ZARZĄDZENIE Nr 11/2021
Wójta Gminy Nowa Sucha
z dnia 18 lutego 2021r

w sprawie wprowadzenia do stosowania dokumentów dotyczących ochrony informacji niejawnych w Urzędzie Gminy Nowa Sucha

Na podstawie art. 14 ust. 1, art. 15 ust. 1 pkt 5 i art. 43 ust. 5 ustawy z dnia 5 sierpnia 2010 r. o ochronie (t. j. Dz.U. z 2019 poz. 742) zarządza się, co następuje:

§1. Wprowadza się do stosowania w Urzędzie Gminy Nowa Sucha następującą dokumentację dotyczącą ochrony informacji niejawnych:

1) „Plan ochrony informacji niejawnych" w brzmieniu stanowiącym załącznik nr 1 do zarządzenia,

2) „Szacowanie ryzyka i poziomu zagrożeń związanych z dostępem osób nieuprawnionych do informacji niejawnych o klauzuli *zastrzeżone* lub ich utratą w Urzędzie Gminy Nowa Sucha" w brzmieniu stanowiącym załącznik nr 2 do zarządzenia,

3) „Instrukcję określającą sposób i tryb przetwarzania informacji niejawnych o klauzuli *zastrzeżone*" w brzmieniu stanowiącym załącznik nr 3 do niniejszego zarządzenia.

§2. Zobowiązuję pracowników do zapoznania się z treścią niniejszego zarządzenia oraz przestrzegania zawartych w zarządzeniu postanowień.

§3. Wykonanie zarządzenia powierzam Pełnomocnikowi ds. Ochrony Informacji Niejawnych.

§4. Zarządzenie wchodzi w życie z dniem podpisania.

GMINY NOWA SUCHA

WÓJT
mgr inż. Maciej Mońka

URZĄD GMINY NOWA SUCHA

PLAN OCHRONY INFORMACJI NIEJAWNYCH

OZNACZONYCH KLAUZULĄ *ZASTRZEŻONE*

W URZĘDZIE GMINY NOWA SUCHA

Wykonał:

Pełnomocnik do spraw ochrony

informacji niejawnych

Elżbieta Grzywacz

DEFINICJE W ROZUMIENIU PLANU OCHRONY INFORMACJI NIEJAWNYCH GMINY NOWA SUCHA

Ustawa – ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2019 r. poz. 742);

- Rękojmia zachowania tajemnicy – zdolność osoby do spełnienia ustawowych wymogów dla zapewnienie ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem, stwierdzona w wyniku przeprowadzenia postępowania sprawdzającego;
- Dokument – każda utrwalona informacja niejawna
- Materiał – dokument lub przedmiot albo dowolna ich część, chroniona jako informacja niejawna
- Przetwarzanie informacji niejawnych – wszelkie operacje wykonywane w odniesieniu do informacji niejawnych i na tych informacjach w szczególności ich wytwarzanie, modyfikowanie, kopiowanie, klasyfikowanie, przechowywanie, przekazywanie lub udostępnianie
- Urząd – Urząd Nowa Sucha
- Kierownik jednostki organizacyjnej - Wójt Gminy Nowa Sucha
- Pełnomocnikiem Ochrony – Pełnomocnik do spraw ochrony informacji niejawnych w Urzędzie Gminy Nowa Sucha
- Stan nadzwyczajny – rozumie się przez to stan wojenny, wyjątkowy, bądź klęski żywiołowej
- Planem – plan ochrony informacji niejawnych w Urzędzie Gminy Nowa Sucha
- Pion Ochrony– wyodrębniona w Urzędzie Gminy Nowa Sucha komórka organizacyjna realizująca zadania z zakresu ochrony informacji niejawnych

POSTANOWIENIA OGÓLNE

1) Plan ochrony informacji niejawnych w Urzędzie Gminy Nowa Sucha 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 art. 15 ust. 1 pkt 5 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2019

r. poz. 742) oraz rozporządzenia Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (Dz. U. poz. 683).

OSOBY ODPOWIEDZIALNE ZA ADMINISTROWANIE BEZPIECZEŃSTWEM INFORMACJI NIEJAWNYCH

1) Za ochronę informacji niejawnych z klauzula *zastrzeżone* w Urzędzie Gminy odpowiada Wójt.
2) Wójt Odpowiada za całość spraw związanych z ochroną informacji niejawnych a w szczególności za zorganizowanie i zapewnienie funkcjonowania tej ochrony.
3) Wójtowi podlega bezpośrednio zatrudniony przez niego pełnomocnik do spraw ochrony informacji niejawnych – zwany dalej „pełnomocnikiem ochrony", który odpowiada za zapewnienie przestrzegania przepisów o ochronie informacji niejawnych.

<u>Do zadań pełnomocnika ochrony należy:</u>

a) zapewnienie ochrony informacji niejawnych, w tym stosowanie środków bezpieczeństwa fizycznego
b) zarządzanie ryzykiem bezpieczeństwa informacji niejawnych, w szczególności szacowanie ryzyka
c) kontrola ochrony informacji niejawnych oraz przestrzegania przepisów o ochronie tych informacji, w szczególności okresowa (co najmniej raz na trzy lata) kontrola ewidencji, materiałów i obiegu dokumentów
d) opracowywanie i aktualizowanie, wymagającego akceptacji kierownika jednostki organizacyjnej, planu ochrony informacji niejawnych w Urzędzie Gminy, w tym w razie wprowadzenia stanu nadzwyczajnego, i nadzorowanie jego realizacji
e) prowadzenie szkoleń w zakresie ochrony informacji niejawnych
f) prowadzenie zwykłych postępowań sprawdzających oraz kontrolnych postępowań sprawdzających
g) prowadzenie aktualnego wykazu osób zatrudnionych w Urzędzie Gminy albo wykonujących czynności zlecone, które posiadają uprawnienia do dostępu do

informacji niejawnych, oraz osób, którym odmówiono wydania poświadczenia bezpieczeństwa lub je cofnięto

h) przekazywanie odpowiednio ABW do ewidencji, danych osób uprawnionych do dostępu do informacji niejawnych, a także osób, którym odmówiono wydania poświadczenia bezpieczeństwa lub wobec których podjęto decyzję o cofnięciu poświadczenia bezpieczeństwa

i) podejmowanie działań zmierzających do wyjaśnienia okoliczności naruszenia przepisów o ochronie informacji niejawnych

4) Zadania o których mowa w pkt.3 pełnomocnik ochrony realizuje przy pomocy wyodrębnionej i podległej mu komórki organizacyjnej do spraw ochrony informacji niejawnych, zwanych dalej „pionem ochrony".

PRZEDMIOT OCHRONY KTÓRY OBEJMUJE PLAN

1) Przedmiotem ochrony są materiały niejawne oznaczone – klauzulą *zastrzeżone*, które są przetwarzane w Urzędzie Gminy Nowa Sucha.
2) Informacjom niejawnym nadaje się klauzulę *zastrzeżone*, jeżeli nie nadano informacjom wyższej klauzuli tajności a ich nieuprawnione ujawnienie może mieć szkodliwy wpływ na wykonywanie przez organy władzy publicznej lub inne jednostki organizacyjne zadań w zakresie obrony narodowej, polityki zagranicznej, bezpieczeństwa publicznego, przestrzegania praw i wolności obywateli, wymiaru sprawiedliwości albo interesów ekonomicznych Rzeczypospolitej Polskiej.

RODZAJE MATERIAŁÓW NIEJAWNYCH PRZETWARZANYCH W URZĘDZIE GMINY NOWA SUCHA.

