

ZARZĄDZENIE NR 9/2022
WÓJTA GMINY KUŚLIN
z dnia 14 lutego 2022 r.

w sprawie określenia procedur realizacji przedsięwzięć w ramach poszczególnych stopni alarmowych i stopni alarmowych CRP, w tym modułów zadaniowych dla każdego stopnia w Urzędzie Gminy Kuślin

Na podstawie art. 16 ust 4 ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz. U. z 2021 r. poz. 2234) w związku z § 3 i 5 rozporządzenia Prezesa Rady Ministrów z dnia 25 lipca 2016 r. w sprawie zakresu przedsięwzięć wykonywanych w poszczególnych stopniach alarmowych i stopniach alarmowych CRP (Dz. U. z 2016 r. poz. 1101 i 1106) zarządza się, co następuje:

§ 1. Wprowadza się do stosowania:

- 1) „Procedury wdrażania stopni alarmowych w Urzędzie Gminy w Kuślinie”, stanowiące załącznik nr 1 do zarządzenia;
- 2) „Procedury realizacji przedsięwzięć w ramach poszczególnych stopni alarmowych i stopni alarmowych CRP, w tym moduły zadaniowe realizowane przez Wójta Gminy Kuślin dla każdego stopnia alarmowego”, stanowiące załącznik nr 2 do zarządzenia.

§ 2. Nadzór nad wdrożeniem i prawidłowym funkcjonowaniem zarządzenia powierza się Sekretarzowi Gminy.

§ 3. Zarządzenie wchodzi z dniem podpisania.

WÓJTA GMINY
mgr Mieczysław Skrzypczak

Procedury wdrażania stopni alarmowych w Urzędzie Gminy w Kuślinie

§ 1. Stopnie alarmowe wprowadza, zmienia i odwołuje, w drodze zarządzenia, w zależności od rodzaju zagrożenia zdarzeniem o charakterze terrorystycznym, Prezes Rady Ministrów, po zasięgnięciu opinii ministra właściwego do spraw wewnętrznych i Szefa ABW, a w przypadkach niecierpiących zwłoki – minister właściwy do spraw wewnętrznych, po zasięgnięciu opinii Szefa ABW, informując o tym niezwłocznie Prezesa Rady Ministrów.

§ 2. W przypadku wprowadzenia stopnia alarmowego lub stopnia alarmowego CRP organy administracji publicznej oraz kierownicy służb i instytucji właściwych w sprawach bezpieczeństwa i zarządzania kryzysowego, wykonują przedsięwzięcia, w ramach poszczególnych stopni alarmowych i stopni alarmowych CRP, we współpracy z właścicielami, posiadaczami samoistnymi i posiadaczami zależnymi obiektów infrastruktury krytycznej w zakresie ochrony tych obiektów

§ 3. Po otrzymaniu informacji o wprowadzeniu stopnia alarmowego lub stopnia alarmowego CRP, organy administracji publicznej oraz kierownicy służb i instytucji właściwych w sprawach bezpieczeństwa i zarządzania kryzysowego niezwłocznie potwierdzają Rządowemu Centrum Bezpieczeństwa fakt otrzymania informacji o wprowadzeniu stopnia alarmowego lub stopnia alarmowego CRP oraz przekazują raport o stanie realizacji zadań wynikających z wprowadzonego stopnia, w czasie nie dłuższym niż 12 godzin od otrzymania informacji.

§ 4. 1. W przypadku zagrożenia wystąpieniem zdarzenia o charakterze terrorystycznym albo w przypadku wystąpienia takiego zdarzenia można wprowadzić jeden z czterech stopni alarmowych:

- 1) pierwszy stopień alarmowy (stopień ALFA);
- 2) drugi stopień alarmowy (stopień BRAVO);
- 3) trzeci stopień alarmowy (stopień CHARLIE);
- 4) czwarty stopień alarmowy (stopień DELTA).

2. W przypadku zagrożenia wystąpieniem zdarzenia o charakterze terrorystycznym dotyczącego systemów teleinformatycznych organów administracji publicznej lub systemów teleinformatycznych wchodzących w skład infrastruktury krytycznej albo w przypadku wystąpienia takiego zdarzenia można wprowadzić jeden z czterech stopni alarmowych CRP:

- 1) pierwszy stopień alarmowy CRP (stopień ALFA-CRP);
- 2) drugi stopień alarmowy CRP (stopień BRAVO-CRP);
- 3) trzeci stopień alarmowy CRP (stopień CHARLIE-CRP);

4) czwarty stopień alarmowy CRP (stopień DELTA-CRP).

3. Pierwszy stopień alarmowy (ALFA, ALFA-CRP) można wprowadzić w przypadku uzyskania informacji o możliwości wystąpienia zdarzenia o charakterze terrorystycznym, którego rodzaj i zakres jest trudny do przewidzenia.

