

**Zarządzenie Nr 34/2019
Wójta Gminy Wiśniewo
z dnia 20 września 2019 r.**

**w sprawie wprowadzenia Planu Ochrony Informacji Niejawnych w Urzędzie
Gminy Wiśniewo**

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), zarządzam co następuje:

§ 1.

W celu zapewnienia ochrony informacji niejawnych oraz dostosowania przepisów o ochronie informacji niejawnych, zatwierdzam i wprowadzam do użytku służbowego „Plan ochrony informacji niejawnych w Urzędzie Gminy Wiśniewo”, stanowiącym załącznik do niniejszego Zarządzenia.

§ 2.

Zobowiązuję poszczególnych pracowników Urzędu Gminy do stosowania ustaleń zawartych w Planie.

§ 3.

Nadzór nad realizacją Zarządzenia powierzam Pełnomocnikowi ds. Ochrony Informacji Niejawnych Urzędu Gminy Wiśniewo.

§ 4.

Traci moc Zarządzenie Nr 24/2012 Wójta Gminy Wiśniewo z dnia 29 października 2012 r. w sprawie wprowadzenia „Planu ochrony informacji niejawnych w Urzędzie Gminy Wiśniewo”.

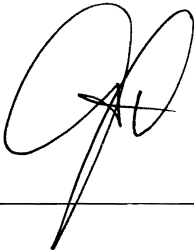
§ 5.

Zarządzenie wchodzi w życie z dniem podpisania.


WÓJT
mgr Grzegorz Woźniak

Załącznik
do Zarządzenia Nr 34/2019
Wójta Gminy Wiśniewo
z dnia 20 września 2019 r.

**PLAN OCHRONY
INFORMACJI NIEJAWNYCH
W URZĘDZIE GMINY WIŚNIEWO**

	Sporządził	Zatwierdził
Data	19.09.2019 r	23.09.2019 r
Osoba	Wojciech Szczęśniak - inspektor UG	Wójt Gminy Wiśniewo Grzegorz Woźniak
Podpis		

Spis treści

I.	Postanowienia ogólne oraz podstawy prawne ochrony informacji niejawnych.....	5
II.	Definicje używane w Planie.....	6
III.	Ocena zagrożeń dla informacji niejawnych.....	7
IV.	Przedmiot ochrony.....	9
V.	Zabezpieczenie informacji niejawnych.....	9
VI.	Ewidencja informacji niejawnych podlegających ochronie.....	9
VII.	Zasady dostępu do informacji niejawnych.....	10
VIII.	Kancelaria Niejawna Urzędu Gminy.....	10
IX.	Zakres udostępniania informacji niejawnych.....	13
X.	Zasady wytwarzania dokumentów zawierających informacje niejawne.....	13
XI.	Wytwarzanie dokumentów niejawnych z wykorzystaniem sprzętu komputerowego.....	13
XII.	Klauzule tajności.....	15
XIII.	Nadzór w zakresie ochrony informacji niejawnych.....	15
XIV.	Odpowiedzialność karna, dyscyplinarna i służbowa za naruszenie przepisów o ochronie informacji niejawnych.....	16
XV.	Archiwizowanie, gromadzenie i niszczenie materiałów niejawnych....	16
XVI.	Ustalenia końcowe.....	18
	Załącznik Nr 1	19
	Załącznik Nr 2	21
	Załącznik Nr 3	22
	Załącznik Nr 4	24
	Załącznik Nr 5	27
	Załącznik Nr 6	28
	Załącznik Nr 7	29
	Załącznik Nr 9	31

I. Postanowienia ogólne oraz podstawy prawne

Przedmiotem ochrony w Urzędzie Gminy Wiśniewo są informacje niejawne oznaczone klauzulą „zastrzeżone”. Plan ochrony informacji niejawnych jest dokumentem określającym sposób i tryb przetwarzania informacji niejawnych o klauzuli „zastrzeżone” w komórkach organizacyjnych Urzędu Gminy, a także sposoby zapewnienia fizycznego bezpieczeństwa informacji.

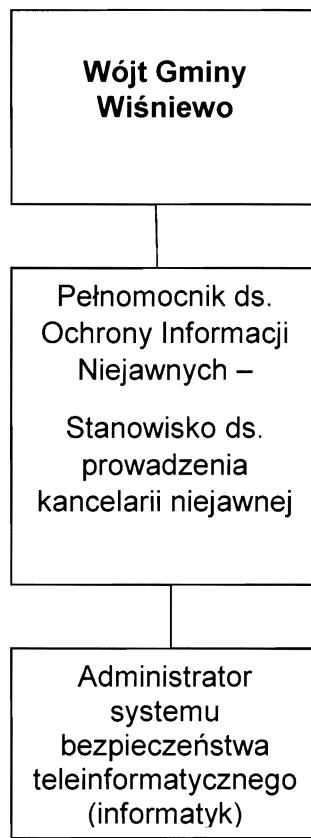
Środki i procedury określone w planie ochrony odnoszą się do informacji niejawnych oznaczonych klauzulą „zastrzeżone” w rozumieniu ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2019 r., poz.742), oraz:

