Załącznik nr 1 do Procedury zarządzania incydentami cyberbezpieczeństwa	**RAPORT INCYDENTU CYBERBEZPIECZEŃSTWA**

RAPORT INCYDENTU CYBERBEZPIECZEŃSTWA

I. OPIS INCYDENTU

1. Data ..... Godzina .....
2. Osoba powiadamiająca o incydencie oraz inne osoby zaangażowane lub odpytane w związku z incydentem (imię, nazwisko, stanowisko służbowe, dane kontaktowe):

.....

3. Lokalizacja zdarzenia *(nr. pokoju, nazwa pomieszczenia, określenie komputerowego stanowiska roboczego, nazwa programu lub aplikacji itp.):*

.....

II ANALIZA INCYDENTU

1. Zadanie publiczne, którego dotyczy zgłoszenie:

……

2. Liczba osób na które incydent miał wpływ

.....

3. Moment wystąpienia i wykrycia incydentu oraz czas jego trwania

.....

4. Zasięg geograficzny obszaru którego incydent dotyczy

.....

5. Przyczyna zaistnienia incydentu:

☐ Podejrzana wiadomość e-mail
☐ Próba oszustwa
☐ Nielegalne treści
☐ Podatności
☐ Złośliwe oprogramowanie
☐ Inny …….

10. Sposób przebiegu incydentu

……..

11. Skutki oddziaływania incydentu na systemy informacyjne podmiotu publicznego

……..

12. Przyczyna i źródło incydentu

……..

13. Informacja o podjętych działaniach zapobiegawczych

……

14. Informacja o podjętych lub planowanych działaniach naprawczych

……

15. Czy doszło do naruszenia danych osobowych

☐ TAK ☐ NIE

W przypadku naruszenia danych osobowych należy dodatkowo uruchomić procedurę zgłaszania naruszeń związanych z ochroną danych osobowych.

W przypadku naruszenia danych osobowych podać nr zgłoszenia z rejestru naruszeń ochrony danych osobowych ……

W przypadku informacji dotyczącej nielegalnych treści zgłoszenie należy przesłać do zespołu Dyżurnet.pl

.....

(podpisy osób obsługujących incydent)

* Do Raportu należy dołączyć kopię zgłoszenia do CSIRT NASK.

Załącznik nr 2 do Procedury zarządzania incydentami cyberbezpieczeństwa	**REJESTR INCYDENTÓW CYBERBEZPIECZEŃSTWA**

REJESTR INCYDENTÓW CYBERBEZPIECZEŃSTWA

Lp.	Data zgłoszenia	Zadanie publiczne, którego dotyczy zgłoszenie	Opis zdarzenia	Kategoria incydentu	Podjęte działania zapobiegawcze	Podjęte działania naprawcze
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						
10.						

Kategorie incydentu:
A – Podejrzana wiadomość e-mail
B – Próba oszustwa
C – Podatności
D – Złośliwe oprogramowanie
E – Nielegalne treści
F - Inny incydent

Załącznik nr 3 do Procedury zarządzania incydentami cyberbezpieczeństwa	**Wykaz osób zapoznanych z Procedurą zarządzania incydentami cyberbezpieczeństwa**

Wykaz osób zapoznanych
z Procedurą zarządzania incydentami cyberbezpieczeństwa

Lp.	Imię i nazwisko pracownika	Podpis
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		
16.		
17.		
18.		
19.		
20.		