4. Drugi stopień alarmowy (BRAVO, BRAVO-CRP) można wprowadzić w przypadku zaistnienia zwiększonego i przewidywalnego zagrożenia wystąpieniem zdarzenia o charakterze terrorystycznym, jednak konkretny cel ataku nie został zidentyfikowany.

5. Trzeci stopień alarmowy (CHARLIE, CHARLIE-CRP) można wprowadzić w przypadku:

1) wystąpienia zdarzenia potwierdzającego prawdopodobny cel ataku o charakterze terrorystycznym, godzącego w:

a) bezpieczeństwo lub porządek publiczny albo

b) bezpieczeństwo Rzeczypospolitej Polskiej, albo

c) bezpieczeństwo innego państwa lub organizacji międzynarodowej oraz stwarzającego potencjalne zagrożenie dla Rzeczypospolitej Polskiej lub

2) uzyskania wiarygodnych i potwierdzonych informacji o planowanym zdarzeniu o charakterze terrorystycznym na terytorium Rzeczypospolitej Polskiej lub

3) uzyskania wiarygodnych i potwierdzonych informacji o planowanym zdarzeniu o charakterze terrorystycznym, którego skutki mogą dotyczyć obywateli polskich przebywających za granicą, lub instytucji polskich albo polskiej infrastruktury mieszczących się poza granicami Rzeczypospolitej Polskiej.

6. Czwarty stopień alarmowy (DELTA, DELTA-CRP) można wprowadzić w przypadku:

1) wystąpienia zdarzenia o charakterze terrorystycznym powodującego zagrożenie:

a) bezpieczeństwa lub porządku publicznego albo

b) bezpieczeństwa Rzeczypospolitej Polskiej, albo

c) bezpieczeństwa innego państwa lub organizacji międzynarodowej oraz stwarzającego zagrożenie dla Rzeczypospolitej Polskiej lub

2) gdy uzyskane informacje wskazują na zaawansowaną fazę przygotowań do zdarzenia o charakterze terrorystycznym na terytorium Rzeczypospolitej Polskiej lub

3) gdy uzyskane informacje wskazują na zaawansowaną fazę przygotowań do zdarzenia o charakterze terrorystycznym, które ma być wymierzone w obywateli polskich przebywających za granicą lub w instytucje polskie albo polską infrastrukturę mieszczące się poza granicami Rzeczypospolitej Polskiej, a zebrane informacje wskazują jednocześnie na nieuchronność takiego zdarzenia.

7. Wyższy albo niższy stopień alarmowy i stopień alarmowy CRP mogą być wprowadzony z pominięciem stopni pośrednich.

8. Stopnie alarmowe i stopnie alarmowe CRP mogą być wprowadzane rozdzielnie lub łącznie.

9. W przypadku wprowadzenia różnych stopni alarmowych i różnych stopni alarmowych CRP należy wykonać zadania przewidziane dla stopnia wyższego.

10. Po wprowadzeniu wyższego stopnia alarmowego, wyższego stopnia alarmowego CRP należy wykonać zadania dla tego stopnia oraz zadania wymienione dla stopni niższych

11. Stopnie alarmowe i stopnie alarmowe CRP odwołuje się niezwłocznie po minimalizacji zagrożenia lub skutków zdarzenia będącego przesłanką do ich wprowadzenia.

WÓJT GMINY
mgr Mieczysław Skrzypczak

Procedury realizacji przedsięwzięć w ramach poszczególnych stopni alarmowych i stopni alarmowych CRP, w tym moduły zadaniowe realizowane przez Wójta Gminy Kuślin dla każdego stopnia alarmowego

Pierwszy stopień alarmowy – ALFA			
Numer i treść procedury	Sposób realizacji	Wykonawca	Uwagi
1. Prowadzić w ramach realizacji zadań administratorów obiektów wzmogoną kontrolę obiektów użyteczności publicznej oraz innych obiektów, które potencjalnie mogą stać się celem zdarzenia o charakterze terrorystycznym.	Przekazać pracownikom Urzędu Gminy Kuślin polecenie nakazujące wzmogoną kontrolę obiektów polegającą na: - dokonywaniu częstszych obchodów obiektów, - kontroli poprawności funkcjonowania systemów ochrony elektronicznej.	Wójt Gminy, Sekretarz Gminy.	
2. Zalecić podległemu personelowi informowanie odpowiednich służb w przypadku zauważenia nieznanych pojazdów na terenie instytucji publicznych, porzuconych paczek i bagaży lub w przypadku zauważenia jakichkolwiek innych oznak nietypowej działalności.	Polecić pracownikom urzędu bezzwłoczne informowanie o wszelkich nieznanych pojazdach oraz pozostawionych bez nadzoru bagażach ujawnionych na terenie urzędu.	Sekretarz Gminy.	
3. Poinformować podległy personel o konieczności zachowania zwiększonej czujności w stosunku do osób zachowujących się	1. Przekazać wszystkim pracownikom urzędu informację o konieczności zachowania wzmogonej czujności. 2. Uzyskać potwierdzenia odbioru wiadomości od wszystkich pracowników.	Pracownik prowadzący sprawy z zakresu zarządzania kryzysowego i obrony cywilnej.	