- Rozporządzenia Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie wzoru decyzji o cofnięciu poświadczenia bezpieczeństwa (Dz.U. z 2010 r Nr 258, poz.1754);
- Rozporządzenia Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie wzoru decyzji o odmowie wydania poświadczenia bezpieczeństwa (Dz.U. z 2010 r Nr 258, poz.1753);
- Rozporządzenia Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie wzorów poświadczenia bezpieczeństwa (Dz.U. z 2015 r., poz.220);
- Rozporządzenia 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 przeprowadzonego szkolenia przez Agencję Bezpieczeństwa Wewnętrznego lub Służbę Kontrwywiadu Wojskowego (Dz.U. z 2015 r., poz.205);

Wprowadzone do stosowania środki i procedury w zakresie ochrony informacji niejawnych określa:

- „Instrukcja sposobu i trybu przetwarzania informacji niejawnych o klauzuli „zastrzeżone” w Urzędzie Gminy Wiśniewo”;

W Urzędzie Gminy Wiśniewo powołany jest Pełnomocnik ds. Ochrony Informacji Niejawnych, a za prowadzenie Kancelarii Niejawnej odpowiada wyznaczony przez Wójta pracownik Urzędu Gminy. Pełnomocnikowi podlega administrator systemu bezpieczeństwa teleinformatycznego (informatyk).



II. Definicje używane w Planie ochrony informacji niejawnych

1/ *informacje niejawne* – to informacje, których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej, albo byłoby z punktu widzenia jej interesów niekorzystne, niezależnie od formy i sposobu ich wyrażania, a także w trakcie ich opracowywania;

2/ *informacje niejawne o klauzuli „zastrzeżone”* – to informacje, których 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;

3/ *rękojmia zachowania tajemnicy* – to zdolność osoby do spełnienia ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem, stwierdzona w wyniku przeprowadzenia postępowania sprawdzającego;

4/ *dokumentem* – jest każda utrwalona informacja niejawna;

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

6/ *przetwarzanie informacji niejawnych* – to wszelkie operacje wykonywane w odniesieniu do informacji niejawnych i na tych informacjach, w szczególności ich wytworzenie, modyfikowanie, kopiowanie, klasyfikowanie, gromadzenie, przechowywanie, przekazywanie lub udostępnianie;

7/ *system teleinformatyczny* – zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie danych;

8/ *sporządzający dokument* – pracownik, który przygotowuje i sporządza projekt dokumentu lub innego niż dokument materiału zawierającego informacje niejawne;

9/ *wytwórca dokumentu* – pracownik upoważniony do podpisania dokumentu lub oznaczania innego niż dokument materiału zawierającego informacje niejawne;

10/ *służby ochrony państwa* – to Agencja Bezpieczeństwa Wewnętrznego;

11/ *Urząd* – to Urząd Gminy Wiśniewo;

12/ *Wójt* – to Wójt Gminy Wiśniewo;

13/ *Pełnomocnik ochrony* – to Pełnomocnik ds. Ochrony Informacji Niejawnych.

III. Ocena zagrożeń dla informacji niejawnych

1/ Zagrożenia zewnętrzne

a/ zagrożeniami zewnętrznymi dla Urzędu Gminy Wiśniewo są:

- możliwość napadu przez zorganizowane grupy przestępcze i terrorystyczne, działające w sposób profesjonalny, przemyślany i zorganizowany,
- możliwość napadu przez pojedynczych przestępców, przypadkowe osoby wykorzystujące nadarzającą się okazję z powodu nieprawidłowości w ochronie mienia Urzędu;

b/ symptomy mogące świadczyć o przygotowaniu napadu lub włamania do budynku:

- wzmożone zainteresowanie osób postronnych obiektami, pomieszczeniami Urzędu objawiające się m.in. podejmowaniem prób uzyskania informacji o obiektach, pomieszczeniach od pracowników podczas rozmów,
- nawiązanie rozmów przez osoby postronne z pracownikami,
- podszywanie się pod byłych pracowników Urzędu i przejawianie zainteresowania tym, co się po latach zmieniło,
- interesowanie się osobami funkcyjnymi oraz sposobem wykonywania obowiązków służbowych,
- obserwacja sposobu działania systemu ochronnego, sekretariatu, sprzątaczek itp.,
- rozpoznawanie systemu technicznych zabezpieczeń, w tym stosowanych urządzeń alarmowych,
- celowe uszkodzanie urządzeń alarmowych, linii telefonicznych, oświetlenia itp.;
- próby pozyskania do grup przestępczych pracowników Urzędu;

c/ czynności uprzedzające ewentualne możliwości zaistnienia zagrożeń:

- systematyczna, skrupulatna i wnikliwa kontrola systemu ochrony przez osoby odpowiedzialne za jego organizację,
- pracownicy pionu ochrony w czasie dnia pracy powinni zwracać szczególną uwagę na możliwość zaistnienia ewentualnych zagrożeń,

- stosowanie zasady niedopuszczania osób niepowołanych do penetracji pomieszczeń Urzędu,
- wykonywanie prac porządkowych, remontowych itp. w Urzędzie wyłącznie pod nadzorem osób odpowiedzialnych.

2/ Zagrożenie wewnętrzne

a/ zagrożenia wewnętrznymi dla Urzędu są:

- próby zaboru dokumentów lub mienia przez pracowników Urzędu,
- próby powielania, kserowania dokumentów służbowych dla celów prywatnych,
- byli pracownicy Urzędu zwolnieni dyscyplinarnie,
- próby wglądu w dokumenty przez osoby nieuprawnione,
- nadmierne spożywanie alkoholu – przesłanka do wykroczeń dyscyplinarnych i przestępstw.

b/ czynności uprzedzające ewentualne możliwości zaistnienia zagrożeń:

- zwracanie szczególnej uwagi na osoby, które mogą być zainteresowane zaborem dokumentów,
- prowadzenie szczególnego nadzoru by nie dokonywano prób kserowania, kopiowania bez zgody przełożonego,
- uwrażliwienie pracowników w trakcie prowadzonych szkoleń na możliwość prób kontaktu grup przestępczych z pracownikami, którzy mają dostęp do dokumentów szczególnie ważnych,
- zastosowanie zasady, że do informacji niejawnych mogą mieć dostęp tylko pracownicy posiadający poświadczenie bezpieczeństwa lub właściwe upoważnienie wydane przez Wójta,
- zwrócenie szczególnej uwagi na osoby, których zachowanie wskazuje na nadmierne spożywanie alkoholu.

3/ Postępowanie w sytuacjach kryzysowych

a/ w przypadku wystąpienia sytuacji kryzysowych należy w pierwszej kolejności powiadomić Wójta Gminy, Pełnomocnika ochrony oraz osoby odpowiedzialne za pomieszczenia, w których przechowuje się dokumenty niejawne;

b/ w pierwszej kolejności należy zabezpieczyć:

- pieczęcie,
- dokumenty o klauzuli „zastrzeżone”,
- kopie zapasowe, jeżeli są przechowywane,
- inne dokumenty i materiały według sporządzonego planu ewakuacji;

c/ dokumenty ewakuuje się w opłombowanych, brezentowych workach ewakuacyjnych, za ewakuację odpowiedzialny jest Pełnomocnik ochrony;

d/ miejscem ewakuacji są pomieszczenia Archiwum Zakładowego z uwzględnieniem zapewnienia odpowiedniej ochrony w miejscu ewakuacji;

e/ w sytuacji, gdy ewakuacja jest niemożliwa, w pierwszej kolejności należy zniszczyć dokumenty o klauzuli „zastrzeżone”, pieczęcie i w miarę możliwości pozostałe dokumenty i materiały;

f/ w przypadku zaistnienia stanów nadzwyczajnych (stan wojny, stan wyjątkowy, stan klęski żywiołowej), powiadamia się Wójta i inne odpowiedzialne osoby, przy pomocy dostępnych środków teletechnicznych, lub gdy jest to możliwe, za pomocą gońca;

g/ sposób i kolejność powiadamiania zamieszczono w „Planie stałego dyżuru”, który przechowywany jest w szafie zamykanej na klucz, w pomieszczeniu będącym

miejscem pracy Pełnomocnika ochrony. Powiadamia się także Policję, Straż Pożarną i inne służby oraz instytucje, w zależności od zaistniałej sytuacji;

h/ metody postępowania w stanach nadzwyczajnych określone są w „Planie stałego dyżuru”;

i/ w przypadku zgłoszenia o podłożeniu ładunku wybuchowego, albo zauważenia w Urzędzie przedmiotu niewiadomego pochodzenia, należy postępować zgodnie z instrukcją stanowiącą załącznik Nr 1 do niniejszego Planu.

IV. Przedmiot ochrony

Przedmiotem ochrony w Urzędzie Gminy są:

- informacje niejawne oznaczone klauzulą „zastrzeżone”,
- pomieszczenie, w którym są przechowywane i opracowywane materiały niejawne,
- autonomiczne stanowisko komputerowe przeznaczone do przetwarzania, wytwarzania i przechowywania informacji niejawnych.

V. Zabezpieczenie informacji niejawnych

1/ Informacje niejawne o klauzuli „zastrzeżone” są przechowywane w budynku Urzędu, parter – magazyn OC.

2/ Informacje niejawne oznaczone klauzulą „zastrzeżone” są przechowywane w szafie metalowej.

5/ Komputer wykorzystywany wyłącznie do przetwarzania i wytwarzania informacji niejawnych znajduje się w Kancelarii Niejawnej. Uruchomienie komputera następuje wyłącznie po podaniu właściwego hasła, po zakończeniu pracy jest on odłączany z sieci elektrycznej.

VI. Ewidencja informacji niejawnych podlegających ochronie

1/ Informacje niejawne oznaczone klauzulą „zastrzeżone” są rejestrowane w dzienniku ewidencji w Kancelarii Niejawnej Urzędu.

2/ Dziennik ewidencji jest urządzeniem ewidencyjnym służącym do ewidencjonowania dokumentów niejawnych wytworzonych w Urzędzie, korespondencji niejawnej otrzymanej (wchodzącej) i wysłanej (wychodzącej).

3/ Każdy dokument niejawny przychodzący lub wychodzący z urzędu, rejestruje się w odrębnej pozycji dziennika ewidencyjnego.

4/ Osoba upoważniona do przyjmowania korespondencji niejawnej wchodzącej w formie listów lub paczek jest Pełnomocnik ochrony. Listy lub paczki zawierające korespondencję niejawną mogą wpływać z zewnątrz jako przesyłki polecone bezpośrednio do Kancelarii Niejawnej lub Sekretariatu Urzędu. Pracownik Sekretariatu po stwierdzeniu, że wewnątrz znajduje się druga koperta oznaczona klauzulą tajności, nie otwiera jej i nie rejestruje w swojej ewidencji, przekazuje ją niezwłocznie Pełnomocnikowi ochrony.

5/ Korespondencji niejawnej skierowanej mylnie nie ewidencjonuje się w Kancelarii Niejawnej, lecz przekazuje łącznie z poprzednim opakowaniem w nowej kopercie właściwemu adresatowi za zwrotnym potwierdzeniem odbioru.

VII. Zasady dostępu do informacji niejawnych

1/ Informacje niejawne oznaczone klauzulą „zastrzeżone” mogą być udostępniane wyłącznie osobie uprawnionej do dostępu do informacji niejawnych o określonej klauzuli niejawności.

2/ Uzyskanie uprawnień do dostępu do informacji niejawnych o klauzuli „zastrzeżone” może nastąpić po:

- a/ pisemnym upoważnieniu danej osoby przez Wójta Gminy, oraz
- b/ odbyciu szkolenia w zakresie ochrony informacji niejawnych.

VIII. Kancelaria Niejawna Urzędu Gminy

1/ Opis techniczny pomieszczenia:

a/ w Urzędzie Gminy Wiśniewo Kancelaria Niejawna znajduje się na parterze – magazyn OC. Dostęp do niej ma tylko Pełnomocnik ochrony oraz osoba zajmująca się prowadzeniem Kancelarii Niejawnej. W pokoju tym są przechowywane i wydawane uprawnionym osobom informacje niejawne o klauzuli „zastrzeżone”. Pokój spełnia wymagania prawne odnośnie ochrony fizycznej informacji niejawnych, co zabezpiecza materiały przed ich nieuprawnionym ujawnieniem, utratą, uszkodzeniem lub zniszczeniem;

b/ środki ochrony fizycznej informacji niejawnych w Kancelarii Niejawnej:

- ściany i stropy wykonane są z materiałów niepalnych, spełniających wymagania w zakresie klasy odporności pożarowej oraz nośności granicznej odpowiadającej co najmniej konstrukcji murowanej,
- drzwi zewnętrzne wyposażone są w zwykły zamek drzwiowy i są objęte monitoringiem, podobnie jak całe pomieszczenie Kancelarii Niejawnej,
- po zakończeniu pracy Urzędu, wejście do pokoju a tym samym dostęp do Kancelarii Niejawnej zabezpieczają drzwi antywłamaniowe,
- szafa stalowa zamykana na klucz dostępny tylko Pełnomocnikowi ochrony,

c/ po zakończeniu pracy Pełnomocnik ochrony jest obowiązany sprawdzić prawidłowość zamknięcia szafy oraz drzwi wejściowych Kancelarii Niejawnej,

2/ Zasady przechowywania kluczy i pieczęci:

a/ po zakończeniu pracy pieczęcie złożone są w szafie metalowej w Kancelarii Niejawnej;

b/ klucze od szaf oraz od drzwi wejściowych zdeponowane są u Pełnomocnika ochrony;

c/ zapasowy komplet kluczy do pomieszczenia Kancelarii Niejawnej zabezpieczony jest w szafie metalowej w pokoju Nr 5 - parter (Urząd Stanu Cywilnego – objęty monitoringiem).

3/ Przyjmowanie, rejestrowanie i obieg korespondencji niejawnej:

a/ osobą upoważnioną do przyjmowania niejawnej korespondencji wchodzącej do Urzędu w formie listów czy paczek jest Pełnomocnik ochrony;

b/ listy lub paczki zawierające korespondencje niejawna mogą wpływać z zewnątrz jako przesyłki polecone bezpośrednio do Kancelarii Niejawnej lub Sekretariatu Urzędu;

c/ pracownik Sekretariatu po stwierdzeniu, że wewnątrz znajduje się druga koperta oznaczona klauzulą tajności, nie otwiera jej i nie rejestruje w swojej ewidencji, przekazuje ją niezwłocznie Pełnomocnikowi ochrony;

d/ Pełnomocnik ochrony przyjmuje przesyłki i dokumenty i odciska na nich pieczęć oraz datę wpływu do Kancelarii Niejawnej;

e/ przyjmując przesyłkę sprawdza się:

- prawidłowość adresu
- całość pieczęci i opakowania,
- zgodność odcisku pieczęci na opakowaniu z nazwą jednostki nadawcy,
- zgodność numeru na przesyłce z numerem tej przesyłki w wykazie lub książce doręczeń,

f/ w razie stwierdzenia uszkodzenia opakowania przesyłki niejawnej lub śladów jej otwierania, osoba przyjmująca przesyłkę sporządza wraz z doręczycielem protokół uszkodzenia w trzech egzemplarzach, z których pierwszy otrzymuje Pełnomocnik ochrony, drugi wysyła się nadawcy, trzeci pozostawia się w aktach doręczyciela,

g/ po otwarciu przesyłki Pełnomocnik ochrony:

- sprawdza, czy zawartość przesyłki odpowiada wyszczególnionym na niej numerom ewidencyjnym,

- ustala, czy liczba załączników i stron jest zgodna z liczbą oznaczoną na poszczególnych dokumentach,

h/ w przypadku stwierdzenia nieprawidłowości Pełnomocnik ochrony sporządza w dwóch egzemplarzach protokół z otwarcia przesyłki zawierający opis nieprawidłowości, jeden egzemplarz przekazuje nadawcy. Fakt sporządzenia protokołu odnotowuje się w dzienniku ewidencji, w rubryce „informacje uzupełniające/Uwagi”;

i/ przekazywanie przesyłek niejawnych bezpośrednio adresatowi z pominięciem Kancelarii Niejawnej jest zabronione, nawet gdy są oznaczone napisem „Do rąk własnych”;

j/ w Kancelarii Niejawnej nie otwiera się przesyłek oznaczonych „Do rąk własnych”. Rejestruje się je w dzienniku ewidencji z adnotacją o ich oznaczeniu, opisuje na opakowaniu datę wpływu, pozycję i numer w dzienniku, a następnie przekazuje bezpośrednio adresatowi, za pokwitowaniem. W razie nieobecności adresata

przesyłkę przekazuje się osobie posiadającej pisemne upoważnienie do odbioru korespondencji niejawnej, za pokwitowaniem w dzienniku ewidencji;

k/ przesyłki oznaczone „Do rąk własnych” po wykorzystaniu zwraca się do Kancelarii Niejawnej w stanie otwartym bądź zamkniętym. Jeśli zwrot nastąpi w stanie zamkniętym, osoba zwracająca dokument zobowiązana jest udzielić Pełnomocnikowi ochrony informacji, czego dokument dotyczy, ile zawiera stron, ilość załączników oraz osobiście odciska pieczęć wpływu, wpisując numer z dziennika ewidencji. Dokument jest przechowywany w Kancelarii Niejawnej lub wraca do pracownika, który go otrzymał;

l/ dokumenty niejawne, wpływające do urzędu, przed zarejestrowaniem wymagają decyzji Wójta w formie pisemnej dekretacji dokonanej w sposób trwały na dokumencie, kierującej ten dokument do konkretnego pracownika do załatwienia;

m/ Pełnomocnik ochrony rejestruje dokument niejawny w dzienniku ewidencyjnym. Pismo wchodzące po rejestracji w Kancelarii Niejawnej trafia do wskazanego w dekretacji uprawnionego pracownika, który kwituje odbiór dokumentu w dzienniku ewidencyjnym. Dokumenty są tematycznie upinane w teczkach i przechowywane w Kancelarii Niejawnej lub innych pomieszczeniach, jeżeli będą umieszczane w meblach biurowych zamykanych na klucz, zgodnie z ustawowymi wymogami;

n/ korespondencji niejawnej mylnie skierowanej nie ewidencjonuje się w Kancelarii Niejawnej, lecz przekazuje łącznie z poprzednim opakowaniem w nowej kopercie właściwemu adresatowi, za zwrotnym potwierdzeniem odbioru;

o/ przesyłki pilne, telegramy i szyfrogramy doręcza się adresatom bezzwłocznie. Przy kwitowaniu tych przesyłek odnotowuje się godzinę doręczenia;

p/ w przypadku otrzymania przesyłki niewiadomego pochodzenia lub budzącej podejrzenia z jakiegokolwiek powodu, należy postępować zgodnie z instrukcją stanowiącą załącznik Nr 2 do Planu;

q/ wytworzony dokument niejawny w Urzędzie oraz wysłaną przesyłkę niejawną, Pełnomocnik ochrony rejestruje w dzienniku ewidencji, odpowiednio w kolejności wytworzenia;

r/ zapisów w dzienniku ewidencji dokonuje się kolorem czarnym lub niebieskim, a zmiany tych zapisów kolorem czerwonym, z datą, powodem dokonania zmiany i czytelnym podpisem dokonującego zmiany. Zabrania się wycierania i zamazywania zapisów w dzienniku ewidencji;

s/ korespondencja niejawna wysyłana jest pocztą, listem poleconym, w podwójnej kopercie, opisanej zgodnie z załącznikiem Nr 3 do Planu. Przygotowaną przesyłkę należy zarejestrować w elektronicznym systemie korespondencyjnym Urzędu Gminy a następnie dostarczyć do wysłania do Sekretariatu Urzędu.

IX. Zakres udostępniania informacji niejawnych

1/ Udostępnianie pracownikowi informacji niejawnych uwarunkowane jest posiadaniem właściwego i ważnego poświadczenia bezpieczeństwa lub upoważnienia Wójta, tylko w zakresie niezbędnym do załatwienia konkretnej sprawy.

2/ Pełnomocnik ochrony współdziała ze służbami ochrony państwa za wiedzą i zgodą Wójta w przypadku naruszenia przepisów o ochronie informacji niejawnych.

3/ Służby ochrony państwa mogą zwracać się do Wójta Gminy z pisemnym wnioskiem o przekazanie informacji oraz udostępnienie niezbędnych dokumentów w celu potwierdzenia danych o osobach sprawdzanych.

X. Zasady wytwarzania dokumentów zawierających informacje niejawne

1/ Propozycję przyznania klauzuli niejawności na wykonywanym dokumencie przedstawia osoba sporządzająca dokument.

2/ Klauzule niejawności na danym dokumencie przyznaje osoba, która jest upoważniona do podpisania dokumentu.

3/ Rękopisy sporządzonych dokumentów zawierające informacje niejawne muszą być wykonane w brulionach (zeszytach) uprzednio zarejestrowanych w dzienniku ewidencji.

4/ Dokumenty niejawne powinny być opisane i oznaczone zgodnie z Rozporządzeniem Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów, umieszczania na nich klauzul tajności, a także zmiany nadanej klauzuli tajności (Dz.U. z 2011 r. Nr 228, poz.1692).

5/ Sposób właściwego opisu dokumentu niejawnego został przedstawiony w załączniku Nr 4 do Planu ochrony.

XI. Wytwarzanie dokumentów niejawnych z wykorzystaniem sprzętu komputerowego

1/ Bezpieczeństwo teleinformatyczne zapewnia się chroniąc informacje przetwarzane w systemach teleinformatycznych przed utratą właściwości gwarantujących to bezpieczeństwo, w szczególności przed utratą poufności, dostępności i integralności.

2/ Bezpieczeństwo teleinformatyczne zapewnia się przed rozpoczęciem oraz w trakcie przetwarzania informacji niejawnych w systemie teleinformatycznym.

3/ Za właściwą organizację bezpieczeństwa teleinformatycznego odpowiada Wójt Gminy, który w szczególności:

a/ zapewnia opracowanie dokumentacji bezpieczeństwa systemu teleinformatycznego;

b/ realizuje ochronę fizyczną systemu teleinformatycznego;

c/ zapewnia niezawodność transmisji oraz kontrolę dostępu do urządzeń systemu teleinformatycznego;

- d/ dokonuje analizy stanu bezpieczeństwa teleinformatycznego oraz zapewnia usunięcie stwierdzonych nieprawidłowości;
- e/ zapewnia przeszkolenie z zakresu bezpieczeństwa teleinformatycznego dla osób uprawnionych do pracy w systemie teleinformatycznym.

4/ Wójt Gminy wyznacza administratora systemu bezpieczeństwa teleinformatycznego (informatyk), który odpowiedzialny jest za:

- a/ funkcjonowanie systemu teleinformatycznego;
- b/ przestrzeganie zasad i wymagań bezpieczeństwa, przewidzianych dla systemu teleinformatycznego.

5/ Administrator systemu powinien posiadać poświadczenie bezpieczeństwa odpowiednie do klauzuli informacji wytwarzanych, przetwarzanych, przechowywanych lub przekazywanych w systemie teleinformatycznym oraz odbyć specjalistyczne szkolenia z zakresu bezpieczeństwa teleinformatycznego, prowadzone przez służby ochrony państwa. Zaświadczenie o odbytym szkoleniu jest przechowywane w aktach osobowych oraz dokumentacji pełnomocnika ochrony.

6/ Systemy teleinformatyczne, w których mają być przetwarzane informacje niejawne o klauzuli:

- a/ „zastrzeżone” – Wójt Gminy udziela akredytacji bezpieczeństwa teleinformatycznego przez zatwierdzenie dokumentacji bezpieczeństwa systemu teleinformatycznego.

7/ Ochrona fizyczna systemu teleinformatycznego polega na zastosowaniu środków zapewniających ochronę przed nieuprawnionym dostępem, podglądem czy podsłuchem.

8/ Ochrona elektromagnetyczna systemu teleinformatycznego polega na niedopuszczeniu do utraty poufności i dostępności informacji niejawnych przetwarzanych w urządzeniach teleinformatycznych:

- a/ utrata poufności następuje w szczególności na skutek wykorzystania elektromagnetycznej emisji ujawniającej, pochodzącej z tych urządzeń;
- b/ utrata dostępności następuje w szczególności na skutek zakłócania pracy urządzeń teleinformatycznych za pomocą impulsów elektromagnetycznych o dużej mocy.

9/ W celu zapewnienia kontroli dostępu do systemu teleinformatycznego:

- a/ Wójt Gminy lub osoba przez niego upoważniona ustala warunki i sposób przydzielania uprawnień osobom uprawnionym do pracy w systemie teleinformatycznym;
- b/ Administrator systemu określa warunki oraz sposób przydzielania tym osobom kont oraz mechanizmów kontroli dostępu, a także zapewnia ich właściwe wykorzystanie.

10/ W sytuacjach wymagających konsultacji lub uzgodnień, Wójt może zwrócić się do Agencji Bezpieczeństwa Wewnętrznego o wydanie opinii lub zleceń w zakresie bezpieczeństwa teleinformatycznego.

11/ Zaleca się wykonywanie kopii zapasowych wykonanych dokumentów niejawnych.

12/ Sposób przechowywania zapasowych kopii jest identyczny jak przechowywanie dokumentów wykonanych w formie tradycyjnej (pismo), w przypadku gdy nośnikiem informacji jest materiał inny niż pismo, klauzule tajności i sygnaturę literowo-cyfrową umieszcza się przez ostemplowanie, nadrukowanie, wpisanie odręczne, trwałe dołączenie metek, nalepek, kalkomanii lub w inny sposób, bezpośrednio, a jeżeli nie jest to możliwe na ich obudowie lub kalkomanii lub w inny sposób, bezpośrednio, a jeżeli nie jest to możliwe na ich obudowie lub opakowaniu.

XII. Klauzule tajności

1/ Oznaczenie materiału klauzulą tajności polega na umieszczeniu na nim klauzuli tajności.

2/ Przyznaną klauzulę tajności nanosi się w sposób wyraźny i w pełnym jej brzmieniu.

3/ Wprowadza się następujące oznaczenie klauzul tajności dla dokumentów niejawnych, stanowiących tajemnicę służbową:

„Z” – dla klauzuli „zastrzeżone”

4/ W przypadku zmian lub znoszenia klauzul tajności, skreśleń i adnotacji dokonuje Pełnomocnik ochrony, albo upoważnione przez Wójta inne osoby.

5/ Skreśleń i adnotacji dokonuje się kolorem czerwonym, w sposób czytelny. Wycieranie, wywabianie lub zamazywanie klauzuli tajności i dokonanych zmian jest niedozwolone.

XIII. Nadzór w zakresie ochrony informacji niejawnych

1/ Za ochronę informacji niejawnych w urzędzie odpowiada Wójt Gminy.

2/ Wójt przeprowadza nie rzadziej niż raz na 5 lat przegląd materiałów w celu ustalenia, czy spełniają ustawowe przesłanki ochrony.

3/ Zadania określone ustawą z dnia 05 sierpnia 2010 r. o ochronie informacji niejawnych w imieniu Wójta wykonuje Pełnomocnik ochrony poprzez:

a/ sprawowanie nadzoru nad realizacją zadań i przestrzeganiem przepisów określonych w Planie ochrony;

b/ sprawowanie kontroli w zakresie ochrony informacji niejawnych oraz przestrzegania procedur związanych z upoważnieniem do dostępu do tych informacji, w odniesieniu do wszystkich komórek organizacyjnych Urzędu.

XIV. Odpowiedzialność karna, dyscyplinarna i służbowa za naruszenie przepisów o ochronie informacji niejawnych

1/ Zakres odpowiedzialności karnej osób, które dopuściły się przestępstwa lub czynu zabronionego przeciwko ochronie informacji niejawnych, został określony przepisami art.266 Kodeksu Karnego (ustawa z dnia 06 czerwca 1997 r. Kodeks Karny – (Dz.U. z 2018 r., poz.1600 z późn.zm.).

2/ W stosunku do pracowników, którzy nie przestrzegają wymagań związanych z ochroną informacji niejawnych i nierzetelnie wykonują swoje obowiązki, dopuszczają się uchybień w zakresie niewłaściwego zabezpieczenia dokumentów i informacji podlegających ochronie stwarzając warunki do ujawnienia tajemnicy osobom nieuprawnionym, zastosowane będą przewidziane prawem sankcje dyscyplinarne i służbowe.

XV. Archiwizowanie, gromadzenie i niszczenie materiałów niejawnych

1/ Archiwizowanie materiałów niejawnych odbywa się z zachowaniem zasad określonych w Rozporządzeniu Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz.U. Nr 14, poz.67 z późn.zm.).

2/ Dokumentacja wytwarzana i gromadzona dzieli się na:

a/ materiały archiwalne – wchodzące do państwowego zasobu archiwalnego;
b/ dokumentację niearchiwalną – inną dokumentację, niestanowiącą materiałów archiwalnych.

3/ Rzeczową klasyfikację oraz kwalifikację dokumentacji ze względu na okresy jej przechowywania, wytwarzania i gromadzenia zawierają jednolite rzeczowe wykazy akt;

4/ Wykazy akt, o których mowa w pkt 3 stanowią podstawę gromadzenia dokumentacji w akta spraw.

5/ Dokumentacja niearchiwalna podlega brakowaniu po upływie okresu przechowywania określonego we właściwym wykazie akt.

6/ Brakowanie dokumentacji niearchiwalnej polega na ocenie jej przydatności do celów praktycznych, wydzieleniu dokumentacji nieprzydatnej i przekazaniu jej na makulaturę.

7/ Brakowanie dokumentacji niearchiwalnej następuje na wniosek Wójta Gminy na podstawie zgody właściwego archiwum. Do wniosku o zgodę dołącza się:

a/ protokół oceny dokumentacji niearchiwalnej;

b/ spis dokumentacji niearchiwalnej przeznaczonej do przekazania na makulaturę lub zniszczenie albo spis dokumentacji technicznej niearchiwalnej przeznaczonej na makulaturę lub zniszczenie.

8/ Protokół oraz spis dokumentacji niearchiwalnej sporządza komisja powołana przez Wójta, w której skład wchodzi: osoba prowadząca archiwum zakładowe, przedstawiciel komórki organizacyjnej, której dokumentacja niearchiwalna podlega brakowaniu oraz Pełnomocnik ochrony.

9/ W przypadku trudności w ocenie brakowanej dokumentacji niearchiwalnej można zwrócić się do miejscowego właściwego archiwum państwowego o przeprowadzenie ekspertyzy.

10/ W archiwum zakładowym Urzędu przechowuje się dokumenty brakowania wraz z dowodami przekazania nieprzydatnej dokumentacji niearchiwalnej na makulaturę bądź protokołem jej zniszczenia.

11/ Uporządkowanie materiałów archiwalnych polega na podziale rzeczowym teczek i prawidłowym ułożeniu materiałów wewnątrz teczek, ich opisaniu, nadaniu właściwego układu, sporządzeniu ewidencji oraz technicznym zabezpieczeniu.

12/ Materiały archiwalne powinny być ułożone wewnątrz teczek w kolejności spraw, a w ramach sprawy – chronologicznie, poczynając od pierwszego pisma wszczynającego sprawę. Poszczególne strony akt znajdujących się w teczce powinny być opatrzone kolejną numeracją.

13/ Akta spraw niejawnych ostatecznie załatwionych Urząd przechowuje w swoim archiwum zakładowym, po wcześniejszym zniesieniu klauzuli tajności.

14/ Przekazywanie akt odbywa się na podstawie spisu zdawczo-odbiorczego przez komórkę, w której dokument niejawny był przechowywany, pod nadzorem Pełnomocnika ochrony.

XVI. Ustalenia końcowe

1/ Pełnomocnik ochrony:

a/ zapozna pracowników Urzędu z ustalenia Planu ochrony;

b/ zapewni bieżące przestrzeganie postanowień Planu ochrony w zakresie ochrony informacji niejawnych, mogących występować na danym stanowisku pracy.

2/ Pełnomocnik ochrony wprowadza jako obowiązującą zasadę zapoznawania z Planem ochrony wszystkie osoby, które podejmują pracę w Urzędzie Gminy.

3/ W przypadku wystąpienia wątpliwości, a także potrzeby przybliżenia zasad dotyczących realizacji zadań związanych z ochroną informacji niejawnych, sporządzania i wykonania dokumentów zawierających informacje niejawne, pracownicy Urzędu mogą w każdym czasie zwracać się o wyjaśnienie czy też instruktaż do Pełnomocnika ochrony.

4/ O wszelkich nieprawidłowościach, będących następstwem naruszenia zasad określonych w Planie ochrony, każdy pracownik jest zobowiązany niezwłocznie informować o tym Pełnomocnika ochrony, który podejmie stosowne działania zmierzające do wyjaśnienia okoliczności powstałej sytuacji, informując o tym Wójta Gminy.

5/ W sprawach nieuregulowanych w Planie ochrony mają zastosowanie odpowiednie przepisy ustawy o ochronie informacji niejawnych, aktów wydanych na jej podstawie oraz odpowiednich zarządzeń Wójta Gminy.