Załącznik
do zarządzenia Generalnego Dyrektora
Ochrony Środowiska z dnia 20 czerwca
2023 r. zmieniającego zarządzenie
w sprawie zakresu przedsięwzięć
wykonywanych w poszczególnych
stopniach alarmowych CRP w Generalnej
Dyrekcji Ochrony Środowiska

Ramowy układ procedury realizacji przedsięwzięć wykonywanych w poszczególnych stopniach alarmowych w Generalnej Dyrekcji Ochrony Środowiska

I. POSTANOWIENIA OGÓLNE

1. Wstęp.

Zdarzeniem o charakterze terrorystycznym jest sytuacja, co do której istnieje podejrzenie, że powstała na skutek przestępstwa o charakterze terrorystycznym, którego celem jest:

- poważne zastraszenie wielu osób,
- zmuszenie organu władzy publicznej Rzeczypospolitej Polskiej lub innego państwa albo organu organizacji międzynarodowej do podjęcia lub zaniechania określonych czynności,
- wywołanie poważnych zakłóceń w ustroju lub gospodarce Rzeczypospolitej Polskiej, innego państwa lub organizacji międzynarodowej

lub zagrożenie zaistnienia takiego przestępstwa.

Skutkiem zaistnienia zdarzenia o charakterze terrorystycznym w obszarze bezpieczeństwa fizycznego jest bezpośrednie zagrożenie życia, zdrowia lub wolności osób albo zniszczenie lub uszkodzenie mienia.

W celu zapobiegania zdarzeniom o charakterze terrorystycznym lub reagowania w przypadku wystąpienia takich zdarzeń prowadzi się działania antyterrorystyczne organów administracji publicznej oraz działania kontrterrorystyczne wobec sprawców, osób przygotowujących lub pomagających w dokonaniu przestępstw o charakterze terrorystycznym.

W przypadku zagrożenia wystąpieniem zdarzenia o charakterze terrorystycznym albo w przypadku wystąpienia takiego zdarzenia można wprowadzić jeden z czterech stopni alarmowych CRP.

2. Cel.

Działania Generalnej Dyrekcji Ochrony Środowiska, zwanej dalej „GDOŚ", polegające na zapobieganiu zdarzeniom o charakterze terrorystycznym, ukierunkowane są na przygotowanie do przejmowania nad nimi kontroli w drodze zaplanowanych przedsięwzięć, reagowanie w przypadku wystąpienia takich zdarzeń oraz usuwanie ich skutków, w tym odtwarzanie zasobów przeznaczonych do reagowania na nie.

Celem ww. działań jest zapewnienie bezpieczeństwa systemów teleinformatycznych GDOŚ:

1) zapewnienie ciągłości funkcjonowania systemów teleinformatycznych GDOŚ;
2) uprzedzenie pracowników o możliwości wystąpienia zagrożenia oraz określenie możliwych symptomów;
3) przeciwdziałanie oraz minimalizacja skutków ewentualnych ataków na systemy teleinformatyczne GDOŚ;
4) bieżące monitorowanie działania systemów teleinformatycznych GDOŚ umożliwiające reagowanie w sytuacji wystąpienia zakłóceń;
5) zapewnienie całodobowej ciągłości funkcjonowania systemów teleinformatycznych GDOŚ.

3. Finansowanie.

Działania GDOŚ polegające na zapobieganiu zdarzeniom o charakterze terrorystycznym lub – w przypadku ich wystąpienia – usuwanie ich skutków, finansowane są ze środków własnych, w ramach budżetu GDOŚ. Realizacja zadań przewidzianych dla trzeciego stopnia (stopień CHARLIE-CRP) i czwartego stopnia alarmowego CRP (stopień DELTA-CRP), może skutkować koniecznością zwiększenia nakładów na ochronę lub właściwe funkcjonowanie systemów teleinformatycznych GDOŚ.

4. Podstawy prawne działań:

1) ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz. U. z 2022 r. poz. 2632);
2) ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2022 r. poz. 1863 i 2666);
3) rozporządzenie Prezesa Rady Ministrów z dnia 25 lipca 2016 r. w sprawie zakresu przedsięwzięć wykonywanych w poszczególnych stopniach alarmowych i stopniach alarmowych CRP (Dz. U. z 2022 r. poz. 2065);

4) zarządzenie Nr 9 Generalnego Dyrektora Ochrony Środowiska z dnia 11 lipca 2022 r. w sprawie sposobu opracowania procedur realizacji przedsięwzięć wykonywanych w poszczególnych stopniach alarmowych i stopniach alarmowych CRP w Generalnej Dyrekcji Ochrony Środowiska i w regionalnych dyrekcjach ochrony środowiska (Dz. Urz. GDOŚ poz. 10 i 18).

II. KONCEPCJA DZIAŁANIA

1. Warunki operacyjne.
   1) Warunki operacyjne realizacji zadania:
      a) wzrost niepokoju wśród pracowników – w ramach wszystkich stopni alarmowych CRP,
      b) możliwe niewłaściwe funkcjonowanie systemów teleinformatycznych – w ramach wszystkich stopni alarmowych CRP,
      c) zaburzenia w dostępie do usług elektronicznych – w ramach wszystkich stopni alarmowych CRP,
      d) możliwa utrata zasobów lub możliwości dostępu do nich – w ramach trzeciego stopnia alarmowego CRP (stopień CHARLIE-CRP) i czwartego stopnia alarmowego CRP (stopień DELTA-CRP),
      e) zakłócenia w przepływie informacji pomiędzy uczestnikami procesu – w ramach trzeciego stopnia alarmowego CRP (stopień CHARLIE-CRP) i czwartego stopnia alarmowego CRP (stopień DELTA-CRP).
   2) Potrzeby w przypadku przedłużających się zadań:
      a) realizacja zadań określonych dla pierwszego stopnia alarmowego CRP w dłuższej perspektywie czasowej nie powinna powodować zwiększonych potrzeb w żadnej z sfer organizacyjnych GDOŚ;
      b) realizacja zadań określonych dla drugiego alarmowego CRP w dłuższej perspektywie czasowej może wpłynąć na właściwe funkcjonowanie Wydziału Informatyki Biura Dyrektora Generalnego, zwanego dalej „BDG”, ze względu na konieczność wprowadzenia całodobowych dyżurów administratorów systemów teleinformatycznych GDOŚ;

c) realizacja zadań określonych dla trzeciego alarmowego CRP w dłuższej perspektywie czasowej wpłynie na właściwe funkcjonowanie Wydziału Informatyki BDG ze względu na konieczność wprowadzenia całodobowych dyżurów administratorów systemów i może spowodować konieczność wydzielenia pozaplanowych środków finansowych na zakup dodatkowych zasobów;

d) realizacja zadań określonych dla czwartego stopnia alarmowego CRP w dłuższej perspektywie czasowej wpłynie na właściwe funkcjonowanie Wydziału Informatyki BDG ze względu na konieczność wprowadzenia całodobowych dyżurów administratorów systemów i może spowodować konieczność wydzielenia pozaplanowych środków finansowych na zakup dodatkowych zasobów.

