

Zarządzenie nr
Wójta Gminy Tworóg
z dnia
2021/2021
02.09.2021

w sprawie regulamin zarządzania incydentami.

Na podstawie art. 22 ustawy z dnia 5 lipca 2018r. o krajowym systemie cyberbezpieczeństwa ustaliam jako obowiązujący w Urzędzie Gminy Tworóg regulamin zarządzania incydentami, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo.

Zarządza się co następuje:

§ 1.

Na dokumentację, o której mowa w ust. 1 składają się:

✓ Regulamin zarządzania incydentami

- Załącznik nr 1

§ 2.

Do stosowania niniejszego zarządzenia zobowiązani są wszyscy pracownicy jednostki oraz podmioty współpracujące.

§ 3.

Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT GMINY
mgr inż. Andrzej Gwóźdź

REGULAMIN ZARZĄDZANIA INCYDENTAMI
W
Urzędzie Gminy Tworóg

Spis treści

I. Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji	3
II. Postępowanie z incydentami	3
III. Ograniczanie skutków incyduentu	5
IV. Odtwarzanie systemu informacyjnego	7
V. Działania po zakończeniu incyduentu	7
VI. Rejestrowanie informacji o incydentach.....	8
VII. Gromadzenie materiału dowodowego	8

I. Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji

1. Wszyscy pracownicy Urzędu oraz pracownicy reprezentujący podmiot zewnętrzny, którzy mają dostęp do systemów teleinformatycznych Urzędu i zobowiązali się do przestrzegania jej regulacji wewnętrznych związanych z bezpieczeństwem informacji, mają obowiązek zgłaszania wszelkich zdarzeń, które naruszają lub mogą naruszyć przepisy prawa oraz polityki, regulaminy i procedury dotyczące bezpieczeństwa informacji.
2. O każdym zdarzeniu informowany jest Zastępca Wójta Gminy/ Administrator systemów informatycznych/ Inspektor ochrony danych osobowych.
3. Osoba dokonująca zgłoszenia jest informowana o wyniku obsługi zgłoszenia.
4. Zastępca Wójta Gminy / Administrator systemów informatycznych ma obowiązek zareagować na alarm wygenerowany przez moduł automatycznego powiadamiania w systemach wykrywania włamań (systemów teleinformatycznych oraz elektronicznych systemów zabezpieczeń).
5. W przypadku powierzenia obowiązków zarządzania systemami informacyjnymi podmiotom zewnętrznym, powiadamianie Zastępcy Wójta Gminy / Administrator systemów informatycznych o zdarzeniu odbywa się na zasadach określonych w umowie o świadczeniu usług.
6. W celu zapewnienia prawidłowości i kompletności zgłaszania oraz obsługi zdarzeń związanych z bezpieczeństwem informacji, Administrator systemów informatycznych dokonuje:
 - 1) comiesięcznych analiz z użyciem raportów tworzonych w ramach realizacji umów z podmiotami zewnętrznymi,
 - 2) przeglądu zdarzeń z wykorzystaniem narzędzi monitorujących środowisko teleinformatyczne jednostki w czasie rzeczywistym.

II. Postępowanie z incydentami

1. Zastępca Wójta Gminy / Administrator systemów informatycznych/ Inspektor ochrony danych dokonuje wstępnej identyfikacji zdarzenia i na podstawie dostępnych informacji oraz analizy okoliczności kwalifikuje zdarzenie (lub serię zdarzeń) jako:
 - 1) zdarzenie nie mające cech naruszenia bezpieczeństwa informacji, np. zaplanowana przerwa technologiczna,
 - 2) błąd w działaniu elementu systemu teleinformatycznego, infrastruktury teleinformatycznej lub infrastruktury biurowej,

