ZARZĄDZENIE NR 60/2020

WÓJTA GMINY SZCZANIEC

z dnia 30 listopada 2020 r.

w sprawie ochrony informacji niejawnych w Urzędzie Gminy Szczaniec

Na podstawie art. 33 ust. 1 i 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t. j. Dz. U z 2020 r. poz. 713 z późniejszymi zmianami), art. 15 ust. 5, art. 43 ust. 5 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (t. j. Dz. U. 2019, poz. 742) zarządza się co następuje:

§ 1. W celu zapewnienia ochrony informacji niejawnych oraz przestrzegania przepisów o ochronie informacji niejawnych, zatwierdza się :

1. Instrukcję dotyczącą sposobu i trybu przetwarzania informacji niejawnych o klauzuli zastrzeżone oraz zakres i warunki stosowania środków bezpieczeństwa fizycznego w celu ich ochrony w Urzędzie Gminy Szczaniec, stanowiąca załącznik nr 1 do niniejszego zarządzenia.
2. Plan ochrony informacji niejawnych w Urzędzie Gminy Szczaniec, stanowiący załącznik nr 2 do niniejszego zarządzenia.
3. Dokumentację określającą poziom zagrożeń dla systemu ochrony informacji niejawnych Urzędu Gminy Szczaniec, stanowiącą załącznik nr 3 do niniejszego zarządzenia.

§ 2. Wykonanie zarządzenia powierza się Pełnomocnikowi do spraw Ochrony Informacji Niejawnych Urzędu Gminy Szczaniec.

§ 3. Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT

Krzysztof Neryng

ZATWIERDZAM
Wójt Gminy Szczaniec

Krzysztof Neryng

Załącznik nr 1
do zarządzenia nr 60/2020
Wójta Gminy Szczaniec
z dnia 30 listopada 2020 r.

INSTRUKCJA

dotycząca sposobu i trybu przetwarzania informacji niejawnych
oznaczonych klauzulą tajności *ZASTRZEŻONE* oraz zakresu i warunków
stosowania środków bezpieczeństwa fizycznego w celu ich ochrony
w Urzędzie Gminy w Szczańcu

ROZDZIAŁ I

WSTĘP

§ 1

Niniejsza instrukcja - zwana dalej instrukcją - określa zasady i sposób postępowania z informacjami niejawnymi oznaczonymi klauzulą *zastrzeżone* oraz zasady ochrony tych informacji w Urzędzie Gminy w Szczańcu.

§ 2

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

ROZDZIAŁ II

KLASYFIKOWANIE
INFORMACJI NIEJAWNYCH

§ 3

Informacjom niejawnym nadaje się klauzule *zastrzeżone,* jeśli nie nadano im wyższej klauzuli tajności, a ich nieuprawnione ujawnienie może mieć szkodliwy wpływ na wykonywanie przez jednostki organizacyjne zadań w zakresie i obrony narodowej, polityki zagranicznej, bezpieczeństwa publicznego, przestrzegania praw i wolności obywateli, wymiaru sprawiedliwości albo interesów ekonomicznych Rzeczypospolitej Polskiej

§ 4

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

§ 5

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

ROZDZIAŁ III

DOSTĘP DO INFORMACJI NIEJAWNYCH O KLAUZULI *ZASTRZEŻONE*

§ 6

Dokumenty niejawne o klauzuli *zastrzeżone* mogą być udostępniane wyłącznie osobom, które spełniają następujące warunki:

1) posiadają ważne poświadczenie bezpieczeństwa upoważniające do dostępu do informacji o klauzuli co najmniej *zastrzeżone* lub upoważnienie Wójta,
2) odbyły przeszkolenie w zakresie ochrony informacji niejawnych i posiadają aktualne zaświadczenie stwierdzające odbycie tego szkolenia (nie starsze niż 5 lat od daty wystawienia),
3) realizują zadania, które wymagają dostępu do określonej informacji zastrzeżonej.

§ 7

Ewidencję poświadczeń bezpieczeństwa oraz upoważnień, o których mowa w § 6 pkt 1 prowadzi Pełnomocnik Ochrony Informacji Niejawnych. Pracownik, który posiada poświadczenie bezpieczeństwa wydane w innej jednostce organizacyjnej, obowiązany jest do przedłożenia oryginału Pełnomocnikowi Ochrony w ciągu 5 dni od chwili poinformowania go o tym fakcie.

§ 8

Pełnomocnik Ochrony Informacji Niejawnych, zwany dalej Pełnomocnikiem Ochrony, zobowiązany jest do informowania Wójta o konieczności wydania upoważnienia pracownikom, których zakres obowiązków wymaga dostępu do dokumentów niejawnych oznaczonych klauzulą *zastrzeżone*.

ROZDZIAŁ IV

OBIEG DOKUMENTÓW I MATERIAŁÓW OZNACZONYCH KLAUZULĄ *ZASTRZEŻONE*

§ 9

1. Korespondencję z zewnątrz Urzędu, zawierającą informacje niejawne zakwalifikowane jako *zastrzeżone*, przekazywane pocztą specjalną, odbiera z Komendy Powiatowej Policji Pełnomocnik Ochrony lub inny wyznaczony przez Wójta pracownik, spełniający wymagania określone w § 6 niniejszej Instrukcji.
2. Dokumenty niejawne oznaczone klauzulą *zastrzeżone* wpływające do sekretariatu urzędu za pośrednictwem Poczty Polskiej lub przesyłek kurierskich przekazywane są pracownikowi spełniającemu wymagania określone w § 7 Instrukcji, który rejestruje je w dzienniku ewidencyjnym i przekazuje Wójtowi lub innemu wskazanemu na kopercie adresatowi.