2. Warunki wprowadzenia poszczególnych stopni alarmowych CRP:

1) pierwszy stopień alarmowy CRP (stopień ALFA-CRP) – uzyskanie informacji o możliwości wystąpienia zdarzenia o charakterze terrorystycznym w odniesieniu do systemów teleinformatycznych organów administracji publicznej lub systemów teleinformatycznych wchodzących w skład infrastruktury krytycznej, którego rodzaj i zakres jest trudny do przewidzenia;

2) drugi stopień alarmowy CRP (stopień BRAVO-CRP) – zaistnienie zwiększonego i przewidywalnego zagrożenia wystąpieniem zdarzenia o charakterze terrorystycznym, jednak konkretny cel ataku nie został zidentyfikowany;

3) trzeci stopień alarmowy CRP (stopień CHARLIE-CRP):

a) wystąpienie zdarzenia potwierdzającego prawdopodobny cel ataku o charakterze terrorystycznym, godzącego w:

– bezpieczeństwo lub porządek publiczny albo

– bezpieczeństwo Rzeczypospolitej Polskiej, albo

– bezpieczeństwo innego państwa lub organizacji międzynarodowej oraz stwarzającego potencjalne zagrożenie dla Rzeczypospolitej Polskiej lub

b) uzyskanie wiarygodnych i potwierdzonych informacji o planowanym zdarzeniu o charakterze terrorystycznym na terytorium Rzeczypospolitej Polskiej, lub

c) uzyskanie wiarygodnych i potwierdzonych informacji o planowanym zdarzeniu o charakterze terrorystycznym, którego skutki mogą dotyczyć obywateli polskich przebywających za granicą lub instytucji polskich albo polskiej infrastruktury mieszczących się poza granicami Rzeczypospolitej Polskiej;

4) czwarty stopień alarmowy (stopień DELTA-CRP):

a) wystąpienie zdarzenia o charakterze terrorystycznym powodującego zagrożenie:

– bezpieczeństwa lub porządku publicznego albo

– bezpieczeństwa Rzeczypospolitej Polskiej, albo

– bezpieczeństwa innego państwa lub organizacji międzynarodowej oraz stwarzającego zagrożenie dla Rzeczypospolitej Polskiej, lub

b) gdy uzyskane informacje wskazują na zaawansowaną fazę przygotowań do zdarzenia o charakterze terrorystycznym na terytorium Rzeczypospolitej Polskiej, lub

c) gdy uzyskane informacje wskazują na zaawansowaną fazę przygotowań do zdarzenia o charakterze terrorystycznym, które ma być wymierzone w obywateli polskich przebywających za granicą lub w instytucje polskie albo polską infrastrukturę mieszczące się poza granicami Rzeczypospolitej Polskiej, a zebrane informacje wskazują jednocześnie na nieuchronność takiego zdarzenia.

3. Organizacja kierowania w GDOŚ.

Całokształtem działań GDOŚ polegających na zapobieganiu zdarzeniom o charakterze terrorystycznym i reagowaniu w przypadku wystąpienia takich zdarzeń oraz usuwaniu ich skutków kieruje i podejmuje samodzielne decyzje we wszystkich sprawach, w których występuje jako organ administracji rządowej, Generalny Dyrektor Ochrony Środowiska [Aleje Jerozolimskie 136, 02-305 Warszawa; tel.: 22 310 67 00; fax: 22 310 61 41; e-mail: sekretariat.gdos@gdos.gov.pl] przy pomocy:

1) Zastępcy Generalnego Dyrektora Ochrony Środowiska [Aleje Jerozolimskie 136, 02-305 Warszawa; tel.: 22 310 67 00; fax: 22 310 61 41; e-mail: sekretariat.gdos@gdos.gov.pl], który przewodniczy „Zespołowi zarządzania kryzysowego" GDOŚ,

2) Dyrektora Generalnego [Aleje Jerozolimskie 136, 02-305 Warszawa; tel.: 22 310 67 00; fax: 22 310 61 41; e-mail: sekretariat.bdg@gdos.gov.pl].

4. Ogólny tryb uruchamiania zasobów.

Generalny Dyrektor Ochrony Środowiska, po powzięciu informacji o wprowadzeniu na obszarze lub w obiekcie, w którym znajduje się siedziba GDOŚ [Aleje Jerozolimskie 136, 02-305 Warszawa] poleca wdrożenie w GDOŚ działań przewidzianych do realizacji w ramach poszczególnych stopni alarmowych CRP. Informacja o wprowadzeniu poszczególnych stopni alarmowych CRP jest przekazywana za pomocą dostępnych technicznych środków łączności, w szczególności za pomocą poczty elektronicznej, telefonii komórkowej, telefonii stacjonarnej, a jeżeli techniczne środki łączności nie funkcjonują, osobiście w godzinach pracy Urzędu – przez pracowników sekretariatów komórek organizacyjnych GDOŚ.

W pierwszej kolejności o wprowadzeniu, zmianie i odwołaniu stopnia alarmowego CRP są powiadamiani:

- Generalny Dyrektor Ochrony Środowiska [tel.: 22 310 67 00; fax: 22 310 61 41; e-mail: sekretariat.gdos@gdos.gov.pl],
- Zastępca Generalnego Dyrektora Ochrony Środowiska [tel.: 22 310 67 00; fax: 22 310 61 41; e-mail: sekretariat.gdos@gdos.gov.pl],
- Dyrektor Generalny GDOŚ [tel.: 22 310 67 00; fax: 22 310 61 41; e-mail: sekretariat.bdg@gdos.gov.pl],
- Dyrektor Biura Dyrektora Generalnego GDOŚ [tel.: 22 310 67 00; fax: 22 310 61 41; e-mail: sekretariat.bdg@gdos.gov.pl],
- Naczelnik Wydziału Informatyki BDG [tel. 885 654 607, fax: 22 310 61 41; e-mail: sekretariat.bdg@gdos.gov.pl],
- Pełnomocnik do spraw Bezpieczeństwa Informacji [tel. 22 310 67 05, fax: 22 310 61 41; e-mail: sekretariat.bdg@gdos.gov.pl],
- pracownik do spraw zarządzania kryzysowego [tel.: 22 120 29 75; fax: 22 310 61 41; e-mail: staly.dyzur@gdos.gov.pl],

następnie, poprzez sekretariat Biura Dyrektora Generalnego GDOŚ [tel.: 22 310 67 00; fax: 22 310 61 41; e-mail: sekretariat.bdg@gdos.gov.pl], wykonawcy modułów zadaniowych w poszczególnych stopniach alarmowych, z wyłączeniem pracowników Wydziału Informatyki Biura Dyrektora Generalnego, zwanego dalej „BDG", którzy powiadamiani są bezpośrednio przez Naczelnika Wydziału Informatyki BDG:

- Naczelnik Wydziału Komunikacji i Promocji BDG,
- Naczelnik Wydziału Kadr BDG,
- Naczelnik Wydziału Organizacyjnego BDG,
- Sekretariat GDOŚ,

oraz wszyscy pracownicy GDOŚ, w formie komunikatu przesyłanego na służbowy adres e-mail lub, jeżeli techniczne środki łączności nie funkcjonują, osobiście w godzinach pracy GDOŚ – przez pracowników sekretariatów komórek organizacyjnych GDOŚ.

III. MODUŁY ZADANIOWE DLA KAŻDEGO STOPNIA ALARMOWEGO CRP, ZAWIERAJĄCE WYKAZ ZADAŃ DO WYKONANIA

Lp.	Przedsięwzięcie	Zadanie	Wykonawca koordynator[1]	Uwagi
I.	**Pierwszy stopień alarmowy CRP (stopień ALFA-CRP)**			
I.1.1	Wprowadzenie pierwszego stopnia alarmowego CRP (stopień ALFA-CRP)	Odebranie informacji o wprowadzeniu pierwszego stopnia alarmowego CRP (stopień ALFA-CRP)	pracownik ds. zarządzania kryzysowego lub sekretariat GDOŚ Generalny Dyrektor	
I.1.2		Przekazanie informacji dla pracowników GDOŚ o wprowadzeniu pierwszego stopnia alarmowego CRP (stopień ALFA-CRP)	Naczelnik Wydziału Komunikacji i Promocji Dyrektor Generalny	
I.1.3		Przekazanie informacji o wprowadzeniu pierwszego stopnia alarmowego CRP (stopień ALFA-CRP) do regionalnych dyrekcji ochrony środowiska, których on dotyczy	pracownik ds. zarządzania kryzysowego Generalny Dyrektor	realizować, jeżeli regionalne dyrekcje ochrony środowiska nie zostały powiadomione w inny sposób
I.2	Wzmożone monitorowanie stanu bezpieczeństwa systemów teleinformatycznych	Analiza logów i innych danych wskazujących na potencjalne nieprawidłowości w funkcjonowaniu sieci, systemów i usług teleinformatycznych	ABT, ATS, AMS Dyrektor Generalny	w godzinach pracy GDOŚ, od momentu ogłoszenia pierwszego stopnia alarmowego CRP
I.3	Monitorowanie i weryfikacja, czy nie doszło do naruszenia bezpieczeństwa komunikacji elektronicznej	Reagowanie na incydenty i zgłoszenia teleinformatyczne	ABT, ATS, AMS, ADO, Pełnomocnik ds. BI Dyrektor Generalny	w godzinach pracy GDOŚ, od momentu ogłoszenia pierwszego stopnia alarmowego CRP
I.4	Sprawdzenie dostępności usług elektronicznych	Weryfikacja poprawności usług elektronicznych (poczta elektroniczna, Intranet i Internet, telefonia	ABT, ATS,	w godzinach pracy GDOŚ, od momentu ogłoszenia

