
RFC 2350

Opis zespołu reagowania na incydenty cyberbezpieczeństwa Zarząd Morskiego Portu Gdynia S.A.

1. Informacje o dokumencie

Niniejszy dokument zawiera opis zespołu odpowiedzialnego za obsługę incydentów cyberbezpieczeństwa w Spółce Zarząd Morskiego Portu Gdynia S.A. (dalej: ZMPG) zgodnie z wytycznymi RFC 2350.

Dokument dostarcza podstawowych informacji dotyczących zespołu, sposobów kontaktu, zakresu odpowiedzialności oraz świadczonych usług w zakresie cyberbezpieczeństwa.

1.1 Data ostatniej aktualizacji

Wersja dokumentu: 1.0

Data publikacji: 13 marca 2026 r.

1.2 Dystrybucja dokumentu

Dokument jest publicznie dostępny i przeznaczony dla wszystkich podmiotów zainteresowanych współpracą w zakresie reagowania na incydenty cyberbezpieczeństwa.

1.3 Miejsce publikacji dokumentu

Aktualna wersja dokumentu dostępna jest na stronie internetowej:

<https://www.port.gdynia.pl>

Należy upewnić się, że wykorzystywana jest najnowsza wersja dokumentu.

1.4 Autentyczność dokumentu

Autentyczność dokumentu wynika z jego publikacji na oficjalnej stronie internetowej ZMPG.

2. Dane kontaktowe

2.1 Nazwa zespołu

Pełna nazwa: **Zespół Reagowania na Incydenty Cyberbezpieczeństwa ZMPG**

Skrócona nazwa: **ZMPG-IT**

2.2 Organizacja

Zarząd Morskiego Portu Gdynia S.A.

2.3 Adres

ul. Rotterdamska 9

81-337 Gdynia

Polska

2.4 Strefa czasowa

UTC +0100 – Czas środkowoeuropejski (CET)

UTC +0200 – Czas środkowoeuropejski letni (CEST)

2.5 Numer telefonu

+48 586213388

2.6 Inne środki komunikacji

Brak.

2.7 Adres poczty elektronicznej

incydent@port.gdynia.pl

2.8 Informacje o szyfrowaniu

Zespół ZMPG-IT nie publikuje obecnie klucza PGP.

W przypadku konieczności przekazania informacji poufnych sposób bezpiecznej wymiany danych może zostać uzgodniony indywidualnie pomiędzy stronami komunikacji.

2.9 Członkowie zespołu

Zespół ZMPG-IT składa się ze specjalistów w dziedzinie cyberbezpieczeństwa oraz administratorów systemów informatycznych odpowiedzialnych za bezpieczeństwo infrastruktury teleinformatycznej Portu Gdynia.

2.10 Dodatkowe informacje

Informacje dotyczące cyberbezpieczeństwa i aktualnych zagrożeń mogą być publikowane na stronie internetowej organizacji.

2.11 Punkt kontaktowy dla zgłoszeń

Preferowaną metodą kontaktu z zespołem ZMPG-IT jest poczta elektroniczna:

incydent@port.gdynia.pl

Jeżeli korzystanie z poczty elektronicznej nie jest możliwe lub nie jest wskazane ze względów bezpieczeństwa, z zespołem można skontaktować się telefonicznie.

Godziny pracy zespołu są ograniczone do regularnych godzin pracy organizacji (7:30-15:30 od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy).

3. Statut

3.1 Misja

Misją zespołu ZMPG-IT jest zwiększanie poziomu bezpieczeństwa systemów teleinformatycznych wykorzystywanych przez ZMPG poprzez wykrywanie, analizowanie oraz reagowanie na incydenty cyberbezpieczeństwa.

Zespół wspiera organizację w ograniczaniu skutków incydentów oraz zwiększaniu odporności infrastruktury informatycznej.

3.2 Zakres działania

Zakres działania zespołu ZMPG-IT obejmuje systemy informatyczne, sieci teleinformatyczne oraz infrastrukturę IT zarządzaną przez ZMPG.

3.3 Finansowanie i przynależność

ZMPG-IT jest jednostką organizacyjną działającą w strukturze ZMPG.

Zespół jest finansowany i wspierany przez organizację.

3.4 Umocowanie

Zespół ZMPG-IT działa na podstawie:

- wewnętrznych regulacji organizacji,
- polityki bezpieczeństwa informacji,
- obowiązujących przepisów prawa w zakresie cyberbezpieczeństwa.

4. Polityki

4.1 Typy incydentów i poziom wsparcia

Zespół ZMPG-IT obsługuje incydenty cyberbezpieczeństwa obejmujące między innymi:

- złośliwe oprogramowanie,
- phishing,
- nieautoryzowany dostęp,
- naruszenia integralności systemów,
- wycieki danych,
- ataki typu DDoS,
- inne zdarzenia wpływające na bezpieczeństwo systemów IT.

Poziom wsparcia zależy od charakteru incydentu, jego wpływu na działalność organizacji oraz dostępności zasobów zespołu.

4.2 Współpraca i wymiana informacji

Zespół ZMPG-IT współpracuje z krajowymi zespołami reagowania na incydenty, w szczególności z:

- CSIRT NASK
- CSIRT GOV
- CSIRT MON

Wymiana informacji odbywa się zgodnie z obowiązującymi przepisami prawa oraz wewnętrznymi regulacjami organizacji.

4.3 Komunikacja i uwierzytelnianie

Preferowaną metodą komunikacji z zespołem ZMPG-IT jest poczta elektroniczna.

W przypadku przekazywania informacji poufnych mogą zostać uzgodnione dodatkowe mechanizmy zabezpieczenia komunikacji.

Autentyczność zgłoszeń może być weryfikowana poprzez kontakt zwrotny lub inne uzgodnione metody.

5. Usługi

5.1 Reagowanie na incydenty

Zespół ZMPG-IT realizuje działania związane z obsługą incydentów cyberbezpieczeństwa, w tym:

- analizę zgłoszeń,
 - koordynację działań reagowania,
 - wsparcie przy usuwaniu skutków incydentów.
-

5.2 Monitorowanie

Zespół prowadzi działania mające na celu wykrywanie zdarzeń bezpieczeństwa oraz analizę ich przyczyn i potencjalnych skutków.

5.3 Działania prewencyjne

Działania obejmują identyfikację podatności systemów informatycznych oraz analizę zagrożeń cybernetycznych.

5.4 Działania proaktywne

Zespół prowadzi działania zwiększające poziom świadomości bezpieczeństwa, w tym szkolenia oraz publikację informacji dotyczących zagrożeń cybernetycznych.

6. Zgłaszanie incydentów

Zgłoszenia incydentów cyberbezpieczeństwa należy kierować na adres:

incydent@port.gdynia.pl

W zgłoszeniu należy w miarę możliwości podać:

- dane kontaktowe osoby zgłaszającej,
 - datę i czas zdarzenia,
 - opis incydentu,
 - systemy objęte incydemtem,
 - dane techniczne (np. adresy IP, logi systemowe),
 - opis podjętych działań.
-

7. Zastrzeżenia

Pomimo zachowania należytej staranności przy przygotowaniu niniejszego dokumentu, ZMPG nie ponosi odpowiedzialności za ewentualne błędy lub pominięcia ani za szkody wynikające z wykorzystania informacji zawartych w tym dokumencie.