§ 10

1. Pracownik urzędu dokonujący odbioru przesyłki zobowiązany jest sprawdzić:
   1) prawidłowość adresu,
   2) całość pieczęci i opakowania,
   3) zgodność odcisku pieczęci na opakowaniu z nazwą jednostki nadawcy,
   4) zgodność numerów na przesyłce z numerami na wykazie przesyłek nadanych lub w książce doręczeń,
   5) odcisnąć na przesyłce pieczęć oraz wpisać datę wpływu do Urzędu.
2. W przypadku stwierdzenia uszkodzenia przesyłki lub śladów jej otwierania, osoba kwitująca odbiór przesyłki sporządza protokół uszkodzenia. Jeden egzemplarz protokołu przekazuje się nadawcy, drugi Pełnomocnikowi Ochrony.

§ 11

1. Wójt lub inny wskazany na kopercie adresat dokonują pisemnej dekretacji, wskazując imiennie pracownika Urzędu odpowiedzialnego merytorycznie za załatwienie sprawy.
2. W przypadku konieczności zapoznania się z treścią dokumentu zastrzeżonego przez kilku pracowników Urzędu , konieczne jest rozszerzenie dekretacji.

§ 12

1. Ostateczny odbiorca dokumentu niejawnego jest zobowiązany uzupełnić brakujące wpisy w dzienniku ewidencyjnym przez podanie pracownikowi prowadzącemu sprawy wynikających z zakresu obowiązków danych niezbędnych do pełnej rejestracji dokumentu.
2. Po otwarciu przesyłki pracownik:
   1) Sprawdza, czy zawartość przesyłki odpowiada wyszczególnionym na niej numerom ewidencyjnym,

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

3. W razie stwierdzenia nieprawidłowości , sporządza w dwóch egzemplarzach protokół z otwarcia przesyłki, zawierający opis nieprawidłowości. Jeden egzemplarz przekazuje nadawcy. Fakt sporządzenia protokołu odnotowuje w dzienniku ewidencyjnym w rubryce „Informacje uzupełniające/uwagi".

§ 13

W przypadku wpływu do Urzędu pisma niejawnego oznaczonego klauzulą *zastrzeżone* lub wyższą i brakiem przez osobę odbierającą korespondencję niejawną odpowiedniego upoważnienia bądź poświadczenia bezpieczeństwa, o otrzymaniu takiej korespondencji należy niezwłocznie zawiadomić Pełnomocnika Ochrony.

§ 14

1. Każdy pracownik, który zapoznał się z treścią dokumentu niejawnego, dokonuje stosownej adnotacji bezpośrednio na dokumencie lub w Karcie zapoznania się z dokumentem „zastrzeżonym".
2. Kartę zakłada pracownik prowadzący sprawy. W przypadku dokumentu, z którym będzie zapoznana większa liczba pracowników, odnotowuje ten fakt na dokumencie.
3. Karta przekazywana jest razem z dokumentem i podlega rozliczeniu podobnie jak dokument zastrzeżony.
4. Za właściwe zabezpieczenie dokumentu zastrzeżonego przed nieuprawnionym dostępem odpowiada osoba, której przekazano dokument niejawny.

§ 15

Wójt przed rozwiązaniem stosunku pracy z pracownikiem posiadającym poświadczenie bezpieczeństwa lub upoważnienie do dostępu do informacji niejawnych o klauzuli *zastrzeżone* przejmuje od niego protokolarnie całość materiałów posiadających klauzule *zastrzeżone* i pisemnie wyznacza pracownika, który ma prowadzić przejętą dokumentację. Protokół sporządza się w dwóch egzemplarzach – dla odchodzącego pracownika i dla Urzędu. Przekazanie przejętej dokumentacji innemu pracownikowi odbywa się na pisemne polecenie Wójta lub jego dekretacji na protokole zdawczo-odbiorczym.

ROZDZIAŁ V

WYTWARZANIE I WYSYŁANIE DOKUMENTÓW OZNACZONYCH KLAUZULĄ *ZASTRZEŻONE*

§ 16

Informacje niejawne oznaczone klauzulą *zastrzeżone*, wytworzone w Urzędzie w formie dokumentu pisemnego, mogą być sporządzane odręcznie, na maszynie do pisania (bez pamięci) lub na komputerze, który uzyskał akredytacje bezpieczeństwa teleinformatycznego zatwierdzoną przez Wójta.

§ 17

Dokumenty o klauzuli *zastrzeżone* są sporządzane i wykonywane przez pracownika merytorycznie odpowiedzialnego za jego opracowanie. Praca z dokumentem zastrzeżonym może odbywać się tylko w pomieszczeniach Urzędu w warunkach umożliwiających zapewnienie ochrony przed jego nieuprawnionym ujawnieniem lub zapoznaniem się przez osoby do tego nieuprawnione. Szczegółowy opis zasad ochrony zawarty został w § 24 - § 27 niniejszej instrukcji.