[1] Koordynator danego zadania jest odpowiedzialny za jego realizację. Koordynator zapisywany jest w danej komórce poniżej podkreślenia „___”. W sytuacji, w której koordynator i wykonawca to ta sama osoba, wykonuje on dane zadanie i jednocześnie odpowiada za jego realizację.

		stacjonarna i komórkowa)	AMS, ADO, Pełnomocnik ds. BI Dyrektor Generalny	pierwszego stopnia alarmowego CRP
I.5	Dokonanie, w razie potrzeby, zmian w dostępie do systemów	Weryfikacja praw dostępu do kluczowych systemów teleinformatycznych GDOŚ	ABT, ATS, AMS, ADO, Pełnomocnik ds. BI Dyrektor Generalny	w godzinach pracy GDOŚ, od momentu ogłoszenia pierwszego stopnia alarmowego CRP
I.6	Poinformowanie pracowników GDOŚ o konieczności zachowania zwiększonej czujności w stosunku do stanów odbiegających od normy, w szczególności pracowników odpowiedzialnych za bezpieczeństwo systemów	Przygotowanie informacji i powiadomienie wszystkich użytkowników systemów teleinformatycznych GDOŚ o możliwości wystąpienia zagrożeń teleinformatycznych i przeciwdziałaniu ich zmaterializowania się (komunikaty intranetowe oraz dedykowane e-maile)	Pełnomocnik ds. BI Dyrektor Generalny	realizacja w ciągu 2 godzin pierwszego dnia roboczego od momentu obowiązywania pierwszego stopnia alarmowego CRP
I.7	Sprawdzenie kanałów łączności z innymi, właściwymi dla pierwszego stopnia alarmowego CRP, podmiotami biorącymi udział w reagowaniu kryzysowym, dokonanie weryfikacji ustanowionych punktów kontaktowych z zespołami reagowania na incydenty bezpieczeństwa teleinformatycznego właściwymi dla GDOŚ	Sprawdzenie, aktualizacja i nawiązanie kontaktów telefonicznych i mailowych z Zespołem Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV Departamentu Bezpieczeństwa Teleinformatycznego Agencji Bezpieczeństwa Wewnętrznego: e-mail: incydent@csirt.gov.pl, telefon: +48 22 58 59 373, fax: +48 22 58 58 833.	Pełnomocnik ds. BI Dyrektor Generalny	realizacja w ciągu 2 godzin pierwszego dnia roboczego od momentu obowiązywania pierwszego stopnia alarmowego CRP

I.8	Dokonanie przeglądu stosownych procedur oraz zadań związanych z wprowadzeniem pierwszego stopnia alarmowego CRP, w szczególności dokonanie weryfikacji posiadanej kopii zapasowej systemów w stosunku do systemów teleinformatycznych wchodzących w skład infrastruktury krytycznej oraz systemów kluczowych dla funkcjonowania GDOŚ oraz weryfikacji czasu wymaganego na przywrócenie poprawności funkcjonowania systemu	Dokonanie przeglądu wewnętrznych procedur operacyjnych Wydziału Informatyki. Weryfikacja aktualnego czasu wymaganego na przywrócenie poprawności funkcjonowania kluczowych systemów teleinformatycznych GDOŚ	ABT, ATS, AMS, Pełnomocnik ds. BI Dyrektor Generalny	realizacja w pierwszym dniu roboczym obowiązywania pierwszego stopnia alarmowego CRP
I.9	Sprawdzenie aktualnego stanu bezpieczeństwa systemów i ocena wpływu zagrożenia na bezpieczeństwo teleinformatyczne na podstawie bieżących informacji i prognoz wydarzeń	Przeprowadzenie analizy ryzyka bezpieczeństwa teleinformatycznego oraz przygotowanie rekomendacji, zaleceń i działań zaradczych	ABT, ATS, AMS, Pełnomocnik ds. BI Dyrektor Generalny	realizacja w pierwszym dniu roboczym obowiązywania pierwszego stopnia alarmowego CRP
I.10	Informowanie na bieżąco o efektach przeprowadzonych działań zespoły reagowania na incydenty bezpieczeństwa	Informowanie zespołu CSIRT GOV poprzez dedykowany kontakt e-mailowy. Przygotowywanie notatek dla Dyrektora Generalnego	ABT, ATS, AMS, Pełnomocnik ds. BI Dyrektor Generalny	realizacja w godzinach pracy GDOŚ od momentu ogłoszenia pierwszego stopnia alarmowego CRP

	teleinformatycznego właściwe dla rodzaju działania GDOŚ			
I.11.1	Raportowanie o stanie realizacji zadań wynikających z wprowadzonego pierwszego stopnia alarmowego CRP	Powiadomienie Dyrektora Generalnego na adres poczty elektronicznej sekretariat.bdg@gdos.gov.pl o zrealizowanych zadaniach w ramach wprowadzonego pierwszego stopnia alarmowego CRP	Pełnomocnik ds. BI Pełnomocnik ds. BI	realizacja nie później niż 8 godzin od otrzymania informacji o wprowadzeniu pierwszego stopnia alarmowego CRP
I.11.2		Powiadomienie Dyrektora Generalnego o zrealizowanych zadaniach w ramach wprowadzonego pierwszego stopnia alarmowego CRP	ABT, ATS, AMS Pełnomocnik ds. BI	realizacja nie później niż 4 godziny od otrzymania z RCB informacji o wprowadzeniu pierwszego stopnia alarmowego CRP
I.11.3		Przekazanie do Dyrektora Generalnego raportu o stanie realizacji zadań wynikających z wprowadzonego pierwszego stopnia alarmowego CRP	Pełnomocnik ds. BI Pełnomocnik ds. BI	realizacja nie później niż 12 godzin od otrzymania z RCB informacji o wprowadzeniu pierwszego stopnia alarmowego CRP
I.12.1	Odwołanie pierwszego stopnia alarmowego CRP (stopień ALFA-CRP)	Odebranie informacji o odwołaniu pierwszego stopnia alarmowego CRP (stopień ALFA-CRP)	pracownik ds. zarządzania kryzysowego lub sekretariat GDOŚ Generalny Dyrektor	realizować, jeżeli taki sygnał zostanie przekazany
I.12.2		Przekazanie informacji dla pracowników GDOŚ o odwołaniu pierwszego stopnia alarmowego CRP (stopień ALFA-CRP)	Naczelnik Wydziału Komunikacji i Promocji Dyrektor Generalny	realizować, jeżeli taka informacja zostanie przekazana
I.12.3		Przekazanie informacji o odwołaniu pierwszego stopnia alarmowego CRP (stopień ALFA-CRP) do regionalnych dyrekcji ochrony środowiska, których odwołanie dotyczy	pracownik ds. zarządzania kryzysowego Generalny Dyrektor	realizować, jeżeli regionalne dyrekcje ochrony środowiska nie zostały powiadomione w inny sposób
II.	**Drugi stopień alarmowy CRP (stopień BRAVO-CRP)**			
II.1.1	Wprowadzenie drugiego	Odebranie informacji o wprowadzeniu drugiego	pracownik ds.	