- 3) awaria techniczna czasowo blokująca dostępność informacji,
 - 4) incydent niskiej kategorii - związany z naruszeniem bezpieczeństwa informacji, a szczególnie jej integralności i poufności, nie generujący kar finansowych, jednak powodujący pośrednio lub bezpośrednio utrudnienia w realizacji jakiegokolwiek procesu głównego jednostki,
 - 5) incydent średniej kategorii - związany z naruszeniem bezpieczeństwa informacji skutkujący pośrednio lub bezpośrednio zatrzymaniem realizacji jakiegokolwiek procesu ustawowego i/lub stratami finansowymi oraz możliwością konsekwencji prawnych i/lub utraty wizerunku,
 - 6) incydent wysokiej kategorii - związany z naruszeniem bezpieczeństwa informacji, którego skutkiem jest destrukcja (zniszczenie, utrata) kluczowych zasobów i przerwanie funkcjonowania procesów jednostki;
2. O możliwości zaistnienia przypadku naruszenia bezpieczeństwa informacji mogą świadczyć:
- 1) nadmierne, w stosunku do wykonywanych zadań (zakresu upoważnienia), uprawnienia użytkownika do zasobów systemu,
 - 2) niestabilna praca systemu teleinformatycznego,
 - 3) korzystanie z zasobów systemu poza godzinami pracy (bez zgody przełożonego),
 - 4) nowe „podejrzane” (nieznane) konta użytkowników,
 - 5) wysoka aktywność kont, które długo pozostawały niewykorzystane,
 - 6) zanotowanie w krótkim czasie dużej liczby nieudanych prób logowania,
 - 7) anomalie w pracy systemu lub programu (świadczące np. o obecności wirusa komputerowego),
 - 8) naruszenie lub wadliwe funkcjonowanie zabezpieczeń fizycznych w pomieszczeniach, w których następuje przetwarzanie informacji w jednostce (uszkodzone zamki, okna, drzwi, naruszone plomby, itp.).
3. O zdarzeniu noszącym znamiona incydentu Zastępca Wójta Gminy / Administrator systemów informatycznych/ powiadamia niezwłocznie Wójta Gminy, który dokonuje ostatecznej jego klasyfikacji.
4. Inspektor ochrony danych osobowych, we współpracy z Administratorem Systemu Informatycznych przeprowadza analizę incydentu.
5. Analiza incydentu uwzględnia następujące kryteria:
- 1) charakter incydentu i jego znaczenie związane z naruszeniem bezpieczeństwa fizycznego lub teleinformatycznego,

- 2) miejsce wystąpienia incydentu - identyfikacja punktu, w którym nastąpiło zdarzenie (lokalizacja, serwer, stacja robocza itp.),
 - 3) liczba jednostek/ komórek organizacyjnych jednostki, zakres zasobów dotkniętych incydem,
 - 4) identyfikację zasobów potrzebnych przy dalszych działaniach w ramach postępowania z incydem związanym z bezpieczeństwem informacji,
 - 5) możliwości rozszerzania się incydemu i sposoby jego ograniczania,
 - 6) szacowany poziom szkód finansowych,
 - 7) rodzaj ujawnionej informacji (jeśli ma zastosowanie – np. dane osobowe),
 - 8) szacunkowy czas, po którym skutki incydemu zostaną zlikwidowane, jeżeli nie ma możliwości natychmiastowego usunięcia stanu naruszenia bezpieczeństwa informacji,
 - 9) skutki organizacyjne i prawne (wstępny szacunek).
6. W przypadku, gdy zasięg incydemu wykracza poza system teleinformatyczny jednostki, Administrator Systemu informatycznego, w porozumieniu z Inspektorem ochrony danych osobowych i z zastrzeżeniem posiadania stosownej umowy o poufności z właściwymi podmiotami zewnętrznymi, może przekazać do podmiotu zewnętrznego informacje o incydencie zawierające:
- 1) typ zdarzenia,
 - 2) informacje o odległym systemie, który może być źródłem naruszenia, w tym nazwy serwerów, adresy IP, identyfikatory użytkowników,
 - 3) wszystkie zapisy z rejestrów zdarzeń w określonym przedziale czasowym,
 - 4) inne informacje określone w umowie z podmiotem zewnętrznym.
7. W przypadku, gdy rodzaj i zasięg incydemu, zidentyfikowany na którymkolwiek z etapów postępowania, uzasadnia potrzebę powiadomienia organów ścigania, to decyzję o sposobie i terminie powiadomienia podejmuje Wójt Gminy.