w sposób wzbudzający podejrzenia.	3. Przekazać informację o wykonaniu zadania Wójtowi Gminy.		
4. Zapewnić dostępność w trybie alarmowym członków personelu niezbędnych do wzmocnienia ochrony obiektów.	Utrzymanie stałego kontaktu z Posterunkiem Policji w Kuślinie oraz Komendantem OSP w Kuślinie.	Sekretarz Gminy lub osoby wyznaczone.	
5. Sprawdzić na zewnątrz i od wewnątrz budynki będące w stałym użytkowaniu pod względem podejrzanych zachowań osób oraz w poszukiwaniu podejrzanych przedmiotów.	Na bazie pracowników sprawdzić na zewnątrz i od wewnątrz obiekty urzędu w celu: - ujawnienia osób zachowujących się podejrzanie, - ujawnienia podejrzanych przedmiotów, - sprawdzenia sposobu zabezpieczenia budynków.	Osoby wyznaczone przez Sekretarza Gminy.	
6. Sprawdzić działanie środków łączności wykorzystywanych w celu zapewnienia bezpieczeństwa.	1. Dokonać sprawdzenia sposobu działania poczty e-mail, faxu, telefonów stacjonarnych. 2. Dokonać sprawdzenia poprawności funkcjonowania łączności radiotelefonicznej.	Osoby wyznaczone przez Sekretarza Gminy Pracownik prowadzący sprawy z zakresu zarządzania kryzysowego i obrony cywilnej.	
7. Dokonać, w ramach realizacji zadań administratorów obiektów sprawdzenia przepustowości dróg ewakuacyjnych.	Dokonać sprawdzenia działania przepustowości dróg ewakuacyjnych.	Pracownik ds. kadrowych i kancelaryjnych.	
8. Dokonać przeglądu wszystkich procedur rozkazów oraz zadań związanych z wprowadzeniem wyższych stopni alarmowych.	Dokonać sprawdzenia oraz w miarę potrzeb aktualizacji tabeli realizacji zadań w ramach stopni alarmowych.	Pracownik prowadzący sprawy z zakresu zarządzania kryzysowego i obrony cywilnej.	
9. Prowadzić akcję informacyjno-instruktażową dla społeczeństwa dotyczącą potencjalnego zagrożenia jego skutków i sposobu postępowania.	Informować na bieżąco pracowników o aktualnej sytuacji oraz w miarę przeprowadzanych analiz o możliwych zmianach stopnia zagrożenia.	Sekretarz Gminy, Osoby wyznaczone przez Sekretarza Gminy.	

Drugi stopień alarmowy - BRAVO			
Numer i treść procedury	Sposób realizacji	Wykonawca	Uwagi
1. Wprowadzić dodatkowe kontrole pojazdów, ludzi oraz budynków publicznych w rejonach zagrożonych.	Wydać pracownikom gospodarczym polecenie nakazujące kontrole osób wchodzących do obiektu. Na bazie wyselekcjonowanych pracowników dokonać dodatkowego sprawdzenia budynku.	Sekretarz Gminy.	
2. Wzmocnić ochronę środków komunikacji publicznej.	Przekazać informację do Kierownika Posterunku Policji w Kuślinie o konieczności wzmocnienia ochrony środków komunikacji publicznej.	Wójt Gminy.	Brak gminnych środków komunikacji publicznej
3. Sprawdzić funkcjonowanie zasilania awaryjnego.	Skontaktować się z Kierownikiem Zakładu Obsługi Komunalnej w celu sprawdzenia prawidłowości funkcjonowania zasilania awaryjnego.	Osoba wyznaczona przez Sekretarza Gminy.	
4. Ostrzec personel o możliwych formach zdarzenia o charakterze terrorystycznym.	- Przekazać wszystkim pracownikom treść informacji o konieczności zachowania wzmożonej czujności. - Uzyskać potwierdzenia odbioru wiadomości od wszystkich pracowników. - Przekazać informację o wykonaniu zadania Wójtowi Gminy.	Pracownik prowadzący sprawy z zakresu zarządzania kryzysowego i obrony cywilnej.	
5. Zapewnić dostępność w trybie alarmowym personelu wyznaczonego do wdrażania procedur działania na wypadek zdarzeń o charakterze terrorystycznym.	- Nawiązać kontakt telefoniczny z wszystkimi osobami wchodzącymi w skład GZZK. - Uprzedzić o możliwej konieczności podjęcia pracy w związku z narastającym zagrożeniem.	Pracownik prowadzący sprawy z zakresu zarządzania kryzysowego i obrony cywilnej.	
6. Sprawdzić i wzmocnić ochronę ważnych obiektów publicznych.	W przypadku stwierdzenia zwiększonego zagrożenia wytypować osoby do ochrony obiektów.	Sekretarz Gminy.	