§ 18

1. Materiały niejawne o klauzuli *zastrzeżone*, przesyłane w postaci listów, nadaje się jako listy polecone ze zwrotnym potwierdzeniem odbioru, zapakowane w dwie nieprzezroczyste koperty.
2. Materiały niejawne o klauzuli *zastrzeżone,* przesyłane w postaci paczek, nadaje się zapakowane w dwie warstwy nieprzezroczystego mocnego papieru

§ 19

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

§ 20

1. W przypadku konieczności zorganizowania narady, w trakcie której ustnie będą omawiane informacje oznaczone klauzulą *zastrzeżone*, uczestnicy spotkania muszą zostać niezwłocznie poinformowani o jego niejawnym charakterze. W spotkaniu mogą uczestniczyć wyłącznie osoby spełniające warunki, o których mowa w § 6 Instrukcji, których zakres obowiązków obejmuje sprawy omawiane na spotkaniu.
2. Spotkanie o charakterze niejawnym nie może być utrwalane na magnetycznych lub cyfrowych nośnikach dźwięku i obrazu. Wszelkie protokoły i notatki z narady należy oznaczyć klauzulą *zastrzeżone* i dokonać ich rejestracji.

ROZDZIAŁ VI

REJESTROWANIE I OZNACZANIE DOKUMENTÓW

OZNACZONYCH KLAUZULĄ *ZASTRZEŻONE*

§ 21

1. Wszystkie dokumenty zawierające informacje *zastrzeżone* podlegają zaewidencjonowaniu w prowadzonym przez pracownika dzienniku ewidencyjnym, którego wzór został określony w załączniku nr 2 do rozporządzenia Rady Ministrów z dnia 7 grudnia 2011r. w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych (Dz. U. nr 276, poz. 1631). Dotyczy to dokumentów wytworzonych w Urzędzie jak i otrzymanych z zewnątrz.
2. Wzór wytworzonego w Urzędzie pisma oznaczonego klauzulą *zastrzeżone* przedstawia załącznik nr 1 do Instrukcji.

§ 22

1. Materiały zawierające informacje niejawne, utrwalone w formie pisemnej, zwane dalej pismem, oznacza się w następujący sposób:
   1) na każdej stronie umieszcza się:
      a) na środku, jako pierwszy element w nagłówku strony, klauzulę tajności (w sposób wyraźny i w pełnym brzmieniu)
      b) numer egzemplarza, a w przypadku gdy dokument wykonano w jednym egzemplarzu, napis „egz. pojedynczy"
      c) sygnaturę literowo-cyfrową, na którą składają się: literowe oznaczenie jednostki lub komórki organizacyjne, symbol oznaczenia klauzuli tajności, numer pod którym dokument został zarejestrowany, rok w którym dokonano rejestracji, a także inne oznaczenia ułatwiające ustalenie miejsce wykonania dokumentu,
      d) numer strony oraz liczbę stron całego dokumentu,
      e) na środku, jako ostatni element w stopce strony, klauzule tajności;
   2) na pierwszej stronie umieszcza się również:
      a) nazwę jednostki organizacyjnej,
      b) nazwę miejscowości i datę podpisania dokumentu,
      c) w przypadku dokumentu, któremu nadano bieg korespondencyjny, imię i nazwisko lub nazwę stanowiska adresata; w przypadku wielu adresatów dokumentu, dopuszcza się możliwość adnotacji „adresaci według rozdzielnika";
   3) na ostatniej stronie pod treścią umieszcza się również:
      a) liczbę załączników,
      b) liczbę stron wszystkich załączników lub informacje określającą rodzaj załączonego materiału i jego odpowiednią jednostkę miary,

c) klauzulę tajności złączników wraz z numerami pod jakimi zostały zarejestrowane oraz liczbę stron każdego załącznika lub informację określającą rodzaj załączonego materiału i jego odpowiednią jednostkę miary,
d) w przypadku, gdy adresatowi wysyła się inną liczbę załączników niż pozostawia w aktach, dodatkowo napis „tylko adresat" – jeśli załączniki mają być przekazane adresatowi bez pozostawienia ich w aktach, lub napis „do zwrotu" – jeżeli załączniki mają zostać zwrócone do nadawcy,
e) stanowisko oraz imię i nazwisko lub inne oznaczenie wskazujące osobę uprawnioną do jego podpisania,
f) liczbę wykonywanych egzemplarzy,
g) adresatów poszczególnych egzemplarzy dokumentu albo adnotację, adresaci według rozdzielnika,
h) dyspozycję „ad acta" w przypadku egzemplarza pozostającego w aktach nadawcy,
i) imię i nazwisko lub inne oznaczenie wskazujące wykonawcę.

