Formularz zgłaszania incydentów do Cyber360-CSIRT

Dane podmiotu zgłaszającego *		
Nazwa podmiotu *		
NIP/REGON/KRS *		
Adres: *	**Ulica**	
	Nr domu	
	Nr mieszkania	
	Miejscowość	
	Kod pocztowy	
	Województwo	
Dane osoby zgłaszającej incydent: *		
Imię		
Nazwisko		
Stanowisko / Funkcja		
E-mail		
Nr telefonu		
Uwagi w zakresie dostępności i preferowanej metody kontaktu (telefon, e-mail)		
Dane osoby upoważnionej do składania wyjaśnień w sprawie incydentu: **		
Imię		
Nazwisko		
Stanowisko / Funkcja		
E-mail		
Nr telefonu		
Uwagi w zakresie dostępności i preferowanej metody kontaktu (telefon, e-mail)		

* Pola obowiązkowe

** Nie dotyczy jeśli osobą kontaktową do wyjaśnienia incydentu jest osoba zgłaszająca incydent

Opis incydentu:	
Klasyfikacja incydentu (poważny, istotny, inny) *	
Data i godzina wykrycia incydentu *	
Data i godzina wystąpienia incydentu *	
Czas trwania incydentu *	
Usługi, systemy i sieci teleinformatyczne, na które incydent miał wpływ *	
Liczba osób, na które incydent miał wpływ *	
Czy incydent dotyczy innych państw członkowskich Unii Europejskiej? (należy podać jakich) *	
Zasięg geograficzny obszaru, którego dotyczy incydent (np. lokalizacje oddziałów firmy) *	
Charakter zdarzenia (np. działanie zamierzone lub niezamierzone, wewnętrzne lub zewnętrzne, trudne do określenia) *	
Skutki incydentu (utrata dostępności, poufności, integralności, inne) *	
Dodatkowe informacje **	

Przebieg incydentu oraz możliwa przyczyna jego wystąpienia *		
Kategoria zdarzenia: ***		Niepożądane treści (np. treści obraźliwe, dezinformacja, spam)
		Oprogramowanie złośliwe (np. wirus, trojan, ransomware, dialer, botnet)
		Zbieranie informacji (np. skanowanie, podsłuch, 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, jej zastosowanie lub usunięcie)
		Oszustwo (np. nieuprawnione wykorzystanie zasobów, naruszenie praw autorskich, podszywanie się, kradzież tożsamości, phishing)
		Podatność (np. błędna konfiguracja, wykrycie podatności)
		Cyberterroryzm (zdarzenie o charakterze terrorystycznym popełnione w cyberprzestrzeni)
		Inne (zdarzenia niemieszczące się w powyższych kategoriach), opisać jakie:

*** Zaznaczyć właściwe używając znaku **X**

Podjęte działania naprawcze *	
Podjęte działania zapobiegawcze *	
Inne istotne informacje *	

Wypełniony formularz należy wysłać w postaci załącznika do wiadomości e-mail na adres:

csirt@cyber360.pl