W Urzędzie Gminy Nowa Sucha przetwarza się informacje niejawne dotyczę zadań z zakresu spraw obrony narodowej zlecanych do wykonania przez Wojewodę Mazowieckiego, Starostwa Powiatowego w Sochaczewie i Wojskowej Komendy Uzupełnień. Dotyczą one dostarczenia dokumentów powołania do czynnej służby wojskowej oraz wykonywania zadań w razie wystąpienia stanów w podwyższonej gotowości obronnej.

DOSTĘP DO INFORMACJI NIEJAWNEJ

1) Uprawnienia do dostępu do informacji niejawnych o klauzuli *zastrzeżone* posiadają wyłącznie osoby, które:

a) posiadają ważne poświadczenie bezpieczeństwa upoważniające do dostępu do informacji niejawnych lub upoważnienie wydane przez Wójta zgodnie z art. 21 ust. 4 ustawy o ochronie informacji niejawnych
b) które odbyły przeszkolenie w zakresie ochrony informacji niejawnych i posiadają aktualne zaświadczenie stwierdzające odbycie tego szkolenia (nie starsze niż 5 lat od daty wystawienia)

2) Informacje niejawne mogą być udostępniane wyłącznie osobie dającej rękojmię zachowania tajemnicy w takim zakresie, jaki jest niezbędny do załatwienia konkretnej sprawy.
3) Ewidencję poświadczeń bezpieczeństwa oraz upoważnień, o których mowa powyżej prowadzi pełnomocnik ochrony.
4) 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.
5) Pełnomocnik ochrony zobowiązany jest do informowania Wójta o konieczności wydania upoważnienia pracownikom, których zakres obowiązków wymaga dostępu do dokumentów niejawnych oznaczonych klauzulą *zastrzeżone.*

PROCEDURA ZARZĄDZANIA UPRAWNIENIAMI DO WEJŚCIA, WYJŚCIA i PRZEBYWANIA W POMIESZCZENIACH GDZIE PRZETWARZANE SĄ INFORMACJE NIEJAWNE

1) Podczas przetwarzania dokumentów niejawnych w pomieszczeniach w których przetwarzane są informacje niejawne mogą przebywać wyłącznie:
a) osoby, które posiadają uprawnienia do dostępu do informacji niejawnych i wykonują czynności na rzecz Urzędu
b) osoby upoważnione do kontroli ochrony informacji niejawnych posiadające uprawnienia do dostępu do informacji niejawnych
2) Sprzątanie, remont pomieszczenia, gdzie przechowywane są informacje niejawne odbywa się w obecności pełnomocnika ochrony lub pracownika pionu ochrony.

OPIS POMIESZCZEŃ LUB OBSZARÓW, W TYM OKREŚLENIE ICH GRANIC I WPROWADZONEGO SYSTEMU KONTROLI DOSTĘPU

1) <u>Pomieszczenia w których przetwarza się informacje niejawne</u>.

Informacje niejawne o klauzuli *zastrzeżone* przetwarza się w pomieszczeniach biurowych nr 1, 20, 15/1 a przechowuje w pomieszczeniu nr 15/1. W pomieszczeniu nr 1 i 20 otwierana jest jedynie korespondencja niejawna oraz podpisywane są dokumenty niejawne. W pomieszczeniu nr 15/1 znajduje się metalowa zamykana na klucz szafa, w której przechowuje się informacje niejawne.

2) System kontroli dostępu.

System kontroli dostępu opary jest na zamkniętych drzwiach pomieszczenia, do którego można uzyskać dostęp za pomocą kluczy wydanych uprawnionym osobom.

OPIS ZASTOSOWANYCH ŚRODKÓW BEZPIECZEŃSTWA FIZYCZNEGO

W celu przeprowadzenia doboru właściwych środków bezpieczeństwa przeprowadzono analizę wszystkich istotnych czynników, które mogą mieć wpływ na bezpieczeństwo informacji niejawnych przetwarzanych w Urzędzie. Szczegółową analizę stanowi odrębny dokument –„Szacowanie ryzyka i poziomu zagrożeń związanych z dostępem osób nieuprawnionych do informacji niejawnych o klauzuli *zastrzeżone* lub ich utratą w Urzędzie Gminy Nowa Sucha". Na podstawie przeprowadzonej analizy określony został poziom zagrożenia o wartości -„Niski".

Zastosowane środki bezpieczeństwa fizycznego:

1) Bariery fizyczne

Budynek w którym znajduje się Urząd Gminy jest murowany i zadaszony. Posiada betonowy strop. W części parterowej budynku oprócz Urzędu mieści się również Gminny Ośrodek Pomocy Społecznej. Z uwagi na publiczny charakter Urzędu, w czasie jego pracy nie obowiązuje system przepustek ani też inny system określający uprawnienie do wejścia, przebywania i wyjścia z Urzędu. Po godzinach urzędowania drzwi wejściowe do budynku zamykane są na klucz. Otoczenie budynku jest oświetlone w celu skutecznej jego kontroli przez pracowników agencji ochrony. Drzwi do pomieszczeń w których przetwarzane są informacje niejawne z klauzulą *zastrzeżone* zamykane są na klucz.

2) System sygnalizacji włamania i napadu

Pomieszczenie w którym przetwarzane są informacje niejawne wyposażony jest system sygnalizacji włamania.

3) Szafy i zamki

Dokumentacja niejawna przechowywana jest w metalowej zamykanej na klucz szafie, która charakteryzują się solidną konstrukcją i wykonaniem. Jej budowa zapewnia odporność na próby nielegalnego otwarcia przez osobę do tego nieprzygotowaną, z użyciem podręcznych, łatwo dostępnych narzędzi ręcznych. Zamki do szaf charakteryzują się odpornością na sprawne działania osoby nieuprawnionej, posługującej się zwykłymi, powszechnie dostępnymi środkami.

4) Personel bezpieczeństwa

Zorganizowany jest w oparciu o pracowników firmy ochroniarskiej, którzy dozorują całodobowo budynek Urzędu Gminy. W przypadku podejrzenia włamania wzywają osoby upoważnione do otwarcia budynku.

PROCEDURA ZARZĄDZANIA I POBIERANIA KLUCZY DOSTĘPU DO SZAFY I POMIESZCZEŃ W KTÓRYCH PRZETWARZANE SĄ MATERIAŁY NIEJAWNE

1) Klucze do pomieszczeń biurowych nr 1 i nr 20 w których przetwarzane są informacje niejawne, zdaje się i pobiera z sekretariatu. Klucze wydawane i przyjmowane są za pokwitowaniem z odnotowaniem nazwisk i imion osób pobierających i zdających zgodnie z listą osób upoważnionych, sporządzaną i aktualizowaną przez referat organizacyjny Urzędu. Duplikaty kluczy, będące kluczami zapasowymi do pomieszczeń Urzędu są przechowywane w zamkniętej gablocie w zabezpieczonym pomieszczeniu socjalnym pracowników obsługi.
2) Pełnomocnik Ochrony prowadzi ewidencję pobrania kluczy do pomieszczenia nr 15/1 w którym przetwarzane, przechowywane są materiały niejawne oraz metalowej szafy w której są przechowywane.
3) Ewidencja obejmuje imię i nazwisko, datę i godzinę pobrania klucza, datę i godzinę zwrotu klucza, podpis pracownika.
4) Klucze do pomieszczenia nr 15/1 oraz metalowej szafy przechowuje pełnomocnik ochrony w zamkniętej szafce biurowej. Drugi egzemplarz kluczy do pomieszczenia nr 15/1 – duplikat przechowywany jest sekretariacie w zamkniętej szafce biurowej.

5) Zabrania się wynoszenia poza Urząd, udostępniania osobom nieuprawnionym kluczy do szafy w której przechowywane są informacje niejawne oraz do pomieszczeń, w którym przetwarzane są materiały niejawne.
6) Pracownikom Urzędu zabrania się samodzielnego dokonywania wymiany zamków bez uzyskania zgody pełnomocnika ochrony.
7) Nad prawidłowością prowadzenia ewidencji kluczy do pomieszczenia nr 15/1 oraz metalowej szafy czuwa pełnomocnik ochrony.

