Załącznik nr 1
Do Zarządzenia Nr 208 / 2020
Burmistrza Biskupca
z dnia **26 czerwca 2020 roku**

Po wprowadzeniu drugiego stopnia alarmowego CRP (stopień BRAVO – CRP) należy wykonać zadania wymienione dla pierwszego stopnia alarmowego CRP oraz kontynuować lub sprawdzić wykonanie tych zadań, jeśli wcześniej był wprowadzony stopień ALFA – CRP.

I. Przedsięwzięcia realizowane w ramach II stopnia BRAVO – CRP:

1) Zapewnić gotowość do niezwłocznego podejmowania działań przez administratorów systemów kluczowych dla funkcjonowania organizacji;
2) Wprowadzić dyżury w trybie alarmowym osób uprawnionych do podejmowania decyzji w sprawach bezpieczeństwa systemów teleinformatycznych;
3) Wprowadzić wzmożone monitorowanie stanu bezpieczeństwa systemów teleinformatycznych, w tym w szczególności wykorzystując zalecenia Szefa Agencji Bezpieczeństwa Wewnętrznego lub komórek odpowiedzialnych za system reagowania, zgodnie z właściwością oraz:
   a) Monitorować i weryfikować, czy nie doszło do naruszenia bezpieczeństwa komunikacji elektronicznej;
   b) Sprawdzać dostępność usług elektronicznych;
   c) W razie potrzeby dokonywać zmian w dostępie do infrastruktury teleinformatycznej.

II. Przedsięwzięcia realizowane w ramach I stopnia alarmowego CRP – ALFA CRP

1. Poinformowanie personelu instytucji, w szczególności odpowiedzialnych za bezpieczeństwo systemów teleinformatycznych, o konieczności zachowania zwiększonej czujności w stosunku do stanów odbiegających od normy;
2. Zapewnienie dostępu w trybie alarmowym personelu odpowiedzialnego za bezpieczeństwo systemów teleinformatycznych;
3. Sprawdzenie kanałów łączności z innymi podmiotami biorącymi udział w reagowaniu kryzysowym właściwymi dla rodzaju stopnia alarmowego CRP, zespołami reagowania na incydenty bezpieczeństwa teleinformatycznego właściwymi dla rodzaju działania organizacji oraz ministrem właściwym do spraw informatyzacji;
4. Dokonanie przeglądu stosownych procedur oraz zadań związanych z wprowadzeniem stopni alarmowych CRP;
5. Sprawdzenie aktualnego stanu bezpieczeństwa infrastruktury teleinformatycznej i ocenić wpływ zagrożenia na bezpieczeństwo teleinformatyczne na podstawie bieżących informacji i prognoz wydarzeń;
6. Informowanie na bieżąco o efektach przeprowadzanych działań zespoły reagowania na incydenty bezpieczeństwa teleinformatycznego właściwe dla rodzaju działania organizacji oraz współdziałające centra zarządzania kryzysowego, a także ministra właściwego do spraw informatyzacji.