ZARZĄDZENIE NR 724/2023
BURMISTRZA SĘPOPOLA
z dnia 4 września 2023 roku

w sprawie wprowadzenia (przedłużenia) stopnia alarmowego CRP (3. stopień CHARLIE-CRP)

Na podstawie Zarządzenia nr 364 Prezesa Rady Ministrów z dnia 31 sierpnia 2023 roku w sprawie wprowadzenia stopnia alarmowego CRP (3. stopień CHARLIE-CRP) oraz na podstawie art. 16 ust. 1 pkt 1 ustawy z dnia 10 czerwca 2016 roku o działaniach antyterrorystycznych (Dz. U. z 2022 roku, poz. 2632 oraz z 2023 r., poz. 1489) **zarządza się, co następuje:**

§ 1

W związku z wprowadzeniem trzeciego stopnia alarmowego CRP (stopień CHARLIE-CRP), obowiązującego od dnia 1 września 2023 r., od godziny 00:00, do dnia 30 listopada 2023 r., do godziny 23:59 poleca się:

Naczelnikom Wydziałów, Dyrektorom, kierownikom jednostek organizacyjnych gminy:

1. poinformować personel instytucji o konieczności zachowania zwiększonej czujności w stosunku do stanów odbiegających od normy, w szczególności personelu odpowiedzialnego za bezpieczeństwo systemów teleinformatycznych;
2. poinformować podległy personel o konieczności zachowania zwiększonej czujności w stosunku do osób zachowujących się w sposób wzbudzający podejrzenia.

Osobie będącej na stanowisku ds. zarządzania kryzysowego:

1. dokonać przeglądu wszystkich procedur, rozkazów oraz zadań związanych z wprowadzeniem stopni alarmowych CRP;
2. informować na bieżąco o efektach przeprowadzanych działań zespołów reagowania na incydenty bezpieczeństwa teleinformatycznego właściwych dla rodzaju działania organizacji oraz współdziałających centrów zarządzania kryzysowego, a także ministra właściwego ds. informatyzacji.

Informatykowi:

1. dokonać przeglądu dostępnych zasobów pod względem możliwości ich wykorzystania w przypadku ataku;
2. przygotować się do uruchomienia planów umożliwiających zachowanie ciągłości działania po wystąpieniu potencjalnego ataku., w tym szybkiego i bezawaryjnego zamknięcia serwerów;
3. sprawdzić aktualny stan bezpieczeństwa systemów;
4. informować na bieżąco o efektach przeprowadzonych działań zespoły reagowania na incydenty bezpieczeństwa;
5. dokonać przeglądu i ewentualnego audytu planów awaryjnych oraz systemów;
6. przygotować się do graniczenia operacji na serwerach.