PROCEDURA REAGOWANIA OSÓB ODPOWIEDZIALNYCH ZA OCHRONĘ INFORMACJI ORAZ PERSONELU BEZPIECZEŃSTWA W PRZYPADKU ZAGROŻENIA UTRATĄ LUB UJAWNIENIA INFORMACJI NIEJAWNYCH.

1) Za ochronę informacji niejawnej w Urzędzie, a w szczególności za zorganizowanie i zapewnienie funkcjonowania tej ochrony w świetle ustawy, odpowiedzialny jest Wójt.
2) Za zapewnienie przestrzegania przepisów o ochronie informacji niejawnych odpowiada pełnomocnik ochrony, który realizuje swoje zadania przy udziale pionu ochrony. W przypadku zagrożenia utratą lub ujawnieniem informacji niejawnych podejmuje środki zapobiegawcze i niezwłocznie informuje o tym Wójta.
3) W przypadku stwierdzenia naruszenia przepisów o ochronie informacji niejawnych pełnomocnik ochrony zawiadamia o tym Wójta i podejmuje niezwłocznie działania zmierzające do wyjaśnienia okoliczności tego naruszenia oraz ograniczenia jego negatywnych skutków.
4) W przypadku naruszenia przepisów o ochronie informacji niejawnej w wyniku działania przestępczego, Wójt powiadamia niezwłocznie Prokuraturę lub najbliższa jednostkę Policji.

PLANY AWARYJNE UWZGLĘDNIAJĄCE POTRZEBĘ OCHRONY INFORMACJI NIEJAWNYCH W RAZIE WYSTĄPIENIA SYTUACJI NADZWYCZAJNYCH, W TYM WPROWADZENIA STANÓW NADZWYCZAJNYCH, W CELU ZAPOBIEŻENIA UTRACIE POUFNOŚCI, INTEGRALNOŚCI LUB DOSTĘPNOŚCI INFORMACJI NIEJAWNYCH.

I. Postępowanie w przypadku wystąpienia sytuacji nadzwyczajnych:

1) Pożar

W przypadku zauważenia pożaru należy niezwłocznie:

a) powiadomić Straż Pożarną,

b) powiadomić pełnomocnika ochrony i pozostałych użytkowników obiektu o pożarze

c) w przypadku konieczności przeprowadzić ewakuacja materiałów niejawnych z zachowaniem bezpieczeństwa własnego

2) Włamanie

W przypadku zauważenia włamania lub próby włamania należy powiadomić:

a) Wójta – postępować zgodnie z jego poleceniami

b) pełnomocnika ochrony

II. Postępowanie w przypadku wprowadzenia stanów nadzwyczajnych.

1) W przypadku szczególnego zagrożenia dla Państwa, gdy zwykłe środki konstytucyjne są niewystarczające, może zostać wprowadzony stan nadzwyczajny. Polska konstytucja umożliwia wprowadzenie stanów nadzwyczajnych:

a) stan wyjątkowy

b) stan wojenny

c) stan klęski żywiołowej

2) W razie wprowadzenie stanu nadzwyczajnego, w celu wzmocnienia bezpieczeństwa Urzędu Gminy przewiduje się:

a) wzmocnienie ochrony budynku Urzędu Gminy w porozumieniu z lokalną Policji

b) wprowadzenie kontroli interesantów Urzędu, poprzez wprowadzenie imiennych przepustek

3) W przypadku bezpośredniego zagrożenia przeprowadza się ewakuację materiałów zawierających informacje niejawne do miejsca zapewniającym im odpowiednie bezpieczeństwo w zaistniałej sytuacji zagrożenia.

a) ewakuacja materiałów następuje na pisemne polecenie Wójta Gminy lub pod jego nieobecność na polecenie pełnomocnika ochrony

b) koordynatorem ewakuacji materiałów jest pełnomocnik ochrony

c) ewakuacja materiałów odbywa się pod nadzorem pełnomocnika ochrony przy udziale pracowników Urzędu aktualne poświadczenie bezpieczeństwa lub upoważnienie Wójta

d) ewakuacja materiałów obejmuje ich zapakowanie i przemieszczenie w bezpieczne miejsce

4) W przypadku braku możliwości ewakuacji materiałów zawierającej informacje niejawne przeprowadza się ich zniszczenie.

a) decyzje o zniszczeniu materiałów podejmuje Wójt, a w przypadku jego nieobecności upoważniona przez niego osoba

b) nadzór nad niszczenia materiałów sprawuje pełnomocnik ochrony

c) niszczenia dokumentacji odbywa się Komisyjne

d) w skład komisji wchodzi pełnomocnik ochrony oraz osoby posiadające aktualne poświadczenie bezpieczeństwa lub upoważnienie Wójta

e) ze zniszczenia dokumentów sporządza się protokół

f) dokument niszczy się w taki sposób, aby niemożliwe było całkowite lub częściowe odtworzenie jego treści

SZKOLENIA W ZAKRESIE OCHRONY INFORMACJI NIEJAWNYCH

1) Szkolenie w zakresie ochrony informacji niejawnych przeprowadza się, w celu zapoznania pracowników Urzędu z:

a) przepisami i zasadami ochrony informacji niejawnych w zakresie niezbędnym do wykonywania pracy

b) sposobami ochrony informacji niejawnych oraz postępowania w sytuacjach zagrożenia dla takich informacji lub w przypadku ich ujawnienia

2) Szkolenie w zakresie ochrony informacji niejawnych przeprowadzają pełnomocnik ochrony.

3) Szkolenie przeprowadza się nie rzadziej niż raz na 5 lat.

ODPOWIEDZIALNOŚĆ ZA NARUSZENIE PRZEPISÓW O OCHRONIE INFORMACJI NIEJAWNYCH.

Pracownicy, którzy nie przestrzegają procedur związanych z ochroną informacji niejawnych, dopuszczają się uchybień w zakresie niewłaściwego zabezpieczania dokumentów, stwarzają warunki do ujawnienia informacji niejawnych osobom nieuprawnionym, mogą ponieść odpowiedzialność dyscyplinarną a także karną wynikającą z obowiązujących przepisów prawa.

POSTANOWIENIA KOŃCOWE

1) Pełnomocnik ochrony zapoznaje z Planem Ochrony Informacji Niejawnych osoby, które podejmują czynności związane z dostępem do informacji niejawnych.
2) Pełnomocni ochrony przeprowadza aktualizację Plan Ochrony Informacji Niejawnych przynajmniej raz w roku w celu wprowadzenia zmian.
3) W przypadku wystąpienia wątpliwości, co do zasad przetwarzania informacji niejawnych, pracownik Urzędu zgłaszają ten fakt do pełnomocnika ochrony.

Sporządził:.....

Załączniki:

Załącznik nr 1 – wykaz osób zapoznanych z planem ochrony informacji niejawnych

Załącznik nr 2 – upoważnienie do dostępu do informacji niejawnej z klauzula zastrzeżone

Załącznik nr 3 – zaświadczenie stwierdzające odbycie szkolenia z zakresu ochrony informacji niejawnych

Załącznik nr 4 – oświadczeni o zapoznaniu się z przepisami o ochronie informacji niejawnych

Załącznik nr 1

Wykaz osób zapoznanych z planem ochrony informacji niejawnych

Urzędu Gminy Nowa Sucha

l.p	Imię i nazwisko	Data zapoznania	podpis

URZĄD GMINY NOWA SUCHA

Załącznik
do zarządzenia nr 11/2021
z dnia 18 lutego 2021r.