	stopnia alarmowego CRP (stopień BRAVO-CRP)	stopnia alarmowego CRP (stopień BRAVO-CRP)	zarządzania kryzysowego lub sekretariat GDOŚ Generalny Dyrektor	
II.1.2		Przekazanie informacji dla pracowników GDOŚ o wprowadzeniu drugiego stopnia alarmowego CRP (stopień BRAVO-CRP)	Naczelnik Wydziału Komunikacji i Promocji Dyrektor Generalny	
II.1.3		Przekazanie informacji o wprowadzeniu drugiego stopnia alarmowego CRP (stopień BRAVO-CRP) do regionalnych dyrekcji ochrony środowiska, których on dotyczy	pracownik ds. zarządzania kryzysowego Generalny Dyrektor	realizować, jeżeli regionalne dyrekcje ochrony środowiska nie zostały powiadomione w inny sposób
II.2	Wzmożone monitorowanie stanu bezpieczeństwa systemów teleinformatycznych	Analiza logów i innych danych wskazujących na potencjalne nieprawidłowości w funkcjonowaniu sieci, systemów i usług teleinformatycznych	ABT, ATS, AMS Dyrektor Generalny	w godzinach pracy GDOŚ, od momentu ogłoszenia drugiego stopnia alarmowego CRP
II.3	Monitorowanie i weryfikacja, czy nie doszło do naruszenia bezpieczeństwa komunikacji elektronicznej	Reagowanie na incydenty i zgłoszenia teleinformatyczne	ABT, ATS, AMS, ADO, Pełnomocnik ds. BI Dyrektor Generalny	w godzinach pracy GDOŚ, od momentu ogłoszenia drugiego stopnia alarmowego CRP
II.4	Sprawdzenie dostępności usług elektronicznych	Weryfikacja poprawności usług elektronicznych (poczta elektroniczna, Intranet i Internet, telefonia stacjonarna i komórkowa)	ABT, ATS, AMS, ADO, Pełnomocnik ds. BI Dyrektor Generalny	w godzinach pracy GDOŚ, od momentu ogłoszenia drugiego stopnia alarmowego CRP
II.5	Dokonanie, w razie potrzeby, zmian w dostępie do systemów	Weryfikacja praw dostępu do kluczowych systemów teleinformatycznych GDOŚ	ABT, ATS, AMS, ADO, Pełnomocnik ds. BI Dyrektor Generalny	w godzinach pracy GDOŚ, od momentu ogłoszenia drugiego stopnia alarmowego CRP

II.6	Poinformowanie pracowników GDOŚ o konieczności zachowania zwiększonej czujności w stosunku do stanów odbiegających od normy, w szczególności pracowników odpowiedzialnych za bezpieczeństwo systemów	Przygotowanie informacji i powiadomienie wszystkich użytkowników systemów teleinformatycznych GDOŚ o możliwości wystąpienia zagrożeń teleinformatycznych i przeciwdziałaniu ich zmaterializowania się (komunikaty intranetowe oraz dedykowane e-maile)	Pełnomocnik ds. BI Dyrektor Generalny	realizacja w ciągu 2 godzin pierwszego dnia roboczego od momentu obowiązywania drugiego stopnia alarmowego CRP
II.7	Sprawdzenie kanałów łączności z innymi, właściwymi dla drugiego stopnia alarmowego CRP, podmiotami biorącymi udział w reagowaniu kryzysowym, dokonanie weryfikacji ustanowionych punktów kontaktowych z zespołami reagowania na incydenty bezpieczeństwa teleinformatycznego właściwymi dla GDOŚ	Sprawdzenie, aktualizacja i nawiązanie kontaktów telefonicznych i mailowych z Zespołem Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV Departamentu Bezpieczeństwa Teleinformatycznego Agencji Bezpieczeństwa Wewnętrznego: e-mail: incydent@csirt.gov.pl, telefon: +48 22 58 59 373, fax: +48 22 58 58 833.	Pełnomocnik ds. BI Dyrektor Generalny	realizacja w ciągu 2 godzin pierwszego dnia roboczego od momentu obowiązywania drugiego stopnia alarmowego CRP
II.8	Dokonanie przeglądu stosownych procedur oraz zadań związanych z wprowadzeniem drugiego stopnia alarmowego CRP, w szczególności dokonanie weryfikacji posiadanej kopii zapasowej systemów w stosunku do systemów teleinformatycznych	Dokonanie przeglądu wewnętrznych procedur operacyjnych Wydziału Informatyki. Weryfikacja aktualnego czasu wymaganego na przywrócenie poprawności funkcjonowania kluczowych systemów teleinformatycznych GDOŚ	ABT, ATS, AMS, Pełnomocnik ds. BI Dyrektor Generalny	realizacja w pierwszym dniu roboczym obowiązywania drugiego stopnia alarmowego CRP

	wchodzących w skład infrastruktury krytycznej oraz systemów kluczowych dla funkcjonowania GDOŚ oraz weryfikacji czasu wymaganego na przywrócenie poprawności funkcjonowania systemu			
II.9	Sprawdzenie aktualnego stanu bezpieczeństwa systemów i ocena wpływu zagrożenia na bezpieczeństwo teleinformatyczne na podstawie bieżących informacji i prognoz wydarzeń	Przeprowadzenie analizy ryzyka bezpieczeństwa teleinformatycznego oraz przygotowanie rekomendacji, zaleceń i działań zaradczych	ABT, ATS, AMS, Pełnomocnik ds. BI Dyrektor Generalny	realizacja w pierwszym dniu roboczym obowiązywania drugiego stopnia alarmowego CRP
II.10	Informowanie na bieżąco o efektach przeprowadzonych działań zespoły reagowania na incydenty bezpieczeństwa teleinformatycznego właściwe dla rodzaju działania GDOŚ	Informowanie zespołu CSIRT GOV poprzez dedykowany kontakt e-mailowy. Przygotowywanie notatek dla Dyrektora Generalnego	ABT, ATS, AMS, Pełnomocnik ds. BI Dyrektor Generalny	realizacja w godzinach pracy GDOŚ od momentu ogłoszenia drugiego stopnia alarmowego CRP
II.11	Zapewnienie dostępności w trybie alarmowym pracowników odpowiedzialnych za bezpieczeństwo systemów	Aktualizacja danych kontaktowych dyrektorów komórek organizacyjnych i ich zastępców oraz naczelników wydziałów w GDOŚ, i ustalenie dostępności kluczowych zasobów kadrowych w trybie alarmowym	Pełnomocnik ds. BI, Naczelnik Wydziału Informatyki Dyrektor Generalny	realizacja w ciągu 1 godziny od otrzymania informacji o wprowadzeniu drugiego stopnia alarmowego CRP
II.12	Sprawdzenie funkcjonowania zasilania awaryjnego	Upewnienie się czy administratorzy obiektów, w ramach realizacji swoich zadań, dokonali przeglądu działania awaryjnych źródeł zasilania	Naczelnik Wydziału Organizacyjnego, Naczelnik Wydziału	

		w energię elektryczną, w tym agregatów prądotwórczych oraz skontrolowali systemy automatycznego uruchamiania zasilania awaryjnego, a także dokonanie przeglądu działania awaryjnych źródeł zasilania w energie elektryczną UPS	Informatyki Dyrektor Biura Dyrektora Generalnego	
II.13	Wprowadzenie całodobowych dyżurów administratorów systemów kluczowych dla funkcjonowania GDOŚ oraz pracowników uprawnionych do podejmowania decyzji w sprawach bezpieczeństwa systemów teleinformatycznych	Opracowanie i uzgodnienie harmonogramu całodobowych dyżurów	Dyrektor Biura Dyrektora Generalnego, Pełnomocnik ds. BI, Naczelnik Wydziału Informatyki, Naczelnik Wydziału Organizacyjnego, Naczelnik Wydziału Kadr Dyrektor Generalny	realizacja w ciągu 2 godzin od otrzymania informacji o wprowadzeniu drugiego stopnia alarmowego CRP
II.14.1	Raportowanie o stanie realizacji zadań wynikających z wprowadzonego drugiego stopnia alarmowego CRP	Powiadomienie Dyrektora Generalnego na adres poczty elektronicznej sekretariat.bdg@gdos.gov.pl o zrealizowanych zadaniach w ramach wprowadzonego drugiego stopnia alarmowego CRP.	Pełnomocnik ds. BI Pełnomocnik ds. BI	realizacja nie później niż 8 godzin od otrzymania informacji o wprowadzeniu drugiego stopnia alarmowego CRP
II.14.2		Powiadomienie Dyrektora Generalnego o zrealizowanych zadaniach w ramach wprowadzonego drugiego stopnia alarmowego CRP.	ABT, ATS, AMS, Pełnomocnik ds. BI	realizacja nie później niż 4 godziny od otrzymania z RCB informacji o wprowadzeniu drugiego stopnia alarmowego CRP
II.14.3		Przekazanie do Dyrektora Generalnego raportu o stanie realizacji zadań wynikających z wprowadzonego drugiego stopnia alarmowego CRP.	Pełnomocnik ds. BI Pełnomocnik ds. BI	realizacja nie później niż 12 godzin od otrzymania z RCB informacji o wprowadzeniu drugiego stopnia alarmowego CRP
II.15.1	Odwołanie drugiego stopnia alarmowego CRP (stopień BRAVO-CRP)	Odebranie informacji o odwołaniu drugiego stopnia alarmowego CRP (stopień BRAVO-CRP)	pracownik ds. zarządzania kryzysowego lub sekretariat GDOŚ	realizować, jeżeli taki sygnał zostanie przekazany

			Generalny Dyrektor	
II.15.2		Przekazanie informacji dla pracowników GDOŚ o odwołaniu drugiego stopnia alarmowego CRP (stopień BRAVO-CRP)	Naczelnik Wydziału Komunikacji i Promocji Dyrektor Generalny	realizować, jeżeli taka informacja zostanie przekazana
II.15.3		Przekazanie informacji o odwołaniu drugiego stopnia alarmowego CRP (stopień BRAVO-CRP) do regionalnych dyrekcji ochrony środowiska, których odwołanie dotyczy	pracownik ds. zarządzania kryzysowego Generalny Dyrektor	realizować, jeżeli regionalne dyrekcje ochrony środowiska nie zostały powiadomione w inny sposób
III.	**Trzeci stopień alarmowy CRP (stopień CHARLIE-CRP)**			
III.1.1	Wprowadzenie trzeciego stopnia alarmowego CRP (stopień CHARLIE-CRP)	Odebranie informacji o wprowadzeniu trzeciego stopnia alarmowego CRP (stopień CHARLIE-CRP)	pracownik ds. zarządzania kryzysowego lub sekretariat GDOŚ Generalny Dyrektor	
III.1.2		Przekazanie informacji dla pracowników GDOŚ o wprowadzeniu trzeciego stopnia alarmowego CRP (stopień CHARLIE-CRP)	Naczelnik Wydziału Komunikacji i Promocji Dyrektor Generalny	
III.1.3		Przekazanie informacji o wprowadzeniu trzeciego stopnia alarmowego CRP (stopień CHARLIE-CRP) do regionalnych dyrekcji ochrony środowiska, których on dotyczy	pracownik ds. zarządzania kryzysowego Generalny Dyrektor	realizować, jeżeli regionalne dyrekcje ochrony środowiska nie zostały powiadomione w inny sposób
III.2	Wzmożone monitorowanie stanu bezpieczeństwa systemów teleinformatycznych	Analiza logów i innych danych wskazujących na potencjalne nieprawidłowości w funkcjonowaniu sieci, systemów i usług teleinformatycznych	ABT, ATS, AMS Dyrektor Generalny	w godzinach pracy GDOŚ, od momentu ogłoszenia trzeciego stopnia alarmowego CRP
III.3	Monitorowanie i weryfikacja, czy nie doszło do naruszenia bezpieczeństwa komunikacji elektronicznej	Reagowanie na incydenty i zgłoszenia teleinformatyczne	ABT, ATS, AMS, ADO, Pełnomocnik ds. BI Dyrektor Generalny	w godzinach pracy GDOŚ, od momentu ogłoszenia trzeciego stopnia alarmowego CRP

III.4	Sprawdzenie dostępności usług elektronicznych	Weryfikacja poprawności usług elektronicznych (poczta elektroniczna, Intranet i Internet, telefonia stacjonarna i komórkowa)	ABT, ATS, AMS, ADO, Pełnomocnik ds. BI Dyrektor Generalny	w godzinach pracy GDOŚ, od momentu ogłoszenia trzeciego stopnia alarmowego CRP
III.5	Dokonanie, w razie potrzeby, zmian w dostępie do systemów	Weryfikacja praw dostępu do kluczowych systemów teleinformatycznych GDOŚ	ABT, ATS, AMS, ADO, Pełnomocnik ds. BI Dyrektor Generalny	w godzinach pracy GDOŚ, od momentu ogłoszenia trzeciego stopnia alarmowego CRP
III.6	Poinformowanie pracowników GDOŚ o konieczności zachowania zwiększonej czujności w stosunku do stanów odbiegających od normy, w szczególności pracowników odpowiedzialnych za bezpieczeństwo systemów	Przygotowanie informacji i powiadomienie wszystkich użytkowników systemów teleinformatycznych GDOŚ o możliwości wystąpienia zagrożeń teleinformatycznych i przeciwdziałaniu ich zmaterializowania się (komunikaty intranetowe oraz dedykowane e-maile)	Pełnomocnik ds. BI Dyrektor Generalny	realizacja w ciągu 2 godzin pierwszego dnia roboczego od momentu obowiązywania trzeciego stopnia alarmowego CRP
III.7	Sprawdzenie kanałów łączności z innymi, właściwymi dla trzeciego stopnia alarmowego CRP, podmiotami biorącymi udział w reagowaniu kryzysowym, dokonanie weryfikacji ustanowionych punktów kontaktowych z zespołami reagowania na incydenty bezpieczeństwa	Sprawdzenie, aktualizacja i nawiązanie kontaktów telefonicznych i mailowych z Zespołem Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV Departamentu Bezpieczeństwa Teleinformatycznego Agencji Bezpieczeństwa Wewnętrznego: e-mail: incydent@csirt.gov.pl, telefon: +48 22 58 59 373, fax: +48 22 58 58 833.	Pełnomocnik ds. BI Dyrektor Generalny	realizacja w ciągu 2 godzin pierwszego dnia roboczego od momentu obowiązywania trzeciego stopnia alarmowego CRP

	teleinformatycznego właściwymi dla GDOŚ			
III.8	Dokonanie przeglądu stosownych procedur oraz zadań związanych z wprowadzeniem trzeciego stopnia alarmowego CRP, w szczególności dokonanie weryfikacji posiadanej kopii zapasowej systemów w stosunku do systemów teleinformatycznych wchodzących w skład infrastruktury krytycznej oraz systemów kluczowych dla funkcjonowania GDOŚ oraz weryfikacji czasu wymaganego na przywrócenie poprawności funkcjonowania systemu	Dokonanie przeglądu wewnętrznych procedur operacyjnych Wydziału Informatyki. Weryfikacja aktualnego czasu wymaganego na przywrócenie poprawności funkcjonowania kluczowych systemów teleinformatycznych GDOŚ	ABT, ATS, AMS, Pełnomocnik ds. BI Dyrektor Generalny	realizacja w pierwszym dniu roboczym obowiązywania trzeciego stopnia alarmowego CRP
III.9	Sprawdzenie aktualnego stanu bezpieczeństwa systemów i ocena wpływu zagrożenia na bezpieczeństwo teleinformatyczne na podstawie bieżących informacji i prognoz wydarzeń	Przeprowadzenie analizy ryzyka bezpieczeństwa teleinformatycznego oraz przygotowanie rekomendacji, zaleceń i działań zaradczych	ABT, ATS, AMS, Pełnomocnik ds. BI Dyrektor Generalny	realizacja w pierwszym dniu roboczym obowiązywania trzeciego stopnia alarmowego CRP
III.10	Informowanie na bieżąco o efektach przeprowadzonych działań zespoły reagowania na incydenty	Informowanie zespołu CSIRT GOV poprzez dedykowany kontakt e-mailowy. Przygotowywanie notatek dla Dyrektora Generalnego	ABT, ATS, AMS, Pełnomocnik ds. BI	realizacja w godzinach pracy GDOŚ od momentu ogłoszenia trzeciego stopnia alarmowego CRP

	bezpieczeństwa teleinformatycznego właściwe dla rodzaju działania GDOŚ		Dyrektor Generalny	
III.11	Zapewnienie dostępności w trybie alarmowym pracowników odpowiedzialnych za bezpieczeństwo systemów	Aktualizacja danych kontaktowych dyrektorów komórek organizacyjnych i ich zastępców oraz naczelników wydziałów w GDOŚ, i ustalenie dostępności kluczowych zasobów kadrowych w trybie alarmowym	Pełnomocnik ds. BI, Naczelnik Wydziału Informatyki Dyrektor Generalny	realizacja w ciągu 1 godziny od otrzymania informacji o wprowadzeniu trzeciego stopnia alarmowego CRP
III.12	Sprawdzenie funkcjonowania zasilania awaryjnego	Upewnienie się czy administratorzy obiektów, w ramach realizacji swoich zadań, dokonali przeglądu działania awaryjnych źródeł zasilania w energię elektryczną, w tym agregatów prądotwórczych oraz skontrolowali systemy automatycznego uruchamiania zasilania awaryjnego, a także dokonanie przeglądu działania awaryjnych źródeł zasilania w energie elektryczną UPS	Naczelnik Wydziału Organizacyjnego, Naczelnik Wydziału Informatyki Dyrektor Biura Dyrektora Generalnego	
III.13	Wprowadzenie całodobowych dyżurów administratorów systemów kluczowych dla funkcjonowania GDOŚ oraz pracowników uprawnionych do podejmowania decyzji w sprawach bezpieczeństwa systemów teleinformatycznych	Opracowanie i uzgodnienie harmonogramu całodobowych dyżurów	Dyrektor Biura Dyrektora Generalnego, Pełnomocnik ds. BI, Naczelnik Wydziału Informatyki, Naczelnik Wydziału Organizacyjnego, Naczelnik Wydziału Kadr Dyrektor Generalny	realizacja w ciągu 2 godzin od otrzymania informacji o wprowadzeniu trzeciego stopnia alarmowego CRP
III.14	Bieżące kierowanie cyberbezpieczeństwem	Przeprowadzenie posiedzenia „Zespołu zarządzania kryzysowego” (ZZK) Generalnej Dyrekcji Ochrony Środowiska	Zastępca Generalnego Dyrektora Ochrony Środowiska Generalny Dyrektor	realizacja, jeżeli istnieje taka potrzeba
III.15	Dokonanie przeglądu dostępnych zasobów	Przeciwdziałanie utracie lub zakłóceniu dostępu do zasobów sieci LAN; sprawdzenie poprawności	ABT, ATS,	realizacja w możliwie jak najkrótszym czasie od

	zapasowych pod względem możliwości ich wykorzystania w przypadku zaistnienia ataku cybernetycznego	wykonania backupów; testowe odtworzenie danych z kluczowych systemów teleinformatycznych	AMS Dyrektor Generalny	otrzymania informacji o wprowadzeniu trzeciego stopnia alarmowego CRP
III.16	Przygotowanie się do uruchomienia planów umożliwiających zachowanie ciągłości działania po wystąpieniu potencjalnego ataku cybernetycznego	Dokonanie przeglądu i ewentualnego audytu planów ciągłości działania i awaryjnych; przygotowanie się do ograniczenia operacji na serwerach, w celu możliwości ich szybkiego i bezawaryjnego zamknięcia	ABT, ATS, AMS, Pełnomocnik ds. BI Dyrektor Generalny	realizacja do 4 godzin od otrzymania informacji o wprowadzeniu trzeciego stopnia alarmowego CRP
III.17	Realizacja innych zadań i przedsięwzięć wynikających z bieżącej sytuacji teleinformatycznej	Sprawdzenie dostępności usług elektronicznych; awaryjna zmiana haseł dostępu do urządzeń brzegowych, systemu finansowo-księgowego na serwerze oraz systemów backupowych i archiwizacji; bieżące reagowanie na incydenty komputerowe i usuwanie podatności teleinformatycznych	ABT, ATS, AMS Dyrektor Generalny	realizacja do 30 minut od podjęcia decyzji o konieczności przeprowadzenia przedmiotowych działań
III.18.1	Raportowanie o stanie realizacji zadań wynikających z wprowadzonego trzeciego stopnia alarmowego CRP	Powiadomienie Dyrektora Generalnego na adres poczty elektronicznej sekretariat.bdg@gdos.gov.pl o zrealizowanych zadaniach w ramach wprowadzonego trzeciego stopnia alarmowego CRP	Pełnomocnik ds. BI Pełnomocnik ds. BI	realizacja nie później niż 8 godzin od otrzymania informacji o wprowadzeniu trzeciego stopnia alarmowego CRP
III.18.2		Powiadomienie Dyrektora Generalnego o zrealizowanych zadaniach w ramach wprowadzonego trzeciego stopnia alarmowego CRP	ABT, ATS, AMS Pełnomocnik ds. BI	realizacja nie później niż 4 godziny od otrzymania z RCB informacji o wprowadzeniu trzeciego stopnia alarmowego CRP
III.18.3		Przekazanie do Dyrektora Generalnego raportu o stanie realizacji zadań wynikających z wprowadzonego trzeciego stopnia alarmowego CRP	Pełnomocnik ds. BI Pełnomocnik ds. BI	realizacja nie później niż 12 godzin od otrzymania z RCB informacji o wprowadzeniu trzeciego

				stopnia alarmowego CRP
III.19.1	Odwołanie trzeciego stopnia alarmowego CRP (stopień CHARLIE-CRP)	Odebranie informacji o odwołaniu trzeciego stopnia alarmowego CRP (stopień CHARLIE-CRP)	pracownik ds. zarządzania kryzysowego lub sekretariat GDOŚ Generalny Dyrektor	realizować, jeżeli taki sygnał zostanie przekazany
III.19.2		Przekazanie informacji dla pracowników GDOŚ o odwołaniu trzeciego stopnia alarmowego CRP (stopień CHARLIE-CRP)	Naczelnik Wydziału Komunikacji i Promocji Dyrektor Generalny	realizować, jeżeli taka informacja zostanie przekazana
III.19.3		Przekazanie informacji o odwołaniu trzeciego stopnia alarmowego CRP (stopień CHARLIE-CRP) do regionalnych dyrekcji ochrony środowiska, których odwołanie dotyczy	pracownik ds. zarządzania kryzysowego Generalny Dyrektor	realizować, jeżeli regionalne dyrekcje ochrony środowiska nie zostały powiadomione w inny sposób
IV.	**Czwarty stopień alarmowy CRP (stopień DELTA-CRP)**			
IV.1.1	Wprowadzenie czwartego stopnia alarmowego CRP (stopień DELTA-CRP)	Odebranie informacji o wprowadzeniu czwartego stopnia alarmowego CRP (stopień DELTA-CRP)	pracownik ds. zarządzania kryzysowego lub sekretariat GDOŚ Generalny Dyrektor	
IV.1.2		Przekazanie informacji dla pracowników GDOŚ o wprowadzeniu czwartego stopnia alarmowego CRP (stopień DELTA-CRP)	Naczelnik Wydziału Komunikacji i Promocji Dyrektor Generalny	
IV.1.3		Przekazanie informacji o wprowadzeniu czwartego stopnia alarmowego CRP (stopień DELTA-CRP) do regionalnych dyrekcji ochrony środowiska, których on dotyczy	pracownik ds. zarządzania kryzysowego Generalny Dyrektor	realizować, jeżeli regionalne dyrekcje ochrony środowiska nie zostały powiadomione w inny sposób
IV.2	Wzmożone monitorowanie stanu bezpieczeństwa systemów teleinformatycznych	Analiza logów i innych danych wskazujących na potencjalne nieprawidłowości w funkcjonowaniu sieci, systemów i usług teleinformatycznych	ABT, ATS, AMS Dyrektor Generalny	w godzinach pracy GDOŚ, od momentu ogłoszenia czwartego stopnia alarmowego CRP
IV.3	Monitorowanie i weryfikacja, czy nie	Reagowanie na incydenty i zgłoszenia teleinformatyczne	ABT, ATS,	w godzinach pracy GDOŚ, od momentu ogłoszenia

	doszło do naruszenia bezpieczeństwa komunikacji elektronicznej		AMS, ADO, Pełnomocnik ds. BI Dyrektor Generalny	czwartego stopnia alarmowego CRP
IV.4	Sprawdzenie dostępności usług elektronicznych	Weryfikacja poprawności usług elektronicznych (poczta elektroniczna, Intranet i Internet, telefonia stacjonarna i komórkowa)	ABT, ATS, AMS, ADO, Pełnomocnik ds. BI Dyrektor Generalny	w godzinach pracy GDOŚ, od momentu ogłoszenia czwartego stopnia alarmowego CRP
IV.5	Dokonanie, w razie potrzeby, zmian w dostępie do systemów	Weryfikacja praw dostępu do kluczowych systemów teleinformatycznych GDOŚ	ABT, ATS, AMS, ADO, Pełnomocnik ds. BI Dyrektor Generalny	w godzinach pracy GDOŚ, od momentu ogłoszenia czwartego stopnia alarmowego CRP
IV.6	Poinformowanie pracowników GDOŚ o konieczności zachowania zwiększonej czujności w stosunku do stanów odbiegających od normy, w szczególności pracowników odpowiedzialnych za bezpieczeństwo systemów	Przygotowanie informacji i powiadomienie wszystkich użytkowników systemów teleinformatycznych GDOŚ o możliwości wystąpienia zagrożeń teleinformatycznych i przeciwdziałaniu ich zmaterializowania się (komunikaty intranetowe oraz dedykowane e-maile)	Pełnomocnik ds. BI Dyrektor Generalny	realizacja w ciągu 2 godzin pierwszego dnia roboczego od momentu obowiązywania czwartego stopnia alarmowego CRP
IV.7	Sprawdzenie kanałów łączności z innymi, właściwymi dla czwartego stopnia alarmowego CRP, podmiotami biorącymi udział w reagowaniu kryzysowym, dokonanie	Sprawdzenie, aktualizacja i nawiązanie kontaktów telefonicznych i mailowych z Zespołem Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV Departamentu Bezpieczeństwa Teleinformatycznego Agencji Bezpieczeństwa Wewnętrznego: e-mail: incydent@csirt.gov.pl,	Pełnomocnik ds. BI Dyrektor Generalny	realizacja w ciągu 2 godzin pierwszego dnia roboczego od momentu obowiązywania czwartego stopnia alarmowego CRP

	weryfikacji ustanowionych punktów kontaktowych z zespołami reagowania na incydenty bezpieczeństwa teleinformatycznego właściwymi dla GDOŚ	telefon: +48 22 58 59 373, fax: +48 22 58 58 833.		
IV.8	Dokonanie przeglądu stosownych procedur oraz zadań związanych z wprowadzeniem trzeciego stopnia alarmowego CRP, w szczególności dokonanie weryfikacji posiadanej kopii zapasowej systemów w stosunku do systemów teleinformatycznych wchodzących w skład infrastruktury krytycznej oraz systemów kluczowych dla funkcjonowania GDOŚ oraz weryfikacji czasu wymaganego na przywrócenie poprawności funkcjonowania systemu	Dokonanie przeglądu wewnętrznych procedur operacyjnych Wydziału Informatyki. Weryfikacja aktualnego czasu wymaganego na przywrócenie poprawności funkcjonowania kluczowych systemów teleinformatycznych GDOŚ	ABT, ATS, AMS, Pełnomocnik ds. BI Dyrektor Generalny	realizacja w pierwszym dniu roboczym obowiązywania czwartego stopnia alarmowego CRP
IV.9	Sprawdzenie aktualnego stanu bezpieczeństwa systemów i ocena wpływu zagrożenia na bezpieczeństwo teleinformatyczne na podstawie bieżących informacji i prognoz wydarzeń	Przeprowadzenie analizy ryzyka bezpieczeństwa teleinformatycznego oraz przygotowanie rekomendacji, zaleceń i działań zaradczych	ABT, ATS, AMS, Pełnomocnik ds. BI Dyrektor Generalny	realizacja w pierwszym dniu roboczym obowiązywania czwartego stopnia alarmowego CRP

IV.10	Informowanie na bieżąco o efektach przeprowadzonych działań zespoły reagowania na incydenty bezpieczeństwa teleinformatycznego właściwe dla rodzaju działania GDOŚ	Informowanie zespołu CSIRT GOV poprzez dedykowany kontakt e-mailowy. Przygotowywanie notatek dla Dyrektora Generalnego	ABT, ATS, AMS, Pełnomocnik ds. BI Dyrektor Generalny	realizacja w godzinach pracy GDOŚ od momentu ogłoszenia czwartego stopnia alarmowego CRP
IV.11	Zapewnienie dostępności w trybie alarmowym pracowników odpowiedzialnych za bezpieczeństwo systemów	Aktualizacja danych kontaktowych dyrektorów komórek organizacyjnych i ich zastępców oraz naczelników wydziałów w GDOŚ, i ustalenie dostępności kluczowych zasobów kadrowych w trybie alarmowym	Pełnomocnik ds. BI, Naczelnik Wydziału Informatyki Dyrektor Generalny	realizacja w ciągu 1 godziny od otrzymania informacji o wprowadzeniu czwartego stopnia alarmowego CRP
IV.12	Sprawdzenie funkcjonowania zasilania awaryjnego	Upewnienie się czy administratorzy obiektów, w ramach realizacji swoich zadań, dokonali przeglądu działania awaryjnych źródeł zasilania w energię elektryczną, w tym agregatów prądotwórczych oraz skontrolowali systemy automatycznego uruchamiania zasilania awaryjnego, a także dokonanie przeglądu działania awaryjnych źródeł zasilania w energie elektryczną UPS	Naczelnik Wydziału Organizacyjnego, Naczelnik Wydziału Informatyki Dyrektor Biura Dyrektora Generalnego	
IV.13	Wprowadzenie całodobowych dyżurów administratorów systemów kluczowych dla funkcjonowania GDOŚ oraz pracowników uprawnionych do podejmowania decyzji w sprawach bezpieczeństwa systemów teleinformatycznych	Opracowanie i uzgodnienie harmonogramu całodobowych dyżurów	Dyrektor Biura Dyrektora Generalnego, Pełnomocnik ds. BI, Naczelnik Wydziału Informatyki, Naczelnik Wydziału Organizacyjnego, Naczelnik Wydziału Kadr Dyrektor Generalny	realizacja w ciągu 2 godzin od otrzymania informacji o wprowadzeniu czwartego stopnia alarmowego CRP
IV.14	Bieżące kierowanie cyberbezpieczeństwem	Przeprowadzenie posiedzenia „Zespołu zarządzania kryzysowego” (ZZK) Generalnej Dyrekcji Ochrony	Zastępca Generalnego Dyrektora	realizacja, jeżeli istnieje taka potrzeba

		Środowiska	Ochrony Środowiska Generalny Dyrektor	
IV.15	Dokonanie przeglądu dostępnych zasobów zapasowych pod względem możliwości ich wykorzystania w przypadku zaistnienia ataku cybernetycznego	Przeciwdziałanie utracie lub zakłóceniu dostępu do zasobów sieci LAN; sprawdzenie poprawności wykonania backupów; testowe odtworzenie danych z kluczowych systemów teleinformatycznych	ABT, ATS, AMS Dyrektor Generalny	realizacja w możliwie jak najkrótszym czasie od otrzymania informacji o wprowadzeniu czwartego stopnia alarmowego CRP
IV.16	Przygotowanie się do uruchomienia planów umożliwiających zachowanie ciągłości działania po wystąpieniu potencjalnego ataku cybernetycznego	Dokonanie przeglądu i ewentualnego audytu planów ciągłości działania i awaryjnych; przygotowanie się do ograniczenia operacji na serwerach, w celu możliwości ich szybkiego i bezawaryjnego zamknięcia	ABT, ATS, AMS, Pełnomocnik ds. BI Dyrektor Generalny	realizacja do 4 godzin od otrzymania informacji o wprowadzeniu czwartego stopnia alarmowego CRP
IV.17.1	Realizacja innych zadań i przedsięwzięć wynikających z bieżącej sytuacji teleinformatycznej	Sprawdzenie dostępności usług elektronicznych; awaryjna zmiana haseł dostępu do urządzeń brzegowych, systemu finansowo-księgowego na serwerze oraz systemów backupowych i archiwizacji; bieżące reagowanie na incydenty komputerowe i usuwanie podatności teleinformatycznych	ABT, ATS, AMS Dyrektor Generalny	realizacja do 30 minut od podjęcia decyzji o konieczności przeprowadzenia przedmiotowych działań
IV.17.2		Współpraca ze stronami umów na świadczenie usług teleinformatycznych w zakresie przywracania ciągłości kluczowych systemów teleinformatycznych; przegląd procedur i zadań związanych z zapewnieniem ciągłości funkcjonowania kluczowych systemów teleinformatycznych w przypadku braku możliwości realizacji zadań GDOŚ w dotychczasowym miejscu pracy; przygotowanie się do przemieszczenia do zapasowego miejsca pracy w sytuacji jednoczesnego	ABT, ATS, AMS, Pełnomocnik ds. BI, dyrektorzy komórek organizacyjnych GDOŚ będący gestorami systemów teleinformatycznych utrzymywanych przez	sprawdzenie procedur przemieszczenia się GDOŚ do zapasowego miejsca pracy, określonych w „POF GDOŚ”

		wprowadzenia wyższych stanów gotowości obronnej państwa	wykonawców zewnętrznych Dyrektor Generalny	
IV.18	Uruchomienie planów awaryjnych lub planów ciągłości działania GDOŚ w zakresie cyberbezpieczeństwa w sytuacjach awarii lub utraty ciągłości działania	Stosownie do sytuacji przystąpienie do realizacji procedur przywracania ciągłości działania w zakresie funkcjonowania kluczowych systemów teleinformatycznych oraz łączności telefonicznej; uruchomienie zapasowego łącza internetowego oraz usług telefonicznych	ABT, ATS, AMS, Pełnomocnik s.. BI Dyrektor Generalny	niezwłocznie po otrzymaniu informacji o wprowadzeniu czwartego stopnia alarmowego CRP
IV.19.1	Raportowanie o stanie realizacji zadań wynikających z wprowadzonego czwartego stopnia alarmowego CRP	Powiadomienie Dyrektora Generalnego na adres poczty elektronicznej sekretariat.bdg@gdos.gov.pl o zrealizowanych zadaniach w ramach wprowadzonego czwartego stopnia alarmowego CRP	Pełnomocnik ds. BI Pełnomocnik ds. BI	realizacja nie później niż 8 godzin od otrzymania informacji o wprowadzeniu czwartego stopnia alarmowego CRP
IV.19.2		Powiadomienie Dyrektora Generalnego o zrealizowanych zadaniach w ramach wprowadzonego czwartego stopnia alarmowego CRP	ABT, ATS, AMS Pełnomocnik ds. BI	realizacja nie później niż 4 godziny od otrzymania z RCB informacji o wprowadzeniu czwartego stopnia alarmowego CRP
IV.19.3		Przekazanie do Dyrektora Generalnego raportu o stanie realizacji zadań wynikających z wprowadzonego czwartego stopnia alarmowego CRP	Pełnomocnik ds. BI Pełnomocnik ds. BI	realizacja nie później niż 12 godzin od otrzymania z RCB informacji o wprowadzeniu czwartego stopnia alarmowego CRP
IV.20.1	Odwołanie czwartego stopnia alarmowego CRP (stopień DELTA-CRP)	Odebranie informacji o odwołaniu czwartego stopnia alarmowego CRP (stopień DELTA-CRP)	pracownik ds. zarządzania kryzysowego lub sekretariat GDOŚ Generalny Dyrektor	realizować, jeżeli taki sygnał zostanie przekazany
IV.20.2		Przekazanie informacji dla pracowników GDOŚ o odwołaniu czwartego stopnia alarmowego CRP (stopień DELTA-CRP)	Naczelnik Wydziału Komunikacji i Promocji Dyrektor Generalny	realizować, jeżeli taka informacja zostanie przekazana
IV.20.3		Przekazanie informacji o odwołaniu czwartego	pracownik ds.	realizować, jeżeli

		stopnia alarmowego CRP (stopień DELTA-CRP) do regionalnych dyrekcji ochrony środowiska, których odwołanie dotyczy	zarządzania kryzysowego Generalny Dyrektor	regionalne dyrekcje ochrony środowiska nie zostały powiadomione w inny sposób

Objaśnienia:

- użyte w treści modułów zadaniowych wyrażenie „*Dyrektor Generalny”* oznacza *Dyrektora Generalnego GDOŚ*,
- użyte w treści modułów zadaniowych wyrażenie „*Generalny Dyrektor”* oznacza *Generalnego Dyrektora Ochrony Środowiska*,
- użyte w treści modułów zadaniowych wyrażenie „*Pełnomocnik ds. BI*” oznacza *Pełnomocnika do spraw Bezpieczeństwa Informacji*,
- użyty w treści modułów zadaniowych skrót „*ABT”* oznacza *Administratora Bezpieczeństwa Teleinformatycznego*,
- użyty w treści modułów zadaniowych skrót „*ADO”* oznacza *Administratora Danych Osobowych*,
- użyty w treści modułów zadaniowych skrót „*AMS”* oznacza *Administratora Merytorycznego Systemu*,
- użyty w treści modułów zadaniowych skrót „*ATS”* oznacza *Administratora Technicznego Systemu,*
- użyty w treści modułów zadaniowych skrót „*GDOŚ”* oznacza *Generalną Dyrekcję Ochrony Środowiska*,
- użyty w treści modułów zadaniowych skrót „*RCB”* oznacza *Rządowe Centrum Bezpieczeństwa*,
- użyty w treści IV modułu zadaniowego skrót *„POF GDOŚ”* oznacza *„Plan operacyjny funkcjonowania Generalnej Dyrekcji Ochrony Środowiska w warunkach zewnętrznego zagrożenia bezpieczeństwa państwa i w czasie wojny”*.