ZARZĄDZENIE NR 127.2017

Wójta Gminy Michałowice
z dnia 14 czerwca 2017 r.

zmieniające Zarządzenie Nr 194/2012 Wójta Gminy Michałowice z dnia 1 października 2012 r. w sprawie wprowadzenia Planu Ochrony Informacji Niejawnych w Urzędzie Gminy Michałowice.

Na podstawie art. 33 ust. 3 ustawy o samorządzie gminnym z dnia 8 marca 1990 r. (Dz. U. z 2016 r., poz. 446 z późn. zm.), oraz na podstawie art. 15 ust. 1 oraz art. 43 ust. 5 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2016 r,, poz. 1167 ze zm.), postanawiam co następuje:

§1

W Zarządzeniu nr 194/2012 Wójta Gminy Michałowice z dnia 1 października 2012 r. w sprawie wprowadzenia Planu Ochrony Informacji Niejawnych w Urzędzie Gminy Michałowice załącznik nr 1 otrzymuje brzmienie załącznika do niniejszego zarządzenia.

§2

Wykonanie zarządzenia polecam Pełnomocnikowi ds. Ochrony Informacji Niejawnych.

§4

Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT GMINY MICHAŁOWICE
mgr inż. Krzysztof Grabka

PEŁNOMOCNIK
ds. Ochrony Informacji Niejawnych
Magdalena Zielińska

RADCA PRAWNY
Joanna Domańska
OI-C-851

Załącznik
do Zarządzenia Nr 127.2017
Wójta Gminy Michałowice
z dnia 14 czerwca 2017 roku

WÓJT GMINY MICHAŁOWICE
ZATWIERDZAM
mgr inż. Krzysztof Grabka
.....
WÓJT GMINY MICHAŁOWICE

Plan Ochrony
Informacji Niejawnych w Urzędzie Gminy Michałowice
2017 r.

Spis treści:

1 Podstawy prawne ochrony informacji niejawnych

- Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2016 r., poz. 1167 ze zm.);
- Rozporządzenie Rady Ministrów z dnia 07 grudnia 2011 r. w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych (Dz. U. Nr 276, poz. 1631);
- Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie wzorów zaświadczeń stwierdzających odbycie szkolenia w zakresie ochrony informacji niejawnych oraz sposobu rozliczania kosztów przeprowadzenia szkolenia przez Agencję Bezpieczeństwa Wewnętrznego lub Służbę Kontrwywiadu Wojskowego (Dz.U. Nr 258, poz. 1751);
- Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz.U. Nr 159, poz. 1948);
- Rozporządzenie Prezesa Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne (Dz.U. Nr 271, poz. 1603).
- Rozporządzenie Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności (Dz.U. Nr 288, poz. 1692);
- Rozporządzenie Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (Dz.U. z 2012 r., poz. 683);

2 Definicje używane w Planie ochrony informacji niejawnych

W rozumieniu planu ochrony informacji niejawnych:

- **Ustawą** - jest ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2016 r., poz 1167 ze zm.);
- **służba ochrony państwa** – Agencja Bezpieczeństwa Wewnętrznego (ABW);
- **rękojmią zachowania tajemnicy** – jest zdolność osoby do spełnienia ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem, stwierdzona w wyniku przeprowadzenia postępowania sprawdzającego;
- **dokumentem** – jest każda utrwalona informacja niejawna;
- **materiałem** – jest dokument lub przedmiot, lub 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;
- **przetwarzaniem informacji niejawnych** – są wszelkie operacje wykonywane w odniesieniu do informacji niejawnych i na tych informacjach, w szczególności ich wytwarzanie, modyfikowanie, kopiowanie, klasyfikowanie, gromadzenie, przechowywanie, przekazywanie lub udostępnianie;
- **systemem teleinformatycznym** – jest system teleinformatyczny w rozumieniu art. 2 pkt 3 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną;
- **kancelaria materiałów niejawnych** – wydzielone, wyodrębnione pomieszczenia przeznaczone do ewidencjonowania, opracowywania, przechowywania dokumentów niejawnych oznaczonych klauzulą „zastrzeżone";
- **Urzędem** – jest Urząd Gminy w Michałowicach;
- **Wójtem** – jest Wójt Gminy Michałowice;
- **pełnomocnikiem ochrony** – jest Pełnomocnik ds. Ochrony Informacji Niejawnych w Urzędzie Gminy w Michałowicach;
- **pracownik kancelarii materiałów niejawnych** – osoba wyznaczona przez Wójta Gminy Michałowice do prowadzenia kancelarii materiałów niejawnych.

3 Przedmiot ochrony

Przedmiotem ochrony w Urzędzie Gminy w Michałowicach są:

1. informacje niejawne oznaczone klauzulą „zastrzeżone";
2. pomieszczenia w których są przechowywane i opracowywane informacje niejawne oznaczone tą klauzulą.

4 Klasyfikacja informacji niejawnych

Informacją niejawną o klauzuli „zastrzeżone", jest informacja, której nie nadano wyższej klauzuli tajności, a jej 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.