SZACOWANIE RYZYKA I POZIMOU ZAGROŻEŃ

ZWIĄZANYCH Z DOSTĘPEM OSÓB NIEUPRAWNIONYCH DO INFORMACJ INIEJAWNYCH

O KLAUZULI *ZASTRZEŻONE* LUB ICH UTRATĄ W URZĘDZIE GMINY NOWA SUCHA

Wykonał:
Pełnomocnik
do spraw ochrony informacji niejawnych
.....Elżbieta Grajewska.....

1. Wprowadzenie

Niniejszy dokument określa poziom zagrożeń związanych z utratą poufności, integralności lub dostępności informacji niejawnych oraz ocenę zastosowanych środków bezpieczeństwa fizycznego dla ochrony informacji niejawnych w Urzędzie Gminy Nowa Sucha. Analiza zagrożeń została przeprowadzona stosownie do załącznika nr 1 do rozporządzenia Rady Ministrów z dnia 29 maja 2012 w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych (Dz. U. poz. 683). Klasyfikacja i ocena środków bezpieczeństwa fizycznego została przeprowadzona stosownie do załącznika nr 2 do wskazanego rozporządzenia.

2. Ocena istotności czynników zagrożeń

Lp.	CZYNNIK	OCENA ISTOTNOŚCI CZYNNIKA			UZASADNIENIE
		BARDZO ISTOTNY (8 pkt)	ISTOTNY (4 pkt)	MAŁO ISTOTNY (1 pkt)	
1	2	3	4	5	6
1	Klauzula tajności przetwarzanych informacji niejawnych			1	Wszystkie informacje niejawne przetwarzane w Urzędzie Gminy Nowa Sucha oznaczone są klauzulą *zastrzeżone*.
2	Liczba materiałów niejawnych			1	Liczba wszystkich materiałów niejawnych zarejestrowanych w Urzędzie Gminy wynosi 42.
3	Postać informacji niejawnych			1	Informacje niejawne przetwarzane w Urzędzie Gminy Nowa Sucha mają postać nieelektroniczną.
4	Liczba osób mających lub mogących mieć dostęp do informacji niejawnych			1	W Urzędzie Gminy upoważnienie do dostępu do informacji niejawnych posiadają cztery osoby. Faktycznie dokumentacja niejawna przetwarzana jest przez jedną osobę.
5	Lokalizacja Urzędu Gminy Nowa Sucha			1	Urząd Gminy mieści się w murowanym, pietrowym, wolnostojącym budynku. Oprócz Urzędu w części parterowej mieści się Gminny Ośrodek Pomocy Społecznej. Budynek chroniony jest całodobowo przez firmę ochroniarską.
6	Dostęp osób do budynku		4		Dostęp do budynku Urzędu Gminy Nowa Sucha jest swobodny dla osób z zewnątrz. Z uwagi na publiczny charakter Urzędu, w czasie jego pracy nie

					obowiązuje system przepustek ani też inny system określający uprawnienie do wejścia, przebywania i wyjścia z Urzędu.
7	Inne czynniki*)		4		W Urzędzie Gminy Nowa Sucha, z uwagi na specyfikę działalności Urzędu oraz charakterystykę klimatu panującego na terenie Gminy za mało prawdopodobne oceniono działanie obcych służb specjalnych, sabotaż, zamach terrorystyczny, czy działanie sił przyrody. Najbardziej prawdopodobnymi czynnikami zagrożeń jest pożar oraz zabór materiałów niejawnych przez osoby nieuprawnione w trakcie ich przetwarzania, w wyniku nie zachowania podstawowych zasad ochrony informacji niejawnych.
Suma punktów			13		

*) 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".

3. Określenie poziomu zagrożeń

Poziom zagrożeń ustalony został na podstawie wyboru "Oceny istotności czynnika" mającego wpływ na ujawnienie lub utratę informacji niejawnych w Urzędzie Gminy Nowa Sucha.

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

W wyniku przeprowadzonej analizy poszczególnych czynników ostateczny poziom zagrożeń mających lub mogących mieć wpływ na bezpieczeństwo informacji niejawnych w Urzędzie Gminy Nowa Sucha określono jako **NISKI** (pkt.13).

4. Podstawowe wymagania bezpieczeństwa fizycznego

Klauzula tajności informacji przetwarzanych w jednostce organizacyjnej	Poziom zagrożeń		
	Niski	**Średni**	**Wysoki**
ZASTRZEŻONE			
Obowiązkowo: kategorie K1+K2+K3	2	2	2
Dodatkowo: kategoria K4, K5 lub K6	-	1	2
Łącznie **suma** punktów	2	3	4

Minimalna liczba punktów do osiągnięcia dla niskiego poziomu zagrożeń i najwyższej klauzuli informacji niejawnych "zastrzeżone", wskazana w tabeli "Podstawowe wymagania bezpieczeństwa fizycznego" wynosi 2. Suma ta musi składać się obowiązkowo z sumy punktów za zastosowanie środków z kategorii 1, 2 oraz 3, a także dodatkowo punktów za zastosowanie środków z kategorii 4, 5 oraz 6.

5. Klasyfikacja środków bezpieczeństwa fizycznego

KATEGORIA K1: Szafy do przechowywania informacji niejawnych

Środek bezpieczeństwa K1S1 - Konstrukcja szafy

Typ/ Punktacja	**Funkcje lub cechy**
Typ 4 4 pkt	Szafa: 1) spełnia co najmniej wymagania klasy odporności na włamanie 0 określone w Polskiej Normie PN-EN 1143-1; 2) jest zabezpieczona dwoma zamkami typu 3 lub 4 z Kategorii K1S2.
Typ 3 3 pkt	Szafa: 1) spełnia co najmniej wymagania klasy odporności na włamanie S2 określone w Polskiej Normie PN-EN 14450; 2) jest zabezpieczona zamkiem typu 3 lub 4 z Kategorii K1S2.
Typ 2 2 pkt	Szafa: 1) spełnia co najmniej wymagania klasy odporności na włamanie S1 określone w Polskiej Normie PN-EN 14450;

	2) jest zabezpieczona zamkiem typu 2 lub 3 z Kategorii K1S2.
Typ 1 **1 pkt**	Szafa charakteryzuje się następującymi cechami: 1) jest to zamykany na klucz mebel biurowy, niewyposażony w żadne szczególne funkcje zabezpieczające, ale charakteryzujący się umiarkowaną odpornością na nieuprawnione próby otwarcia; 2) jest zabezpieczona zamkiem typu 1 lub 2 z Kategorii K1S2.

Środek bezpieczeństwa K1S2 - Zamek do szafy

Typ/ Punktacja	**Funkcje lub cechy**
Typ 4 **4 pkt**	Zamek charakteryzuje się wysokim poziomem odporności na fachowe i profesjonalne działania osoby nieuprawnionej posługującej się wyjątkowo zaawansowanymi narzędziami i umiejętnościami, które nie są powszechnie dostępne. Zamek jest zamkiem szyfrowym i spełnia co najmniej wymagania klasy B określone w Polskiej Normie PN-EN 1300. Rozróżnia się: 1) zamek mechaniczny szyfrowy co najmniej 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 pokrętło jest przekręcone więcej niż o 1 kreskę podziałki po obu stronach właściwej kreski podziałki, a w przypadku zanika czterotarczowego wartość ta wynosi 1,25. Zamek powinien być odporny na manipulację przez eksperta, również przy użyciu specjalistycznych narzędzi, przez okres 20 roboczogodzin. Zamek powinien być zabezpieczony przed działaniem destrukcyjnym, w tym przed przewierceniem i prześwietleniem (atakiem) radiologicznym (promieniowanie z radioaktywnego źródła nieprzekraczającego równowartości 10 curie, Co-60 z odległości 760 mm przez 20 godzin). Zmiana kombinacji powinna być blokowana i uaktywniana kluczem od tyłu obudowy zamka. Szafa powinna być wyposażona w dwa komplety kluczy od ustawiania szyfru; 2) zamek elektroniczny szyfrowy spełnia te same wymagania co zamek mechaniczny szyfrowy oraz nie generuje sygnałów, które mogą być wykorzystane do otwarcia zamka przez okres 20 roboczogodzin.
Typ 3 **3 pkt**	Zamek charakteryzuje się wysokim poziomem odporności na fachowe i profesjonalne działania osoby nieuprawnionej posługującej się wyjątkowo zaawansowanymi narzędziami i umiejętnościami, dostępnymi powszechnie dla profesjonalistów. Zamek jest zamkiem szyfrowym i spełnia co najmniej wymagania klasy B określone w Polskiej Normie PN-EN 1300. Rozróżnia się: 1) zamek mechaniczny szyfrowy co najmniej 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 pokrętło 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 szyfrowy spełnia te same wymagania co zamek mechaniczny szyfrowy oraz nie generuje sygnałów, które mogą być wykorzystane do otwarcia zamka przez okres 20 roboczogodzin.
Typ 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 najsłabszy element (ściana, podłoga, strop, drzwi, okna).

