

Warszawa, dnia 24 października 2017 r.

Poz. 34

ZARZĄDZENIE NR 30
MINISTRA CYFRYZACJI¹⁾

z dnia 22 października 2017 r.

w sprawie utworzenia Centrum Operacyjnego Ministra Cyfryzacji

Na podstawie art. 4 ust. 1 pkt 2 - 6 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2017 r. poz. 209 i 1566) zarządza się, co następuje:

§ 1. 1. Tworzy się Centrum Operacyjne Ministra Cyfryzacji, zwane dalej „Centrum”.

2. Centrum wspiera realizację zadań Ministra Cyfryzacji z zakresu cyberbezpieczeństwa,

- 1) zarządzania kryzysowego oraz obronności, w szczególności w sprawach:
- 2) bezpieczeństwa sfery cywilnej cyberprzestrzeni RP;
- 3) systemu reagowania na incydenty teleinformatyczne;
- 4) planowania cywilnego.

§ 2. 1. Centrum może służyć jako wydzielone miejsce pełnienia stałego dyżuru w rozumieniu § 5 ust. 3 pkt 2 zarządzenia Nr 20 Ministra Cyfryzacji z dnia 15 czerwca 2016 r. w sprawie systemu stałego dyżuru (Dz. Urz. Min. Cyf. poz. 22).

2. Centrum może służyć jako punkt kontaktowy HNS w rozumieniu § 1 ust. 2 pkt 1 zarządzenia Nr 19 Ministra Cyfryzacji z dnia 15 czerwca 2016 r. w sprawie funkcjonowania systemu HNS w dziale administracji rządowej informatyzacja na potrzeby realizacji zadań wynikających z obowiązków państwa-gospodarza (Dz. Urz. Min. Cyf. poz.21).

¹⁾ Minister Cyfryzacji kieruje działem administracji rządowej – informatyzacja, na podstawie § 1 ust. 2 rozporządzenia Prezesa Rady Ministrów z dnia 17 listopada 2015 r. w sprawie szczegółowego zakresu działania Ministra Cyfryzacji (Dz. U. poz. 1910 i 2090).

§ 3. Regulamin funkcjonowania Centrum określony został w załączniku do Zarządzenia.

§ 4. Zarządzenie wchodzi w życie z dniem następującym po dniu ogłoszenia.

- ANNA STREŻYŃSKA
MINISTER CYFRYZACJI

Załącznik
do zarządzenia Nr 30
Ministra Cyfryzacji
z dnia 22 października 2017 r.

REGULAMIN FUNKCJONOWANIA

CENTRUM OPERACYJNEGO MINISTRA CYFRYZACJI

§ 1. 1. Regulamin funkcjonowania Centrum Operacyjnego Ministra Cyfryzacji (zwany dalej „Regulaminem”) określa organizację i zadania realizowane przez Centrum Operacyjne Ministra Cyfryzacji, zwane dalej „Centrum”.

2. Centrum służy wspieraniu realizacji zadań Ministra Cyfryzacji, zwanego dalej „Ministrem”, z zakresu bezpieczeństwa narodowego, w szczególności: cyberbezpieczeństwa, zarządzania kryzysowego oraz obronności.

3. Centrum uruchamiane, w razie potrzeby na polecenie Ministra, członka Kierownictwa Ministerstwa Cyfryzacji lub, w zależności od charakteru zagrożenia lub zdarzenia, na wniosek kierownika komórki organizacyjnej wskazanej w Instrukcji Centrum Operacyjnego, zwanej dalej „Instrukcją”.

4. Centrum uruchamiane jest przez właściwego kierownika komórki organizacyjnej na potrzeby ćwiczeń z zakresu cyberbezpieczeństwa, zarządzania kryzysowego oraz obronności.

5. Centrum uruchamiane jest w budynku Ministerstwa Cyfryzacji zwanego dalej „Ministerstwem”, przy ul. Królewskiej 27 w Warszawie.

6. W przypadku zagrożenia dla budynku Ministerstwa wymienionego w ust. 5 Minister albo członek Kierownictwa Ministerstwa może postanowić o uruchomieniu Centrum w innym budynku.

§ 2. 1. Do zadań Centrum należy:

- 1) wspieranie Ministra w kierowaniu Narodowym Centrum Cyberbezpieczeństwa zwanym dalej „NCC” funkcjonującym w ramach Państwowego Instytutu Badawczego – Naukowej i Akademickiej Sieci Komputerowej, jednostki nadzorowanej przez Ministra w zakresie reagowania na incydenty teleinformatyczne;
- 2) zapewnienie ścisłej współpracy z pozostałymi podmiotami zaangażowanymi w reagowanie na incydenty teleinformatyczne w szczególności z Agencją Bezpieczeństwa Wewnętrznego, Rządowym Centrum Bezpieczeństwa i Policją;

- 3) nadzór i koordynacja działań jednostek podległych i nadzorowanych przez Ministra w sytuacji kryzysowej lub w sytuacji szczególnych zagrożeń, jeżeli jest to uzasadnione rozmiarem lub skutkami zaistniałej sytuacji;
- 4) przekazywanie właściwym komórkom organizacyjnym Ministerstwa propozycji opracowania projektów decyzji, stanowisk, wytycznych i rekomendacji dotyczących cyberbezpieczeństwa, zarządzania kryzysowego oraz spraw obronnych na potrzeby kierownictwa Ministerstwa i Zespołu Zarządzania Kryzysowego Ministra Cyfryzacji;
- 5) analiza sytuacji, koordynowanie i kierowanie działaniami Ministerstwa w przypadku wystąpienia sytuacji kryzysowej powodującej zakłócenia w funkcjonowaniu systemów informatycznych, sieci lub usług telekomunikacyjnych lub gdy takie zakłócenie miało wpływ na usługi kluczowe (podstawowe) świadczone ludności lub na systemy, rejestry i publikatory administracji publicznej;
- 6) monitorowanie rozwoju sytuacji kryzysowej, jeżeli uzasadnione jest to jej zasięgiem lub skutkami;
- 7) zapewnienie stałej łączności z Urzędem Komunikacji Elektronicznej i NCC w przypadku wystąpienia zakłócenia w funkcjonowaniu systemów informatycznych, sieci lub usług telekomunikacyjnych lub gdy takie zakłócenie miało wpływ na usługi kluczowe (podstawowe) świadczone ludności lub na systemy, rejestry i publikatory administracji publicznej;
- 8) zapewnienie obiegu informacji w sytuacji kryzysowej na potrzeby kierownictwa Ministerstwa i Zespołu Zarządzania Kryzysowego Ministra Cyfryzacji;
- 9) zapewnienie miejsca do pełnienia dyżurów w trybie alarmowym w przypadku wprowadzenia stopni alarmowych lub stopni alarmowych CRP dla osób uprawnionych do podejmowania decyzji w sprawach bezpieczeństwa systemów teleinformatycznych – zgodnie z przepisami ustawy o działaniach antyterrorystycznych;
- 10) zapewnienie obiegu informacji na potrzeby zadań ujętych w wykazie przedsięwzięć i procedur systemu zarządzania kryzysowego;
- 11) koordynacja wydzielonego wsparcia wynikającego z obowiązków państwa-gospodarza (HNS) w Ministerstwie, Urzędzie Komunikacji Elektronicznej i przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym w rozumieniu art. 6 ust. 1 pkt 2 i art. 18 ust. 1 i 3 ustawy z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej (Dz. U. z 2017 r. poz. 430);

12) pełnienie funkcji wsparcia głównego stanowiska kierowania Ministra w głównej siedzibie.

2. Szczegółowe działania Centrum służące realizacji poszczególnych zadań określone zostaną w Instrukcji i procedurach operacyjnych Centrum stanowiących załącznik do Instrukcji.

3. Instrukcje Centrum określi kierownik komórki organizacyjnej właściwej w zakresie cyberbezpieczeństwa po uzgodnieniu z pozostałymi kierownikami organizacyjnymi Ministerstwa.

§ 3. 1. Obsadę Centrum stanowią:

- 1) kierownik zmiany dyżurnej;
- 2) dyżurni;
- 3) łącznicy.

2. Komórki organizacyjne Ministerstwa zapewniają obsadę centrum na stanowisku kierownika zmiany dyżurnej i co najmniej dwóch dyżurnych.

3. Jednostki podległe i nadzorowane przez Ministra zapewniają obsadę Centrum na stanowiskach łączników, na podstawie odrębnych umów i porozumień.

4. Centrum w czasie pełnienia dyżuru współpracuje z Rzecznikiem Prasowym Ministerstwa w zakresie monitorowania mediów i prowadzenia polityki informacyjnej.

5. Kierownika zmiany dyżurnej oraz dyżurnych i łączników wyznacza kierownik komórki organizacyjnej wskazanej w Instrukcji Centrum jako właściwej ze względu na charakter zadania lub zagrożenia, które spowodowało uruchomienie Centrum.

6. Szczegółową obsadę Centrum przez jednostki wymienione w ust. 2 i 3 określi Instrukcja Centrum, biorąc pod uwagę charakter zadania lub zagrożenia, które spowodowało uruchomienie Centrum.

§ 4. 1. Do zadań kierownika zmiany dyżurnej należy:

- 1) koordynacja działań pozostałych członków obsady Centrum;
- 2) sporządzanie raportów z działania Centrum i rozwoju sytuacji kryzysowej;
- 3) przedstawienie Ministrowi lub członkowi Kierownictwa Ministerstwa propozycji działań w zakresie zadań realizowanych przez Centrum;
- 4) sporządzanie projektów decyzji, stanowisk, wytycznych i rekomendacji w zakresie zadań realizowanych przez Centrum;

5) prowadzenie ewidencji wytwarzanych informacji niejawnych – w porozumieniu z Kierownikiem Kancelarii Tajnej Ministerstwa.

2. Kierownik zmiany dyżurnej jest uprawniony do:

- 1) powierzania wykonywania zadań członkom obsady Centrum;
- 2) zobowiązania członków obsady Centrum do przedstawienia w wyznaczonym terminie informacji o stanie realizacji powierzonych przedsięwzięć objętych zakresem działania Centrum;
- 3) zobowiązywania członków obsady Centrum do przedstawiania opinii, ekspertyz lub projektów dokumentów mających na celu realizację zadań Centrum.

3. Realizacja zadań lub przekazanie informacji, o których mowa ust. 2, następuje w terminach wyznaczonych przez kierownika zmiany dyżurnej.

4. Kierownika zmiany dyżurnej podczas jego nieobecności zastępuje wyznaczony przez niego dyżurny.

§ 5. Do zadań dyżurnych i łączników należy:

- 1) monitorowanie rozwoju sytuacji kryzysowej;
- 2) pozyskiwanie informacji z jednostek współpracujących z Centrum, baz danych i systemów teleinformatycznych;
- 3) wymiana informacji z obsadą Centrum i jednostkami współpracującymi z Centrum;
- 4) analiza pozyskanych informacji;
- 5) przygotowywanie raportów w zakresie swojej właściwości i przekazywanie ich do kierownika zmiany dyżurnej;
- 6) reagowanie zgodnie z Instrukcją i procedurami operacyjnymi Centrum;
- 7) prowadzenie dziennika działań w postaci elektronicznej.

§ 6. 1. W przypadku uruchomienia Centrum pełni ono dyżur w godzinach urzędowania Ministerstwa lub, w razie potrzeby, w trybie zmianowym 24 godziny na dobę przez 7 dni w tygodniu – w zależności od charakteru zagrożenia, które spowodowało uruchomienie Centrum.

2. Podział dyżuru na zmiany i wzór grafiku dyżurów określony zostanie w Instrukcji, w szczególności biorąc pod uwagę wymogi dotyczące pełnienia stałego dyżuru i realizacji zadań wynikających z ochrony cyberprzestrzeni Rzeczypospolitej Polskiej oraz realizacji Krajowego Planu Zarządzania Kryzysowego.

3. Grafiki dyżurów określa kierownik jednostki organizacyjnej uruchamiającej Centrum.

4. Grafik dyżurów, w stosunku do pracowników Ministerstwa, podlega uzgodnieniu i zatwierdzeniu przez Dyrektora Generalnego Ministerstwa.

§ 7. Tryb i schemat przekazywania informacji określa Instrukcja, w szczególności biorąc pod uwagę wymogi dotyczące pełnienia stałego dyżuru i realizacji zadań wynikających z ochrony cyberprzestrzeni Rzeczypospolitej Polskiej oraz realizacji Krajowego Planu Zarządzania Kryzysowego.

§ 8. 1. Dokumentacja i korespondencja Centrum jest prowadzona w postaci elektronicznej, a wyjątki od tej zasady określa Instrukcja.

2. Obsługę kancelaryjno-biurową Centrum zapewnia Departament Cyberbezpieczeństwa z wykorzystaniem elektronicznego zarządzania dokumentacją.

3. Obsługę w zakresie korespondencji niejawnej zapewnia Kancelaria Tajna Ministerstwa.

4. Zasady ewidencji otrzymanych i wytworzonych informacji niejawnych po godzinach pracy Kancelarii Tajnej Ministerstwa określa Kierownik Kancelarii Tajnej Ministerstwa.

5. Zasady ruchu osobowego i udziału w dyżurach osób z zewnątrz, w tym łączników, określi Biuro Dyrektora Generalnego.

6. Obsługa Centrum w zakresie wskazania miejsca do odpoczynku oraz dostarczenia posiłków jest uzgadniana każdorazowo z Biurem Dyrektora Generalnego.

7. Obsługa transportowa Centrum jest uzgadniana każdorazowo z Biurem Dyrektora Generalnego.

8. Obsługę Centrum w zakresie wsparcia teleinformatycznego zapewnia Departament Infrastruktury Państwa.