5 Dostęp do informacji niejawnych oznaczonych klauzulą „zastrzeżone"

1. Informacje niejawne oznaczone klauzulą „zastrzeżone" mogą być udostępniane wyłącznie osobie uprawnionej do dostępu do informacji niejawnych o określonej klauzuli niejawności.
2. Uzyskanie uprawnień dostępu do informacji niejawnych o klauzuli „zastrzeżone" może nastąpić:

- po uzyskaniu przez pracownika upoważnienia dostępu do informacji niejawnych oznaczonych klauzulą „zastrzeżone", wydanego przez Wójta Gminy Michałowice,
- po przeszkoleniu danej osoby w zakresie przepisów ustawy o ochronie informacji niejawnych i uzyskaniu odpowiedniego zaświadczenia.

6 Zasady wykonywania i przetwarzania dokumentów niejawnych

1. Propozycje przyznania klauzuli niejawności na wykonywanym dokumencie przedstawia osoba sporządzająca dokument.
2. Klauzulę niejawności na danym dokumencie przyznaje osoba, która jest upoważniona do odpisania dokumentu.
3. Rękopisy sporządzanych dokumentów niejawnych powinny być opracowywane w brulionach (zeszytach pracy) uprzednio zarejestrowanych w kancelarii materiałów niejawnych.
4. Dokumenty niejawne powinny być opisane w oznaczone zgodnie z Rozporządzeniem Prezesa Rady Ministrów z dnia 13 sierpnia 2010 r. w sprawie sposobu oznaczania materiałów umieszczania na nich klauzul tajności, a także zmiany nadanej klauzuli tajności (Dz. U. Nr 159, poz. 1069). Wzór sposobu opisania dokumentu stanowi załącznik do Planu ochrony.

7 Wykonywanie dokumentów zawierających informacje niejawne za pomocą komputera

Pracownicy, którzy do opracowywania i wykonywania dokumentów zawierających informacje niejawne oznaczone klauzulą „zastrzeżone", wykorzystują urządzenia komputerowe, obowiązani są zabezpieczyć informacje podlegające ochronie przed ich nieuprawnionym ujawnieniem, a także przed dotarciem do tych informacji przez osoby, które nie powinny zapoznać się z ich treścią.

1. Bezpieczeństwo teleinformatyczne zapewnia się, chroniąc informacje przetwarzane w systemach i sieciach 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 lub sieci teleinformatycznej;

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

   1) zapewnia opracowanie dokumentacji bezpieczeństwa teleinformatycznego;

   2) realizuje ochronę fizyczną, elektromagnetyczną i kryptograficzną systemu lub Sieci teleinformatycznej;

   3) zapewnia niezawodność transmisji oraz kontrolę dostępu do urządzeń systemu lub sieci teleinformatycznej;

   4) dokonuje analizy systemu bezpieczeństwa teleinformatycznego dla osób uprawnionych do pracy w systemie lub sieci teleinformatycznej;

   5) zapewnia przeszkolenie z zakresu bezpieczeństwa teleinformatycznego dla osób uprawnionych do pracy w systemie lub Siecie teleinformatycznej;

   6) zawiadamia właściwą służbę ochrony państwa o zaistniałym incydencie bezpieczeństwa teleinformatycznego dotyczącym informacji niejawnych oznaczonych co najmniej klauzulą „poufne".

4 Ochrona fizyczna systemu lub Siecie teleinformatycznej polega na:

   1) umieszczeniu urządzeń systemu lub sieci teleinformatycznej w strefie kontrolowanego dostępu w zależności od:

   - klauzuli tajności,
   - ilości,
   - zagrożeń dla poufności, integralności lub dostępności informacji niejawnych;

   2) zastosowaniu środków zapewniających ochronę fizyczną, w szczególności przed:

      a) nieuprawnionym dostępem;

      b) podglądem;

      c) podsłuchem.

5 Ochrona elektromagnetyczna systemu lub sieci teleinformatycznej polega na niedopuszczaniu do utraty poufności i dostępności informacji niejawnych przetwarzanych w urządzeniach teleinformatycznych:

   1) utrata poufności następuje w szczególności na skutek wykorzystania elektromagnetycznej emisji ujawniającej pochodzącej z tych urządzeń;

   2) utrata dostępności następuje w szczególności na skutek zakłócania pracy urządzeń teleinformatycznych za pomocą impulsów elektromagnetycznych o dużej mocy.

6. Ochronę elektromagnetyczną systemu lub sieci teleinformatycznej zapewnia się w szczególności przez umieszczenie urządzeń teleinformatycznych, połączeń i linii w strefach kontrolowanego dostępu, spełniających wymagania w zakresie tłumienności elektromagnetycznej odpowiednio do wyników szacowania ryzyka dla informacji niejawnych lub zastosowanie odpowiednich urządzeń teleinformatycznych, połączeń i linii o obniżonym poziomie emisji lub ich ekranowanie z jednoczesnym filtrowaniem zewnętrznych linii zasilających i sygnałowych.

7. W celu zapewnienia kontroli dostępu do systemu sieci teleinformatycznej:

1. Wójt lub osoba przez niego upoważniona ustala warunki i sposób przedzielania uprawnień osobom uprawnionym do pracy w systemie lub sieci teleinformatycznej,
2. Administrator systemów określa warunki oraz sposób przydzielania tym osobom kont oraz mechanizmów kontroli dostępu, a także zapewnia ich właściwe wykorzystanie.

8. System lub sieć teleinformatyczną wyposaża się w mechanizmy kontroli dostępu odpowiednie do klauzuli tajności informacji niejawnych w nich przetwarzanych.
9. Systemy i sieci teleinformatyczne, w których mają być wytwarzane, przetwarzane, przechowywane lub przekazywane informacje niejawne, podlegają akredytacji.
10. Wójt udziela akredytacji bezpieczeństwa teleinformatycznego dla systemu teleinformatycznego przeznaczonego do przetwarzania informacji niejawnych o klauzuli „zastrzeżone", przez zatwierdzenie dokumentacji bezpieczeństwa teleinformatycznego.
11. W ciągu 30 dni od udzielenia akredytacji bezpieczeństwa teleinformatycznego, o której mowa w ust. 10, Wójt przekazuje do ABW dokumentację bezpieczeństwa systemu teleinformatycznego.
12. W ciągu 30 dni od otrzymania dokumentacji bezpieczeństwa systemu teleinformatycznego, ABW może przedstawić Wójtowi, który udzielił akredytacji bezpieczeństwa teleinformatycznego, zalecenia dotyczące konieczności przeprowadzenia dodatkowych czynności związanych z bezpieczeństwem informacji niejawnych. Wójt w terminie 30 dni od otrzymania zalecenia informuje ABW o realizacji zaleceń. W szczególnie uzasadnionych przypadkach ABW może nakazać wstrzymanie przetwarzania informacji niejawnych w systemie teleinformatycznym, posiadającym akredytację bezpieczeństwa teleinformatycznego.
13. **Dokument szczególnych wymagań bezpieczeństwa systemu teleinformatycznego** powinien zawierać w szczególności wyniki procesu szacowania ryzyka dla bezpieczeństwa informacji niejawnych przetwarzanych w systemie teleinformatycznym oraz określać przyjęte w ramach zarządzania ryzykiem sposoby osiągania i utrzymywania odpowiedniego poziomu bezpieczeństwa systemu, a także opisywać aspekty jego budowy, zasady działania, i eksploatacji, które mają związek z bezpieczeństwem systemu lub wpływają na jego bezpieczeństwo. Przebieg i wyniki proces szacowania ryzyka mogą zostać przedstawione w odrębnym dokumencie niż dokument szczególnych wymagań bezpieczeństwa.
14. Dokument szczególnych wymagań bezpieczeństwa opracowuje się na etapie projektowania, w razie potrzeby konsultuje z ABW, na bieżąco uzupełnia na etapie wdrażania i modyfikuje na etapie eksploatacji przed dokonaniem zmian w systemie teleinformatycznym.
15. **Dokument procedur bezpiecznej eksploatacji** opracowuje się na etapie wdrażania oraz modyfikuje na etapie eksploatacji przed dokonaniem zmian w systemie teleinformatycznym.
16. Podstawą dokonywania wszelkich zmian w systemie teleinformatycznym jest przeprowadzenie procesu szacowania ryzyka dla bezpieczeństwa informacji niejawnych przetwarzanych w tym systemie.

17. Wójt akceptuje wyniki procesu szacowania ryzyka dla bezpieczeństwa informacji niejawnych oraz jest odpowiedzialny za właściwą organizację bezpieczeństwa teleinformatycznego.
18. Wójt wyznacza:
    1. pracownika pełniącego funkcję **inspektora bezpieczeństwa teleinformatycznego**, odpowiedzialnego za weryfikację i bieżącą kontrolę zgodności funkcjonowania systemu teleinformatycznego ze szczególnymi wymaganiami bezpieczeństwa oraz przestrzegania procedur bezpiecznej eksploatacji;
    2. osobę niepełniącą funkcji inspektora bezpieczeństwa teleinformatycznego, odpowiedzialnego za funkcjonowanie systemu teleinformatycznego oraz za przestrzeganie zasad i wymagań bezpieczeństwa przewidzianych dla systemu teleinformatycznego, zwana **administratorem systemu**.
19. W sytuacjach wymagających konsultacji lub uzgodnień Wójt może zwrócić się do Agencji Bezpieczeństwa Wewnętrznego o wydanie opinii lub zaleceń w zakresie bezpieczeństwa teleinformatycznego.
20. Funkcje administratora systemu oraz inspektora bezpieczeństwa teleinformatycznego mogą zajmować lub pełnić osoby, posiadające poświadczenia bezpieczeństwa odpowiednie do klauzuli informacji wytwarzanych, przetwarzanych, przechowywanych lub przekazywanych w systemach lub sieciach teleinformatycznych, po odbyciu specjalistycznych szkoleń z zakresu bezpieczeństwa teleinformatycznego prowadzonych przez służby ochrony państwa.
21. Zaświadczenie o odbytym szkoleniu jest przechowywane w aktach osobowych oraz dokumentacji Pełnomocnika ochrony.

8 Ochrona fizyczna

1. Budynek i znajdujące się w nim pomieszczenia stanowiące siedzibę Urzędu podlegają ochronie. Ochrona fizyczna polega na stałym monitoringu budynku i znajdujących się w nim pomieszczeń poprzez system alarmowy.
2. Kody do instalacji alarmowej do budynku Urzędu mogą posiadać: Wójt Gminy Michałowice oraz upoważnieni pracownicy odpowiedzialni za otwieranie i zamykanie budynku Urzędu.
3. Pomieszczenia, w których znajdują się dokumenty zawierające informacje niejawne oznaczone klauzulą „zastrzeżone", po godzinach pracy są zamykane, a karty/klucze zabierane.
4. Sprzątanie pomieszczenia, w którym przechowywane są dokumenty zawierające informacje niejawne powinno odbywać się w obecności upoważnionego pracownika przed zakończeniem pracy.
5. Informacje niejawne oznaczone klauzulą „zastrzeżone" powinny być przechowywane w szafach metalowych zamykanych na klucz.
6. Szafy metalowe, w których przechowuje się dokumenty o klauzuli „zastrzeżone" po zakończeniu pracy należy zamknąć.

9 Ocena zagrożeń wewnętrznych i zewnętrznych

9.1 zagrożenia wewnętrzne

9.1.1 rodzaje zagrożeń

Zagrożeniami wewnętrznymi dla urzędu są:

- próby zaboru dokumentów lub mienia przez pracowników Urzędu;
- próby powielania, kserowania dokumentów służbowych dla celów prywatnych;
- byli pracownicy zwolnieni dyscyplinarnie;
- rozpoznanie organizacji pracy Urzędu celem łatwiejszej pracy grup przestępczych na terenie Urzędu Gminy;
- próby wglądu w dokumenty niejawne przez osoby nieuprawnione;
- spożywanie alkoholu – przesłanka do wykroczeń dyscyplinarnych i przestępstw.

9.1.2 Wnioski

W związku z przedstawionymi kierunkami zagrożeń należy wykonywać następujące czynności uprzedzające ewentualne możliwości zaistnienia zagrożeń:

- zwracanie szczególnej uwagi na osoby, które mogą być zainteresowane zaborem dokumentu;
- prowadzenie szczególnego nadzoru, by nie dokonywano prób kserowania, kopiowania bez zgody przełożonego;
- uwrażliwianie 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 jednorazowe upoważnienie wydane przez Wójta;
- wprowadzenie szczególnej uwagi, na osoby, których zachowanie wskazuje na nadmierne spożywanie alkoholu.

9.2 zagrożenia zewnętrzne

9.2.1 rodzaje zagrożeń:

Zagrożeniami zewnętrznymi dla Urzędu Gminy są:

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

9.2.2 Symptomy mogące świadczyć o przygotowaniu napadu lub włamania do budynku Urzędu:

- wzmożone zainteresowanie osób postronnych obiektem, pomieszczeniami urzędu objawiające się między innymi: podejmowaniem prób uzyskania informacji o danym

obiekcie, pomieszczeniu od pracowników podczas luźnych rozmów po „przypadkowym" spotkaniu;

- nawiązywanie 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, sposobem wykonywania przez nich obowiązków służbowych;
- obserwacja działania systemu obronnego, pracy sprzątaczek itp.;
- próby pozyskania do grup przestępczych pracowników Urzędu;
- rozpoznawanie systemu technicznych zabezpieczeń, w tym stosowanych zabezpieczeń alarmowych;
- celowe uszkadzanie urządzeń alarmowych, linii telefonicznych, oświetlenia itp.

9.2.3 Wnioski

W związku z przedstawionymi kierunkami zagrożeń należy wykonywać następujące czynności uprzedzające ewentualne możliwości zaistnienia zagrożeń:

- systematyczną, skrupulatną i wnikliwą kontrolę systemu ochrony przez osoby odpowiedzialne za jego organizację;
- pracownicy pionu ochrony w czasie dnia pracy powinni zwracać szczególną uwagę na możliwość zaistnienia ewentualnych zagrożeń;
- stosować zasadę niedopuszczania osób niepowołanych do penetracji punktu przyjęcia dokumentów niejawnych;
- wykonywanie prac porządkowych, remontowych itp. w strefie bezpieczeństwa, wyłącznie pod nadzorem osób odpowiedzialnych.

10 Postępowanie w przypadku naruszenia ustawy o ochronie informacji niejawnych i przepisów wykonawczych do ustawy

1. Za ochronę informacji niejawnych w Urzędzie odpowiada Wójt. Zadania określone ustawą o ochronie informacji niejawnych w imieniu Wójta wykonuje Pełnomocnik Ochrony Informacji Niejawnych poprzez:

- sprawowanie nadzoru nad realizacją zadań i przestrzeganiem przepisów określonych w Planie ochrony;
- sprawowanie kontroli w zakresie ochrony informacji niejawnych oraz przestrzegania związanych z upoważnieniem do dostępu do tych informacji, w odniesieniu do wszystkich komórek organizacyjnych Urzędu.

2. W przypadku ujawnienia informacji niejawnych przez podległych pracowników, Wójt lub upoważniony przez niego pracownik zawiadamia na piśmie pełnomocnika ochrony, podając jaka informacja niejawna została ujawniona lub jakie naruszenie przepisów zostało stwierdzone.
3. Pełnomocnik ochrony przeprowadza okresowe kontrole przestrzegania ustawy o ochronie informacji niejawnych w Urzędzie. W przypadku stwierdzenia naruszenia

przepisów o ochronie informacji niejawnych Pełnomocnik Ochrony Informacji Niejawnych przedkłada Wójtowi pisemną informację o naruszeniu przepisów i wnioski do podjęcia decyzji.

11 Instrukcja postępowania w przypadku otrzymania przesyłki niewiadomego pochodzenia

W przypadku otrzymania jakiejkolwiek przesyłki niewiadomego pochodzenia lub budzącej podejrzenia z jakiegokolwiek innego powodu:

- brak nadawcy;
- brak adresu nadawcy;
- przesyłka pochodzi od nadawcy lub z miejsca, z którego się nie spodziewamy;
- inne podejrzenia;

Nie należy otwierać tej przesyłki.

Należy:

1. umieścić przesyłkę w grubym plastikowym worku, szczelnie zamknąć, zakleić taśmą lub plastrem.
2. Umieścić w drugim plastikowym worku, szczelnie zamkniętym, zakleić taśmą lub plastrem.
3. Paczki nie należy przemieszczać, należy pozostawić ją na miejscu.
4. Powiadomić:

- Komendę powiatowa policji (tel. 997);
- Komendę Powiatową Państwowej Straży Pożarnej (tel. 998).

Służby te podejmą wszelkie niezbędne kroki w celu bezpiecznego przejęcia przesyłki. W przypadku gdy podejrzana przesyłka została otwarta i zawiera jakąkolwiek podejrzaną zawartość o stałej formie np. galaretę, pianę, pył lub inną, należy:

1. Nie naruszyć zawartości, nie rozsypywać, nie dotykać, nie przenosić, nie wąchać, nie powodować ruchu powietrza w pomieszczeniu (zamknąć okna, wyłączyć systemy wentylacyjne).
2. Całą zawartość umieścić w worku, zamknąć go i zakleić taśmą.
3. Dokładnie umyć ręce.
4. Zaklejony worek umieścić w drugim worku, zamknąć go i zakleić.
5. Ponownie umyć ręce.
6. Powiadomić:

- Komendę Powiatową Policji (tel. 997);
- Komendę Powiatową Państwowej Straży Pożarnej (tel. 998);
- Powiatową Stacje Sanitarno-Epidemiologiczną (tel. 22 758 75 26);
- Pogotowie Ratunkowe (tel. 999).

Po przybyciu służ należy bezwzględnie stosować się do jej zaleceń.

12 Instrukcja alarmowa w przypadku zgłoszenia o podłożeniu lub znalezieniu ładunku wybuchowego w budynku Urzędu Gminy Michałowice

12.1 Alarmowanie

1. osoba, która przyjęła zgłoszenie o podłożeniu ładunku wybuchowego albo zauważyła w obiekcie przedmiot niewiadomego pochodzenia mogący być ładunkiem wybuchowym jest obowiązania powiadomić o tym:

- Wójta;
- Komendanta Powiatowego Policji;

2. Zawiadamiając Policję należy podać treść rozmowy ze zgłaszającym o podłożeniu ładunku wybuchowego, którą należy prowadzić wg poniższych wskazówek:

- miejsce i opis zlokalizowanego przedmiotu, który może być ładunkiem wybuchowym;
- numer telefonu z którego prowadzona jest rozmowa i zajmowane stanowisko;
- uzyskać od Policji potwierdzenie przyjętego zawiadomienia.

12.2 Akcja poszukiwawcza ładunku wybuchowego

1. Do czasu przybycia Policji akcją kieruje Wójt, a w czasie jego nieobecności ... (Pełnomocnik ds. Ochrony informacji niejawnych)

2. Kierujący akcja zarządza, aby użytkownicy pomieszczeń dokonali sprawdzenia, czy w tych pomieszczeniach znajdują się:

a) przedmioty, urządzenia lub rzeczy, paczki itp., których wcześniej nie było i wnieśli ich użytkownicy pomieszczeń;

b) ślady przemieszczania elementów wyposażenia pomieszczeń;

c) zmiany w wyglądzie zewnętrznym przedmiotów, rzeczy, urządzeń, które przedtem w pomieszczeniu były oraz emitowane z nich sygnały (np. dźwięki mechanizmów zegarowych.

3. Pomieszczenia ogólnodostępne takie jak: korytarze, klatki schodowe, toalety itp. oraz najbliższe otoczenie zewnętrzne obiektu powinny być sprawdzone przez wyznaczonych do tego pracowników.

4. Zlokalizowanych przedmiotów, rzeczy, urządzeń, których w ocenie użytkowników obiektów, przedtem nie było, a zachodzi podejrzenie, że mogą to być ładunki wybuchowe nie wolno dotykać. O ich umiejscowieniu należy natychmiast powiadomić Wójta oraz Policję.

5. W przypadku gdy użytkownicy pomieszczeń faktycznie stwierdzą obecność przedmiotów (rzeczy, urządzeń), których wcześniej nie było lub zmiany w wyglądzie i usytuowaniu przedmiotów stale znajdujących się w tych pomieszczeniach, należy domniemywać, że pojawienie się tych przedmiotów oraz dotyczących ich zmian (wygląd, usytuowanie itp.) mogły nastać na skutek działania sprawcy podłożenia ładunku wybuchowego. W takiej sytuacji kierujący akcją może wydać decyzję o ewakuacji osób z zagrożonego obiektu przed przyjazdem Policji.

6. Należy zachować spokój i opanowanie, by nie dopuścić do zaistnienia paniki.

Współpraca z policją w czasie akcji

1. Po przybyciu do obiektu policjanta bądź policyjnej grupy interwencyjnej kierujący akcją powinien przekazać im wszelkie informacje dotyczące zdarzenia wskazać miejsce zlokalizowanych przedmiotów, rzeczy, urządzeń obcego pochodzenia i punkty newralgiczne w obiekcie,

2. Policjant lub Dowódca grupy interwencyjnej przejmuje kierowanie akcją, a kierujący dotychczas akcją powinien udzielić następcy bezwzględnej pomocy.

3. Na wniosek policjanta kierującego akcja Wójt podejmuje decyzje o ewakuacji użytkowników i innych osób z obiektu, o ile wcześniej ewakuacja nie miała miejsca.

4. Identyfikacja i rozpoznaniem przedmiotów, rzeczy, urządzeń obcych oraz neutralizowaniem podłożonych ładunków wybuchowych zajmują się uprawnione i wyspecjalizowane służby, z wykorzystaniem specjalistycznych środków technicznych.

5. Policjant kierujący akcją po zakończeniu działań protokolarnie przekazuje obiekt Wójtowi.

12.3 Postanowienia końcowe dotyczące działań w przypadku zgłoszenia o podłożeniu ładunku wybuchowego

1. Osobom przyjmującym zgłoszenie o podłożeniu ładunku wybuchowego oraz Wójtowi nie wolno lekceważyć żadnej informacji na ten temat. Każdorazowo osoby te powinny zawiadamiać o tym Policję.

2. Wójt powinien na bieżąco organizować szkolenia pracowników w zakresie sposobu zachowania w sytuacjach wyżej wymienionych w Planie oraz powinien znać rozmieszczenie newralgicznych punktów takich jak węzły energetyczne i wodne, które udostępnia się na żądanie funkcjonariusza Policji prowadzącego akcję.

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

Zakres odpowiedzialności karnej osób, które dopuściły się przestępstwa lub czynu zabronionego przeciwko ochronie informacji niejawnych został określony przepisami Kodeksu Karnego w art. 266 (ustawa z dnia 06 czerwca 1997 r. Kodeks Karny, Dz.U. Nr 88, poz. 553 ze zm.) i brzmi :"funkcjonariusz publiczny, który ujawnia osobie nieuprawnionej informację niejawną o klauzuli „zastrzeżone" lub „poufne" lub informację, którą uzyskał w związku z wykonywaniem czynności służbowych, a której ujawnienie może narazić na szkodę prawnie chroniony interes, podlega karze pozbawienia wolności do lat 3".

14 Okresy ochronne dla dokumentów zawierających informacje niejawne

1. Informacje niejawne podlegają ochronie do czasu zniesienia lub zmiany klauzuli tajności.

2. Zniesienie lub zmiana klauzuli tajności są możliwe wyłącznie po wyrażeniu pisemnej zgody przez osobę która nadała klauzulę tajności i jest uprawniona do podpisania dokumentu lub oznaczenia innego niż dokument materiału, albo jej przełożonego w przypadku ustania lub zmiany ustawowych przesłanek ochrony.

15 Ustalenia końcowe

1. Wójt, Pełnomocnik Ochrony, pracownicy pionu ochrony :
   1) zapoznają podległych pracowników z ustaleniami Planu Ochrony Informacji Niejawnych,
   2) zapewnią bieżące przestrzeganie postanowień Planu Ochrony w zakresie ochrony informacji niejawnych, mogących występować na poszczególnych stanowiskach pracy.
2. Osoby wymienione w pkt 1, wprowadzą jako obowiązującą zasadę, zapoznawania z Planem Ochrony wszystkie osoby, które podejmują pracę w komórkach organizacyjnych.
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 wyjaśnienia czy też instruktaż do: Pełnomocnika Ochrony bądź pracowników pionu ochrony.
4. Integralną część Planu ochrony stanowią załączniki, wyspecyfikowane w dołączonym do Planu ochrony zestawieniu załączników.

16 Zestawienie załączników do Planu ochrony Informacji Niejawnych w Urzędzie Gminy w Michałowicach

1. Wykaz stanowisk i funkcji, z którymi może się łączyć dostęp do informacji niejawnych stanowiących tajemnicę służbową.
2. Wykaz informacji niejawnych mogących występować w zakresie działania Urzędu Gminy w Michałowicach.
3. Sposób oznaczania dokumentów zawierających informacje niejawne oraz sposób umieszczania na nich klauzul tajności.
4. Wzór zaświadczenia stwierdzającego odbycie szkolenia w zakresie ochrony informacji niejawnych.
5. Wzór upoważnienia do dostępu do informacji niejawnych o klauzuli „zastrzeżone.
6. Protokół otwarcia szafy metalowej.
7. Instrukcja dotycząca sposobu i trybu przetwarzania informacji niejawnych o klauzuli „zastrzeżone".

1. Wykaz stanowisk i funkcji, z którymi może się łączyć dostęp do informacji niejawnych stanowiących tajemnicę służbową

1) Oznaczonych klauzulą „poufne"

- Pełnomocnik ds. Ochrony Informacji Niejawnych

2) Oznaczonych klauzulą „zastrzeżone"

- Wójt Gminy
- Inspektor ds. ewidencji ludności
- Podinspektor ds. działalności gospodarczej
- Podinspektor ds. obronności i OC
- Podinspektor ds. kancelaryjnych
- Kierownik Referatu Spraw Obywatelskich
- Kierownik Referatu informatyki
- Inspektor ds. informatyki

2. Wykaz informacji niejawnych mogących występować w zakresie działania Urzędu Gminy w Michałowicach

1) Plan Akcji Kurierskiej
2) Plan Stałego Dyżuru w Urzędzie Gminy Michałowice
3) Plan Operacyjny Funkcjonowania Gminy Michałowice w warunkach zewnętrznego zagrożenia bezpieczeństwa państwa i w czasie wojny.
4). Karty realizacji zadań operacyjnych – dot. obronności.
5). Inne według potrzeb i uznania Wójta Gminy Michałowice

3. Sposób oznaczania dokumentów zawierających informacje niejawne oraz sposób umieszczania na nich klauzul tajności

STRONA PIERWSZA DOKUMENTU

.....

Miejscowość, data sporządzenia dokumentu

KLAUZULA TAJNOŚCI
Egz. Nr .....

.....

Nazwa jednostki organizacyjnej

- sygnatura literowo-cyfrowa
- numer z dziennika korespondencji
  łamany przez rok lub dwie ostatnie cyfry roku

ADRESAT

/treść dokumentu/

KLAUZULA TAJNOŚCI
Nr strony / ilość stron całego dokumentu

STRONA DRUGA I KOLEJNE STRONY DOKUMENTU

KLAUZULA TAJNOŚCI
Egz. Nr .....

- sygnatura literowo-cyfrowa
- numer z dziennika korespondencji
  łamany przez rok lub dwie ostatnie cyfry roku

/ciąg dalszy treści dokumentu/

KLAUZULA TAJNOŚCI
Nr strony / ilość stron całego dokumentu

STRONA OSTATNIA DOKUMENTU

KLAUZULA TAJNOŚCI

Egz. Nr .....

- sygnatura literowo- cyfrowa
- numer z dziennika ewidencji
  łamany przez rok lub dwie ostatnie cyfry roku

/ciąg dalszy treści dokumentu/

Pod treścią - informacja o załącznikach jeśli występują

- Liczba załączników
- Klauzule tajności załączników wraz z nr ewidencyjnym
- Liczba stron lub kart każdego załącznika
- W przypadku gdy adresatowi wysyła się inna liczbę załączników niż pozostawia w aktach, dodatkowo napis „tylko adresat"
- W przypadku gdy załączniki należy zwrócić napis „do zwrotu"

.....
stanowisko oraz imię i nazwisko
osoby podpisującej dokument

- Liczba wykonanych egzemplarzy
- Adresaci poszczególnych egzemplarzy
- Nazwisko osoby, która sporządziła dokument
- Nazwisko osoby, która wykonała dokument

KLAUZULA TAJNOŚCI
Nr strony / ilość stron całego dokumentu

Załącznik
do Planu Ochrony Informacji Niejawnych
w Urzędzie Gminy Michałowice 2017 r.

PLAN
postępowania z materiałami zawierającymi informacje niejawne w razie wprowadzenia stanu nadzwyczajnego w Urzędzie Gminy Michałowice

Na podstawie art. 18 ust 1 pkt 5 ustawy z dnia 8 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2016 r., poz. 1167 ze zm.) ustala się określone w PLANIE zasady postępowania w razie konieczności zabezpieczenia materiałów niejawnych, w przypadku wprowadzenia stanu nadzwyczajnego.

Konieczność podjęcia działań zmierzających do zabezpieczenia materiałów zawierających informacje niejawne o klauzuli „ZASTRZEŻONE", może mieć miejsce w przypadkach
1. spodziewanego zagrożenia Państwa,
2. wprowadzenia stanu nadzwyczajnego,
3. wybuchu konfliktu zbrojnego mającego bezpośredni związek z Państwem Polskim,
4. zagrożeń wewnętrznych spowodowanych klęskami żywiołowymi.

1. Zabezpieczeniu podlegają wszystkie materiały zawierające informacje niejawne o klauzuli "ZASTRZEŻONE", jeśli ilość materiałów zastrzeżonych znajdujących się w kancelarii niejawnej jest niewielka.
2. W przypadku przechowywania w kancelarii niejawnej, większej ilości dokumentów o klauzuli „ZASTRZEŻONE ":
a) w pierwszej kolejności zabezpieczeniu podlegają materiały z ostatniego roku,
b) w drugiej kolejności, gdy czas i warunki na to pozwolą, pozostałe materiały niejawne.

1. Zabezpieczenia materiałów, o których mowa w niniejszym PLANIE, dokonuje się poprzez ich ewakuowanie z zagrożonych pomieszczeń.
2. Ewakuacji materiałów z zagrożonych pomieszczeń dokonywać należy, w zależności od stopnia i umiejscowienia zagrożenia:
a) korytarzami i klatką schodową prowadzącymi do głównego lub awaryjnego wyjścia z budynku Urzędu
b) przez okno przy bezwzględnym zagwarantowaniu bezpiecznego odbioru materiałów na zewnątrz budynku Urzędu.
3. Wszystkie decyzję w sprawie zabezpieczenia i ewakuacji materiałów podejmuje Wójt lub inny upoważniony przez niego pracownik.
4. W przypadkach uzasadnionych, pod nieobecność Wójta lub innego upoważnionego przez niego pracownika decyzje podejmuje Pełnomocnik kierownik komórki organizacyjnej lub jego zastępca w której przechowywane są dokumenty, podlegające zabezpieczeniu i ewakuacji.
Miejsce zabezpieczenia materiałów podlegających ewakuacji ustala Pełnomocnik Ochrony Informacji Niejawnych.

W celu wykonania zadań związanych z zabezpieczeniem materiałów będących przedmiotem

zabezpieczenia konieczne jest:
1. Wydanie stosownego polecenia pracownikowi kancelarii niejawnej w którego posiadaniu są dokumenty.
2. W przypadkach konieczności zabezpieczenia materiałów w godzinach pozasłużbowych, osoba podejmująca decyzję o konieczności zabezpieczania materiałów, zarządza ściągnięcie pracownika kancelarii niejawnej przy użyciu wszelkich dostępnych środków.
3. Zapewnienie niezbędnego środka transportu oraz pracowników w ilości niezbędnej do zapakowania i przemieszczenia materiałów wymagających zabezpieczenia.
4. Zabezpieczenia i ewakuacja materiałów niejawnych dokonać należy w obecności pracownika kancelarii niejawnej, a w przypadku jego nieobecności, zabezpieczenia materiałów dokonuje komisja wyznaczona przez osobę zarządzająca zabezpieczeniem materiałów.
5. Komisja o której mowa w § 7 pkt 4. dokonuje otwarcia kancelarii oraz w której przechowywane są dokumenty podlegające zabezpieczeniu i ewakuacji na podstawie przepisów niniejszego PLANU i realizując czynności związane z zabezpieczeniem części lub całości materiałów sporządza protokół z którego musi wynikać:
a) zasadność otwarcia kancelarii pod nieobecność osób wymienionych powyżej.
b) określenie rodzaju i ilości materiałów poddanych zabezpieczeniu i ewakuacji
c) określenie materiałów, które pozostały w ewakuowanym pomieszczeniu, a więc tych materiałów, które nie zostały objęte zabezpieczeniem.
d) określenie sposobu zabezpieczenia materiałów w nowym miejscu ich przechowywania
e) określenie sposobu zabezpieczenia materiałów, które pozostały w ewakuowanym pomieszczeniu.
6. Komisja wymieniona przystępując do otwarcia kancelarii, a więc wykonująca polecenie zarządzającego dokonania zabezpieczenia materiałów, wykorzystuje:
a) klucze do kancelarii pozostawione przez pracownika kancelarii w szafie metalowej w pomieszczeniu nr 126,

W celu umożliwienia sprawnego wykonania zawartych w PLANIE zadań związanych z zabezpieczeniem materiałów osoby wymienione w PLANIE obowiązane są:

1. Wydzielić i gromadzić materiały, które podlegałyby zabezpieczeniu w myśl postanowień niniejszego PLANU a tym samym zapewnić na bieżąco warunki do sprawnego zabezpieczenia I ewakuacji właściwych materiałów, także pod nieobecność ww. osób.
2. Oznaczyć szafę lub szafy z materiałami podlegającymi zabezpieczeniu i ewakuacji w sposób trwały i widoczny na zewnątrz tych szaf poprzez umieszczenie na nich napisu **„Ewakuacja”.**
3. Na wewnętrznej stronie drzwi szafy, w której przechowywane są materiały podlegające zabezpieczeniu umieścić informację wskazującą, z których półek i w jakiej kolejności (gdy czas byłby ograniczony) zdejmować materiały do zabezpieczenia, mając na względzie ważność i aktualność materiałów wymagających zabezpieczenia.
4. W widocznym miejscu, na zewnętrznej stronie drzwi szafy, należy oznaczyć miejsce przechowywania worków przeznaczonych do zabezpieczania i przemieszczania materiałów.
5. Worki w miarę możliwości, przechowywać należy w miejscu dostępnym i nie wymagającym korzystania z kluczy.

Realizację postanowień PLANU w zakresie:
1. przygotowania materiałów już posiadanych, do ewentualnego zabezpieczenia.
2. bieżącego gromadzenia materiałów, z myślą o wymaganiach związanych z ewentualnością ich zabezpieczenia powierza się pracownikowi kancelarii.
3. Nadzór nad realizacją postanowień PLANU sprawuje Pełnomocnik do Spraw Ochrony Informacji Niejawnych Urzędu.