Środek bezpieczeństwa K2S1 - Konstrukcja pomieszczenia

Typ/ Punktacja	**Funkcje lub cechy**
Typ 4 **4 pkt**	Konstrukcja pomieszczenia charakteryzuje się następującymi cechami: 1) zapewnia wysoką odporność na próby wymuszenia otwarcia oraz otwarcia z wykorzystaniem wielu różnych zaawansowanych narzędzi ręcznych i zasilanych prądem; 2) zapewnia wysoki poziom odporności na potajemne próby uzyskania nieuprawnionego dostępu; 3) zbudowane zostało ze zbrojonego betonu o grubości 15 cm lub materiału o podobnej wytrzymałości; 4) drzwi i okna spełniają co najmniej wymagania klasy 4 określone w Polskiej Normie PN-EN 1627; 5) drzwi są wyposażone w zamek typu 4 z Kategorii K2S2.
Typ 3 **3 pkt**	Konstrukcja pomieszczenia charakteryzuje się następującymi cechami: 1) zapewnia wysoką odporność na działania osoby nieuprawnionej próbującej uzyskać dostęp siłą lub za pomocą różnorodnych narzędzi ręcznych; 2) zapewnia wysoki poziom odporności na potajemne próby uzyskania nieuprawnionego dostępu; 3) zbudowane zostało z cegły lekkiej o grubości 25 cm lub materiału o podobnej wytrzymałości; 4) drzwi i okna spełniają co najmniej wymagania klasy 3 określone w Polskiej Normie PN-EN 1627; 5) drzwi są wyposażone w zamek typu 2 lub 3 z Kategorii K2S2.
Typ 2 **2 pkt**	Konstrukcja pomieszczenia charakteryzuje się następującymi cechami: 1) zapewnia względną odporność na działania osoby nieuprawnionej próbującej uzyskać dostęp siłą lub za pomocą ograniczonej liczby narzędzi ręcznych; 2) zapewnia wysoki poziom odporności na potajemne próby uzyskania nieuprawnionego dostępu; 3) zbudowane zostało z cegły lekkiej o grubości 15 cm lub materiału o podobnej wytrzymałości albo ze sklejki 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 spełniające najmniej wymagania klasy 1 określone w Polskiej Normie PN-EN 1627. **Uwaga:** Jeżeli wymagane jest, by takie pomieszczenie było zabezpieczone przed długotrwałymi potajemnymi próbami uzyskania dostępu (na przykład w nocy lub podczas weekendu), standard drzwi i ich zaników oraz standard zabezpieczenia okien powinien być odpowiednio wyższy, adekwatnie do poziomu zagrożeń.

Środek bezpieczeństwa K2S2 - Zamek do drzwi pomieszczenia

Typ/ Punktacja	Funkcje lub cechy
Typ 4 **4 pkt**	Zamek spełniający co najmniej wymagania klasy 7 określone w Polskiej Normie PN-EN 12209.
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 najsłabszy jego element zewnętrzny.

Typ/ Punktacja	Funkcje lub cechy
Typ 4	Budynek charakteryzuje się wytrzymałą konstrukcją i następującymi cechami:

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

KATEGORIA K4: Kontrola dostępu

Środek bezpieczeństwa K4S1 - Systemy kontroli dostępu

Typ/ Punktacja	**Funkcje lub cechy**
Typ 4	Elektroniczny automatyczny system kontroli dostępu: 1) obejmuje wszystkie wejścia i wyjścia kontrolowanego pomieszczenia lub obszaru;

4 pkt	2) spełnia co najmniej wymagania systemu, w którym rozpoznanie następuje w wyniku powiązania odczytu identyfikatora (karty, klucza itp.) z wprowadzeniem informacji zapamiętanej (hasło, osobisty numer identyfikacyjny PIN) lub powiązania odczytu cech biometrycznych (odciski palców, kształt dłoni, tęczówka oka, układ naczyń krwionośnych itp.) z wprowadzeniem informacji zapamiętanej, lub powiązania odczytu identyfikatora z odczytem cech biometrycznych, a na przejściach stosuje się uzależnienie uprawnień dostępu od czasu oraz rejestruje zdarzenia; 3) zapewnia właściwy stopień ochrony, wymagający jedynie minimalnego nadzoru przez personel bezpieczeństwa; 4) 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, albo bez uprzedniego wejścia do poprzedzającej go strefy; 5) przekazuje sygnały ostrzeżeń i alarmów do stacji monitoringu obsługiwanej przez personel bezpieczeństwa.
Typ 3 **3 pkt**	Elektroniczny automatyczny system kontroli dostępu: 1) obejmuje wszystkie wejścia i wyjścia kontrolowanego pomieszczenia lub obszaru; 2) spełnia co najmniej wymagania systemu, w którym rozpoznanie następuje w wyniku powiązania odczytu identyfikatora (karty, klucza itp.) z wprowadzeniem informacji zapamiętanej (hasło, osobisty numer identyfikacyjny PIN) lub powiązania odczytu cech biometrycznych (odciski palców, kształt dłoni, tęczówka oka, układ naczyń krwionośnych itp.) z wprowadzeniem informacji zapamiętanej, lub powiązania odczytu identyfikatora z odczytem cech biometrycznych, a na przejściach stosuje się uzależnienie uprawnień dostępu od czasu oraz rejestruje zdarzenia; 3) wstęp jest kontrolowany przez odpowiednią barierę, która może wymagać bezpośredniego nadzoru przez personel bezpieczeństwa.
Typ 2 **2 pkt**	Dopuszcza się zastosowanie jednego z poniższych rozwiązań: 1) elektroniczny automatyczny system kontroli dostępu: a) obejmuje wszystkie wejścia i wyjścia kontrolowanego obszaru, b) spełnia co najmniej wymagania systemu, w którym rozpoznanie następuje w wyniku odczytu identyfikatora (karty, klucza itp.) lub odczytu cech biometrycznych (odciski palców, kształt dłoni, tęczówka oka, układ naczyń krwionośnych itp.), a na przejściach stosuje się uzależnienie uprawnień dostępu od czasu oraz rejestruje zdarzenia, c) wstęp jest kontrolowany przez odpowiednią barierę, która może wymagać bezpośredniego nadzoru strażnika; 2) system kontroli dostępu obejmujący wszystkie wejścia i wyjścia z kontrolowanego obszaru, wymagający: a) obecności personelu bezpieczeństwa, b) zastosowania fotografii lub systemu wstępu na podstawie unikalnych przepustek; w zależności od ustaleń związanych z przyznawaniem wstępu mogą być akceptowane również inne dokumenty identyfikacyjne, np. legitymacja służbowa.
Typ 1 **1 pkt**	System tego typu może być stosowany do zabezpieczania obszarów, w których są przetwarzane informacje niejawne najwyżej o klauzuli "poufne". System kontroli dostępu oparty na zamkniętych drzwiach pomieszczenia lub obszaru, do którego można uzyskać dostęp za pomocą: 1) kodów - weryfikowanych przez elektroniczny automatyczny system kontroli dostępu, w którym rozpoznanie następuje w wyniku wprowadzenia informacji zapamiętanej (hasło, osobisty numer identyfikacyjny PIN), a na przejściach stosuje się uzależnienie uprawnień dostępu od czasu oraz rejestruje zdarzenia, 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 okresowych kontroli zabezpieczeń podczas weekendów lub dni wolnych od pracy.
Typ 3 **3 pkt**	Personel bezpieczeństwa organizuje się w następujący sposób: 1) zadania personelu bezpieczeństwa mogą wykonywać pracownicy firmy zewnętrznej; 2) patrol ograniczony jest do kontroli terenu i jego granic, podczas którego strażnicy sprawdzają zabezpieczenia budynków, ale nie mają do nich dostępu; 3) częstotliwość patroli powinna zależeć od środowiska operacyjnego i poziomu zagrożenia.
Typ 2 **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 ogrodzenia; 2) strażnicy nie mają uprawnień dostępu do danego obiektu lub budynku, ale w przypadku podejrzenia włamania zareagują poprzez wezwanie osoby posiadającej klucze.