2. W przypadku pisma o klauzuli *zastrzeżone* dopuszcza się odstąpienie od umieszczania oznaczeń, które wymieniono wyżej używając podkreślenia.
3. Na dokumencie nieelektronicznym można zamieścić dyspozycję dotyczącą:
   1) braku zgody na kopiowanie lub tłumaczenie części lub całości dokumentu,
   2) braku zgody na udzielenie informacji o treści dokumentu,
   3) określenia daty lub wydarzenia, po którym nastąpi zniesienie lub zmiana klauzuli tajności całości lub części dokumentu.
4. Na dokumencie stanowiącym załącznik na pierwszej stronie umieszcza się dodatkowo informacje: „Załącznik nr ...do dokumentu nr... z dnia....".
5. Jeżeli przy piśmie przewodnim przesyłane są załączniki to:
   1) klauzula pisma przewodniego lub dokumentu nie może być niższa niż klauzula załącznika o najwyższym stopniu tajności,
   2) na piśmie przewodnim, jeżeli jego klauzula jest inna lub dokument jest jawny po trwałym odłączeniu załączników – na każdej stronie pod numerem egzemplarza umieszcza się adnotację o jawności klauzuli albo tajności dokumentu po odłączeniu załączników.

§ 23

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

ROZDZIAŁ VII

PRZECHOWYWANIE, NISZCZENIE I ARCHIWIZOWANIE DOKUMNETÓW OZNACZONYCH KLAUZULĄ „*ZASTRZEŻONE*".

§ 24

1. Dokumenty oznaczone klauzulą *zastrzeżone* podlegają obowiązkowej ochronie przed kradzieżą i nieuprawnionym ujawnieniem.
2. Dokumenty *zastrzeżone* przechowuje się zamknięte w szafach metalowych zamykanych na co najmniej jeden zamek
3. Drzwi od pomieszczenia, w którym przechowywane są dokumenty *zastrzeżone*, są wyposażone w zamki patentowe, bez możliwości wejścia osób nieupoważnionych po godzinach pracy.
4. Klucze do urządzeń biurowych, w których przechowywane są dokumenty oznaczone klauzulą zastrzeżone, po zakończonym dniu pracy muszą być zabezpieczone przez pracownika w pomieszczeniu, o którym mowa w ust. 2 - w miejscu niedostępnym i nieznanym powszechnie.
5. Zabrania się wynoszenia poza urząd, jak również udostępniania kluczy do pomieszczeń oraz urządzeń biurowych, w których przechowywane są dokumenty niejawne oznaczone klauzulą zastrzeżone osobom nieuprawnionym. Pracownikom urzędu zabrania się samodzielnego dokonywania wymiany bez uzyskania zgody ze strony Pełnomocnika Ochrony.

6. 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 zabezpieczone są w miejscu niedostępnym i nieznanym powszechnie.

§ 25

1. Dokumenty *zastrzeżone* gromadzone są przez pracowników upoważnionych do dostępu do tych informacji w teczkach akt z klauzulą *zastrzeżone*. Dokumentów niejawnych oznaczonych klauzulą *zastrzeżone* nie wolno przechowywać razem z dokumentami jawnymi, chyba że stanowią integralną część dokumentacji.
2. W przypadku spraw ostatecznie zakończonych, gdy dokument jest nadal chroniony, teczka akt o klauzuli *zastrzeżone* jest przechowywana do czasu zniesienia klauzuli tajności. Gdy dokument staje się jawny teczkę przekazuje się do archiwum zakładowego.

§ 26

1. W celu zniszczenia materiałów niejawnych oznaczonych klauzulą *zastrzeżone*, które nie podlegają trwałemu przechowywaniu i utraciły praktyczne znaczenie, powołuje się komisję złożoną z co najmniej dwóch pracowników spełniających warunki, o których mowa w § 6 Instrukcji.
2. W skład komisji obligatoryjnie wchodzi pracownik prowadzący sprawy informacji niejawnych lub Pełnomocnik Ochrony. Komisja sporządza protokoły oceny dokumentacji niearchiwalnej oraz spisy dokumentacji niearchiwalnej przeznaczonej do zniszczenia. W oparciu o przygotowaną dokumentację Wójt występuje z wnioskiem o udzielenie zgody na zniszczenie do dyrektora właściwego archiwum państwowego.
3. Fakt zniszczenia materiałów niejawnych dokumentuje się protokolarnie oraz odnotowuje w rubryce *„Uwagi"* Dziennika Ewidencyjnego z adnotacją o treści *„Zniszczono na podstawie protokołu z dnia... "*. Protokół zniszczenia przechowuje się w pomieszczeniu, gdzie przechowywane są informacje niejawne.

§ 27

1. Informacje niejawne oznaczone klauzulą *zastrzeżone*, utrwalone na papierze niszczy się przez pocięcie w niszczarce, która zapewnia zniszczenie materiału, po czym następuje komisyjne spalenie zniszczonych dokumentów.
2. Informacje niejawne oznaczone klauzulą *zastrzeżone* zapisane w formie elektronicznej niszczy się przez fizyczne zniszczenie nośnika.

ROZDZIAŁ VIII

POSTANOWIENIA KOŃCOWE

§ 28

1. Każdy pracownik Urzędu posiadający na zajmowanym stanowisku dostęp do informacji niejawnych oznaczonych co najmniej klauzulą *zastrzeżone*, jest zobowiązany zapoznać się z niniejszą instrukcją i stosować zawarte w niej przepisy.
2. Osobą odpowiedzialną za zapoznanie pracowników z *Instrukcją* jest Pełnomocnik Ochrony.
3. Każdy pracownik Urzędu jest zobowiązany niezwłocznie powiadomić bezpośredniego przełożonego przez Pełnomocnika Ochrony o wszelkich nieprawidłowościach związanych z naruszeniem zapisów niniejszej Instrukcji.

