FORMULARZ ZGŁASZANIA INCYDENTÓW **CSIRT MON**

DANE ADRESOWE

1. Nazwa instytucji / firmy*
2. Adres*
3. Kod pocztowy
4. Miasto*
5. NIP

ZGŁASZAJĄCY INCYDENT

6. Imię i Nazwisko*
7. Stanowisko*
8. Tel.* dostępność ☐ 8-16 ☐ 8-22 ☐ 24h
9. e-mail*

OSOBA UPRAWNIONA DO SKŁADANIA WYJAŚNIEŃ W SPRAWIE INCYDENTU

10. Imię i Nazwisko*
11. Stanowisko*
12. Tel.* dostępność ☐ 8-16 ☐ 8-22 ☐ 24h
13. e-mail*

OPIS INCYDENTU

14. Data wystąpienia incydentu* Czas trwania incydentu
15. Data wykrycia incydentu*
16. Pola stanowiące tajemnice prawnie chronione, w tym przedsiębiorstwa (podaj nr pól po przecinku lub w przedziale np. 4. – 8.)
17. Zadanie publiczne na które incydent miał wpływ*
18. Liczba osób, na które incydent miał wpływ* ☐ 1-50 ☐ 51-100 ☐ 101-200 ☐ 201-300 ☐ >300 ☐ Brak danych
19. Zasięg geograficzny obszaru, którego dotyczył incydent* ☐ Instytucja ☐ Polska ☐ Unia Europejska ☐ Świat ☐ Brak danych
20. Rodzaj działania* ☐ Celowe ☐ Niecelowe

21. Kategoria zdarzenia*

- ☐ Treści obraźliwe |np. obrażanie , pornografia dziecięca, przemoc
- ☐ Oprogramowanie złośliwe | np. wirus, trojan, ransomware, dialer, botnet
- ☐ Zbieranie informacji | np.. skanowanie, podsłuch, SPAM, inżynieria społeczna
- ☐ Próby włamania | np. próby wykorzystania znanych błędów, próby logowania
- ☐ Włamanie | np. włamanie na konto, do aplikacji, do systemu, do infrastruktury
- ☐ Utrata dostępności usługi | np. DoS, DDoS, sabotaż, awaria, zaniedbanie, prace techniczne
- ☐ Bezpieczeństwo informacji | np. nieuprawniony dostęp do informacji, nieuprawniona zmiana informacji lub jej skasowanie
- ☐ Oszustwo | np. nieuprawnione wykorzystanie zasobów, naruszenie praw autorskich, podszycie się, kradzież tożsamości, phishing
- ☐ Podatność | np. błędna konfiguracja, wykrycie podatności
- ☐ Cyberterroryzm | zdarzenie o charakterze terrorystycznym popełnione w cyberprzestrzeni
- ☐ Inne | zdarzenie niemieszczące się w powyższych kategoriach
- ☐ Test |kategoria ćwiczebna

22. Skutki incydentu*

- ☐ utrata dostępności danych / usług
- ☐ utrata poufności danych / usług
- ☐ utrata integralności danych / usług
- ☐ próba infekcji oprogramowaniem złośliwym
- ☐ próba uzyskania nieuprawnionego dostępu
- ☐ inne

dodatkowe informacje

23. Przebieg incydentu oraz możliwa przyczyna jego wystąpienia*

24. Podjęte działania zapobiegawcze*

25. Podjęte działania naprawcze*

26. Inne istotne informacje

27. Kategoria TLP**

- ☐ White
- ☐ Green
- ☐ Amber
- ☐ Red

***Pola wymagane**
****TLP (Traffic Light Protocol**) – protokół wymiany informacji określający możliwość propagacji informacji oraz grupę odbiorców.

TLP: RED – Odbiorcy nie mogą dzielić się informacjami z nikim, z wyjątkiem innych odbiorców tych wiadomości.
TLP: AMBER – Odbiorcy mogą dzielić się informacjami jedynie w obrębie swojej organizacji z osobami, które muszą poznać te informacje oraz jedynie w zakresie niezbędnych do podjęcia działań.
TLP: GREEN – Odbiorcy mogą dzielić się informacjami ze swoimi współpracownikami, w ramach swojej i partnerskich organizacji oraz swoim środowisku. Nie można jednak udostępniać tych informacji przez publiczne kanały informacyjne.
TLP: WHITE – Dystrybucja informacji Ne podlega żadnym ograniczeniom (z wyjątkiem praw autorskich).

Wypełniony formularz należy wysłać w postaci załącznika do wiadomości e-mail na adres: csirt-mon@ron.mil.pl