7. Wprowadzić zakaz wstępu do przedszkola i szkół osobom postronnym.	Przekazać informację o zakazie wstępu do szkoły.	Wójt Gminy, Stanowisko pracy ds. oświaty.	
8. Wprowadzić kontrolę wszystkich przesyłek pocztowych kierowanych do urzędu lub instytucji.	Wydać polecenie kontroli wszystkich przesyłek i paczek pocztowych wpływających do urzędu i jednostek podległych i nadzorowanych.	Sekretarz Gminy.	Wyznaczyć miejsce kontroli
9. Zamknąć i zabezpieczyć nieużywane regularnie budynki i pomieszczenia.	1. Dokonać sprawdzenia budynków i pomieszczeń nieużywanych regularnie. 2. Zamknąć i zabezpieczyć budynki i pomieszczenia.	Osoby wskazane przez Sekretarza Gminy.	
10. Dokonać przeglądu zapasów materiałowych i sprzętu w tym dostępności środków i materiałów medycznych z uwzględnieniem możliwości wykorzystania w przypadku wystąpienia zdarzenia o charakterze terrorystycznym.	1. Dokonać przeglądu i w razie potrzeby dodatkowo wyposażać biuro w materiały biurowe niezbędne do zapewnienia ciągłości działania biura. 2. Dokonać sprawdzenia prawidłowości funkcjonowania zastępczych urządzeń przewidzianych do wykorzystania w przypadku awarii sprzętu podstawowego.	Osoby wskazane przez Sekretarza Gminy.	

Trzeci stopień alarmowy - CHARLIE			
Numer i treść procedury	Sposób realizacji	Wykonawca	Uwagi
1. Wprowadzić na polecenie ministra właściwego do spraw wewnętrznych, całodobowe dyżury we wskazanych urządach lub jednostkach organizacyjnych organów administracji publicznej.	Wprowadzić całodobowe dyżury.	Wójt Gminy.	Zadanie zabezpiecza GZZK. W skład całodobowych dyżurów mogą być włączeni inni pracownicy urzędu wchodzący w

				skład stałego dyżuru
2. Wprowadzić dyżury dla osób funkcyjnych odpowiedzialnych za wprowadzenie procedur działania na wypadek ataków terrorystycznych.	1. Powiadomić wyznaczone osoby o wprowadzeniu dyżurów. 2. Zapoznać wszystkich zainteresowanych z grafiką pełnienia dyżuru.	Sekretarz Gminy.		
3. Sprawdzić dostępność obiektów wyznaczonych na zastępcze miejsca czasowego pobytu na wypadek ewakuacji ludności	Zgodnie z planem ewakuacji, dokonać sprawdzenia dostępności obiektu.	Pracownik prowadzący sprawy z zakresu zarządzania kryzysowego i obrony cywilnej.		
4. Ograniczyć do minimum liczbę miejsc ogólnodostępnych w obiekcie i rejonie obiektu.	1. Ustalić liczbę miejsc do których dostęp będzie ograniczony ze względu na narastające zagrożenie. 2. Ograniczyć dostęp do tych miejsc i obiektów zgodnie z przyjętymi ustaleniami.	Wójt Gminy, Sekretarz Gminy.		
5. Wprowadzić w uzasadnionych przypadkach ścisłą kontrolę osób i pojazdów przy wejściu i wjeździe na teren obiektów.	W przypadku widocznych symptomów narastania zagrożenia należy dążyć do zorganizowania: - ścisłą kontrolę osób wchodzących na teren obiektu, - kontrolę pojazdów wjeżdżających na teren parkingów wokół urzędu, - dokonać sprawdzenia osób wnoszących na teren urzędu przedmioty o dużych gabarytach.	Osoby wskazane przez Sekretarza Gminy.		
6. Ograniczyć możliwość parkowania pojazdów przy obiektach chronionych.	Wyznaczyć pracownika w celu ograniczenia możliwości parkowania przy obiektach chronionych.	Sekretarz Gminy.		
7. Wprowadzić dodatkowy całodobowy nadzór miejsc, które tego wymagają, do tej pory nie objętych nadzorem.	1. Ustalić wykaz miejsc wymagających całodobowej ochrony. 2. Nawiązać współpracę z Posterunkiem Policji w Kuślinie oraz Komendantem OSP w Kuślinie.	Wójt Gminy, Sekretarz Gminy.		