Załącznik nr 1
do Instrukcji

WZÓR PISMA O KLAUZULI *„ZASTRZEŻONE”*

ZASTRZEŻONE

Nazwa jednostki organizacyjnej

Miejscowość, data.....

Sygnatura literowo-cyfrowa
nr egzemplarza lub egz. pojedynczy

Imię, nazwisko
lub stanowisko adresata
(lub adresaci wg rozdzielnika)

TREŚĆ PISMA

.....
.....
.....
.....

Bezpośrednio pod treścią pisma:
- liczba załączników i liczba stron wszystkich załączników (np. 2 załączniki na 10 stronach)
- klauzule tajności załączników z numerami pod jakimi zostały zarejestrowane oraz liczbę stron poszczególnych załączników (np. zał. Nr 1 – zastrzeżone – „nazwa załącznika i numer rejestracji – 6 str. – tylko adresat; zał. Nr 2 – zastrzeżone – nazwa załącznika i numer rejestracji – 4 str. do zwrotu)

Stanowisko, imię i nazwisko
osoby uprawnionej do podpisania

- liczba wykonanych egzemplarzy
- adresatów poszczególnych egzemplarzy
- dyspozycję „ad acta” w przypadku egzemplarza pozostającego w aktach nadawcy
- imię i nazwisko wykonawcy

Numer strony/liczba stron

ZASTRZEŻONE

(Dyspozycje podkreślone mogą lecz nie muszą być uwzględnione w pismach o klauzuli *zastrzeżone*)

ZATWIERDZAM
Wójt Gminy Szczaniec

Krzysztof Neryng

Załącznik nr 2
do Zarządzenia nr 60/2020
Wójta Gminy Szczaniec
z dnia 30 listopada 2020 r.

PLAN OCHRONY INFORMACJI NIEJAWNYCH URZĘDU GMINY W SZCZAŃCU

Rozdział I

Postanowienia ogólne

1. Plan Ochrony Informacji Niejawnych Urzędu Gminy w Szczańcu określa zasady i tryb postepowania z informacjami niejawnymi oaz 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. 2019 poz. 742).
3. Przedmiotem ochrony w Urzędzie są informacje niejawne oznaczone klauzulą „zastrzeżone".
4. Podstawy prawne ochrony informacji niejawnych:
    1) Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. 2019 poz.742).
    2) Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie wzoru decyzji o cofnięciu poświadczenia bezpieczeństwa (Dz. U 2015, poz.220).
    3) Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie wzoru decyzji o odmowie wydania poświadczenia bezpieczeństwa (Dz. U. 2015, poz. 220).
    4) Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie wzorów poświadczeń bezpieczeństwa (Dz. U. 2015, poz. 220).
    5) Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie wzorów zaświadczeń stwierdzających odbycie szkolenia w zakresie ochrony informacji niejawnych oraz sposobu rozliczania kosztów przeprowadzenia szkolenia przez Agencje Bezpieczeństwa Wewnętrznego lub Służbę Kontrwywiadu Wojskowego (Dz. U. 2015, poz. 205).
    6) Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie przekazywania informacji, udostępniania dokumentów oraz udzielania pomocy służbom i instytucjom uprawnionym do prowadzenia poszerzonych postępowań sprawdzających, kontrolnych postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego (Dz. U. 2017, poz. 2334).
    7) Rozporządzenie Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzuli tajności (Dz. U. 2011 nr 288, poz. 1692).

8) Rozporządzenie Prezesa Rady Ministrów z dnia 27 kwietnia 2011 r. w sprawie przygotowania i przeprowadzenia kontroli stanu zabezpieczenia informacji niejawnych.
9) Rozporządzenie Rady Ministrów z dnia 7grudnia 2011 r. w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych (Dz. U 2011 nr 276, poz. 1631).
10) Rozporządzenie Prezesa Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne (Dz. U 2011 nr 271, poz. 1603).
11) Rozporządzenie Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (Dz. U 2012, poz. 683).

5. Definicje używane w Planie ochrony informacji niejawnych:
W rozumieniu planu ochrony informacji niejawnych:
1) Ustawa- ustawa z dnia 5 sierpnia 2010 r, o ochronie informacji niejawnych
2) Rękojmia zachowania tajemnicy – zdolność osoby do spełnienia ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem, stwierdzona w wyniku przeprowadzenia postępowania sprawdzającego.
3) Dokumenty – każda utrwalona informacja niejawna.
4) Materiały – dokumenty lub przedmiot albo dowolna ich cześć, chronione jako informacja niejawna, a zwłaszcza urządzenie, wyposażenie lub broń wyprodukowane albo będące w trakcie produkcji, a także składnik użyty do ich wytworzenia.
5) Przetwarzane informacje niejawne - wszelkie operacje wykonywane w odniesieniu do operacji niejawnych i na tych informacjach, w szczególności ich wytwarzanie, modyfikowanie, kopiowanie, klasyfikowanie, gromadzenie, przechowywanie, przekazywanie lub udostępnianie.
6) System teleinformatyczny – system teleinformatyczny w rozumieniu art. 2 pkt 3 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. 2020, poz. 344).
7) Dokumenty szczególnych wymagań bezpieczeństwa – systematyczny opis sposobu zarządzania bezpieczeństwem systemu teleinformatycznego.
8) Akredytacja bezpieczeństwa teleinformatycznego – dopuszczenie systemu teleinformatycznego do przetwarzania informacji niejawnych.
9) Certyfikaty – proces potwierdzenia zdolności urządzenia, narzędzia lub innego środka do ochrony informacji niejawnych.
10) Urząd- Urząd Gminy w Szczańcu
11) Wójt – Wójt Gminy Szczaniec
12) Pełnomocnik ochrony – Pełnomocnik ds. ochrony Informacji Niejawnych w Urzędzie Gminy w Szczańcu.

