FORMULARZ ZGŁASZANIA INCYDENTÓW CYBERBEZPIECZEŃSTWA GMINY LUBLIN

CZĘŚĆ A: DANE GMINY LUBLIN	
1. Nazwa podmiotu zgłaszającego	**Gmina Lublin**
2. Siedziba i adres zgłaszającego	**plac Króla Władysława Łokietka 1, 20-109 Lublin**
3. NIP zgłaszającego	**9462575811**
CZĘŚĆ B: DANE ZGŁASZAJĄCEJ JEDNOSTKI ORGANIZACYJNEJ (uzupełnia osoba zgłaszająca z jednostki organizacyjnej, w której wystąpił incydent)	
4. Pełna nazwa jednostki organizacyjnej, w której wystąpił incydent *	
5. Siedziba i adres jednostki organizacyjnej, w której wystąpił incydent *	
CZĘŚĆ C: DANE OSOBY ZGŁASZAJĄCEJ Z JEDNOSTKI ORGANIZACYJNEJ (uzupełnia osoba zgłaszająca z jednostki organizacyjnej, w której wystąpił incydent)	
6. Imię i nazwisko osoby z jednostki organizacyjnej, zgłaszającej incydent *	
7. Stanowisko służbowe osoby z jednostki organizacyjnej, zgłaszającej incydent *	
8. Numer telefonu służbowego osoby z jednostki organizacyjnej, zgłaszającej incydent *	**Dostępność podanego numeru:** ○ **7:30 – 15:30** ○ **w godzinach :** ○ **24h**
9. Adres poczty elektronicznej osoby z jednostki organizacyjnej, zgłaszającej incydent *	
CZĘŚĆ D: OSOBA UPRAWNIONA DO SKŁADANIA WYJAŚNIEŃ W SPRAWIE INCYDENTU	
10. Imię i nazwisko osoby uprawnionej do składania wyjaśnień dotyczących zgłaszanych informacji	Pan **Andrzej Wojewódzki** – Pełnomocnik Prezydenta Miasta Lublin ds. Systemu Zarządzania Bezpieczeństwem Informacji oraz Pan **Witold Przeszlakowski** – Dyrektor Biura Bezpieczeństwa Informacji Urzędu Miasta Lublin
11. Numer telefonu służbowego osoby uprawnionej do składania wyjaśnień dotyczących zgłaszanych informacji	tel. **814662010** lub **814661770** dostępny w godzinach **7:30 – 15:30**
12. Adres poczty elektronicznej osoby uprawnionej do składania wyjaśnień dotyczących zgłaszanych informacji	cyberkontakt@lublin.eu

CZĘŚĆ E: OPIS INCYDENTU (uzupełnia osoba zgłaszająca z jednostki organizacyjnej, w której wystąpił incydent)	
13. Data wystąpienia incydentu * **orientacyjny czas trwania incydentu**	**podany czas jest** ○ **przybliżony** ○ **dokładny**
14. Data wykrycia incydentu * **oraz stan incydentu** **incydent nadal trwa/wygasł/został obsłużony**	○ **nadal trwa** ○ **wygasł** ○ **został obsłużony**
15. Zadanie publiczne, na które incydent miał wpływ *	
16. Liczba osób, na które incydent miał wpływ *	○ **1 – 50** ○ **51 – 500** ○ **501 – 1.000** ○ **l.000 – 10.000** ○ **> 10.000** ○ **brak danych**
17. Zasięg geograficzny obszaru, którego dotyczy incydent *	○ **Instytucja** ○ **Miasto/Województwo** ○ **Polska** ○ **Unia Europejska** ○ **Świat** ○ **brak danych**
18. Rodzaj działania * **Celowe–świadome / Niecelowe–nieświadome**	○ **Celowe** ○ **Niecelowe**

19. Kategoria zdarzenia *	☐ **Podejrzana wiadomość e–mail | np. podejrzane załączniki, phishing, szantaż** ☐ **Zbieranie informacji | np. skanowanie, podsłuch, SPAM, inżynieria społeczna** ☐ **Treści obraźliwe | np. obrażanie, pornografia dziecięca, przemoc i inne nielegalne treści (informacje dla zespołu Dyzurnet.pl)** ☐ **Oprogramowanie złośliwe | np. wirus, trojan, ransomware, dialer, botnet** ☐ **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 autorski, podszywanie się, kradzież tożsamości** ☐ **Podatność | np. błędna konfiguracja, wykrycie podatności** ☐ **Cyberterroryzm | zdarzenie o charakterze terrorystycznym popełnione w cyberprzestrzeni** ☐ **Inne | zdarzenia niemieszczące się w powyższych kategoriach** ☐ **Test | kategoria ćwiczebna**
20. Skutki oddziaływania incydentu na systemy informacyjne Instytucji *	☐ **utrata dostępności danych / usługi** ☐ **utrata poufności danych / usługi** ☐ **utrata integralności danych / usługi** ☐ **próba infekcji oprogramowaniem złośliwym** ☐ **próba uzyskania nieuprawnionego dostępu** ☐ **inne**
dodatkowe informacje	

21. Przebieg incydentu oraz możliwa przyczyna jego wystąpienia *	
22. Podjęte działania zapobiegawcze *	
23. Podjęte działania naprawcze *	

24. Inne istotne informacje *	
25. Pola stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa (podaj nr pól po przecinku lub w przedziale np. 16. – 24.)	

Pola oznaczone * są polami wymaganymi.

Wypełniony formularz należy niezwłocznie wysłać w postaci załącznika do wiadomości e-mail na adres: **cyberincydent@lublin.eu** .

Jeśli pojawią się nowe informacje dotyczące incydentu należy niezwłocznie je przekazać uzupełniając formularz i przekazując go również na adres cyberincydent@lublin.eu