikiem.

§ 27

Pełnomocnik powiadamia o fakcie naruszenia przepisów o ochronie informacji niejawnych Starostę i podejmuje niezwłocznie postępowanie wyjaśniające zmierzające do:

- 1) wyjaśnienia okoliczności naruszenia przepisów i ustalenia osób winnych tych naruszeń,
- 2) określenia stopnia szkody i zminimalizowania skutków jej powstania,
- 3) podjęcia przedsięwzięć prewencyjnych.

§28

Pełnomocnik powiadamia o fakcie naruszenia przepisów o ochronie informacji niejawnych o klauzuli „poufne” Agencję Bezpieczeństwa Wewnętrznego.

§ 29

Po zakończeniu postępowania wyjaśniającego, Pełnomocnik występuje do Starosty o wszczęcie przeciwko osobom winnym postępowania służbowego lub dyscyplinarnego.

§ 30

W stosunku do osób posiadających aktualne poświadczenie bezpieczeństwa, które w sposób rażący naruszyły przepisy, Pełnomocnik przeprowadza kontrolne postępowanie sprawdzające.

§ 31

Kontrolę przestrzegania instrukcji w Starostwie sprawuje Pełnomocnik.

Załącznik nr 1
do Instrukcji dotyczącej sposobu
i trybu przetwarzania informacji
niejawnych o klauzuli „poufne”
w Starostwie Powiatowym w Jarocinie

WZÓR

Jarocin, dnia

KARTA POKWITOWANIA DOKUMENTU Nr ...

Oznaczenie dokumentu:

Numer ewidencyjny dokumentu:

L.p.	Imię i nazwisko, stanowisko osoby, której dokument udostępniono	Nr egz. / liczba ark Zapoznanie*	Data	Podpis	Uwagi
1	2	3	4	5	6

*W przypadku zapoznania się z dokumentem pracownik wpisuje „zapoznałem się”

strona 1/2



ZATWIERDZAM
OIN.1410.1.2013.KR

Instrukcja
dotycząca sposobu i trybu przetwarzania
informacji niejawnych o klauzuli
„zastrzeżone”
W
Starostwie Powiatowym w Jarocinie

Pełnomocnik ds. Ochrony
Informacji Niejawnych

Roman Król

Wstęp

§ 1

Instrukcja określa zasady i sposób postępowania z informacjami niejawnymi oznaczonymi klauzulą „zastrzeżone” oraz zasady ochrony tych informacji w Starostwie Powiatowym w Jarocinie, zwanym dalej Starostwem.

§ 2

Instrukcja dotyczy wszystkich pracowników Starostwa bez względu na zajmowane przez nich stanowiska, jeśli łączą się one z dostępem do informacji niejawnych oznaczone klauzulą „zastrzeżone”.

Rozdział I

Przetwarzanie i dostęp do informacji niejawnych oznaczonych klauzulą „zastrzeżone”

§ 3

1. Starostwo przetwarza informacje niejawne o klauzuli „zastrzeżone”, zwane dalej dokumentami „zastrzeżonymi”.
2. Przez przetwarzanie informacji niejawnych o klauzuli „zastrzeżone” rozumie się wszelkie operacje wykonywane w odniesieniu do informacji niejawnych i na tych informacjach, w szczególności ich wytwarzanie, modyfikowanie, kopiowanie, klasyfikowanie, gromadzenie, przechowywanie, przekazywanie lub udostępnianie.
3. Informacjami niejawnymi o klauzuli „zastrzeżone” w Starostwie są informacje dotyczące m.in.:
 - 1) realizacji zadań obronnych związanych z bezpieczeństwem państwa,
 - 2) realizacji poszczególnych zadań operacyjnych w warunkach zewnętrznego zagrożenia bezpieczeństwa państwa i w czasie wojny,
 - 3) organizacji i prowadzenia akcji kurierskiej,
 - 4) ochrony informacji niejawnych
 - 5) inne – zgodnie z decyzją osób uprawnionych do podpisywania dokumentów „zastrzeżonych”.

