

KOMUNIKAT REKTORA POWIŚLAŃSKIEJ SZKOŁY WYŻSZEJ

z dnia 30 kwietnia 2022 r.

Szanowni Państwo,

uprzejmie informuję, iż wykonując postanowienia Zarządzenia nr 87 z dnia 15 kwietnia 2022 roku Prezesa Rady Ministrów na podstawie art. 16 ust. 1 ustawy z dnia 10 czerwca 2016 roku o działaniach antyterrorystycznych (Dz. U. z 2021 r. poz. 2234) w sprawie wprowadzenia Zarządzenia nr 107 z dnia 29 kwietnia 2022 roku w sprawie wprowadzenia drugiego stopnia alarmowego (2. stopień BRAVO) na całym terytorium Rzeczypospolitej Polskiej oraz Zarządzenia nr 108 z dnia 29 kwietnia 2022 roku w sprawie wprowadzenia trzeciego stopnia alarmowego CRP (3. stopień CHARLIE-CRP), obowiązującego od dnia 1 maja 2022 r. od godz. 00.00 do dnia 15 maja 2022 r. do godz. 23.59, należy postąpić jak poniżej.

W związku z:

Ogłoszeniem trzeciego stopnia alarmowego CRP (stopień CHARLIE-CRP) wskazuje się w szczególności na konieczność wykonania wszystkich zadań wymienionych dla pierwszego stopnia alarmowego (ALFA-CRP) oraz drugiego stopnia alarmowego (BRAVO-CRP), oraz jak poniżej:

1. zapewnienia dostępności w trybie alarmowym personelu odpowiedzialnego za bezpieczeństwo systemów;
2. wprowadzenia całodobowych dyżurów administratorów systemów kluczowych dla funkcjonowania organizacji oraz personelu uprawnionego do podejmowania decyzji w sprawach bezpieczeństwa systemów teleinformatycznych;
3. przeglądu zapasów materiałowych i sprzętu, w tym dostępności środków i materiałów medycznych, z uwzględnieniem możliwości wykorzystania w przypadku wystąpienia zdarzenia o charakterze terrorystycznym.

Po wprowadzeniu trzeciego stopnia alarmowego CRP (stopień CHARLIE-CRP) należy wykonać zadania wymienione dla pierwszego i drugiego stopnia alarmowego CRP oraz kontynuować lub sprawdzić wykonanie tych zadań.

Oznacza to konieczność:

- 1) wprowadzić dyżury całodobowe dla osób funkcyjnych odpowiedzialnych za uruchomienie procedur działania na wypadek zdarzeń o charakterze terrorystycznym;
- 2) prowadzić, w uzasadnionych przypadkach, szczegółowe kontrole osób wchodzących na teren uczelni, z jednoczesnym ograniczeniem osób w obrębie instytucji do niezbędnego minimum;
- 3) zakazać parkowania pojazdów przy wejściu do budynku Uczelni;
- 4) ograniczyć do minimum ilość miejsc ogólnodostępnych w obiektach administracyjnych przez uczelnię oraz w jej rejonie;
- 5) wzmocnić częstotliwość patrolowania obiektu Uczelni;
- 6) zapewnić ochronę środków transportu służbowego poza terenem uczelni, sprawdzać pojazd przed zajęciem w ni miejsca i uruchomieniem silnika.

Ogłoszenie pierwszego stopnia alarmowego CRP (stopień ALFA-CRP) wskazuje w szczególności na konieczność:

1. zapewnienia dostępności w trybie alarmowym personelu odpowiedzialnego za bezpieczeństwo systemów;
2. wprowadzenia całodobowych dyżurów administratorów systemów kluczowych dla funkcjonowania organizacji oraz personelu uprawnionego do podejmowania decyzji w sprawach bezpieczeństwa systemów teleinformatycznych;
3. przeglądu zapasów materiałowych i sprzętu, w tym dostępności środków i materiałów medycznych, z uwzględnieniem możliwości wykorzystania w przypadku wystąpienia zdarzenia o charakterze terrorystycznym.

Po wprowadzeniu drugiego stopnia alarmowego CRP (stopień ALFA-CRP) należy wykonać zadania wymienione dla pierwszego stopnia alarmowego CRP oraz kontynuować lub sprawdzić wykonanie tych zadań.

