Załącznik Nr 3 do
Zarządzenia Nr 103.2020
Wójta Gminy Kozielice
z dnia 1 grudnia 2020 r.

Procedury realizacji przedsięwzięć w ramach poszczególnych stopni alarmowych CRP w tym moduły zadaniowe dla każdego stopnia z wykazem zadań do wykonania.

Pierwszy stopień alarmowy – ALFA - CRP

Treść procedury	Sposób realizacji	Wykonawca	Czas
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: - monitorować i weryfikować czy niedoszło do naruszenia bezpiecz. komunikacji elektronicznej, - sprawdzić dostępność usług elektronicznych, - dokonywać, w miarę potrzeb, zmian w dostępie do systemów.	1.Przekazać Sekretarzowi Gminy informację o konieczności wzmożenia monitorowania systemu dla stopnia ALFA - CRP. 2.Przekazać Sekretarzowi Gminy informację o konieczności stałego monitoringu ruchu sieciowego pod katem 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 katem przydzielonych praw dostępowych do aktywów Systemu Informatycznego Urzędu wynikającego z zawartych umów serwisowych, gwarancyjnych oraz na podstawie przydzielonych uprawnień dla właścicieli poszczególnych aplikacji. W przypadku stwierdzenia możliwości ograniczenia lub cofnięcia	Wójt Gminy, Sekretarz Gminy, osoba odpowiedzialna za bezpieczeństwo teleinformatyczne	Podjęcie działań w czasie do 15 minut od ogłoszenia stopnia alarmowego

	uprawnień celem zwiększenia bezpieczeństwa, osoba odpowiedzialna za bezpieczeństwo teleinformatyczne występuje z wnioskiem do Wójta Gminy o zgodę na cofniecie określonych uprawnień na czas obowiązywania stopnia ALFA - CRP. Po akceptacji Wójta Gminy dostęp zostaje w trybie natychmiastowym ograniczony.		
Poinformować pracowników Urzędu Gminy w Kozielicach o konieczności zachowania zwiększonej czujności w stosunku do stanów odbiegających od normy, w szczególności osoby odpowiedzialne za bezpieczeństwo systemów teleinformatycznych.	1.Poinformować wszystkich pracowników Urzędu Gminy w Kozielicach poprzez przekazanie wiadomości o wprowadzeniu stopnia ALFA - CRP z poświadczeniem jej odebrania.	Sekretarz Gminy	Podjęcie działań w czasie do 20 minut od ogłoszenia stopnia alarmowego
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.	1.Osoba odpowiedzialna za bezpieczeństwo teleinformatyczne dokonuje: - weryfikacji poprawnego działania łączy internetowych, - sprawdzenie działania systemów zabezpieczających sieci (routery, Firewal-e, bramy internetowe itp.), - poprawności funkcjonowania zestawionych łączy VPN. - z przeprowadzonych prób, weryfikacji przygotowuje raporty w formie notatek służbowych, które przekazuje Sekretarzowi Gminy. 2.W przypadku stwierdzenia jakichkolwiek nieprawidłowości decyzje o naprawie zaistniałej sytuacji podejmuje Wójt Gminy po konsultacji z Sekretarzem, osobą odpowiedzialną za bezpieczeństwo teleinformatyczne, Pełnomocnikiem Ochrony Informacji Niejawnych oraz pracownikiem prowadzącym sprawy z zakresu Zarządzania Kryzysowego..	Sekretarz Gminy, osoba odpowiedzialna za bezpieczeństwo teleinformatyczne	Rozpoczęcie działań w czasie do 2 godzin od ogłoszenia stopnia alarmowego
Dokonać przeglądu stosownych	1.Sekretarz Gminy zleca osobie odpowiedzialnej za		

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.	bezpieczeństwo teleinformatyczne oraz wyznaczonym pracownikom urzędu w trybie natychmiastowym sporządzenie pełnego zestawienia w formie pisemnej i elektronicznej informacji o: - posiadanych kopiach aktywów oraz formach ich wykonania (backup przyrostowy, różnicowy itp.), - miejscami przechowywania poszczególnych kopii oraz formie ich zapisu (macierz, dyski zewnętrzne itp.), - przewidywanym czasie niezbędnym do odtworzenia poszczególnych zasobów oraz czynności niezbędnych związanych z ich odtworzeniem (przywróceniem systemu, odtworzenie baz danych itp.), - stanem zabezpieczenia technicznego, fizycznego i teleinformatycznego infrastruktury backupu w chwili wprowadzenia stopnia zagrożenia. 2.Po przygotowaniu zestawień, zostanie sporządzana notatka z ewentualnym uwzględnieniem i opisaniem stwierdzonych potencjalnych zagrożeń jak np. nieprawidłowość wykonania ostatniej kopii zapasowej. Notatka przekazywana jest wraz z zestawieniem do Sekretarza Gminy. 3.Sekretarz Gminy wraz z osobą odpowiedzialną za bezpieczeństwo teleinformatyczne dokonują: - weryfikacji zestawień informacji o kopiach zapasowych, - uzupełnienia zestawień informacji o kopiach zapasowych o ewentualne inne zabezpieczenia wprowadzone w poszczególnych komórkach, - określenia wytycznych związanych z koniecznością natychmiastowego sporządzenia kopii zapasowej dla wybranego zasobu informatycznego w przypadku stwierdzenia błędów w wykonaniu kopii	Sekretarz Gminy, wyznaczeni pracownicy urzędu, osoba odpowiedzialna za bezpieczeństwo teleinformatyczne	Podjęcie działań w czasie do 60 minut od ogłoszenia stopnia alarmowego

	lub jej braków. 4.Sekretarz Gminy sporządza notatkę służbową i przekazuje ją Wójtowi Gminy celem zarządzenia wprowadzenia ewentualnych zmian w polityce backup-u lub innych czynności takich jak próbne odtworzenie lub uzupełnienie informacji z pkt-u 1 o dane dotyczące kopii zapasowych.		
Sprawdzić aktualny stan bezpieczeństwa systemów i ocenić wpływ zagrożenia na bezpieczeństwo teleinformatyczne na podstawie bieżących informacji i prognoz wydarzeń.	1.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. 2.Wramach przeprowadzonego spotkania następuje wymiana zgromadzonych informacji w oparciu o które podejmowana jest decyzja o dalszych działaniach. Sekretarz Gminy sporządza notatkę z ustaleń, którą podpisują osoby uczestniczące w spotkaniu.	Wójt Gminy, Sekretarz Gminy	Podjęcie działań w czasie do 2 godzin od ogłoszenia stopnia alarmowego
Informować na bieżąco o efektach przeprowadzanych działań zespoły reagowania na incydenty bezpieczeństwa teleinformatycznego właściwe dla rodzaju działania organizacji oraz współdziałające centra zarządzania kryzysowego.	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 pomiędzy wszystkimi jednostkami organizacyjnymi. 3.W ramach przeprowadzanych spotkań Wójt Gminy podejmuje decyzje o przekazywaniu informacji na inne szczeble (powiatowy, wojewódzki).	Wójt Gminy, Sekretarz Gminy	Podjęcie działań w czasie do 5 godzin od ogłoszenia stopnia alarmowego

Drugi stopień alarmowy – BRAVO - CRP

Treść procedury	Sposób realizacji	Wykonawca	Czas
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	Do 3godz.od ogłoszenia stopnia alarmowego
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 Sekretarz Gminy określa grafik dyżurów telefonicznych poza miejscem pracy. 2.Sekretarz Gminy zbiera wszelkie dane kontaktowe wszystkich osób wskazanych do pełnienia dyżuru oraz koordynuje realizacje zadań. 3.Po każdorazowym incydencie Sekretarz Gminy oraz osoba odpowiedzialna za bezpieczeństwo teleinformatyczne sporządzają raport w formie notatki służbowej o zaistniałej sytuacji. 4.Sekretarz 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	Do 4godz.od ogłoszenia stopnia alarmowego

Trzeci stopień alarmowy – CHARLI - CRP

Treść procedury	Sposób realizacji	Wykonawca	Czas
Wprowadzić całodobowe dyżury administratorów systemów kluczowych dla funkcjonowania urzędu i jednostek organizacyjnych oraz personelu uprawnionego do podejmowania decyzji w sprawach bezpieczeństwa systemów teleinformatycznych.	1.Wójt Gminy w porozumieniu z Sekretarzem określa grafik dyżurów telefonicznych poza miejscem pracy. 2.Sekretarz zbiera wszelkie dane kontaktowe wszystkich osób wskazanych do pełnienia dyżuru oraz koordynuje realizacje zadań. 3.Sekretarz 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	Do 4godz.od ogłoszenia stopnia alarmowego
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. Z przeprowadzonych czynności sporządza notatki, które przekazuje Sekretarzowi Gminy. 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. Z przeprowadzonych czynności sporządza notatki, które przekazuje Sekretarzowi Gminy. 3.Sekretarz w oparciu o otrzymane notatki przygotowuje wspólnie z osobą odpowiedzialna za bezpieczeństwo teleinformatyczne raport o	Sekretarz Gminy, osoba odpowiedzialna za bezpieczeństwo teleinformatyczne	Do 4godz.od ogłoszenia stopnia alarmowego

	możliwości zabezpieczenia infrastruktury teleinformatycznej urzędu w oparciu o dostępne zasoby zapasowe. Raport przekazuje Wójtowi Gminy.		
Przygotować się do uruchomienia planów umożliwiających zachowanie ciągłości działania po wystąpieniu potencjalnego ataku w tym; - dokonać przeglądu planów awaryjnych oraz systemów, - przygotować się do ograniczenia operacji na serwerach w celu możliwości ich szybkiego i bezawaryjnego zamknięcia.	1.Osoba odpowiedzialna za bezpieczeństwo teleinformatyczne dokonuje przeglądu istniejących procedur awaryjnych dla poszczególnych systemów informatycznych oraz elementów technicznych infrastruktury teleinformatycznej. 2.W przypadku stwierdzenia braku procedur opracowuje niezbędne procedury awaryjne oraz przekazuje je Sekretarzowi Gminy. 3.Osoba odpowiedzialna za bezpieczeństwo teleinformatyczne dokonuje analizy pod kątem niezmiennego funkcjonowania kluczowych systemów oraz możliwości ograniczenia dokonywanych operacji w systemach o mniejszym znaczeniu. Wyniki analizy zostają zawarte w formie raportu, który zostaje przekazany Wójtowi Gminy.	Sekretarz Gminy, osoba odpowiedzialna za bezpieczeństwo teleinformatyczne	Podjęcie działań w czasie do 15 minut od ogłoszenia stopnia alarmowego

Czwarty stopień alarmowy – DELTA - CRP

Treść procedury	Sposób realizacji	Wykonawca	Czas
Uruchomić plany awaryjne lub plany ciągłości działania w sytuacji awarii lub utraty ciągłości działania.	1.Wójt Gminy w porozumieniu z Sekretarzem 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	Podjęcie działań w czasie do 30 minut od ogłoszenia stopnia alarmowego

	3.Wprzypadku stwierdzenia braków z zakresu planów ciągłości działania, pracownicy w trybie natychmiastowym uzupełniają niezbędne procedury. Spotkanie robocze dotyczące planów ciągłości działania zostaje opisane w formie notatki przez Sekretarza Gminy.		
Stosownie do sytuacji przystąpić do przywracania ciągłości działania.	1.Osoba odpowiedzialna za bezpieczeństwo teleinformatyczne podejmuje zestawy 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	Podjęcie działań w czasie do 2 godz. od ogłoszenia stopnia alarmowego