Rozdział II

Charakterystyka obiektu

1. Pomieszczenia, w których przechowywane są materiały niejawne oznaczone klauzulą *zastrzeżone* usytuowane są na piętrze budynku wolnostojącego

zlokalizowanego w Urzędzie Gminy w Szczańcu przy ulicy Herbowej 30, 66-225 Szczaniec. Budynek jest mieniem Gminy Szczaniec.
2. Budynek o konstrukcji murowanej, składający się z parteru i piętra oraz strychu, częściowo podpiwniczony, stropy drewniane, konstrukcja dachowa drewniana pokryta dachówką, stolarka okienna i drzwiowa zewnętrzna z PCV.
3. W promieniu około 50 metrów od budynku urzędu swoją siedzibę mają: szkoła, wylęgarnia drobiu, centrum usług społecznych oraz budynki jednorodzinne.

Rozdział III
Zasady udostępniania, przechowywania i zabezpieczania dokumentów zawierających informacje niejawne

§ 3

Udostępnianie zasobów materiałów niejawnych odbywa się na zasadach określonych w ustawie, tj. osobom posiadającym odpowiednie poświadczenie bezpieczeństwa lub upoważnienie kierownika jednostki oraz zaświadczenie o przeszkoleniu.

§ 4

1. Urządzenia, w których przechowuje się dokumenty zawierające informacje niejawne są codziennie po zakończeniu pracy zamykane.
2. Klucze do pomieszczeń biurowych, w tym także do serwerowni, przechowywane są w kodowanej, metalowej skrzynce na klucze. Każdego dnia z rana pobierane są przez pracowników i zdawane po zakończeniu pracy.
3. Do pomieszczeń, w których przechowywane są dokumenty zawierające informacje niejawne, poza godzinami pracy urzędu nikt nie ma dostępu. Osoby sprzątające wykonują prace podczas obecności osoby posiadającej odpowiednie poświadczenie bezpieczeństwa.

§ 5

1. Obowiązek zabezpieczenia materiałów zawierających informacje niejawne powstaje w przypadku wprowadzenie stanu nadzwyczajnego. Jako stany nadzwyczajne uważa się stany określone w art. 228 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. nr 78, poz. 483 z późn. zm.), tj. stan wojenny, stan wyjątkowy lub stan klęski żywiołowej. Stan nadzwyczajny może być wprowadzony tylko na podstawie ustawy, w drodze rozporządzenia, które podlega dodatkowemu podaniu do publicznej wiadomości.
2. W związku z wprowadzeniem stanu nadzwyczajnego działania podjęte w celu ochrony dokumentów niejawnych będących w posiadaniu Urzędu muszą odpowiadać stopniowi zagrożenia podstawowych interesów RP w zakresie obronności, bezpieczeństwa, stosunków gospodarczych i międzynarodowych państwa.
3. Ewakuacja materiałów zawierających informacje niejawne następuje na polecenie Wójta.
4. Koordynatorem ewakuacji jest pełnomocnik ochrony, który współpracuje z wyznaczonymi pracownikami urzędu.
5. Materiały niejawne przechowywane w Urzędzie, pracownik prowadzący sprawy informacji oznakowuje symbolami „Z" i „E" (Zniszczyć,

Ewakuować), który dokonuje tej czynności w uzgodnieniu z wytwórcami merytorycznymi.

6. Zabezpieczeniu podlegają:
   1) wszystkie materiały zawierające informacje niejawne – jeśli ilość tych materiałów jest niewielka,
   2) w przypadku przechowywania w jednostce organizacyjnej – większej ilości dokumentów zawierających informacje niejawne:
      a) w pierwszej kolejności zabezpieczeniu podlegają materiały niezbędne do wykonywania przez Urząd zadań obronnych w stanach nadzwyczajnych oraz zapewniające ciągłość jego funkcjonowania - oznakowane symbolem „E",
      b) w drugiej kolejności - gdy czas i warunki na to pozwolą – pozostałe materiały niejawne;
   3) materiały niejawne oznakowane symbolem „Z" należy zniszczyć np. w niszczarce.
7. Przed ewakuacją sporządza się w miarę możliwości w 2 egzemplarzach spis dokumentów przeznaczonych do ewakuacji oraz do zniszczenia; jeden egzemplarz przekazuje się kierownikowi jednostki, drugi zabiera wraz z ewakuowaną dokumentacją.
8. Decyzje w sprawie zabezpieczenia – ewakuacji materiałów podejmuje Wójt Gminy Szczaniec na wniosek pełnomocnika ochrony informacji niejawnych.
9. Miejsce zabezpieczenia materiałów podlegających ewakuacji ustala osoba podejmująca decyzje o ewakuacji.
10. Ewakuacja powinna obejmować:
    1) zapakowanie materiałów do worków ewakuacyjnych,
    2) przemieszczenie worków na środek transportu,
    3) przewiezienie do wyznaczonego przez kierownika jednostki miejsca ewakuacji.
11. Koordynatorem ewakuacji jest pełnomocnik ochrony informacji niejawnych.
12. Pracownicy Urzędu zobowiązani są na żądanie pełnomocnika do udzielenia natychmiastowej pomocy.