Oznacza to konieczność:

- 1) prowadzenia wzmożonej kontroli dużych skupisk ludności, które potencjalnie mogą stać się celem zdarzenia o charakterze terrorystycznym, w tym imprez masowych i zgromadzeń publicznych;
- 2) prowadzenia, w ramach realizacji zadań administratorów obiektów, wzmożonej kontroli obiektów użyteczności publicznej oraz innych obiektów, które potencjalnie mogą stać się

celem zdarzenia o charakterze terrorystycznym;

- 3) zalecenia podległemu personelowi informowanie odpowiednich służb w przypadku zauważenia: nieznanymi pojazdami na terenie instytucji publicznych lub innych ważnych obiektów, porzuconych paczek i bagaży lub jakichkolwiek innych oznak nietypowej działalności;
- 4) poinformowania podległy personel o konieczności zachowania zwiększonej czujności w stosunku do osób zachowujących się w sposób wzbudzający podejrzenia;
- 5) zapewnienia dostępności w trybie alarmowym członków personelu niezbędnych do wzmocnienia ochrony obiektów;
- 6) przeprowadzenia kontroli pojazdów wjeżdżających oraz osób wchodzących na teren obiektów;
- 7) sprawdzania, na zewnątrz i od wewnątrz, budynków będących w stałym użyciu w zakresie podejrzanych zachowań osób oraz w poszukiwaniu podejrzanych przedmiotów;
- 8) sprawdzenia działania środków łączności wykorzystywanych w celu zapewnienia bezpieczeństwa;
- 9) dokonania, w ramach realizacji zadań administratorów obiektów, sprawdzenia działania instalacji alarmowych, przepustowości dróg ewakuacji oraz funkcjonowania systemów rejestracji obrazu;
- 10) dokonania przeglądu wszystkich procedur, rozkazów oraz zadań związanych z wprowadzeniem wyższych stopni alarmowych;
- 11) prowadzenia akcji informacyjno-instruktażowej dla społeczeństwa dotyczącej potencjalnego zagrożenia, jego skutków i sposobu postępowania.

Wprowadza się w szczególności do wykonania następujące zadania:

- 1) wzmożone monitorowanie stanu bezpieczeństwa systemów teleinformatycznych organów administracji publicznej lub systemów teleinformatycznych wchodzących w skład infrastruktury krytycznej, zwanych dalej "systemami", w szczególności wykorzystując zalecenia Szefa Agencji Bezpieczeństwa Wewnętrznego lub komórek odpowiedzialnych za system reagowania zgodnie z właściwością, oraz:
 - a) monitorowanie i weryfikację, czy nie doszło do naruszenia bezpieczeństwa komunikacji elektronicznej,
 - b) kontrolę dostępności usług elektronicznych,

- c) zmianę, w razie konieczności, w dostępie do systemów.
- 2) informowanie personelu instytucji o konieczności zachowania zwiększonej czujności w stosunku do stanów odbiegających od normy, w szczególności personelu odpowiedzialnego za bezpieczeństwo systemów;
 - 3) kontrolę kanałów łączności z innymi, właściwymi dla rodzaju stopnia alarmowego CRP, podmiotami biorącymi udział w reagowaniu kryzysowym, weryfikację ustanowionych punktów kontaktowych z zespołami reagowania na incydenty bezpieczeństwa teleinformatycznego właściwymi dla rodzaju działania organizacji oraz ministrem właściwym do spraw informatyzacji;
 - 4) realizację przeglądu stosownych procedur oraz zadań związanych z wprowadzeniem stopni alarmowych CRP, w szczególności należy dokonać weryfikacji posiadanej kopii zapasowej systemów w stosunku do systemów teleinformatycznych wchodzących w skład infrastruktury krytycznej oraz systemów kluczowych dla funkcjonowania organizacji, oraz zweryfikować czas wymagany na przywrócenie poprawności funkcjonowania systemu;
 - 5) kontrolę aktualnego stanu bezpieczeństwa systemów i ocenić wpływ zagrożenia na bezpieczeństwo teleinformatyczne na podstawie bieżących informacji i prognoz wydarzeń;
 - 6) wprowadzić bieżącą komunikację / informację dotyczącą efektów przeprowadzanych działań zespołów reagowania na incydenty bezpieczeństwa teleinformatycznego właściwe dla rodzaju działania organizacji oraz współdziałające centra zarządzania kryzysowego, a także ministra właściwego do spraw informatyzacji.

Ogłoszenie drugiego stopnia alarmowego CRP (stopień BRAVO-CRP) wskazuje w szczególności na konieczność:

1. zapewnienia dostępności w trybie alarmowym personelu odpowiedzialnego za bezpieczeństwo systemów;
2. wprowadzenia całodobowych dyżurów administratorów systemów kluczowych dla funkcjonowania organizacji oraz personelu uprawnionego do podejmowania decyzji w sprawach bezpieczeństwa systemów teleinformatycznych;
3. przeglądu zapasów materiałowych i sprzętu, w tym dostępności środków i materiałów medycznych, z uwzględnieniem możliwości wykorzystania w przypadku wystąpienia zdarzenia o charakterze terrorystycznym.

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.

Oznacza to konieczność:

- 1) prowadzenia wzmożonej kontroli dużych skupisk ludności, które potencjalnie mogą stać się celem zdarzenia o charakterze terrorystycznym, w tym imprez masowych i zgromadzeń publicznych;

- 2) prowadzenia, w ramach realizacji zadań administratorów obiektów, wzmożonej kontroli obiektów użyteczności publicznej oraz innych obiektów, które potencjalnie mogą stać się celem zdarzenia o charakterze terrorystycznym;
- 3) zalecenia podległemu personelowi informowanie odpowiednich służb w przypadku zauważenia: nieznanymi pojazdami na terenie instytucji publicznych lub innych ważnych obiektów, porzuconych paczek i bagaży lub jakichkolwiek innych oznak nietypowej działalności;
- 4) poinformowania podległy personel o konieczności zachowania zwiększonej czujności w stosunku do osób zachowujących się w sposób wzbudzający podejrzenia;
- 5) zapewnienia dostępności w trybie alarmowym członków personelu niezbędnych do wzmocnienia ochrony obiektów;
- 6) przeprowadzenia kontroli pojazdów wjeżdżających oraz osób wchodzących na teren obiektów;
- 7) sprawdzania, na zewnątrz i od wewnątrz, budynków będących w stałym użyciu w zakresie podejrzanych zachowań osób oraz w poszukiwaniu podejrzanych przedmiotów;
- 8) sprawdzenia działania środków łączności wykorzystywanych w celu zapewnienia bezpieczeństwa;
- 9) dokonania, w ramach realizacji zadań administratorów obiektów, sprawdzenia działania instalacji alarmowych, przepustowości dróg ewakuacji oraz funkcjonowania systemów rejestracji obrazu;
- 10) dokonania przeglądu wszystkich procedur, rozkazów oraz zadań związanych z wprowadzeniem wyższych stopni alarmowych;
- 11) prowadzenia akcji informacyjno-instruktażową dla społeczeństwa dotyczącej potencjalnego zagrożenia, jego skutków i sposobu postępowania.

Wprowadza się w szczególności do wykonania następujące zadania:

- 1) wzmożone monitorowanie stanu bezpieczeństwa systemów teleinformatycznych organów administracji publicznej lub systemów teleinformatycznych wchodzących w skład infrastruktury krytycznej, zwanych dalej "systemami", w szczególności wykorzystując zalecenia Szefa Agencji Bezpieczeństwa Wewnętrznego lub komórek odpowiedzialnych za system reagowania zgodnie z właściwością, oraz:
 - a) monitorowanie i weryfikację, czy nie doszło do naruszenia bezpieczeństwa komunikacji elektronicznej,
 - b) kontrolę dostępności usług elektronicznych,
 - c) zmianę, w razie konieczności, w dostępie do systemów.

- 2) informowanie personelu instytucji o konieczności zachowania zwiększonej czujności w stosunku do stanów odbiegających od normy, w szczególności personelu odpowiedzialnego za bezpieczeństwo systemów;
- 3) kontrolę kanałów łączności z innymi, właściwymi dla rodzaju stopnia alarmowego CRP, podmiotami biorącymi udział w reagowaniu kryzysowym, weryfikację ustanowionych punktów kontaktowych z zespołami reagowania na incydenty bezpieczeństwa teleinformatycznego właściwymi dla rodzaju działania organizacji oraz ministrem właściwym do spraw informatyzacji;
- 4) realizację przeglądu stosownych procedur oraz zadań związanych z wprowadzeniem stopni alarmowych CRP, w szczególności należy dokonać weryfikacji posiadanej kopii zapasowej systemów w stosunku do systemów teleinformatycznych wchodzących w skład infrastruktury krytycznej oraz systemów kluczowych dla funkcjonowania organizacji, oraz zweryfikować czas wymagany na przywrócenie poprawności funkcjonowania systemu;
- 5) kontrolę aktualnego stanu bezpieczeństwa systemów i ocenić wpływ zagrożenia na bezpieczeństwo teleinformatyczne na podstawie bieżących informacji i prognoz wydarzeń;
- 6) wprowadzić bieżącą komunikację / informację dotyczącą efektów przeprowadzanych działań zespołów reagowania na incydenty bezpieczeństwa teleinformatycznego właściwe dla rodzaju działania organizacji oraz współdziałające centra zarządzania kryzysowego, a także ministra właściwego do spraw informatyzacji.

W odniesieniu do ogłoszonego I stopnia alarmowego (stopień ALFA) wyznacza się miejsce zbiórki w przypadku ewakuacji z budynku:

- Powiślańskiej Szkoły Wyższej z siedziby głównej w Kwidzynie (patrz rys. nr 1.) parking przy Uczelni przy małym parku - stosowne oznakowanie umieszczone,
- Filii Powiślańskiej Szkoły Wyższej w Gdańsku (patrz rys. nr 2.) Park Miejski przy ul. Wodopój- stosowne oznakowanie umieszczone,

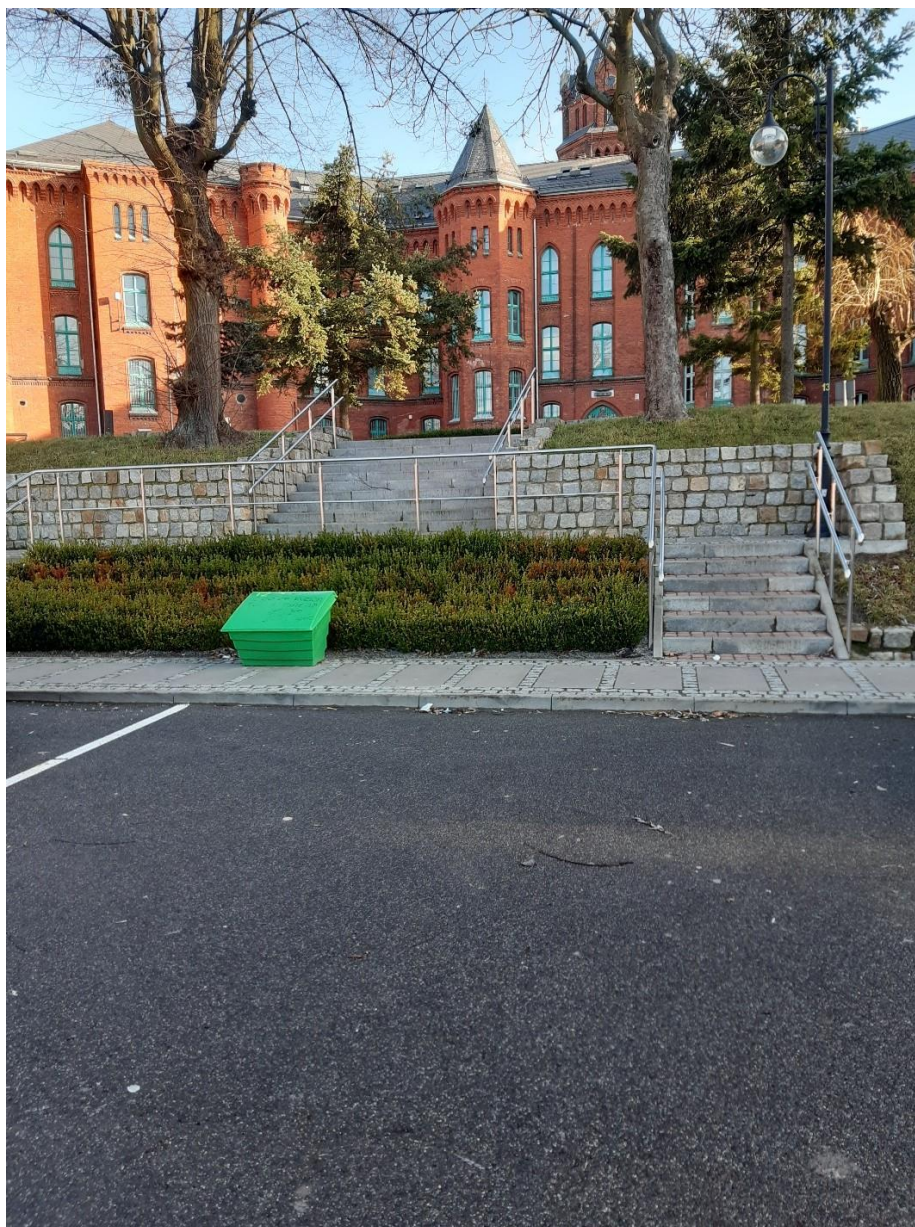
wskazane poniżej z zachowaniem zasad przeprowadzania ewakuacji.

Prof. dr hab. Krystyna Strzała



Rektor

Miejsce zbiórki podczas ewakuacji z budynku Powiślańskiej Szkoły Wyższej
siedziba główna w Kwidzynie



Rysunek nr 2.

Miejsce zbiórki podczas ewakuacji
z budynku Filii Powiślańskiej Szkoły Wyższej w Gdańsku