§ 4

1. Przetwarzanie dokumentów „zastrzeżonych” może odbywać się wyłącznie w warunkach zapewniających ochronę przed dostępem osób nieupoważnionych, przy zastosowaniu środków ochrony fizycznej i zachowaniu zasad bezpieczeństwa teleinformatycznego.
2. Nadzór nad przetwarzaniem dokumentów „zastrzeżonych” w Starostwie prowadzi Pion Ochrony.
3. W komórkach organizacyjnych Starostwa za przetwarzanie dokumentów „zastrzeżonych” odpowiadają ich kierownicy.
4. Pracownik Starostwa odpowiada za dokumenty „zastrzeżone” które przetwarza.

§ 5

1. Systemy komputerowe, w których przetwarzane są informacje niejawne muszą posiadać akredytację bezpieczeństwa teleinformatycznego, zgodnie z przepisami ustawy o ochronie informacji niejawnych.
2. Systemami komputerowymi przystosowanymi do przetwarzania informacji niejawnych, które posiadają akredytację bezpieczeństwa teleinformatycznego, zarządza Pion ochrony Starostwa.
3. Wytwarzanie dokumentów „zastrzeżonych” z wykorzystaniem sprzętu komputerowego nieposiadającego akredytacji jest zabronione i podlega odpowiedzialności służbowej.

§ 6

1. Dostęp do dokumentów „zastrzeżonych” może mieć osoba posiadająca pisemne upoważnienie wydane przez kierownika jednostki organizacyjnej, jeżeli nie posiada poświadczenia bezpieczeństwa upoważniającego do dostępu do informacji niejawnych oznaczonych klauzulą, co najmniej „zastrzeżone” oraz po odbyciu szkolenia w zakresie ochrony informacji niejawnych.
2. Upoważnienie do dostępu do informacji niejawnych oznaczonych klauzulą „zastrzeżone” wydawane jest dla pracowników Starostwa, którzy będą mieli dostęp do informacji niejawnych oznaczonych klauzulą

- „zastrzeżone” na podstawie przepisów prawa lub wykonywania innych czynności wynikających z zakresu obowiązków lub poleceń przełożonych na zajmowanym stanowisku służbowym.
3. Kierownicy komórek organizacyjnych Starostwa składają pisemny wniosek o upoważnienie pracownika do dostępu do tych informacji niejawnych oznaczonych klauzulą „zastrzeżone” do Pełnomocnika ds. ochrony informacji niejawnych. Wzór wniosku określa załącznik do Instrukcji.
 4. Pełnomocnik ds. ochrony informacji niejawnych dokonuje sprawdzenia i weryfikacji wniosku.
 5. Upoważnienie do dostępu do informacji niejawnych podpisuje Starosta lub Pełnomocnik ds. ochrony informacji niejawnych z upoważnienia kierownika jednostki organizacyjnej. Wzór upoważnienia określa załącznik do Instrukcji.
 6. Pełnomocnik ds. ochrony informacji niejawnych organizuje szkolenie pracowników z zakresu ochrony informacji niejawnych.
 7. Materiał zawierający informacje niejawne oznaczony klauzulą „zastrzeżone” może przetwarzać wyłącznie osoba spełniająca warunki określone w ust. 1.
 8. Aktualny wykaz osób, które posiadają uprawnienia do dostępu informacji niejawnych prowadzi Pełnomocnik ds. ochrony informacji niejawnych.

§ 7

1. Wszystkie dokumenty „zastrzeżone” wpływające, wytworzone i wychodzące w Starostwie są ewidencjonowane.
2. Ewidencje dokumentów „zastrzeżonych” prowadzi Kancelaria niejawna.
3. Kancelaria niejawna wydaje dokumenty „zastrzeżone” upoważnionym pracownikom Starostwa.
4. Kancelaria niejawna dokonuje rozliczenia pracownika z wydanych dokumentów „zastrzeżonych”.

Rozdział II

Wpływ i przyjmowanie materiałów zawierających informacje niejawne oznaczone klauzulą „zastrzeżone”

§ 8

Przesyłki zawierające dokumenty „zastrzeżone” wpływają do Starostwa za pośrednictwem operatora pocztowego, przewoźnika lub są dostarczone przez nadawcę.

§ 9

1. Przesyłki zawierające dokumenty „zastrzeżone” wpływające do Starostwa dostarczane za pośrednictwem operatora pocztowego odbierają pracownicy biura obsługi lub sekretariatu Starostwa, którzy przekazują przesyłki do Kancelarii niejawnej.
2. Pracownik Starostwa, biura obsługi lub sekretariatu, po stwierdzeniu, że przesyłka zawiera dokumenty „zastrzeżone” (adnotacja „zastrzeżone” na wewnętrznej kopercie) nie otwiera wewnętrznej koperty lecz odciska na niej pieczęć wpływu Starostwa z datą i przekazuje do Kancelarii niejawnej.

§ 10

Przesyłki zawierające dokumenty „zastrzeżone” wpływające do Starostwa dostarczane przez przewoźnika lub nadawcę odbierają pracownicy Pionu Ochrony – Kancelarii niejawnej.

§ 11

Korespondencja zawierająca dokumenty „zastrzeżone” nie podlega wprowadzaniu i przechowywaniu w elektronicznym systemie obiegu dokumentów.

§ 12

1. W razie stwierdzenia uszkodzenia opakowania wewnętrznej przesyłki oznaczone klauzulą „zastrzeżone” lub śladów jej otwierania, pracownicy biura obsługi, sekretariatu Starostwa lub osoba przyjmująca lub odbierająca przesyłkę sporządza wraz z doręczycielem protokół uszkodzenia w trzech egzemplarzach, z których pierwszy otrzymuje Pełnomocnik ds. ochrony informacji niejawnych, drugi wysyła się nadawcy, a trzeci pozostawia się w aktach doręczyciela.

2. W przypadku stwierdzenia nieprawidłowości w zawartości przesyłki zawierającej dokumenty „zastrzeżone” pracownik Kancelarii niejawnej lub przyjmujący przesyłkę sporządza w dwóch egzemplarzach protokół z otwarcia przesyłki zawierający opis nieprawidłowości, jeden egzemplarz przekazuje do kancelarii nadawcy a drugi Kancelarii niejawnej. Fakt sporządzenia protokołu odnotowuje się w „Dzienniku ewidencji” w rubryce „Informacje uzupełniające/Uwagi”.

Rozdział III

Obieg, ewidencja, dekretacja i oznaczenie materiałów niejawnych oznaczonych klauzulą „zastrzeżone”

§ 13

1. Dokumenty „zastrzeżone” wpływające do Starostwa w postaci przesyłek przekazywane są bez zbędnej zwłoki do Kancelarii niejawnej.
2. Otrzymywaną albo wysyłaną przesyłkę bądź wytworzony dokument lub inny materiał o klauzuli „zastrzeżone” rejestruje się Kancelarii niejawnej w „Dzienniku ewidencji” odpowiednio w kolejności otrzymania, wysłania lub wytworzenia.
3. Zapisów w „Dzienniku ewidencji” dokonuje się atramentem lub tuszem w kolorze niebieskim lub czarnym. Zmian dokonuje się kolorem czerwonym, umieszczając datę, imię i nazwisko oraz podpis osoby dokonującej zmiany. Anulowania zapisu dokonuje się tak samo, z tym że należy podać powód anulowania zapisu.
4. Przekazywanie dokumentów „zastrzeżonych” bezpośrednio adresatowi z pominięciem Kancelarii niejawnej jest zabronione, nawet gdy są oznaczone napisem „Do rąk własnych”.
5. Kancelaria niejawna dokumenty „zastrzeżone” po zarejestrowaniu przekazuje do dekretacji, z zastrzeżeniem korespondencji imiennej, którą bez otwierania koperty przekazuje bezpośrednio adresatowi po zarejestrowaniu.
6. Dekretację dokumentów „zastrzeżonych” dokonuje Starosta, Pełnomocnik ds. ochrony informacji niejawnych lub adresat.
7. Wydawanie dokumentów „zastrzeżonych” adresatom lub osobom wskazanym w dekretacji odbywa się za pokwitowaniem w „Dzienniku ewidencyjnym” lub na „Karcie pokwitowania dokumentu”.
8. Dekretacji nie umieszcza się na planach i dokumentach stanowiących załączniki do planów.
9. Dekretowanie i wydawanie dokumentów „zastrzeżonych” osobie nieposiadającej ważnego poświadczenia bezpieczeństwa lub upoważnienia jest zabronione.

§ 14

1. Pracownicy przetwarzający informacje niejawne nanoszą na materiał informację określającą klauzulę tajności i zmianę lub zniesienie nadanej klauzuli, a także umieszczają dodatkowe dyspozycje.
2. Dokumenty „zastrzeżone” oznacza się klauzulą tajności w sposób wyraźny i w pełnym brzmieniu - „zastrzeżone”.
3. W przypadku gdy poszczególnym częściom materiału zostały nadane różne klauzule tajności bądź gdy niektóre z tych części są jawne, wyodrębnione części oddziela się oznaczeniem odpowiedniej klauzuli tajności wskazanej w pełnym brzmieniu lub określeniem „jawne”. Części materiału zawierające tekst lub obraz oddziela się przez odpowiednie ich oznaczenie przed rozpoczęciem i po zakończeniu tekstu lub obrazu.
4. Jeżeli poszczególnym częściom materiału zostały nadane różne klauzule tajności, materiał oznacza się klauzulą tajności co najmniej równą najwyższej klauzuli tajności, jaką nadano części materiału.
5. Kontrolę prawidłowości oznaczenia dokumentów „zastrzeżonych” przed zarejestrowaniem w „Dzienniku ewidencyjnym” przeprowadza Kancelista.
6. Klauzula nie może być zmieniona lub zniesiona bez zgody osoby odpowiedzialnej za przyznanie klauzuli tajności lub jej przełożonego.
7. Zawyżanie lub zaniżanie klauzuli tajności jest niedopuszczalne
8. Sposób oznaczania dokumentów „zastrzeżonych”, określa 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).

Rozdział IV

Wysyłanie lub przekazywanie materiałów zawierających informacje niejawne oznaczone klauzulą „zastrzeżone”

§ 15

1. Przesyłki zawierające dokumenty „zastrzeżone” mogą być wysyłane za pomocą operatora pocztowego, przewoźnika lub dostarczane do adresata.
2. Przesyłka zawierająca dokumenty „zastrzeżone” powinna być opakowana w dwie koperty lub dwa opakowania: zewnętrzne i wewnętrzne.

§ 16

1. Dokumenty „zastrzeżone” wysyła się za pośrednictwem biura obsługi Starostwa, jako przesyłki pocztowe polecone, za zwrotnym potwierdzeniem odbioru i za potwierdzeniem wysyłki przez biuro obsługi w „Wykazie przesyłek nadanych”.
2. Przesyłki zawierające dokumenty „zastrzeżone” przekazuje się za pośrednictwem przewoźnika do adresata. Przewoźnik przyjmuje przesyłkę do przewozu i potwierdza przyjęcie w „Wykazie przesyłek nadanych”.
3. Przesyłki zawierające dokumenty „zastrzeżone” dostarczają adresatom wyznaczeni pracownicy Starostwa posiadający odpowiednie poświadczenie bezpieczeństwa, najkrótszą drogą, z wykorzystaniem teczki umożliwiającej właściwe zabezpieczenie przesyłki (szyfrowany zamek). Według tych zasad odbywa się również transport tych materiałów do podpisu między budynkami Starostwa. Do potwierdzeń dostarczenia dokumentów niejawnych adresatowi używa się „Książki doręczeń przesyłek miejscowych”, „Wykazu przesyłek nadanych” lub adresat pisemnie potwierdza odbiór.

§ 17

Przekazywanie dokumentów „zastrzeżonych” do przewozu lub przewożonych, osobie nieposiadającej ważnego poświadczenia bezpieczeństwa jest zabronione.

§ 18

Sposób pakowania, adresowania, przesyłania i przewożenia materiałów zawierających informacje niejawne oznaczone klauzulą „zastrzeżone” w postaci przesyłek i paczek określa rozporządzenie Prezesa Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne (Dz. U. z 2011 r. Nr 271, poz.1603).

Rozdział V

Przechowywanie materiałów zawierających informacje niejawne oznaczone klauzulą „zastrzeżone”

§ 19

1. Przechowywanie dokumentów „zastrzeżonych” może odbywać się wyłącznie w warunkach zapewniających ochronę przed dostępem osób nieupoważnionych, przy zastosowaniu środków ochrony fizycznej oraz zachowaniu zasad bezpieczeństwa teleinformatycznego.
2. Dokumenty „zastrzeżone” przechowuje się w Starostwie w strefach ochronnych.
3. Pomieszczenie zlokalizowane w strefach ochronnych są zabezpieczone w sposób gwarantujący niemożność niekontrolowanego dostępu osób nieuprawnionych. Klucze do tych pomieszczeń przechowywane są zgodnie z Planem ochrony.

§ 20

1. Dokumenty „zastrzeżone” można przechować na stanowiskach pracy, poza strefami, w meblach biurowych zamykanych na klucz usytuowanych w pomieszczeniach codziennie zamykanych po zakończeniu pracy.
2. Przechowywanie dokumentów „zastrzeżonych” poza strefami ochronnymi może odbywać się wyłącznie w warunkach zapewniających ochronę przed dostępem osób nieupoważnionych, przy zastosowaniu środków ochrony fizycznej określony w przepisach.

3. Za właściwe zabezpieczenie dokumentu „zastrzeżonego”, przechowywanego poza strefami ochronnymi, odpowiada osoba, która dokument wykonuje lub pobrała z Kancelarii niejawnej.

§ 21

1. Dokumenty „zastrzeżone” niezbędne do wykonywania pracy z Kancelarii niejawnej pobiera pracownik, który potwierdza odbiór tych materiałów.
2. Dokumenty „zastrzeżone” w czasie godzin pracy mogą być przechowywane w pomieszczeniach biurowych, pod warunkiem ich zabezpieczenia przed dostępem osób nieupoważnionych.
3. Po zakończeniu pracy dokumenty „zastrzeżone” przechowuje się w pomieszczeniach biurowych, pod warunkiem ich zabezpieczenia przed dostępem osób nieupoważnionych lub strefach ochronnych albo zdaje się do Kancelarii niejawnej.

§ 22

Dokumenty „zastrzeżone” są przechowywane w teczkach akt i oznaczone zgodnie z jednolitym rzeczowym wykazem akt (rozporządzenie Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt (JRWA) oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych - Dz.U. Nr 14, poz. 67).

§ 23

1. Dokumenty „zastrzeżone” w komórkach Starostwa przechowuje się do czasu kiedy utracą praktyczne znaczenie dla potrzeb komórek Starostwa.
2. Dokumentom „zastrzeżonym”, które utraciły praktyczne znaczenie znosi się klauzulę tajności.
3. Dokumenty „zastrzeżone” którym zniesiono klauzulę i utraciły praktyczne znaczenie dla potrzeb komórek Starostwa oraz dla celów kontrolnych przekazuje się do archiwum zakładowego lub niszczy.

Rozdział VI

Niszczenie materiałów zawierających informacje niejawne oznaczone klauzulą „zastrzeżone”

§ 24

Dokumenty „zastrzeżone”, które utraciły praktyczne znaczenie a nie podlegają trwałemu przechowywaniu, są brakowane zgodnie z obowiązującymi przepisami archiwalnymi. Dokumenty „zastrzeżone” wybrakowane niszczy wykonawca w obecności osoby odpowiedzialnej za ewidencję materiałów niejawnych, a fakt zniszczenia odnotowuje się w rubryce „Uwagi” „Dziennika ewidencyjnego”.

§ 25

Dokumenty „zastrzeżone” utrwalone na papierze niszczy się przez pocięcie w niszczarce, która zapewnia zniszczenie materiału w sposób uniemożliwiający odtworzenie jego treści.

§ 26

Dokumenty „zastrzeżone” zapisane w formie elektronicznej niszczy się przez fizyczne zniszczenie nośnika.

Rozdział VII

Przepisy końcowe.

§ 27

Kierownicy komórek organizacyjnych Starostwa zapewniają i nadzorują stosowanie ustaleń zawartych w instrukcji.

§ 28

W przypadku stwierdzenia nieuprawnionego ujawnienia informacji niejawnych o klauzuli „zastrzeżone”, należy o tym fakcie natychmiast powiadomić przełożonego i Pełnomocnika ds. ochrony informacji niejawnych, zwanego dalej Pełnomocnikiem.

§ 29

Pełnomocnik powiadamia o fakcie naruszenia przepisów o ochronie informacji niejawnych Starostę i podejmuje niezwłocznie postępowanie wyjaśniające zmierzające do:

- 1) wyjaśnienia okoliczności naruszenia przepisów i ustalenia osób winnych tych naruszeń,
- 2) określenia stopnia szkody i zminimalizowania skutków jej powstania,
- 3) podjęcia przedsięwzięć prewencyjnych.

§ 30

Po zakończeniu postępowania wyjaśniającego, Pełnomocnik występuje do Starosty o wszczęcie przeciwko osobom winnym postępowania służbowego lub dyscyplinarnego.

§ 31

W stosunku do osób posiadających upoważnienie do dostępu do informacji niejawnych oznaczonych klauzulą „zastrzeżone”, które w sposób rażący naruszyły przepisy, upoważnienie zostaje cofnięte.

§ 32

Kontrolę przestrzegania instrukcji w Starostwie sprawuje Pełnomocnik.

Załącznik nr 1
do Instrukcji dotyczącej sposobu
i trybu przetwarzania informacji
niejawnych o klauzuli „zastrzeżone”
w Starostwie Powiatowym w Jarocinie

WZÓR

Jarocin, dnia

KARTA POKWITOWANIA DOKUMENTU Nr ...

Oznaczenie dokumentu:

Numer ewidencyjny dokumentu:

L.p.	Imię i nazwisko, stanowisko osoby, której dokument udostępniono	Nr egz. / liczba ark Zapoznanie*	Data	Podpis	Uwagi
		Pokwitowanie odbioru dokumentu			
		Pokwitowanie zwrot dokumentu			
1	2	3	4	5	6

*W przypadku zapoznania się z dokumentem pracownik wpisuje „zapoznałem się”

strona 1/2

Załącznik nr 2
do Instrukcji dotyczącej sposobu
i trybu przetwarzania informacji
niejawnych o klauzuli „zastrzeżone”
w Starostwie Powiatowym w Jarocinie
WZÓR

Jarocin, dnia
Starosta Jarociński
za pośrednictwem
Pełnomocnika ds. oin

Wniosek

Na podstawie art. 21 ust. 1 pkt 4 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228 z zm.) wnioskuję o dopuszczenie do pracy* lub wykonania pracy zleconej* i wydanie „Upoważnienia”*** do dostępu do informacji niejawnych oznaczonych klauzulą „Zastrzeżone” dla osoby nie posiadającej poświadczenia bezpieczeństwa Pana/Pani:***

1. Nazwisko (w tym przybrane)
2. Imię (imiona)
3. PESEL
4. Imię ojca
4. Data i miejsce urodzenia
5. Miejsce zamieszkania lub pobytu

związanej z dostępem do informacji niejawnych o klauzuli „zastrzeżone” w

.....
(nazwa komórki organizacyjnej Starostwa lub stanowiska)

związanych z wykonywaniem obowiązków pracowniczych* lub pracy zleconej w zakresie*

.....
(nazwa zadania lub dokumentacji)

.....
(kierownik komórki organizacyjnej lub
osoba odpowiedzialna za realizację
zadania związanego z dostępem do IN)

Opinie i uwagi

Wyżej wymieniona osoba została przeszkolona w zakresie ochrony informacji niejawnych.*
Opinia.* Brak przeciwwskazań*.

.....

.....
(Pełnomocnik ds. oin)

Data szkolenia i nr „Zaświadczenia”:

Numer i data wydanego „Upoważnienia”:

* - Niepotrzebne skreślić

** - Upoważnienie zostanie wydane tylko po odbyciu szkolenia w zakresie ochrony informacji niejawnych. Upoważnienie traci ważność w przypadku pozbawienia uprawnień, zmiany stanowiska, rozwiązania lub wygaśnięcia stosunku pracy oraz zaprzestania świadczenia usług.* niepotrzebne skreślić

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

Załącznik nr 3
do Instrukcji dotyczącej sposobu
i trybu przetwarzania informacji
niejawnych o klauzuli „zastrzeżone”
w Starostwie Powiatowym w Jarocinie
WZÓR

UPOWAŻNIENIE Nr .../ROK
do dostępu do informacji niejawnych oznaczonych klauzulą
„zastrzeżone”
w Starostwie Powiatowym w Jarocinie

Na podstawie art. 21 ust. 4 pkt 1 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2010 r., Nr 182, poz. 1228) upoważniam do dostępu* do informacji niejawnych oznaczonych klauzulą tajności „Zastrzeżone” następującą osobę:

1. Imię (imiona)
2. Nazwisko(w tym przybrane)
3. PESEL

Upoważnienie wydane jest na okres od dnia wydania do odwołania** i może być cofnięte w każdym czasie

Z upoważnienia Starosty

Jarocin, data

.....
(imienna pieczęć i podpis pełnomocnika ds. oin)

* W zakresie określonym drugostronnie.

** Upoważnienie traci ważność w przypadku pozbawienia uprawnień, zmiany stanowiska, rozwiązania lub wygaśnięcia stosunku pracy oraz zaprzestania świadczenia usług.

ZAKRES DOSTĘPU OSOBY DO INFORMACJI NIEJAWNYCH

Drugostronnie wymieniona osoba posiada dostępem do informacji niejawnych o klauzuli „Zastrzeżone” w Starostwie Powiatowym w Jarocinie

.....
(nazwa komórki organizacyjnej Starostwa lub stanowiska)
związanych z wykonywaniem obowiązków pracowniczych* lub pracy zleconej w zakresie*

.....
(nazwa zadania lub dokumentacji)

* Niepotrzebne skreślić

OŚWIADCZENIE

Potwierdzam odbiór upoważnienia i informacji o moim zakresie dostępu do informacji niejawnych o klauzuli „Zastrzeżone” wynikającym z upoważnienia i oświadczam, że zapoznałam/em się z przepisami dotyczącymi ochrony informacji niejawnych:

1. Ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych.
2. Instrukcją dotyczącą sposobu i trybu przetwarzania informacji niejawnych o klauzuli „zastrzeżone” w Starostwie Powiatowym w Jarocinie.

Jednocześnie oświadczam, że:

- zapewnię ochronę informacji niejawnych przetwarzanym w Starostwie Powiatowym w Jarocinie zgodnie z obowiązującą w tym zakresie przepisami;
- zachowam w tajemnicy przez cały okres zatrudnienia, także po ustaniu stosunku pracy, informacje niejawne, z którymi zapoznałam/em się z racji wykonywanej pracy w Starostwie Powiatowym w Jarocinie i z informacjami dotyczącymi oraz związanymi z przetwarzaniem tych informacji i sposobami zabezpieczenia tych informacji;
- natychmiast zgłoszę przełożonemu i Pełnomocnikowi ds. oin, stwierdzenia próby lub faktu naruszenia ochrony lub bezpieczeństwa przetwarzanych informacji niejawnych.
- w przypadku utraty uprawnień zaprzestane działań do których zostałam/em uprawniona/ny w upoważnieniu.

Jarocin, dnia

.....
(podpis pracownika)

Strona 2/2