Środek bezpieczeństwa K5S2 - Systemy sygnalizacji napadu i włamania

Typ/ Punktacja	**Funkcje lub cechy**
Typ 4 **4 pkt**	System, charakteryzuje się następującymi cechami: 1) spełnia wymagania systemu stopnia 4 określone w normie PN-EN 50131-1; 2) obejmuje ochroną cały obszar, w tym szafy służące do przechowywania informacji niejawnych i sygnalizuje co najmniej: a) otwarcie drzwi, okien i innych zamknięć chronionego obszaru, b) penetrację drzwi, okien i innych zamknięć chronionego obszaru bez ich otwierania, c) penetrację ścian, sufitów i podłóg, d) poruszanie się w chronionym obszarze (pułapkowe - nadzór nad wybranymi miejscami, w których występuje wysokie prawdopodobieństwo wykrycia), e) atak na szafy służące do przechowywania informacji niejawnych; 3) stosowany jest wraz z systemem dozom wizyjnego z obowiązkową rejestracją w rozdzielczości nie mniejszej niż 400 linii telewizyjnych i przechowywaniem zarejestrowanego zapisu przez czas nie krótszy niż 30 dni, nie obejmującym pomieszczeń służących wyłącznie jako

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

	Uwaga: 1 pkt przyznaje się również w przypadku systemu wykonanego przed wejściem w życie rozporządzenia, zgodnie z wymaganiami systemu co najmniej klasy SA3 określonymi w Polskiej Normie PN-93/E-08390, pod warunkiem spełnienia wymagań w zakresie ochrony i nadzoru określonych w pkt 2 dla typu 2.

KATEGORIA K6: Granice

Środek bezpieczeństwa K6S1 - Ogrodzenie

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

	2) minimalna wysokość wynosi 250 cm.
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 zdeterminowany włamywacz/intruz.

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.

6. 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)	2
Środek bezpieczeństwa K1S2 - Zamek do szafy	
Liczba punktów za środek bezpieczeństwa (K1S2 = 4, 3, 2 lub 1 pkt)	2
Liczba punktów za kategorię K1 stanowiąca iloczyn liczby punktów za oba powyższe środki bezpieczeństwa (K1=K1S1xK1S2)	4
KATEGORIA K2: Pomieszczenia	
Środek bezpieczeństwa K2S1 - Konstrukcja pomieszczenia	
Liczba punktów za środek bezpieczeństwa (K2S1 = 4, 3, 2 lub 1 pkt)	1
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=K2S1xK2S2)	2
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)	1
Środek bezpieczeństwa K4S2 - Kontrola osób nieposiadających stałego upoważnienia do wejścia na obszar jednostki organizacyjnej (interesantów)	
Liczba punktów za środek bezpieczeństwa (K4S2 = 3 lub 1 pkt)	0
Liczba punktów za kategorię K4 stanowiąca sumę liczby punktów za oba powyższe środki bezpieczeństwa (K4=K4S1+K4S2)	1
KATEGORIA K5: Personel bezpieczeństwa i systemy sygnalizacji napadu i włamania	
Środek bezpieczeństwa K5S1 - Personel bezpieczeństwa	
Liczba punktów za środek bezpieczeństwa (K5S1 = 5, 4, 3, 2 lub 1 pkt)	3
Środek bezpieczeństwa K5S2 - Systemy sygnalizacji napadu i włamania	
Liczba punktów za środek bezpieczeństwa (K5S2 = 4, 3, 2 lub 1 pkt)	1
Liczba punktów za kategorię K5 stanowiąca sumę liczby punktów za oba powyższe środki bezpieczeństwa (K5=K5S1+K5S2)	4
Ogólna liczba punktów stanowiąca sumę punktów za wszystkie kategorie PUNKTY=K1+K2+K3+K4+K5+K6	13

Ogólna liczba punktów stanowiąca sumę punktów za wszystkie kategorie obowiązkowe K1+K2+K3 oraz w kategoriach dodatkowych K4+K5 dla poziomu zagrożenia w stopniu niskim (minimum 2pkt .) wynosi **13**. Dobrane środki bezpieczeństwa fizyczne są wystarczające do osiągnięcia założonego poziomu ochrony dla informacji niejawnych o klauzuli *zastrzeżone*.

Sporządził:

.....

URZĄD GMINY NOWA SUCHA

Załącznik

do zarządzenia nr 11/2021

z dnia 18 lutego 2021r.

INSTRUKCJA

dotycząca sposobu i trybu przetwarzania informacji niejawnych oznaczonych klauzulą „zastrzeżone" w Urzędzie Gminy Nowa Sucha.

Sporządził:

Pełnomocnik do spraw ochrony

informacji niejawnych

Elżbieta Grzywacz

POSTANOWIENIA OGÓLNE

§ 1

Instrukcja określa zasady i sposób postępowania z dokumentami niejawnymi oznaczonymi klauzulą „zastrzeżone" oraz zasady ochrony tych dokumentów w Urzędzie Gminy Nowa Sucha (zwanym dalej Urzędem).

§ 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".

§ 3

Celem instrukcji jest zapewnienie bezpieczeństwa fizycznego informacjom niejawnym o klauzuli „zastrzeżone" występującym w Urzędzie Gminy Nowa Sucha, sposobu i trybu przetwarzania tych informacji oraz zakres i warunki stosowania bezpieczeństwa fizycznego w celu ich ochrony.

§ 4

Informacjom niejawnym nadaje się klauzulę „zastrzeżone", jeżeli nie nadano im wyższej klauzuli tajności, a ich nieuprawnione ujawnienie może mieć szkodliwy wpływ na wykonywanie przez organy władzy publicznej zadań w zakresie obrony narodowej, polityki zagranicznej, bezpieczeństwa publicznego, przestrzegania praw i wolności obywateli, wymiaru sprawiedliwości albo interesów ekonomicznych Rzeczpospolitej Polskiej.

§ 5

1) Klauzulę tajności nadaje osoba, która jest 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.
2) Zniesienie lub zmiana klauzuli tajności są możliwe wyłącznie po wyrażeniu pisemnej zgody przez osobę o której mowa w pkt.1, albo jej przełożonego w przypadku ustania lub zmiany ustawowych przesłanek ochrony.
3) Wójt przeprowadzają nie rzadziej niż raz na 5 lat przegląd materiałów w celu ustalenia , czy spełniają ustawowe przesłanki ochrony.