Czwarty stopień alarmowy – DELTA			
Numer i treść procedury	Sposób realizacji	Wykonawca	Uwagi
1. Wprowadzić w uzasadnionych przypadkach, ograniczenia komunikacyjne w rejonach zagrożonych.	Wyznaczyć pracownika, którego obowiązkiem będzie kierowanie komunikacją w rejonie zagrożenia oraz wprowadzanie ograniczeń ruchu.	Sekretarz Gminy.	
2. Przeprowadzić identyfikację wszystkich pojazdów znajdujących się już w rejonie obiektu oraz, w uzasadnionych przypadkach ich relokację poza obszar obiektu.	1. Dokonać sprawdzenia wszystkich pojazdów znajdujących się w rejonie obiektu. 2. Ustalić pojazdy które zajmują od dłuższego czasu miejsce parkingowe bądź wyglądają jak porzucone. 3. Na podstawie kontaktu z Policją ustalić właściciela. 4. Zobowiązać właściciela do natychmiastowego usunięcia pojazdu bądź odholować pojazd na parking strzeżony.	Osoby wskazane przez Sekretarza Gminy.	
3. Kontrolować wszystkie pojazdy wjeżdżające na teren obiektu i ich ładunek.	1. Wyznaczyć pracownika, którego zadaniem będzie kontrolowanie wszystkich pojazdów wjeżdżających na parkingi wokół urzędu. 2. Zakazać wjazdu pojazdom wzbudzającym jakiegolwiek podejrzenia. 3. Podejmować decyzje o informowaniu Policji o podejrzanych pojazdach.	Osoby wskazane przez Sekretarza Gminy.	W razie potrzeby odpowiednio oznakować.
4. Kontrolować wszystkie wnoszone na teren obiektu walizki, torby i paczki.	1. Wydać polecenie pracownikom gospodarczym nakazujące kontrolę wszystkich torebek, paczek, plecaków itp. wnoszonych na teren obiektu. 2. Zakazać wnoszenia jakiegokolwiek zbędnych bagaży na teren urzędu. 3. Osoby przeciwwstawiające się tym zaleceniom nie wpuszczać na teren obiektu.	Osoby wskazane przez Sekretarza Gminy.	Wyznaczyć miejsce kontroli

5. Przeprowadzać częste kontrole na zewnątrz budynku i na parkingach.	Wzmocnić częstotliwość kontroli na zewnątrz obiektu ze szczególnym zwróceniem uwagi na zabezpieczenie obiektu.	Osoby wskazane przez Sekretarza Gminy.
6. Ograniczyć liczbę podróży służbowych osób zatrudnionych w obiekcie i wizyt osób niezatrudnionych w instytucji.	1. Zapoznać się z planem wyjazdu służbowych pracowników urzędu. 2. Poinformować pracowników urzędu o wstrzymaniu wszystkich wyjazdów służbowych. 3. Odwołać wszystkie wizyty osób spoza urzędu.	Sekretarz Gminy.
7. Przygotować się do zapewnienia ciągłości funkcjonowania organu w przypadku braku możliwości realizacji zadań w dotychczasowym miejscu pracy.	1. Dokonać przeglądu dokumentacji przeniesienia w zapasowe miejsce pracy. 2. Przygotować osoby funkcyjne do przeniesienia urzędu w zapasowe miejsce.	Sekretarz Gminy, Pracownik prowadzący sprawy z zakresu zarządzania kryzysowego i obrony cywilnej.

Pierwszy stopień alarmowy CRP – ALFA-CRP		
Numer i treść procedury	Sposób realizacji	Wykonawca
1. Wprowadzić wzmożone monitorowanie stanu bezpieczeństwa systemów teleinformatycznych urzędu i jednostek organizacyjnych zwanych dalej systemami w szczególności wykorzystując zalecenia szefa ABW lub komórek odpowiedzialnych za system reagowania zgodnie z właściwością oraz:	1. Przekazać Sekretarzowi Gminy informację o konieczności wzmocnienia monitorowania systemu dla stopnia ALFA CRP. 2. Przekazać Sekretarzowi Gminy informację o konieczności stałego monitoringu ruchu sieciowego pod kątem ciągłości działania i prób ataku oraz monitoringu poprawnego działania infrastruktury teleinformatycznej. 3. Przekazać osobie odpowiedzialnej za bezpieczeństwo teleinformatyczne informację o konieczności natychmiastowej weryfikacji dostępności Aktywów Informatycznych urzędu oraz stałego monitoringu ich działania. 4. Osoba odpowiedzialna za bezpieczeństwo teleinformatyczne dokonuje analizy pod kątem	Wójt Gminy, Sekretarz Gminy, osoba odpowiedzialna za bezpieczeństwo teleinformatyczne.
• monitorować i weryfikować czy nie doszło do naruszenia bezpieczeństwa komunikacji elektronicznej, • sprawdzić		

dostępność usług elektronicznych, • dokonywać, w miarę potrzeby, zmian w dostępie do systemów.	przydzielonych praw dostępowych do aktywów Systemu Informatycznego Urzędu wynikających z zawartych umów serwisowych, gwarancyjnych oraz na podstawie przydzielonych uprawnień dla właścicieli poszczególnych aplikacji. W przypadku stwierdzenia możliwości ograniczenia lub cofnięcia uprawnień celem zwiększenia bezpieczeństwa, osoba odpowiedzialna za bezpieczeństwo teleinformatyczne występuje z wnioskiem do Wójta Gminy o zgodę na cofnięcie określonych uprawnień na czas obowiązywania stopnia ALFA CRP. Po akceptacji Wójta Gminy dostęp zostaje w trybie natychmiastowym ograniczony.		
2. Poinformować personel urzędu o konieczności zachowania zwiększonej czujności w stosunku do stanów odbiegających od normy, w szczególności personel odpowiedzialny za bezpieczeństwo systemów.	Poinformować wszystkich pracowników Urzędu o wprowadzeniu stopnia ALFA CRP z potwierdzeniem przyjęcia informacji.	Sekretarz Gminy.	
3. Sprawdzić kanały łączności z innymi właściwymi dla rodzaju stopnia alarmowego CRP podmiotami biorącymi udział w reagowaniu kryzysowym, dokonać weryfikacji ustanowionych punktów kontaktowych z zespołami reagowania na incydenty bezpieczeństwa teleinformatycznego właściwymi dla rodzaju działania oraz	1. Osoba odpowiedzialna za bezpieczeństwo teleinformatyczne dokonuje: - weryfikacji poprawnego działania łączy internetowych, - poprawnego działania systemów zabezpieczających sieci (routery, Firewall-e, bramy internetowe itp.), - poprawności funkcjonowania zestawionych łączy VPN. 2. Przygotowuje raporty, które przekazuje Sekretarzowi Gminy. 3. W przypadku stwierdzenia jakiegokolwiek nieprawidłowości decyduje o naprawie zaistniałej	Osoba odpowiedzialna za bezpieczeństwo teleinformatyczne Sekretarz Gminy.	

ministrem właściwym ds. informatyzacji.	sytuacji podejmowane w gronie Wójta Gminy, Sekretarza Gminy oraz osoby odpowiedzialnej za bezpieczeństwo teleinformatyczne z udziałem Pełnomocnika Ochrony Informacji Niejawnych lub Inspektora Bezpieczeństwa Teleinformatycznego oraz pracownika prowadzącego sprawy z zakresu Zarządzania Kryzysowego i Obrony Cywilnej.		
4. Dokonać przeglądu stosownych procedur oraz zadań związanych z wprowadzeniem stopni alarmowych CRP, w szczególności dokonać weryfikacji posiadanej kopii zapasowej systemów kluczowych dla funkcjonowania urzędu i jednostek organizacyjnych oraz weryfikacji czasu wymaganego na przywrócenie poprawności funkcjonowania systemu.	1. Sekretarz Gminy zleca osobie odpowiedzialnej za bezpieczeństwo teleinformatyczne oraz wyznaczonym pracownikom urzędu w trybie natychmiastowym sporządzenie pełnego zestawienia w formie pisemnej i elektronicznej informacji o: a. posiadanych kopiach aktywów oraz formach ich wykonania (backup przyrostowy, różnicowy itp.), b. miejscami przechowywania poszczególnych kopii oraz formie ich zapisu (macierz, dyski zewnętrzne itp.), c. przewidywanym czasie niezbędnym do odtworzenia poszczególnych zasobów oraz czynności niezbędnych związanych z ich odtworzeniem (przywróceniem systemu, odtworzenie baz danych itp.), d. stanem zabezpieczenia technicznego, fizycznego i teleinformatycznego infrastruktury backupu w chwili wprowadzenia stopnia zagrożenia. 2. Po przygotowaniu zestawień, zostanie sporządzona notatka z ewentualnym uwzględnieniem i opisaniem stwierdzonych potencjalnych zagrożeń jak np. nieprawidłowość wykonania ostatniej kopii zapasowej. 3. Sekretarz Gminy wraz z osobą odpowiedzialną za bezpieczeństwo teleinformatyczne dokonują:	Sekretarz Gminy, wyznaczeni pracownicy urzędu, osoba odpowiedzialna za bezpieczeństwo teleinformatyczne.	

	a. weryfikacji zestawień informacji o kopiach zapasowych, b. uzupełnienia zestawień informacji o kopiach zapasowych o ewentualne inne zabezpieczenia wprowadzone w poszczególnych komórkach, c. określenia wytycznych związanych z koniecznością natychmiastowego sporządzenia kopii zapasowej dla wybranego zasobu informatycznego w przypadku stwierdzenia błędów w wykonaniu kopii lub jej braków. 4. Sekretarz Gminy sporządza notatkę służbową i przekazuje ją Wójtowi Gminy celem zarządzania wprowadzenia ewentualnych zmian w polityce backup-u lub innych czynności – jak próbne odtworzenia lub uzupełnienie informacji z punktu 1 o dane dotyczące kopii zapasowych.		
5. Sprawdzić aktualny stan bezpieczeństwa systemów i ocenić wpływ zagrożenia na bezpieczeństwo teleinformatyczne na podstawie bieżących informacji i prognoz wydarzeń.	Wójt Gminy zarządza spotkanie robocze z udziałem: Sekretarza Gminy (Pełnomocnika ds. Ochrony Informacji Niejawnych) ,osoby odpowiedzialnej za bezpieczeństwo teleinformatyczne oraz pracownika prowadzącego sprawy z zakresu Zarządzania Kryzysowego i Obrony Cywilnej. W ramach przeprowadzonego spotkania następuje wymiana zgromadzonych informacji w oparciu o które podejmowana jest decyzja o dalszych działaniach.	Wójt Gminy, Sekretarz Gminy.	
6. Informować na bieżąco o efektach przeprowadzanych działań zespoły reagowania na incydenty bezpieczeństwa teleinformatycznego właściwe dla rodzaju działania organizacji oraz współdziałające centra zarządzania	1. Sekretarz Gminy przekazuje na bieżąco wszelkie informacje na temat poszczególnych zasobów informatycznych związanych z wprowadzeniem stopnia zagrożenia bezpośrednio Wójtowi Gminy. 2. Wójt Gminy samodzielnie lub na wniosek Sekretarza Gminy zarządza spotkania robocze w celu pełnej i wzajemnej wymiany informacji	Wójt Gminy, Sekretarz Gminy.	

kryzysowego, a także ministra właściwego ds. informatyzacji.	połączyć wszystkimi komórkami organizacyjnymi. 3. W ramach przeprowadzanych spotkań Wójt Gminy podejmuje decyzje o przekazywaniu informacji na inne szczeble.	
--	---	--

Drugi stopień alarmowy CRP – BRAVO-CRP			
Numer i treść procedury	Sposób realizacji	Wykonawca	Uwagi
1. Zapewnić dostępność w trybie alarmowym, personelu odpowiedzialnego za bezpieczeństwo systemów.	1. Sekretarz Gminy określa dostępne zasoby kadrowe na czas wprowadzenia stopnia zagrożenia oraz pozyskuje dane umożliwiające całodobowy kontakt z wyznaczoną osobą. 2. Pozyskane informacje Sekretarz przekazuje do Wójta Gminy.	Sekretarz Gminy.	
2. Wprowadzić całodobowe dyżury administratorów systemów kluczowych dla funkcjonowania organizacji oraz personelu uprawnionego do podejmowania decyzji w sprawach bezpieczeństwa systemów teleinformatycznych.	1. Wójt Gminy w porozumieniu z Sekretarzem Gminy określa grafik dyżurów telefonicznych poza miejscem pracy. 2. Sekretarz Gminy zbiera wszelkie dane kontaktowe wszystkich osób wskazanych do pełnienia dyżuru oraz koordynuje realizację zadań. 3. Po każdorazowym incydencie Sekretarz Gminy oraz osoba odpowiedzialna za bezpieczeństwo teleinformatyczne sporządzają raport w formie notatki służbowej o zaistniałej sytuacji. 4. Sekretarz Gminy raz na dobę składa Wójtowi Gminy raport z trwającego dyżuru z podaniem osób które brały w nim udział oraz informacji o wszelkich incydentach.	Wójt Gminy, Sekretarz Gminy, osoba odpowiedzialna za bezpieczeństwo teleinformatyczne.	Zadanie zabezpiecza Administrator systemu TI. W skład całodobowych dyżurów mogą być włączeni inni pracownicy urzędu.

Trzeci stopień alarmowy CRP – CHARLI - CRP			
Numer i treść procedury	Sposób realizacji	Wykonawca	Uwagi
1. Wprowadzić całodobowe dyżury administratorów systemów kluczowych dla funkcjonowania urzędu i jednostek organizacyjnych oraz personelu uprawnionego do podejmowania decyzji w sprawach bezpieczeństwa systemów.	1. Wójt Gminy w porozumieniu z Sekretarzem Gminy określa grafik dyżurów telefonicznych poza miejscem pracy. 2. Sekretarz Gminy zbiera wszelkie dane kontaktowe wszystkich osób wskazanych do pełnienia dyżuru oraz koordynuje realizację zadań. 3. Sekretarz Gminy raz na dobę składa Wójtowi Gminy raport z trwającego dyżuru z podaniem osób które brały w nim udział oraz informacji o wszelkich incydentach.	Wójt Gminy, Sekretarz Gminy.	Zadanie Administrator systemu TI. W skład całodobowych dyżurów mogą być włączeni inni pracownicy urzędu.
2. Dokonać przeglądu dostępnych zasobów zapasowych pod względem możliwości ich wykorzystania w przypadku zaistnienia ataku.	1. Osoba odpowiedzialna za bezpieczeństwo teleinformatyczne dokonuje analizy pod kątem stworzenia środowisk zapasowych oraz koniecznych mocy obliczeniowych dla ich prawidłowego funkcjonowania. 2. Osoba odpowiedzialna za bezpieczeństwo teleinformatyczne dokonuje analizy obciążenia systemów i wolnych przestrzeni dyskowych. Dokonuje weryfikacji rozlokowania i dostępności kluczowych elementów infrastruktury sieciowej niezbędnej do prawidłowego działania aplikacji. 3. Sekretarz Gminy w oparciu o otrzymane informacje przygotowuje wspólnie z osobą odpowiedzialną za bezpieczeństwo teleinformatyczne raport o możliwości zabezpieczenia infrastruktury teleinformatycznej urzędu w oparciu o dostępne	Osoba odpowiedzialna za bezpieczeństwo teleinformatyczne, Sekretarz Gminy.	

	zasoby zapasowe. Raport przekazuje Wójtowi Gminy.		
3. Przygotować się do uruchomienia planów umożliwiających zachowanie ciągłości działania po wystąpieniu potencjalnego ataku w tym m. in.	1. Osoba odpowiedzialna za bezpieczeństwo teleinformatyczne dokonuje przeglądu istniejących procedur awaryjnych dla poszczególnych systemów informatycznych oraz elementów technicznych infrastruktury teleinformatycznej.	Osoba odpowiedzialna za bezpieczeństwo teleinformatyczne, Wójt Gminy, Sekretarz Gminy.	
•dokonać przeglądu planów awaryjnych oraz systemów.	2. W przypadku stwierdzenia braku procedur opracowuje niezbędne procedury awaryjne oraz przekazuje je Sekretarzowi Gminy.		
•przygotować się do ograniczenia operacji na serwerach w celu możliwości ich szybkiego i bezawaryjnego zamknięcia.	3. Osoba odpowiedzialna za bezpieczeństwo teleinformatyczne dokonuje analizy pod kątem niezmiennego funkcjonowania kluczowych systemów oraz możliwości ograniczenia dokonywanych operacji w systemach o mniejszym znaczeniu. Raport z analizy zostaje przekazany Wójtowi Gminy.		

Czwarty stopień alarmowy CRP – DELTA-CRP			
Numer i treść procedury	Sposób realizacji	Wykonawca	Uwagi
1. Uruchomić plany awaryjne lub plany ciągłości działania w sytuacji awarii lub utraty ciągłości działania.	1. Wójt Gminy w porozumieniu z Sekretarzem Gminy zarządza spotkanie robocze z pracownikami odpowiedzialnymi za zachowanie ciągłości pracy systemów informatycznych urzędu. 2. Pracownicy przekazują informację w zakresie posiadania procedur awaryjnych związanych z ciągłością działania nadzorowanych systemów teleinformatycznych.	Wójt Gminy, Sekretarz Gminy, osoba odpowiedzialna za bezpieczeństwo teleinformatyczne.	

	3. W przypadku stwierdzenia braków z zakresie planów ciągłości działania, w trybie natychmiastowym w opracowują niezbędne procedury. Spotkanie robocze dotyczące planów ciągłości działania zostaje opisane w formie notatki przez Sekretarza Gminy.		
2. Stosownie do sytuacji przystąpić do przywracania ciągłości działania.	1. Osoba odpowiedzialna za bezpieczeństwo teleinformatyczne podejmuje zestaw procedur odtworzeniowych w celu utrzymania ciągłości działania. 2. Osoba odpowiedzialna za bezpieczeństwo teleinformatyczne każdorazowo po wykonaniu procedury przywracania ciągłości wykonuje raport z przeprowadzonej czynności i przekazuje go Sekretarzowi Gminy.	Sekretarz Gminy, osoba odpowiedzialna za bezpieczeństwo teleinformatyczne.	

WÓJT GMINY



mgr Mieczysław Skrzyżczak