ZARZĄDZENIE NR 167/2019
BURMISTRZA ALEKSANDROWA ŁÓDZKIEGO
z dnia 28 sierpnia 2019r.

w sprawie wprowadzenia pierwszego stopnia alarmowego (stopień ALFA) oraz pierwszego stopnia alarmowego CRP (stopień ALFA-CRP) na terenie gminy Aleksandrów Łódzki obowiązujący od dnia 28 sierpnia 2019 r od godz. 00.01 do dnia 03 września 2019 r. do godz. 23.59.

Na podstawie art. 16 ust. 1 ustawy z dnia 10 czerwca 2016r. o działaniach antyterrorystycznych (Dz. U. z 2019r. poz. 796) w związku z Zarządzeniem nr 141 z dnia 27 sierpnia 2019r. Prezesa Rady Ministrów w sprawie wprowadzenia pierwszego stopnia alarmowego ALFA (stopień ALFA) oraz pierwszego stopnia alarmowego CRP (stopień ALFA-CRP) na całym terytorium RP obowiązujący od dnia 28 sierpnia 2019 r od godz. 00.01 do dnia 03 września 2019 r. do godz. 23.59., zarządza się co następuje:

§1

W związku z wprowadzeniem przez Prezesa Rady Ministrów od dnia 28 sierpnia 2019 r od godz. 00.01 do dnia 03 września 2019 r. do godz. 23.59., pierwszego stopnia alarmowego ALFA (stopień ALFA) oraz pierwszego stopnia alarmowego CRP (stopień ALFA-CRP), zarządzam wprowadzenie na terenie gminy Aleksandrów Łódzki pierwszego stopnia alarmowego ALFA (stopień ALFA) oraz pierwszego stopnia alarmowego CRP (stopień ALFA-CRP) oraz polecam wykonanie zadań określonych w rozporządzeniu Prezesa Rady Ministrów z dnia 25 lipca 2016r. w sprawie zakresu przedsięwzięć wykonywanych w poszczególnych stopniach alarmowych i stopniach alarmowych CRP (Dz. U. z 2016r., poz. 1101), w tym w szczególności:

1. Pracownicy Urzędu są zobowiązani do informowania Wydziału Obsługi Informatycznej o wszelkich nieprawidłowościach w funkcjonowaniu użytkowanych systemów teleinformatycznych oraz do zachowania szczególnej czujności w stosunku do osób zachowujących się w sposób podejrzany jak również do informowania odpowiednich służb w przypadku zauważenia porzuconych paczek, bagaży etc.
2. Wydział Obsługi Informatycznej jest zobowiązany do:
   a) Zachowania zwiększonej czujności w stosunku do stanów odbiegających od normy w zakresie bezpieczeństwa systemów teleinformatycznych,
   b) Bieżącego sprawdzania kanałów łączności z innymi podmiotami biorącymi udział w reagowaniu kryzysowym właściwymi dla stopnia CRP, zespołami reagowania na incydenty bezpieczeństwa teleinformatycznego właściwymi dla działaniami Urzędu oraz ministrem właściwym do spraw informatyzacji,
   c) Dokonania przeglądu procedur oraz zadań związanych z wprowadzeniem stopni alarmowych CRP i bezpieczeństwa teleinformatycznego obowiązujących w Urzędzie,
   d) Bieżącego sprawdzania aktualnego stanu bezpieczeństwa infrastruktury teleinformatycznej i oceniania wpływu zagrożenia na bezpieczeństwo teleinformatyczne na podstawie bieżących informacji i prognoz wydarzeń,
   e) Wykonywania, co najmniej raz dziennie w każdy dzień roboczy:
      - przeglądu logów zapory ogniowej,
      - przeglądu logów programu antywirusowego w tym stanu aktualizacji stacji roboczych oraz aktualności sygnatur baz wirusów,

- sprawdzenia czy nie ma obcych urządzeń podłączonych do sieci na poziomie serwera DHCP lub za pomocą dedykowanej aplikacji, sprawdzenie czy serwerownia oraz inne pomieszczenia, w których przechowywane są kluczowe elementy infrastruktury informatycznej nie noszą znamion ingerencji osoby niepowołanej,
- przeglądu informacji dotyczących bezpieczeństwa uzyskanych z systemu monitorowania sieci,
- przeglądu informacji dotyczących bezpieczeństwa z programu do audytu usług katalogowych,
- sprawdzenia aktualności wersji systemów operacyjnych serwerów w szczególności w zakresie poprawek krytycznych dotyczących bezpieczeństwa i w razie potrzeby dokonanie jego aktualizacji

f) zapewnienia gotowości do niezwłocznego podejmowania działań przez administratorów systemów kluczowych dla funkcjonowania Urzędu, w tym systemów dla których Urząd Miejski jest administratorem danych,
g) prowadzenie wzmożonego monitorowania stanu bezpieczeństwa systemów teleinformatycznych, w tym w szczególności wykorzystywania zaleceń Szefa Agencji Bezpieczeństwa Wewnętrznego lub komórek odpowiedzialnych za system reagowania, zgodnie z właściwością oraz:
   - monitorowania i weryfikowania, czy nie doszło do naruszenia bezpieczeństwa komunikacji elektronicznej,
   - sprawdzania dostępności usług elektronicznych,
   - w razie potrzeby dokonywania zmian w dostępie do infrastruktury teleinformatycznej,

h) bieżącego sprawdzania działania środków łączności wykorzystywanych w celu zapewnienia bezpieczeństwa;

3. Naczelnik Wydziału Obsługi Informatycznej:
   a) Zapewnia wykonanie działań wskazanych w pkt 2,
   b) Zapewnia dostępność w trybie alarmowym pracowników Wydziału Obsługi Informatycznej odpowiedzialnych za bezpieczeństwo systemów teleinformatycznych,
   c) Na bieżąco informuje Miejski Zespół Zarządzania Kryzysowego Urzędu Miejskiego w Aleksandrowie Łódzkim o efektach przeprowadzonych działań oraz za pośrednictwem Miejskiego Zespołu Zarządzania Kryzysowego Urzędu Miejskiego zespoły reagowania na incydenty bezpieczeństwa teleinformatycznego właściwe dla rodzaju działalności Urzędu oraz współdziałające centra zarzadzania kryzysowego.

§ 2

Zarządzenie wchodzi w życie z dniem podpisania.