UDOSTĘPNIANIE MATERIAŁÓW NIEJAWNYCH O KLAUZULI „ZASTRZEŻONE"

§ 6

Materiały niejawne o klauzuli „zastrzeżone" mogą być udostępniane wyłącznie osobom:

1) posiadającymi ważne poświadczenie bezpieczeństwa upoważniające do dostępu do informacji niejawnych lub upoważnienie wydane przez Wójta zgodnie z art. 21 ust. 4 ustawy o ochronie informacji niejawnych
2) które odbyły przeszkolenie w zakresie ochrony informacji niejawnych i posiadają aktualne zaświadczenie stwierdzające odbycie tego szkolenia (nie starsze niż 5 lat od daty wystawienia)

§ 7

1) Informacje niejawne z klauzulą „zastrzeżone" mogą być udostępniane uprawnionym osobom w takim zakresie, jaki jest niezbędny do załatwienia konkretnej sprawy, wynikającej z zakresu czynności.
2) Powyższe informacje mogą być udostępniane tylko osobom uprawnionym, na podstawie §6 do dostępu do informacji niejawnej, z uwzględnieniem ograniczenia wskazane go ust. 1.
3) Pełnomocnik ds. ochrony informacji niejawnych odmawia udostępnienia informacji niejawnej osobie nieuprawnionej.

§ 8

Ewidencję poświadczeń bezpieczeństwa oraz upoważnień, o których mowa w § 6 pkt 1, prowadzi Pełnomocnik ds. Ochrony Informacji Niejawnych (zwany dalej pełnomocnikiem ochrony).

§9

Pełnomocnik ochrony zobligowany jest do informowania Wójta o konieczności wydania upoważnienia pracownikom, których zakres obowiązków wymaga dostępu do dokumentów niejawnych oznaczonych klauzulą „zastrzeżone".

OBIEG MATERIAŁÓW NIEJAWNYCH OZNACZONYCH KLAUZULĄ „ZASTRZEŻONE"

§ 10

Korespondencja przychodząca Urzędu za pośrednictwem poczty polskiej lub przesyłek kurierskich przyjmowana jest w sekretariacie.

§ 11

1) Odbiór przychodzącej do Urzędu przesyłki następuje za pokwitowaniem, odciska się na niej pieczęć oraz datę wpływu do jednostki organizacyjnej.
2) Przyjmując przesyłkę sprawdza się;
    a) prawidłowość oznaczenia nadawcy i adresata
    b) całość pieczęci i opakowania
    c) zgodność odcisku pieczęci na opakowaniu z nazwą jednostki organizacyjnej nadawcy
3) W przypadku stwierdzenia uszkodzenia przesyłki lub śladów jej otwierania osoba kwitująca odbiór przesyłki sporządza, wraz z doręczającym, protokół uszkodzenia. Jeden egzemplarz protokołu przekazuje się nadawcy, drugi otrzymuje pełnomocnikowi ochrony, a w przypadku, gdy w obiegu przesyłek pośredniczył przewoźnik– kolejny egzemplarz protokołu przekazuje się także jemu.
4) Po ustaleniu, iż korespondencja dotyczy informacji niejawnej bez otwierania przekazywana jest pełnomocnikowi ochrony a pod jego nieobecność pracownikowi pionu ochrony.

§ 12

1) Po otwarciu przesyłki pełnomocnik ochrony a pod jego nieobecność pracownik pionu ochrony:

a) sprawdza, czy zawartość przesyłki odpowiada wyszczególnionym na niej numerom ewidencyjnym

b) ustala, czy liczba stron i załączników jest zgodna z liczbą oznaczoną na poszczególnych materiałach

2) W przypadku stwierdzenia nieprawidłowości w wyniku czynności o których mowa w pkt.1 pełnomocnik ochrony a pod jego nieobecność pracownik pionu ochrony sporządza w dwóch egzemplarzach protokół z otwarcia przesyłki, zawierający opis

nieprawidłowości, jeden egzemplarz przekazując do nadawcy a drugi pozostawia w Urzędzie. Fakt sporządzenia protokołu odnotowuje się w „Dzienniku ewidencji", w rubryce „Informacje uzupełniające/Uwagi".

§13

Materiał niejawnych, który wpłynął do Urzędu pełnomocnik ochrony a pod jego nieobecność pracownik pionu ochrony rejestruje niezwłocznie w dzienniku ewidencyjnym i przekazuje Wójtowi, który dokonuje pisemnej dekretacji, wskazując imiennie pracownika Urzędu odpowiedzialnego merytorycznie załatwienie sprawy lub kierownika komórki organizacyjnej Urzędu upoważnionego do wyznaczenia takiego pracownika.

§ 14

1) Po zarejestrowaniu materiału niejawnego pełnomocnik ochrony a pod jego nieobecność pracownik pionu ochrony, zgodnie z dekretacją Wójta przekazuje za pokwitowaniem dokument odbiory.
2) Po odbiorze materiału niejawnego jego odbiorca ponosi pełna odpowiedzialność za bezpieczeństwo dokumentu i informacji w nim zawartych.

§ 15

1) W przypadku wpływu przesyłki oznaczonej „do rąk własnych", w dzienniku ewidencyjnym wpisuje się nadawcę, numer i datę wpływu przesyłki, w rubryce „Informacje uzupełniające/Uwagi odnotowuje się, że przesyłka była oznaczona „do rąk własnych".
2) Na opakowaniu przesyłki o której mowa powyżej wpisuje się datę wpływu i numer, pod którym zarejestrowano przesyłkę.
3) Przesyłkę nie otwiera się i przekazuje za pokwitowaniem bezpośrednio adresatowi, a w razie jego nieobecności osobie przez niego pisemnie upoważnionej do odbioru.
4) Po odbiorze materiału niejawnego jego odbiorca ponosi odpowiedzialność za bezpieczeństwo dokumentu i informacji w nim zawartych.

§ 16

Wójt przed rozwiązaniem stosunku pracy z pracownikiem posiadającym poświadczenie bezpieczeństwa lub upoważnienie do dostępu do informacji niejawnych o klauzuli

„zastrzeżone" za pośrednictwem pełnomocnika ochrony przejmuje od pracownika całość materiałów posiadających klauzulę tajności.

WYTWARZANIE I WYSYŁANIE MATERIAŁÓW NIEJAWNYCH OZNACZONYCH KLAUZULĄ „ZASTRZEŻONE".

§ 17

Materiały niejawne wytworzone są w Urzędzie w formie dokumentu pisanego, mogą być sporządzane odręcznie, na maszynie do pisania (bez pamięci).

§ 18

1) Materiały niejawne sporządzane są i wykonywane przez pracownika merytorycznie odpowiedzialnego za jego opracowanie.
2) Praca z materiałem niejawnym, w tym sporządzanie i wykonanie może odbywać się tylko w Urzędzie.

§ 19

1) Materiały niejawne nadawane za pośrednictwem przewoźnika w postaci listów opakowuje się w dwie nieprzezroczyste koperty.
2) Materiały niejawne przesyłane za pośrednictwem przewoźnika w postaci paczek opakowuje się w dwie nieprzeźroczyste warstwy papieru.
3) Osobą upoważnioną do przygotowania, spakowania i wysłania dokumentu niejawnego jest pełnomocnik ochrony a pod jego nieobecność pracownik pionu ochrony.
4) Przesłanie korespondencji następuje za zwrotnym potwierdzeniem jego odbioru, które przechowuje następnie pełnomocnik ochrony.
5) Szczegółowe zasady pakowania, oznaczania kopert i paczek, adresowania i przesyłania dokumentów zastrzeżonych określa Rozporządzenie Prezesa Rady Ministrów z dnia 07 grudnia 2011 r. w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne (Dz. U. z 2011 r. Nr 271, poz. 1603).