Załącznik nr 3 do zarządzenia nr 60/2020
Wójta Gminy Szczaniec z dnia 30 listopada 2020 r.

ZATWIERDZAM
WÓJT GMINY SZCZANIEC

Krzysztof Neryng

Dokumentacja określająca poziom zagrożeń dla systemu ochrony informacji niejawnych w Urzędzie Gminy Szczaniec

Szczaniec, dnia 30 listopad 2020 r.

Niniejsza dokumentacja opracowana została na podstawie § 3 Rozporządzenia Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (Dz. U. 2012 poz. 683). Celem opracowania jest określenie poziomu zagrożeń dla systemu ochrony informacji niejawnych w Urzędzie Gminy Szczaniec. Dotyczy ono również oceny zastosowanych środków bezpieczeństwa w przedmiotowym systemie pod kątem wymagań określonych w w/w rozporządzeniu. Przedmiotową analizą objęty został obiekt stanowiący własność gminy Szczaniec, zlokalizowany przy ulicy Herbowej 30, 66-225 Szczaniec, w którym mieści się punkt będący miejscem przetwarzania informacji niejawnych o klauzuli *„zastrzeżone"*.

Część I

Analiza poziomu zagrożeń

uwzględniająca istotne czynniki mogące mieć wpływ na bezpieczeństwo informacji niejawnych w Urzędzie Gminy w Szczańcu

Na podstawie Rozporządzenia Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych w załączeniu do niniejszego pisma przedkładam tabelę oceny istotnych czynników zagrożeń. Przedmiotowa tabela wraz z uzasadnieniem jest indywidualną oceną znaczenia poszczególnych czynników składających się w całości na analizę poziomu zagrożeń w Urzędzie Gminy Szczaniec. Określenie poziomu zagrożeń jest indywidualną oceną znaczenia czynników, o których mowa w § 3 ust. 6 rozporządzenia, mogących mieć wpływ na bezpieczeństwo informacji niejawnych w naszej jednostce. Przedmiotowa tabela wskazuje czynniki mające lub mogące mieć wpływ na bezpieczeństwo informacji niejawnych. Każdy z czynników podlega indywidualnej ocenie pod kątem znaczenia dla zagrożenia ujawnieniem lub utratą informacji niejawnych, to znaczy jest oceniony jako czynnik, który ma: „bardzo istotne znaczenie", „istotne znaczenie", „małe znaczenie". Wybór danego czynnika znajduje się w uzasadnieniu. Wartości punktowe natomiast przypisano odpowiednio „ocenie istotności" a nie czynnikom. Aby dokonać odpowiedniej oceny należy kierować się „Wskazówkami" z kolumny nr 7 w poniższej tabeli. Na koniec należy zsumować przypisane punkty. Uzyskany wynik wskazuje poziom zagrożenia, zgodnie ze skalą, który określony jest w *Tabeli do określania poziomu zagrożeń.*

Tabela oceny istotności czynników zagrożeń

l.p.	Czynnik	OCENA ISTOTNOŚCI CZYNNIKA			UZASADNIENIE	WSKAZÓWKI
		BARDZO ISTOTNY (8pkt)	ISTOTNY (4pkt)	MAŁO ISTOTNY (1pkt)		
1	2	3	4	5	6	7
1	Klauzula tajności			1	Bardzo mała liczba informacji niejawnych oznaczonych klauzula „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 należy przyjąć wartości szacunkowe.
2	Liczba materiałów niejawnych			1	Stosunkowo mała liczba dokumentów zawierających informacje niejawne.	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 należy przyjąć wartości szacunkowe.
3	Postać informacji niejawnych			1	Dokumenty zawierające informacje niejawne o klauzuli „ZASTRZEŻONE" wytwarzane są na komputerze nie mającym dostępu do internetu.	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 należy przyjąć wartości szacunkowe.
4	Liczba osób				Mała liczba pracowników upoważnionych do dostępu do	Przy ocenie istotności tego czynnika należy uwzględnić pracowników jednostki organizacyjnej mających lub

				1	informacji niejawnych w stosunku do wszystkich zatrudnionych.	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 należy przyjąć wartości szacunkowe.
5	Lokalizacja			1	Obiekt nie jest użytkowany z innymi jednostkami, nie jest w zabudowie zwartej z innymi budynkami.	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			1	Budynek urzędu zamknięty jest w godzinach nocnych. W godzinach urzędowania dostępny powszechnie, jednak poruszanie się po nim jest dozorowane poprzez pracownika z biura obsługi klienta oraz przez kamery znajdujące się na zewnątrz.	Na wzrost oceny istotności tego czynnika ma wpływ możliwość swobodnego poruszania się po budynku osób niebędących pracownikami jednostki organizacyjnej, np. gości, interesantów (w obiektach użyteczności publicznej).
7	Inne czynniki*			1	Brak zdefiniowanych zagrożeń.	Poziom zagrożeń powinien uwzględnić inne czynniki wynikające ze specyfiki jednostki organizacyjnej, niewykazanej 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		**7**				

*) 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 utrata 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 OKREŚLENIA POZIOMU ZAGROŻEŃ

POZIOM ZAGROŻEŃ		
NISKI	ŚREDNI	WYSOKI
7pkt – 16 pkt	17 pkt-32 pkt	Powyżej 32 pkt

Część II

Środki bezpieczeństwa fizycznego

W zależności od określonego poziomu zagrożeń należy rozpocząć poziom doboru środków bezpieczeństwa fizycznego, o którym mowa w § 4-8 rozporządzenia. W załączniku nr 2 do rozporządzenia, cześć II określa *Podstawowe wymagania bezpieczeństwa fizycznego*, zawierające kategorie obowiązkowe i dodatkowe, które należy uwzględnić jako pierwsze, a następnie przejść do szczegółowej *Klasyfikacji środków bezpieczeństwa,* czyli dokonać wyboru określonych środków bezpieczeństwa, przy którym należy posługiwać się tabelą z III części. Z tabeli tej należy odczytać liczbę punktów odpowiadającą wybranemu środkowi bezpieczeństwa i wpisać ją w odpowiednie miejsce w tabeli w części IV *Punktacja zastosowanych środków bezpieczeństwa.* Jeśli nie zastosujemy żadnego środka należy wpisać 0. Przy dokonywaniu wyboru konieczne jest uwzględnienie wymagań określonych w rozporządzeniu oraz w samej tabeli z części III *„Klasyfikacja środków bezpieczeństwa fizycznego"*. Dobór odpowiednich środków bezpieczeństwa fizycznego musi zapewnić uzyskanie zarówno minimalnej łącznej sumy punktów wymaganych do osiągnięcia założonego poziomu ochrony informacji niejawnych jak i uzyskanie minimalnej liczby punktów odpowiadających każdej z grup kategorii środków bezpieczeństwa fizycznego. 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.

Punktacja zastosowanych środków bezpieczeństwa fizycznego
w Urzędzie Gminy Szczaniec po uwzględnieniu odpowiedniej metodyki doboru środków.

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)	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 stanowiącą iloczyn liczby punktów za oba powyższe środki bezpieczeństwa (K1=K1S1xK1S2)	**1**
KATEGORIA K2: POMIESZCZENIA	
Środek bezpieczeństwa K2S1 – Konstrukcja pomieszczenia	
Liczba punktów za środek bezpieczeństwa (K2S1=4,3,2 lub 1 pkt)	1
Środek bezpieczeństwaK2S2 – zamek do drzwi pomieszczenia	
Liczba punktów za środek bezpieczeństwa (K2S2=4,3,2 lub 1pkt)	1
Liczba punktów za kategorię K2 stanowiącą iloczyn liczby punktów za oba powyższe środki bezpieczeństwa (K2=K2S1xK2S2)	**1**
KATEGORIA K3: Budynki	
Liczba punktów za kategorię (K3=5, 3, 2 lub 1 pkt)	**2**
KATEGORIA K4:Kontrola dostępu	
Środek bezpieczeństwa K4S1- Systemy kontroli dostępu	
Liczba punktów za środek bezpieczeństwa (K4S1=4,3,2 lub 1 pkt)	0
Środek bezpieczeństwa K4S2 – Kontrola osób nieposiadających stałego upoważnienia do wejścia na obszar jednostki organizacyjnej (interesantów)	
Liczba punktów za środek bezpieczeństwa (K4S2=3 lub 1 pkt)	0
Liczba punktów za kategorię K4 stanowiąca sumę liczby punktów za oba powyższe środki bezpieczeństwa (K4=K4S1+K4S2)	0
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 – Systemy sygnalizacji napadu i włamania	

Liczba punktów za środek bezpieczeństwa (K5S2=4,3,2 lub 1 pkt)	0
Liczba punktów za kategorię K5 stanowiąca sumę liczby punktów za oba powyższe środki bezpieczeństwa (K5=K5S1+K5S2)	0
KATEGORIA K6 - GRANICE	
Środek bezpieczeństwa K6S1 - Ogrodzenie	
Liczba punktów za środek bezpieczeństwa (K6S1=4,3,2 lub 1 pkt)	0
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)	0
Środek bezpieczeństwa K6S6 – System dozoru wizyjnego granic	
Liczba punktów za środek bezpieczeństwa (K6S6=1 lub 0 pkt)	0
Liczba punktów za kategorie K6 stanowiąca sumę liczby punktów za powyższe środki bezpieczeństwa (K6=K6S1+K6S2+K6S3+K6S4+K6S5+K6S6)	0
Ogólna liczba punktów stanowiąca sumę punktów za wszystkie kategorie PUNKTY=K1+K2+K3+K4+K5+K6	**4**

W związku z powyższym uzyskana punktacja w ilości ogółem 4 punktów wskazuje, że jednostka spełnia wymagania dotyczące środków bezpieczeństwa fizycznego. Zastosowanie obecnych środków ochrony odpowiada wymaganiom określonym w Rozporządzeniu Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych.