

**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.\*

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 stanowiące tajemnicę przedsiębiorstwa (podaj nr pól po przecinku lub w przedziale np. 4. -8.)

17. Zadanie publiczne/usługa na które incydent miał wpływ\*

18. Liczba osób, na które incydent miał wpływ\*  1 - 50  50 - 500  500 - 1.000  
 1.000 - 10.000  > 10.000  Brak danych

19. Zasięg geograficzny obszaru, którego dotyczy incydent\*  Instytucja  Miejscowość/Gmina/Województwo  Polska  
 Unia Europejska  Świat  Brak danych

20. Kategoria zdarzenia\*

- Podejrzana wiadomość e-mail | podejrzane załączniki, phishing, szantaż
  - Złośliwe oprogramowanie | trojan, banker, spyware, ransomware, zagrożenia mobilne
  - Oszustwa internetowe | fałszywa działalność w sieci, kradzież tożsamości,
  - Włamania | serwer, aplikacja, konto, system, itp.
  - Utrata dostępności usługi | DoS, DDoS, sabotaż, awaria, zaniedbanie, prace techniczne
  - Naruszenia bezpieczeństwa informacji | nieuprawniony dostęp do informacji, nieuprawniona zmiana informacji lub jej skasowanie
  - Podatności | błędy w oprogramowaniu lub aplikacjach
  - Nielegalne treści | zgłoszenia przeznaczone dla Zespołu Dyżurnet.pl
  - Cyberterroryzm | działania o charakterze terrorystycznym popełnione w sieci
  - Inne | wszystkie inne niewskazane powyżej
- 

21. Przebieg incydentu oraz  
możliwa przyczyna jego  
wystąpienia\*

22. Skutki oddziaływania  
incydentu na systemy  
informacyjne firmy/institucji\*

23. Podjęte działania  
zapobiegawcze\*

24. Podjęte działania  
naprawcze\*

25. Inne istotne informacje