

Zarządzenie Nr 0050.58.2020

Wójta Gminy Legnickie Pole

z dnia 31 sierpnia 2020 r.

w sprawie zatwierdzenia Planu Informacji Niejawnych w Urzędzie Gminy Legnickie Pole

Na podstawie art. 15 ust. 1 pkt 5 ustawy z dnia 5 sierpnia 2010 o ochronie informacji niejawnych (Dz. U. z 2018 poz. 412 ze zm.) oraz § 9 ust. 1 rozporządzenia Rady Ministrów z dnia 29 maja 2012 (Dz. U. z 2012 poz. 683) Wójt Gminy Legnickie Pole zarządza co następuje:

§ 1

W celu zapewnienia ochrony informacji niejawnych zatwierdza się „Plan Ochrony Informacji Niejawnych” w Urzędzie Gminy Legnickie Pole, który stanowi załącznik do niniejszego zarządzenia.

§ 2

Traci moc zarządzenie nr 31/2015 Wójta Gminy Legnickie Pole z dnia 2 czerwca 2015 r. w sprawie zatwierdzenia „Planu Ochrony Informacji Niejawnych w Urzędzie Gminy Legnickie Pole ”

§ 3

Wykonanie zarządzenia powierza się Pełnomocnikowi do spraw Informacji Niejawnych w Urzędzie Gminy Legnickie Pole.

§ 4

Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT GMINY
Rafał Plezia



Załącznik do zarządzenia
Nr 0050.58.2020
Wójta Gminy Legnickie Pole
z dnia 31.08.2020

Plan Ochrony Informacji Niejawnych w Urzędzie Gminy Legnickie Pole

Opracował:

Magdalena Pilich-Zaremba

Pełnomocnik ds. Ochrony Informacji Niejawnych

Zatwierdził:

WOJEWÓDZKI
Rafał Plezia
Rafał Plezia

Legnickie Pole, 31 sierpień 2020 r.

I. Postanowienia ogólne.

1. Plan Ochrony Informacji niejawnych w Urzędzie Gminy Legnickie Pole określa zasady i tryb postępowania z informacjami niejawnymi oraz zapewnia jednolity sposób postępowania z tymi informacjami.
2. Plan ochrony informacji niejawnych opracowany został na podstawie wytycznych wynikających z art. 15 ust. 1 pkt 5 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2019 poz. 742 ze zm.).
3. Przedmiotem ochrony w Urzędzie są informacje niejawne oznaczone klauzulą „zastrzeżone”.
4. Pion ochrony informacji niejawnych tworzą:
 - Pełnomocnik ds. Ochrony Informacji Niejawnych,
 - Osoby upoważnione mające dostęp do ochrony informacji niejawnych.
5. Definicje używane w Planie ochrony informacji niejawnych:
 - 1) Ustawa - jest ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2019 poz. 742 ze zm.),
 - 2) Urzędem- jest Urząd Gminy w Legnickim Polu;
 - 3) Wójtem - jest Wójt Gminy Legnickie Pole;
 - 4) pełnomocnikiem ochrony - jest Pełnomocnik ds. Ochrony Informacji Niejawnych w Urzędzie Gminy w Legnickie Pole,
 - 5) Osoby upoważnione - Osoby upoważnione mające dostęp do ochrony informacji niejawnych.

II. Opis pomieszczeń lub obszarów dla informacji niejawnych o klauzuli „zastrzeżone”, w tym określenie ich granic i wprowadzanie systemu kontroli dostępu.

1. Budynek Urzędu Gminy jest czterokondygnacyjny z podpiwniczeniem, wolno stojący, konstrukcji murowanej. Pomieszczenia biurowe od pozostałych są oddzielone ścianami działowymi. Urząd jest właścicielem budynku, część pomieszczeń użycza dla Gminnej Przychodni Zdrowia. Budynek jest wyposażony w alarm oraz kamery, które monitorują bezpośrednie otoczenie budynku Urzędu Gminy Legnickie Pole w tym wejście do budynku oraz parking znajdujący się w obrębie budynku gminy.
2. Dokumenty zastrzeżone przechowywane są zamknięte w szafach metalowych zamykanych na co najmniej jeden zamek.
3. Drzwi od pomieszczenia, w którym przechowywane są dokumenty zastrzeżone, są wyposażone w zamki, bez możliwości wejścia osób nieupoważnionych po godzinach pracy.
4. Po zakończeniu pracy, pracownik Urzędu wychodzący z pomieszczenia, w którym przechowywane są dokumenty oznaczone klauzulą zastrzeżone, zobowiązany jest do zamknięcia drzwi na wszystkie zamki. Klucze od pomieszczeń deponowane są w miejscu wyznaczonym.

III. Procedury zarządzania uprawnieniami wejścia, wyjścia i przebywania i przebywania w pomieszczeniu, w którym przechowywane są informacje niejawne.

Dostęp do strefy ochronnej mają pracownicy Wydziału Rozwoju i Organizacji Gminy (pełnomocnik i upoważnieni pracownicy) oraz wójt. Natomiast w uzasadnionych pełnieniu obowiązków służbowych okolicznościach w strefie ochrony mogą przebywać nw. Osoby (zwane dalej goście): posiadające stosowne upoważnienia oraz poświadczenie bezpieczeństwa

i zaświadczenie o odbyciu szkolenia na temat ochrony informacji niejawnych, pracownicy służb lub organów ścigania, posiadający stosowne upoważnienia oraz poświadczenie bezpieczeństwa i zaświadczenie o odbyciu szkolenia na temat ochrony informacji niejawnych, kontrolerzy badający funkcjonowanie systemu ochrony informacji niejawnych. Kontrolę ewidencjonowania i przebywania gości w strefie ochrony prowadzi pracownik pionu ochrony.

IV. Ochrona fizyczna. Opis zastosowanych środków bezpieczeństwa fizycznego.

1. Aby informacje niejawne mogły być prawidłowo przetwarzane należy stosować środki bezpieczeństwa fizycznego odpowiednie do poziomu zagrożenia w związku z uniemożliwieniem osobom nieuprawnionym dostępu do tych informacji lub ich utraty. W celu przeprowadzenia doboru właściwych środków bezpieczeństwa przeprowadzono analizę wszystkich istotnych czynników mogących mieć wpływ na bezpieczeństwo informacji niejawnych przetwarzanych w urzędzie. Szczegółową analizę opisuje załącznik nr 1 niniejszego Planu OIN. Określony został poziom zagrożeń o wartości ŚREDNI, gdyż ocena istotności czynników wskazała wartość 20 punktów.
2. Proces doboru środków bezpieczeństwa fizycznego powinien zapewnić elastyczność ich stosowania w zależności od określonego poziomu zagrożeń. Klasyfikację środków bezpieczeństwa zwraca załącznik nr 2 do niniejszego Planu OIN.

V. Procedury bezpieczeństwa dla obszaru, w którym przetwarza się informacje niejawne.

W pomieszczeniu osób, które przetwarzają informacje niejawne przetwarzane są dokumenty niejawne o klauzuli tajności „zastrzeżone”. Podczas przetwarzania dokumentów niejawnych w pomieszczeniu mogą przebywać wyłącznie:

- 1) Osoby zatrudnione w Urzędzie albo wykonujące czynności zlecone, które posiadają uprawnienia do dostępu do informacji niejawnych,
- 2) Kontrolerzy badający funkcjonowanie systemu ochrony informacji niejawnych, pracownicy służby lub organów ścigania posiadający stosowne upoważnienie lub poświadczenie bezpieczeństwa.

Podczas wykonywania powyższych czynności drzwi są zamknięte. Weryfikacji przedstawionych upoważnień/poświadczeń bezpieczeństwa przedstawionych przez kontrolujących dokonuje Pełnomocnik. Podczas przebywania osób nie posiadających stałego upoważnienia do pomieszczeń, w których wytwarzane są dokumenty niejawne, a także innych pracowników Urzędu i klientów wszystkie dokumenty niejawne muszą być zdeponowane i zamknięte w szafie do tego wyznaczonej.

Sprzątanie pomieszczenia, w którym wytwarzane są dokumenty niejawne odbywa się wyłącznie po zakończeniu pracy z dokumentami niejawnymi.

VI. Procedury zarządzania kluczami do szaf, pomieszczeń w których przetwarzane są informacje niejawne.

Dokumenty oznaczone klauzulą zastrzeżone przechowywane są zamknięte w szafach metalowych zamykanych na co najmniej jeden zamek. Drzwi od pomieszczenia, w którym przechowywane są dokumenty zastrzeżone, są wyposażone w zamki patentowe, bez możliwości wejścia osób nieupoważnionych po godzinach pracy.

Po zakończeniu pracy, pracownik Urzędu wychodzący z pomieszczenia, w którym przechowywane są dokumenty oznaczone klauzulą zastrzeżone, zobowiązany jest do zamknięcia drzwi na wszystkie zamki.

Klucze do pomieszczeń biurowych przechowywane są w zamykanej szafce w sekretariacie Urzędu i wydawane codziennie rano pracownikom.

Budynek jest wyposażony w alarm oraz kamery, które monitorują bezpośrednie otoczenie budynku Urzędu Gminy Legnickie Pole, w tym wejście do budynku oraz parking znajdujący się w obrębie budynku gminy.

VII. Procedury reagowania osób odpowiedzialnych za ochronę informacji niejawnych.

1. Za ochronę informacji niejawnych w Urzędzie odpowiada Wójt.
2. Zadania określone ustawą o ochronie informacji niejawnych w imieniu Wójta wykonuje Pełnomocnik Ochrony poprzez:
 - 1) Sprawowanie nadzoru nad realizacją zadań i przestrzeganiem przepisów określonych w Planie Ochrony,
 - 2) Sprawowanie kontroli w zakresie ochrony informacji niejawnych oraz przestrzegania dostępu do tych informacji, w odniesieniu do wszystkich komórek organizacyjnych Urzędu.
 - 3) W przypadku ujawnienia informacji niejawnych przez podległych pracowników Urzędu Wójt lub upoważniony przez niego pracownik zawiadamia na piśmie Pełnomocnika Ochrony podając jaka informacja niejawna została ujawniona lub jakie naruszenie przepisów zostało stwierdzone.
 - 4) W przypadku kiedy Pełnomocnik Ochrony stwierdzi naruszenie w Urzędzie przepisów o ochronie informacji niejawnych zawiadamia o tym fakcie Wójta.
 - 5) W obu wyżej opisanych przypadkach Pełnomocnik Ochrony bez zbędnej zwłoki podejmuje działania zmierzające do wyjaśnienia okoliczności tego naruszenia oraz ograniczenia jego negatywnych skutków.
 - 6) Wyjaśnienie okoliczności obejmuje wskazanie przyczyn oraz osób winnych naruszeń.
 - 7) Pełnomocnik Ochrony przeprowadza okresowe kontrole przestrzegania ustawy o ochronie informacji niejawnych w Urzędzie.
 - 8) W przypadku stwierdzenia naruszenia przepisów o ochronie informacji niejawnych Pełnomocnik Ochrony przekłada Wójtowi pisemną informację o naruszeniu przepisów i wnioski do podjęcia decyzji, aby do takich naruszeń nie dochodziło w przyszłości.
 - 9) Wójt określa stopień szkody, jaką ponosi społecznie uzasadniony interes lub stopień niebezpieczeństwa ujawnienia tajemnicy oraz decyduje o ewentualnym karaniu dyscyplinarnym osób winnych, a także podejmuje decyzje, co do dokumentów zagubionych, jeżeli taka utrata miała miejsce.

VIII. Plany awaryjne uwzględniające potrzebę ochrony informacji niejawnych w razie występowania sytuacji szczególnych, w tym wprowadzenia stanów nadzwyczajnych, w celu zabezpieczenia utraty poufności, integralności lub dostępności informacji niejawnych.

1. Konieczność podjęcia działań zmierzających do zabezpieczania materiałów (dokumentów) zawierających informacje niejawne o klauzuli „zastrzeżone” może mieć miejsce w przypadku wprowadzenia stanu nadzwyczajnego: stan wojenny, stan wyjątkowy lub klęski żywiołowej.

2. Działania podjęte w celu ochrony materiałów niejawnych będących w posiadaniu Urzędu muszą odpowiadać stopniowi zagrożenia podstawowych interesów Rzeczypospolitej Polskiej w zakresie obronności, bezpieczeństwa stosunków gospodarczych i międzynarodowych państwa.
3. W przypadku wdrożenia stanu wojennego lub stanu wyjątkowego wzmacnia się ochronę budynku Urzędu, w tym również pomieszczeń pracowników upoważnionych. Wzmocnienie ochrony w przypadku stanu wojennego ma na celu zabezpieczenie budynku przed grupami dywersyjnymi i sabotażowymi oraz przed ewentualnymi demonstracjami czy też uczestnikami starć z siłami porządkowymi w przypadku wprowadzenia stanu wojennego. W analogiczny sposób postępuje się w przypadku wystąpienia zdarzeń kryzysowych, gdy jest to konieczne. Działania jakie zostaną podjęte obejmują” m.in.:
 - 1) wprowadzenie kontroli interesantów w oparciu o imienne przepustki,
 - 2) wzmocnienie ochrony obiektu funkcjonariuszami służb mundurowych.
4. W przypadku bezpośredniego zagrożenia przeprowadza się ewakuację materiałów niejawnych. W przypadku nagłego zagrożenia decyzję o zniszczeniu materiałów niejawnych podejmuje Wójt, a w przypadku jego nieobecności Pełnomocnik. Bezpośrednie zagrożenie może wynikać z działań wojennych, w wyniku których materiały niejawne mogą dostać się w ręce agresora.
5. Ewakuacja akt powinna obejmować: zapakowanie materiałów do worków, przemieszczenie worków na środek transportu i przewiezienie ich w wyznaczone przez Wójta miejsce ewakuacji.
6. Nadzór i ochronę transportu do miejsca ewakuacji dokumentów zapewniają pracownicy pionu ochrony.
7. W sytuacji kiedy ewakuacja staje się konieczna, ewakuacji podlegają wszystkie dokumenty niejawne przechowywane w Urzędzie. Niszczenie dokonywane jest za pomocą niszczarki dokumentów lub ich spalania. Protokół zniszczenia materiałów niejawnych winien zawierać opis okoliczności w jakich dokonano zniszczenia, gdzie, kiedy, na czyje polecenie i w jaki sposób oraz spis zniszczonych dokumentów.
8. Osoby, które stwierdziły jakiegokolwiek naruszenie przepisów, zagrożenie dla bezpieczeństwa informacji niejawnych zobowiązane są niezwłocznie powiadomić Pełnomocnika, jak również zobowiązane są do:
 - 1) Zabezpieczenia miejsca zdarzenia, śladów dowodów,
 - 2) Zabezpieczenia informacji niejawnych przed ewentualnym dalszym ujawnieniem,
 - 3) Złożenie szczegółowych wyjaśnień dotyczących zdarzenia osobom prowadzącym postępowanie wyjaśniające.
9. W przypadku stwierdzenia naruszenia w Urzędzie przepisów o ochronie informacji niejawnych Pełnomocnik zawiadamia o tym Wójta i podejmuje niezwłocznie działania zmierzające do wyjaśnienia okoliczności tego naruszenia oraz ograniczenia jego negatywnych skutków. Pełnomocnik ustala czy i jakie informacje zostały ujawnione lub zniszczone czy też była to jedynie próba zdobycia informacji przez osobę nieuprawnioną.
10. W przypadku stwierdzenia zaistnienia uzasadnionego podejrzenia popełnienia przestępstwa ujawnienia informacji niejawnych (art. 266 KK) istnieje obowiązek niezwłocznego zawiadomienia właściwego organu ścigania (Prokuratura lub Agencja Bezpieczeństwa Wewnętrznego). Naruszenie przepisów o ochronie informacji niejawnych przez pracownika posiadającego poświadczenie bezpieczeństwa może stanowić podstawę do wdrożenia postępowania kontrolnego niezależnie od odpowiedzialności dyscyplinarnej lub karnej.

TABELA OCENY ISTOTNOŚCI CZYNNIKÓW ZAGROZEŃ

Lp.	Czynniki	Ocena istotności czynnika			Uzasadnienie	Wskazówki
		BARDZO ISTOTNY (8 PKT)	ISTOTNY (4 PKT)	MAŁO ISTOTNY (1 PKT)		
1.	Klauzula tajności przetwarzania informacji niejawnych	3	4	5	6	7
1.				X	W urzędzie przetwarzane są tylko informacje o klauzuli „zastrzeżone”	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			X	W urzędzie występuje niewielka liczba dokumentów zawierających informacji niejawnych	Przy ocenie istotności czynnika należy brać pod uwagę wszystkie materiały niejawne zarejestrowane w urządzeniach ewidencyjnych, pozostające w faktycznej dyspozycji jednostki organizacyjnej. W uzasadnieniu należy odnieść się do przybliżonej ogólnej liczby wszystkich materiałów, stosując zasadę: im więcej informacji niejawnych o najwyższych klauzulach tajności, tym czynnik ma istotniejsze znaczenie. W przypadku nowo organizowanej jednostki organizacyjnej należy przyjąć wartości szacunkowe.
3.	Postać informacji niejawnych			X	W urzędzie występuje niewielka liczba dokumentów zawierających informacji niejawnych Dostęp do komputera, na którym są ewentualnie przetwarzane informacje został ograniczony, a poszczególne dokumenty są wytwarzane	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				osobiście przez upoważnionych pracowników	Faktyczny stały dostęp do dokumentów niejawnych o klauzuli „zastrzeżone” ma stosunkowo niewiele osób do liczby zatrudnionych. Dodatkowo ze względu organizacyjnych każda osoba z obecnej kadry kierowniczej posiada stosowne upoważnienie.	X	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			X	Budynek Urzędu jest chroniony całodobowo, posiada monitoring. Urząd wynajmuje część pomieszczeń budynku Gminnej Przychodni Zdrowia w Legnickim Polu.			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.
6.	Dostęp osób do budynku		X		Urząd nie posiada wyodrębnionej strefy obsługi interesantów. Dostęp do poszczególnych biur w godzinach urzędowania jest nieograniczony. Do budynku mają także dostęp klienci Gminnej Przychodni Zdrowia w Legnickim Polu			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			X	Klauzula chronionych dokumentów jest niższa. Bezpośredni dostęp do dokumentów niejawnych jest ograniczony. Ze względu na		X	Poziom zagrożen powinien uwzględnić 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

					<p>przestępcza, pożar, działanie sił przyrody (np. obszar zagrożony powodzią) lub szkody górnicze.</p>
					<p>powyższe mało prawdopodobne są czynniki tj. działanie obcych służb specjalnych, sabotaż, zamach terrorystyczny. Bardziej istotne czynniki to kradzież lub inna działalność przestępcza przez pracowników/osoby trzecie. Mogą również wystąpić takie czynniki jak pożar, działanie sił przyrody, awaria wewnętrznych sieci.</p>
Suma punktów					20

*) 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” zostałaby 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 OKREŚLANIA POZIOMU ZAGROŻEŃ

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

PUNKTACJA ZASTOSOWANYCH ŚRODKÓW BEZPIECZEŃSTWA FIZYCZNEGO

ŚRODKI 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)	1
Środek bezpieczeństwa K1S2 – Zamek do szafy	
Liczba punktów za środek bezpieczeństwa (K1S2 = 4,3,2 lub 1 pkt)	1
Liczba punktów za kategorię K1 stanowiąca iloczyn liczby punktów za oba powyższe środki bezpieczeństwa (K1=K1S1xK1S1)	1
KATEGORIA K2: Pomieszczenia	
Środek bezpieczeństwa K2S1 – konstrukcja pomieszczenia	
Liczba punktów za środek bezpieczeństwa (K2S1 = 4,3,2 lub 1 pkt)	2
Środek bezpieczeństwa K2S2 – Zamek do drzwi pomieszczenia	
Liczba punktów za środek bezpieczeństwa (K2S2 = 4,3,2 lub 1 pkt)	1
Liczba punktów za kategorię K2 stanowiąca iloczyn liczby punktów za oba powyższe środki bezpieczeństwa (K2=K2S2xK2S2)	2
KATEGORIA K3: Budynki	
Liczba punktów za kategorię (K3 = 5, 4,3,2 lub 1 pkt)	3
KATEGORIA K4: kontrola dostępu	
Środek bezpieczeństwa K4S1 – System kontroli dostępu	
Liczba punktów za środek bezpieczeństwa (K4S1 = 4,3,2 lub 1 pkt)	1
Środek bezpieczeństwa K4S2 – Kontrola osób nieposiadających stałego upoważnienia do wejścia na obszar jednostki organizacyjnej (interesantów)	
Liczba punktów za środek bezpieczeństwa (K4S2 = 4,3,2 lub 1 pkt)	0
Liczba punktów za kategorię K4 stanowiąca sumę liczby punktów za oba powyższe środki bezpieczeństwa (K4 = K4S1xK4S2)	1
KATEGORIA K5: Personel bezpieczeństwa i systemy sygnalizacji napadu i włamania	
Środek bezpieczeństwa K5S1 – Personel bezpieczeństwa	
Liczba punktów za środek bezpieczeństwa (K5S1 = 5, 4,3,2 lub 1 pkt)	0
Środek bezpieczeństwa K5S2 – System sygnalizacji napadu i włamania	
Liczba punktów za środek bezpieczeństwa (K5S2 = 4,3,2 lub 1 pkt)	2
Liczba punktów za kategorię K5 stanowiąca sumę liczby punktów za oba powyższe środki bezpieczeństwa (K5=K5S1+K5S2)	2

KATEGORIA K6: Granice	
Środek bezpieczeństwa K6S1 – Ogrodzenie	
Liczba punktów za środek bezpieczeństwa (K6S1 = 4,3,2 lub 1 pkt)	1
Środek bezpieczeństwa K6S2 – Kontrola w punktach dostępu	
Liczba punktów za środek bezpieczeństwa (K6S2 = 1 lub 0 pkt)	0
Środek bezpieczeństwa K6S3 – System kontroli osób i przedmiotów przy wejściu/wyjściu	
Liczba punktów za środek bezpieczeństwa (K6S3 = 1 lub 0 pkt)	0
Środek bezpieczeństwa K6S4 – System wykrywania naruszenia ogrodzenia	
Liczba punktów za środek bezpieczeństwa (K6S4 = 1 lub 0 pkt)	0
Środek bezpieczeństwa K6S5 – Oświetlenie chronionego obszaru	
Liczba punktów za środek bezpieczeństwa (K6S5 = 1 lub 0 pkt)	1
Środek bezpieczeństwa K6S6 – System dozoru wizyjnego granic	
Liczba punktów za środek bezpieczeństwa (K6S6 = 1 lub 0 pkt)	1
Liczba punktów za kategorię K6 stanowiącą sumę liczby punktów za powyższe środki bezpieczeństwa (K6=K6S1+K6S2+K6S3+K6S4+K6S5+K6S6)	3
Ogólna liczba punktów stanowiąca sumę punktów za wszystkie kategorie PUNKTY = K1+K2+K3+K4+K5+K6	12