REJESTROWANIE MATERIAŁÓW NIEJAWNYCH OZNACZONYCH KLAUZULĄ „ZASTRZEŻONE".

§ 20

Wszystkie otrzymane, wysłana bądź wytworzone materiały niejawny rejestruje się w dzienniku ewidencyjnym w kolejności otrzymania, wysłania lub wytworzenia.

OZNACZNIE DOKUMENTÓW NIEJAWNYCH OZNACZONYCH KLAUZULĄ „ZASTRZEŻONE".

§ 21

1) Na każdej stronie dokumentu umieszcza się:
a) na środku jako pierwszy element w nagłówku strony, klauzulę tajności
b) numer egzemplarza, a w przypadku gdy dokument wykonano w jednym egzemplarzu, napis „egz.pojedyńczy"
c) sygnaturę literowo-cyfrową, na którą składają się: literowe oznaczenie jednostki lub komórki organizacyjnej, symbol oznaczenia klauzuli tajności, numer, pod którym dokument został zarejestrowany w dzienniku ewidencji, i rok, w którym dokonano rejestracji, a także w zależności od potrzeb można umieścić inne oznaczenie uławiające ustalenie miejsca wykonania dokumentu w jednostce lub komórce organizacyjnej jednostki lub też przynależność do określonej sprawy
d) numer strony łamany przez liczbę stron całego dokumentu
e) na środku jako ostatni element w stopce strony, klauzulę tajności
2) Na pierwszej stronie dokumentu umieszcza się również:
a) nazwę jednostki lub komórki organizacyjnej
b) nazwę miejscowości i datę podpisania dokumentu
c) w przypadku dokumentu, któremu nadano bieg korespondencyjny, nazwę stanowiska adresata oraz imię i nazwisko; w przypadku wielu adresatów dokumentu, któremu nadano bieg korespondencyjny, dopuszcza się możliwość umieszczenia jedynie adnotacji „adresaci według rozdzielnika"
3) Na ostatniej stronie dokumentu pod treścią umieszcza się:
a) liczbę załączników

b) liczbę stron wszystkich załączników, jeżeli są dołączone do dokumentu lub informację określającą rodzaj załączonego materiału i jego odpowiednią jednostkę miary

c) klauzule tajności załączników wraz z numerami, pod jakimi zostały zarejestrowane w Dzienniku Ewidencji 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" – jeżeli załączniki mają być przekazane adresatowi bez pozostawiania ich w aktach, napis „do zwrotu" jeżeli załączniki mają zostać zwrócone nadawcy

e) stanowisko oraz imię i nazwisko lub inne oznaczenie wskazujące osobę uprawnioną do jego podpisania

f) liczba wykonanych egzemplarzy

g) adresatów poszczególnych egzemplarzy dokumentu albo adnotacje, „adresaci wg. rozdzielnika"

h) dyspozycję „ad acta" w przypadku egzemplarza pozostającego w aktach nadawcy

i) imię i nazwisko lub inne oznaczenie wskazujące wykonawcę

4) Na wytworzonym dokumencie można zamieścić dyspozycje dotyczącą:

a) braku zgody na kopiowanie, tłumaczenie części lub całości dokumentu

b) braku zgody na udzieleni informacji o treści dokumentu

c) określenia daty lub wydarzenia, po którym nastąpi zniesienie lub zmiana klauzuli tajności całości lub części dokumentu

5) Na dokumencie stanowiącym załącznik na pierwszej stronie umieszcza się dodatkowo informacje: „Załącznik nr... do dokumentu nr... z dnia..."

6) Wykonanie kopii, odpisów, wyciągów dokumentu o klauzuli „zastrzeżone" odbywa się na podstawie pisemnego polecenia Wójta.

7) Jeżeli wraz z dokumentem przesyła się załączniki oznaczone klauzulą „zastrzeżone", to klauzula dokumentu również posiada klauzulę „zastrzeżone". Jeżeli po trwałym odłączeniu załączników dokument jest jawny, to na każdej stronie, zamieszcza się dyspozycje: „jawne po odłączeniu załączników".

8) Zgody na zniesienie klauzuli tajności udziela się w odrębnym dokumencie podlegającym rejestracji lub przez oznaczenie w postaci umieszczenia informacji na dokumencie.

9) Oznaczenie zniesienia klauzuli tajności na dokumencie dokonuje się następująco:

a) skreśla się wszystkie dotychczasowe oznaczenia znoszonej klauzuli tajności

b) na pierwszym w kolejności skreślonym oznaczeniem klauzuli tajności umieszcza się napis „Zniesiono klauzulę tajności" oraz datę, podpis, imię i nazwisko lub inne oznaczenie wskazujące osobę dokonującą tych adnotacji oraz wskazuje się podstawę dokonania czynności

10) Skreśleń oraz pozostałych wpisów dokonuje się kolorem czerwonym, w sposób czytelny.

11) Wycieranie, wywabianie lub zamazywanie klauzuli tajności, która podlega zmianie lub zniesieniu, jest niedozwolone.

12) Czynności związane ze zniesieniem klauzuli, wykonuje pełnomocnik ochrony na pisemne polecenie Wójta.

13) Szczegółowe zasady oznaczania materiałów niejawnych, określa Rozporządzenie Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności (Dz. U. 2011.288.1692).

PRZECHOWYWANIE, NISZCZENIE I ARCHIWIZOWANIE DOKUMENTÓW OZNACZONYCH KLAUZULĄ „ZASTRZEŻONE"

§ 22

1) Dokumenty niejawne z klauzula „zastrzeżone" przechowuje się w metalowej, zamykanej na klucz szafie, zgodnie z procedurą zawartą w Planie Ochrony Informacji Niejawnych w Urzędzie Gminy Nowa Sucha.
2) Dokumenty niejawne podlegają obowiązkowej ochronie przed utratą i nieuprawnionym ujawnieniem ich treści.
3) Po realizacji czynności zwianych z otrzymanym dokumentem niejawnym, pracownik zdaje dokument pełnomocnikowi ochrony.
4) W przypadku spraw ostatecznie zakończonych, gdy dokument jest nadal chroniony, przechowuje się go do czasu zniesienia klauzuli tajności.
5) W przypadku zniesienia klauzuli tajności przekazuje się dokument do archiwum zakładowego.

§ 23

1) Dokument, który nie jest przewidziany do dalszego wykorzystania, o ile nie stanowi materiału archiwalnego, może zostać zniszczony, z zastrzeżeniem przepisów o narodowym zasobie archiwalnym i archiwach.
2) Dokument niszczy się w taki sposób, aby niemożliwe było całkowite lub częściowe odtworzenie jego treści.
3) Po protokolarnym zniszczeniu dokumentu uzupełnia się rejestry, dzienniki i inne informacje dotyczące jego rejestracji.

POSTANOWIENIA KOŃCOWE

§ 24

1) Każdy pracownik Urzędu mający dostęp do informacji niejawnych oznaczonych klauzulą „zastrzeżone" jest zobowiązany zapoznać się z niniejszą Instrukcją i stosować zawarte w niej przepisy.
2) Fakt zapoznania należy potwierdzić podpisem na „karcie zapoznania". Osobą odpowiedzialną za zapoznanie pracowników z instrukcją jest pełnomocnik ochrony.

§ 25

Zabrania się:

1) Pozostawiania materiałów niejawnych bez nadzoru.
2) Przekazywania, ujawniania treści materiałów niejawnych osobom trzecim.
3) Wynoszenie materiałów niejawnych poza budynek Urzędu.

§ 26

Każdy pracownik Urzędu jest zobowiązany niezwłocznie powiadomić pełnomocnika ochrony o wszelkich nieprawidłowościach związanych z naruszaniem zapisów niniejszej Instrukcji.

Opracował: