ZARZĄDZENIE NR 09/21
Wójta Gminy Radziłów

z dnia 22 stycznia 2021 r.

w sprawie zatwierdzenia „ Planu ochrony informacji niejawnych w Urzędzie Gminy Radziłów"

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 Zatwierdzam „ Plan ochrony informacji niejawnych w Urzędzie Gminy Radziłów", stanowiący załącznik do niniejszego zarządzenia.

§ 2 Wykonanie zarządzenia powierzam Pełnomocnikowi do spraw ochrony informacji niejawnych.

§ 3 Traci moc Zarządzenie nr 64/09 Wójta Gminy Radziłów z dnia 25 września 2009 roku w sprawie zatwierdzenia „Planu Ochrony Informacji Niejawnych w Urzędzie Gminy Radziłów".

§ 4 Zarządzenie wchodzi w życie z dniem podpisania.

URZĄD GMINY RADZIŁÓW

Wójt Gminy Radziłów
Krzysztof Milewski

10) Rozporządzenie Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych.

§ 2. Definicje używane w Planie ochrony informacji niejawnych

1) **ustawa** - ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych;
2) **rękojmia zachowania tajemnicy** – zdolność osoby do spełnienia ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem, stwierdzona w wyniku przeprowadzenia postępowania sprawdzającego;
3) **dokument** – każda utrwalona informacja niejawna;
4) **materiał** – 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;
5) **przetwarzanie informacji niejawnych** – wszelkie operacje wykonywane w odniesieniu do informacji niejawnych i na tych informacjach, w szczególności ich wytwarzanie, modyfikowanie, kopiowanie, klasyfikowanie, gromadzenie, przechowywanie przekazywanie lub udostępnianie;
6) **system teleinformatyczny** – system teleinformatyczny w rozumieniu art. 2 pkt 3 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną;
7) **dokument szczególnych wymagań bezpieczeństwa** – systematyczny opis sposobu zarządzania bezpieczeństwem systemu teleinformatycznego;
8) **dokument procedur bezpiecznej eksploatacji systemu teleinformatycznego** – opis sposobu i trybu postępowania w sprawach związanych z bezpieczeństwem informacji niejawnych przetwarzanych w systemie teleinformatycznym oraz zakres odpowiedzialności użytkowników systemu teleinformatycznego i pracowników mających do niego dostęp;
9) **dokumentacja bezpieczeństwa systemu teleinformatycznego** – dokument szczególnych wymagań bezpieczeństwa oraz dokument procedur bezpiecznej eksploatacji systemu teleinformatycznego, opracowane zgodnie z zasadami określonymi w ustawi
10) **Urząd** - Urząd Gminy Radziłów
11) **Wójt** – Wójt Gminy Radziłów;
12) **Pełnomocnik ochrony** - Pełnomocnik do spraw ochrony niejawnych w Urzędzie Gminy w Radziłowie;
13) **ryzykiem** - jest kombinacja prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji;
14) **szacowaniem ryzyka** - jest całościowy proces analizy i oceny ryzyka;
15) **zarządzaniem ryzykiem** - są skoordynowane działania w zakresie zarządzania bezpieczeństwem informacji, z uwzględnieniem ryzyka;

16) **zatrudnieniem** - jest również odpowiednio powołanie, mianowanie lub wyznaczenie.

§ 3. 1. Na działalność Urzędu Gminy w Radziłowie mogą wpływać zagrożenia:

1) zewnętrzne,
2) wewnętrzne.

2. Zagrożeniami zewnętrznymi dla Urzędu są:

1) możliwość napadu przez zorganizowane grupy przestępcze i terrorystyczne, działające w sposób profesjonalny, przemyślany i zorganizowany,
2) możliwość napadu przez pojedynczych przestępców, możliwość napadu przez przypadkowe osoby wykorzystujące nadarzającą się okazję z powodu nieprawidłowości i ochronie mienia urzędu,
3) zagrożenia naturalne (związane z działalnością sił przyrody) i cywilizacyjne (związane z działalnością człowieka.

3. Symptomy mogące świadczyć o przygotowaniu napadu lub włamania do budynku:

1) wzmożone zainteresowanie osób postronnych obiektami, pomieszczeniami Urzędu objawiające się m. in. podejmowaniem prób uzyskania informacji o obiekt ach lub pomieszczeniach podczas rozmów z pracownikami,
2) nawiązanie rozmów przez osoby postronne z pracownikami,
3) podszywanie się pod byłych pracowników Urzędu i przejawianie zainteresowania tym, co się po latach zmieniło,
4) interesowanie się osobami funkcyjnymi, w tym także ich przywarami oraz sposobem wykonywania obowiązków służbowych,
5) obserwacja sposobu działania systemu ochronnego, sekretariatu, sprzątaczek itp., rozpoznawanie systemu technicznych zabezpieczeń, w tym stosowanych urządzeń alarmowych,
6) celowe uszkadzanie urządzeń alarmowych, linii telefonicznych, oświetlenia itp.,
7) próby uzyskania do grup przestępczych pracowników Urzędu.

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

1) systematyczną, skrupulatną i wnikliwą kontrolę systemu ochrony przez osoby odpowiedzialne za jego organizację,
2) pracownicy pionu ochrony w czasie dnia pracy powinni zwracać szczególną uwagę na możliwość zaistnienia ewentualnych zagrożeń,
3) stosować zasadę niedopuszczania osób niepowołanych do penetracji pomieszczeń w których przechowywane są informacje niejawne
4) wykonywanie prac porządkowych, remontowych itp. w strefie bezpieczeństwa wyłącznie pod nadzorem osób odpowiedzialnych,
5) wykorzystanie ostrzeżeń dotyczących zagrożeń naturalnych i cywilizacyjnych dla bu-

dynku Urzędu.

5. Zagrożeniami wewnętrznymi dla Urzędu są:

1) próby zaboru dokumentów lub mienia przez pracowników Urzędu,
2) próby powielania, kserowania dokumentów służbowych dla celów prywatnych,
3) byli pracownicy Urzędu zwolnieni dyscyplinarnie,
4) rozpoznanie organizacji pracy Urzędu celem łatwiejszej pracy grup przestępczych na terenie Urzędu,
5) próby wglądu w dokumenty niejawne przez osoby nieuprawnione,
6) spożywanie alkoholu lub używanie środków odurzających - przesłanka do wykroczeń dyscyplinarnych i przestępstw,
7) świadome lub nieświadome nieupoważnione zapoznanie się z dokumentami niejawnymi,
8) nieznajomość przepisów o ochronie informacji niejawnych,
9) bagatelizowanie przepisów o ochronie informacji niejawnych oraz potencjalnych zagrożeń.

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

1) zwracanie szczególnej uwagi na osoby, które mogą być zainteresowane zaborem dokumentu,
2) prowadzenie szczególnego nadzoru by nie dokonywano prób kserowania, kopiowania bez zgody przełożonego,
3) uwrażliwienie pracowników w trakcie prowadzonych szkoleń na możliwość prób kontaktu grup przestępczych z pracownikami, którzy mają dostęp do dokumentów szczególnie ważnych,
4) zastosowanie zasady, że do informacji niejawnych mogą mieć dostęp tylko pracownicy posiadający poświadczenie bezpieczeństwa lub właściwe upoważnienie jednorazowe wydane przez Wójta
5) staranne szkolenie osób w zakresie ochrony informacji niejawnych,
6) materiały zawierające informacje niejawne muszą być przetwarzane i wykonywane tak, aby minimalizować ryzyko ich zniszczenia na skutek wypadków losowych,
7) zwrócenie szczególnej uwagi na osoby, których zachowanie wskazuje na spożywanie alkoholu.

§ 4 Przedmiotem ochrony w Urzędzie są :

1) informacji e niejawne oznaczone klauzulą „ *zastrzeżone* ",
2) pomieszczenia, w których są przechowywane i opracowywane materiały niejawne.

§ 5 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 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.

§ 6 1. Pomieszczenie stanowiące kancelarię materiałów „Zastrzeżonych" znajduje się na pierwszym piętrze budynku UG Radziłów i wyposażone jest 1 szafę metalową – do przechowywania dokumentów niejawnych o klauzuli „Zastrzeżone".

2. Dostęp do tego pomieszczenia jest możliwy tylko z korytarza przez drzwi zamykane na dwa zamki.

3. Kody do instalacji alarmowej do budynku Urzędu mogą posiadać: Wójt, Sekretarz Gminy, kierownik USC oraz upoważnieni pracownicy odpowiedzialni za otwieranie i zamykanie budynku Urzędu.

4. Kopie kodów znajdują się w opieczętowanej kopercie w metalowej kasetce będącej pod bezpośrednim nadzorem Pełnomocnika.

5. Pomieszczenie, w którym znajdują się informacje niejawne zamykane jest na klucz. Upoważnienie do pobierania kluczy posiada Pełnomocnik. Klucz przechowywany jest w pokoju nr 7 w dyspozytorze kluczy zamykanym zamkiem szyfrowym.

6. W kancelarii funkcjonuje ewidencja wejść i wyjść. Ewidencja prowadzona jest w formie tabeli z podaniem imienia i nazwiska osoby wchodzącej, daty, godziny wejścia i wyjścia.

7. Dokumenty niejawne umieszczane są w szafie metalowej zamykanej kluczem dwupiórowym. Klucz do szafy znajduje się w miejscu niewidocznym w Kancelarii.

8. Kopie zapasowe kluczy do pomieszczenia, szafy metalowej znajdują się w opieczętowanej kopercie w metalowej kasetce pod bezpośrednim nadzorem Pełnomocnika.

9. Do Kancelarii, poza godzinami pracy Urzędu, nikt nie ma dostępu. Osoby sprzątające wykonują prace porządkowe pod nadzorem Pełnomocnika.

§ 7. 1 Informacje niejawne oznaczone klauzulą „zastrzeżone" mogą być udostępniane wyłącznie osobie uprawnionej do dostępu do informacji niejawnych o określonej klauzuli w zakresie, jaki jest niezbędny do załatwienia konkretnej sprawy i wynikającym z zakresu czynności pracownika .

2. Uzyskanie uprawnień do dostępu do informacji niejawnych o klauzuli „zastrzeżone" może nastąpić po:

1) uzyskaniu poświadczenia bezpieczeństwa upoważniające do dostępu do informacji niejawnych lub otrzymaniu pisemnego upoważnienia przez Wójta oraz
2) odbyciu szkolenia w zakresie ochrony informacji niejawnych.

3. Szkolenie w zakresie ochrony informacji w Urzędzie przeprowadza Pełnomocnik do spraw ochrony informacji niejawnych.

4. Ewidencję poświadczeń bezpieczeństwa oraz upoważnień, o których mowa w § 6 ust 2 pkt 1) prowadzi Pełnomocnik.

§ 8. 1. Dokumenty niejawne wpływające do Urzędu ewidencjonowane są w dzienniku ewidencyjnym materiałów niejawnych.

§ 9. 1. Dokumenty zawierające informacje niejawne mogą być sporządzane przez osoby załatwiające daną sprawę i posiadające wymagane uprawnienie do dostępu do informacji niejawnych.

2. Sporządzane i wykonane w Urzędzie dokumenty zawierające informacje niejawne powinny posiadać wszystkie oznaczenia wymagane rozporządzeniem Prezesa Rady Ministrów z dnia 22 grudnia 201I r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności.

3. Sporządzone i wykonane w Urzędzie dokumenty z informacjami niejawnymi podlegają obowiązkowi zarejestrowania w dzienniku ewidencji dokumentów niejawnych.

4. Dokumenty zawierające informacje niejawne powinny zostać wykonane tylko w takiej ilości egzemplarzy, jaka jest niezbędna dla załatwienia sprawy.

§ 10. Korespondencji niejawnej mylnie skierowanej nie ewidencjonuje się jako korespondencji wpływającej lecz przekazuje łącznie z poprzednim opakowaniem do nadawcy za zwrotnym potwierdzeniem odbioru.

§11.1 Propozycję przyznania klauzuli tajności na sporządzonym dokumencie przedstawia osoba sporządzająca dokument.

2. Klauzulę tajności, jaką ostatecznie ma być opatrzony dokument, przyznaje Wójt lub inna osoba upoważniona do podpisania dokumentu.

3. W przypadku ustania lub zmiany ustawowych przesłanek klauzulę tajności znosi osoba, która tę klauzulę nadała.

§ 12.1. Dokumenty niejawne mogą być wytwarzane, przetwarzane, przechowywane przy wykorzystaniu pomocy komputera.

2. Przed rozpoczęciem oraz w trakcie przetwarzania informacji niejawnych w systemie teleinformatycznym zapewnia się bezpieczeństwo teleinformatyczne.

3. Wójt w drodze odrębnego zarządzenia udziela akredytacji bezpieczeństwa teleinformatycznego dla systemu.

4. Na dokumentację bezpieczeństwa teleinformatycznego składają się:

1) dokument szczególnych wymagań bezpieczeństwa systemu teleinformacyjnego, który zawiera w szczególności wyniki szacowania ryzyka dla bezpieczeństwa informacji niejawnych oraz określa przyjęte w ramach zarządzania ryzykiem sposoby osiągania i utrzymania odpowiedniego poziomu, a także opisuje aspekty jego budowy, zasady działania i eksploatacji, które mają bezpośredni związek z bezpieczeństwem systemu lub wpływają na jego bezpieczeństwo.

2) Dokument procedur bezpiecznej eksploatacji.

5. W przypadku przetwarzania informacji niejawnych w systemie teleinformatycznym Wójta wyznacza inspektora bezpieczeństwa teleinformatycznego i administratora systemu.

6. Zatwierdzona przez Wójta dokumentacja bezpieczeństwa teleinformacyjnego przesyłana jest w ciągu 30 dni do Agencji Bezpieczeństwa Wewnętrznego.

§ 13. 1. Za ochronę informacji niejawnych w Urzędzie Gminy w Radziłowie odpowiada Wójt.

2. Zadania określone ustawą z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych w imieniu Wójta wykonuje Pełnomocnik do spraw ochrony informacji niejawnych poprzez:

1) sprawowaniem nadzoru nad przestrzeganiem przepisów zawartych w Planie ochrony;

2) sprawowanie nadzoru w zakresie ochrony informacji niejawnych oraz przestrzegania procedur związanych z upoważnieniem do dostępu do tych informacji.

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

4. Odpowiedzialność kamą osób, które dopuściły się przestępstwa lub czynu zabronionego przeciwko ochronie informacji niejawnych, określają przepisy Kodeks Karnego (ustawa z dnia 06 czerwca 1997 r. Kodeks Kamy, Dz. U. z 2020 r., poz. 1443) w art. 266:

„§ l. Kto, wbrew przepisom ustawy lub przyjętemu na siebie zobowiązaniu, ujawnia lub wykorzystuje informację, z którą zapoznał się w związku z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną, gospodarczą lub naukową, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2 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”

Załącznik do Planu ochrony:

1. Instrukcja alarmowa, w przypadku zgłoszenia o podłożeniu lub znalezieniu ładunku wybuchowego w budynkach danej jednostki.
2. Instrukcja postępowania w przypadku otrzymania przesyłki niewiadomego pochodzenia.
3. Plan postępowania z materiałami zawierającymi informacje niejawne w razie wprowadzenia stanu nadzwyczajnego w Urzędzie Gminy Radziłów.

Załącznik Nr 1

Planu ochrony informacji niejawnych w Urzędzie Gminy Radziłów"

Instrukcja alarmowa, w przypadku zgłoszenia o podłożeniu lub znalezieniu ładunku wybuchowego w Urzędzie Gminy Radziłów.

1. Alarmowanie.

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

a) Wójta lub jego zastępcę,

b) Policję.

2) Zawiadamiając policję należy podać:

a) miejsce i opis zlokalizowanego przedmiotu, który może być ładunkiem wybuchowym,

b) numer telefonu, z którego prowadzona jest rozmowa i swoje stanowisko

3) uzyskać od policji potwierdzenie przyjętego powyższego zawiadomienia.

2. Akcja poszukiwawcza ładunku wybuchowego po uzyskaniu informacji o jego podłożeniu

1) Do czasu przybycia policji akcją kieruje Wójta, a w czasie jego nieobecności osoba przez niego upoważniona.

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

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

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, świecące elementy elektroniczne, itp.).

3) Pomieszczenia ogólnodostępne takie jak: korytarze, klatki schodowe, toalety itp. oraz najbliższe otoczenia zewnętrzne obiektu powinno być sprawdzone przez pracowników.

4) Zlokalizowanych przedmiotów, rzeczy, urządzeń, których w ocenie użytkowników obiek-

tu, przedtem nie było, a zachodzi podejrzenie, iż mogą to być ładunki wybuchowe, nie wolno dotykać. O ich umiejscowieniu należy natychmiast powiadomić osobę kierującą akcją i policję.

W przypadku, gdy użytkownicy pomieszczeń faktycznie stwierdzą obecność przedmiotów (rzeczy, urządzeń), których wcześniej nie było lub zmiany w wyglądzie i usytuowaniu przedmiotów stałych znajdujących się w tych pomieszczeniach, należy domniemywać, że pojawienie się tych przedmiotów lub zmiany w ich wyglądzie i usytuowaniu mogły nastąpić na skutek działania sprawcy podłożenia ładunku wybuchowego. W takiej sytuacji kierujący akcją może wydać decyzję ewakuacji osób z zagrożonego obiektu przed przybyciem policji.

5) Należy zachować spokój i opanowanie, aby nie dopuścić do przejawów paniki.

3. Współpraca z policją w czasie akcji

1) Po przybyciu do obiektu policjanta lub policyjnej grupy interwencyjnej osoba kierująca akcją powinna przekazać im wszelkie informacje dotyczące zdarzenia oraz wskazać miejsca zlokalizowanych przedmiotów, rzeczy, urządzeń obcego pochodzenia i punkty newralgiczne w obiekcie.

2) Policjant lub dowódca grupy policjantów przejmuje kierowanie akcją, a administrator obiektu powinien udzielić mu wszechstronnej pomocy podczas jej prowadzenia.

3) Na wniosek policjanta, kierujący akcją podejmuje decyzję o ewakuacji użytkowników i innych osób z obiektu — o ile wcześniej to nic nastąpiło.

4) Identyfikacją i rozpoznaniem zlokalizowanych przedmiotów, rzeczy, urządzeń obcych oraz neutralizowaniem ewentualnie podłożonych ładunków wybuchowych zajmują się uprawnione i wyspecjalizowane ogniwa organizacyjne policji, przy wykorzystaniu specjalistycznych środków technicznych,

5) Policjant kierujący akcją, po zakończeniu działań, przekazuje protokolarnie obiekt Wójtowi lub osobie przez niego upoważnionej.

4. 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 i każdorazowo powinni powiadomić o tym

policję, która z urzędu dokona sprawdzenia wiarygodności każdego zdarzenia.

1) Wójt powinien na bieżąco organizować szkolenia pracowników w zakresie sposobu zachowania w sytuacjach wymienionej w tej części planu oraz winien znać rozmieszczenie newralgicznych punktów — węzły energetyczne i wodne, które udostępnia się na żądanie policjanta kierującego akcją.

5. Z informacjami tej części planu powinni być zapoznani wszyscy pracownicy urzędu.

Załącznik Nr 2

Planu ochrony informacji niejawnych w Urzędzie Gminy Radziłów

Instrukcja postępowania w przypadku otrzymania przesyłki niewiadomego pochodzenia.

1) 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 nie spodziewamy się,
- inne podejrzenia.

Nie należy otwierać tej przesyłki.

Należy:

- umieścić tę przesyłkę w grubym worku plastikowym, szczelnie zamknąć
- worek ten należy umieścić w drugim plastikowym worku, szczelnie zamknąć, zawiązać supeł i zakleić taśmą klejącą,
- paczki nie należy przemieszczać, należy pozostawić ją na miejscu,
- **powiadomić:**

Policję - 997 lub 112,

Straż pożarną - 998

Służby te podejmują wszystkie niezbędne kroki w celu bezpiecznego przejęcia przesyłki.

2) W przypadku, gdy podejrzana przesyłka została otwarta i zawiera jakąkolwiek podejrzaną zawartość w formie stałej (galaretę, pianę, pył lub inną).

Należy:

- **NIC NARUSZAĆ TEJ ZAWARTOŚCI** - nie rozsypywać, nic przenosić, nie dotykać, nie wąchać, nic powodować ruchu powietrza w pomieszczeniu (wyłączyć systemy wentylacyjne i klimatyzacji, zamknąć okna),
- całą zawartość umieścić w worku w worku plastikowym, zamknąć go i zakleić taśmą lub plastrem, dokładnie umyć ręce, o zaklejony worek umieścić w drugim worku, zamknąć go

i zakleić,

- ponownie umyć ręce,
- powiadomić:

Policję - 997 lub 112,

Straż pożarną - 998

Po przybyciu właściwych służb należy bezwzględnie stosować się do ich zaleceń.

Załącznik Nr3

Plan postępowania z materiałami zawierającymi informacje niejawne w razie wprowadzenia stanu nadzwyczajnego w Urzędzie Gminy Radziłów.

§ 1. Konieczność podjęcia działań zmierzających do zabezpieczenia materiałów zawierających informacje niejawne stanowiące tajemnicę państwową może mieć miejsce w przypadkach:

1) Spodziewanego zagrożenia państwa.

2) Wprowadzenia stanu nadzwyczajnego.

3) Wybuchu konfliktu zbiorowego mającego bezpośredni związek z Państwem Polskim.

4) Zagrożeniami wewnętrznymi spowodowanymi klęskami żywiołowymi.

§ 2. 1. Zabezpieczeniu podlegają wszelkie materiały zawierające informacje niejawne, jeżeli ilość materiałów znajdujących się w Kancelarii Materiałów Niejawnych jest niewielka.

2. Priorytet w zakresie zabezpieczenia dokumentów oznaczonych klauzulą „zastrzeżone" mają dokumenty dotyczące:

1) Akcji kurierskiej;

2) Planów i zestawień świadczeń osobistych i rzeczowych na rzecz obronności państwa.

3) Realizacji poszczególnych zadań operacyjnych w warunkach zewnętrznego zagrożenia bezpieczeństwa państwa i w czasie wojny.

§ 3.1. Decyzję w sprawie zabezpieczenia i ewakuacji materiałów niejawnych podejmuje Wójt Gminy Radziłów, a koordynatorem akcji jest Pełnomocnik ds. ochrony informacji niejawnych.

1. Zabezpieczenie dokumentów dokonuje się poprzez ich ewakuowanie z pomieszczeń Kancelarii Materiałów Niejawnych. Ewakuacja tych dokumentów następuje w warunkach pozwalających doprowadzić do ulokowania ich w miejscu zapewniającym wystarczające bezpieczeństwo w zaistniałej sytuacji zagrożenia, możliwie spełniając wymogi ustawy o ochronie informacji niejawnych.

§ 4 Ewakuacji materiałów z zagrożonych pomieszczeń dokonać należy w zależności od stopnia
i umiejscowienia zagrożenia:

1) korytarzami i klatką schodową do głównego lub awaryjnego wyjścia z budynku Urzę-

du;

§ 6. Urząd ewakuacją sporządza się, w miarę możliwości, w 2 egzemplarzach spis dokumentów przeznaczonych do ewakuacji, jeden egzemplarz przekazuje się kierownikowi jednostki, drugi zabiera wraz z ewakuowaną dokumentacją.

2. Wzór protokołu otwarcia szafy/biurka stanowi załącznik do Planu postępowania.

§ 7 Ewakuacja powinna obejmować:

1) zapakowanie materiałów do worków ewakuacyjnych lub skrzyń pakowych,

2) przemieszczenie worków na środek transportu,

3) przewiezienie do wyznaczonego przez kierownika jednostki miejsca ewakuacji.

§ 8 W celu wykonania zadań związanych z zabezpieczeniem materiałów będących przedmiotem zabezpieczenia, merytoryczni pracownicy - wytwórcy dokumentów niejawnych na żądanie Pełnomocnika ds. ochrony informacji niejawnych zobowiązani są do udzielenia pomocy w szczególności w zakresie:

1) zorganizowania przeniesienia zasobów z Kancelarii Materiałów Niejawnych, czy ze stanowisk pracy, na których znajdują się takie dokumenty,

2) użyczenia środków transportu,

3) organizowania stanowiska przeznaczonego do zabezpieczenia dokumentów po ewakuacji.

Załącznik do

Planu postępowania z materiałami zawierającymi informacje niejawne w razie wprowadzenia stanu nadzwyczajnego w Urzędzie Gminy Radziłów

W dniu.....

Komisja w składzie:

1. ....
(imię i nazwisko)

2.....
(imię i nazwisko)

3.....
(imię i nazwisko)

Dokonała otwarcia szafy/biurka znajdującej się w pomieszczeniu

.....
.....
(nazwa referatu, pokoju)

Którego użytkownikiem jest

.....
(imię i nazwisko - stanowisko)

Z szafy/biurka zostały zabrane następujące dokumenty (materiały, przedmioty):

1. .....

2.....

3.....

4.....

Którymi obecnie dysponuje Pan/i

.....
(imię i nazwisko - stanowisko)

Podpisy członków komisji:

1.....
(imię i nazwisko)

2.....
(imię i nazwisko)

3.....
(imię i nazwisko)