III. Ograniczanie skutków incydemu

1. Administrator systemów informatycznych prowadzi bieżącą dokumentację incydemu. Dokumentacja ta w szczególności obejmuje:
 - 1) wszystkie zdarzenia zachodzące w systemie informacyjnym (zapisy systemowych dzienników audytu zdarzeń i dzienników audytu, lub zapisy z elektronicznych systemów zabezpieczeń),
 - 2) wszystkie podejmowane działania (opatrzone datą i czasem),

- 3) wszystkie przeprowadzone rozmowy (osoba rozmówcy, data i czas zdarzenia, treść rozmowy).
2. Dokumentacja incydentu podlega rygorom ochrony przez tworzenie autoryzowanych kopii tych elementów systemu, które mają zastosowanie przy postępowaniu z incydem tzn. rejestry urządzeń, systemów operacyjnych i aplikacji, kopie zapasowe, pliki konfiguracyjne i systemowe (zgodnie z rygorami tworzenia materiału dowodowego), bezpieczne przechowywanie tych kopii, przyjęcia dokumentacji oraz jej wszystkich części.
3. Administrator systemów informatycznych przeprowadza działania zmierzające do ograniczenia skutków incydentu i zidentyfikowania źródła naruszenia bezpieczeństwa. W tym celu może spowodować zablokowanie części systemu lub dostępnych usług.
4. W przypadku, gdy działania opisane w ust. 3 obejmują wyłączenie lub ograniczenie funkcjonowania zasobów niezbędnych do realizowania celów ustawowych bądź statutowych Urzędu Gminy, Administrator systemów informatycznych przedstawia decyzję do akceptacji Wójtowi Gminy, wraz z rekomendacją.
5. Rekomendacja uwzględnia:
 - 1) uzależnienie jednostki od systemu teleinformatycznego (jak długo jednostka może funkcjonować przy całkowitym lub częściowym wyłączeniu systemu),
 - 2) stopień narażenia informacji przetwarzanych w systemach teleinformatycznych jednostka na ujawnienie w przypadku utrzymywania się stanu naruszenia zabezpieczenia,
 - 3) stopień uświadomienia użytkowników (jaka może być reakcja użytkowników na anormalne zachowanie się systemu – np. niemożność zarejestrowania się, wyłączenie niektórych funkcji, itp.),
 - 4) konieczność schwytania i ewentualnego ukarania sprawcy (przy założeniu, że istnieją okoliczności umożliwiające takie działanie),
 - 5) konieczność angażowania zasobów systemu informatycznego (jaka część i jak długo),
 - 6) aspekt finansowy, organizacyjny i ludzki podejmowanych działań (jak długo działanie ma trwać, w jakim stopniu zakłóca normalne funkcjonowanie jednostka, jakie są tego koszty).
6. Przy ograniczaniu skutków incydentu Administrator systemów informatycznych, w uzgodnieniu z Wójtem Gminy, może korzystać z konsultantów zewnętrznych, jeśli

Urząd Gminy wcześniej zawarł w umowach z tymi podmiotami stosowne zapisy o przekazywaniu i ochronie informacji.

IV. Odtwarzanie systemu informacyjnego

1. Z zastrzeżeniem ust. 3, Administrator systemów informatycznych przystępuje do odtworzenia systemu po zidentyfikowaniu i usunięciu lub zablokowaniu źródła incydentu.
2. Odtwarzanie systemu odnosi się do punktu odtworzenia, co do którego Administrator Systemów informatycznych ma uzasadnioną pewność, że nie zawiera źródła incydentu.
3. Zasoby w postaci oprogramowania oraz danych są odtwarzane z oryginalnych źródeł dystrybucji oprogramowania oraz kopii zapasowych.
4. Wójt Gminy, po zasięgnięciu opinii Administratora systemów informatycznych, może podjąć decyzję o podjęciu przetwarzania mimo braku pewności usunięcia źródła incydentu, jeśli szacowane negatywne skutki braku przetwarzania przewyższają potencjalne ryzyko podjęcia działania.

V. Działania po zakończeniu incydentu

1. Administrator systemów informatycznych, sporządza raport z incydentu, zgodnie ze wzorem zamieszczonym w **załączniku nr 3** do niniejszego regulaminu oraz przedstawia go Wójtowi Gminy.
2. Jeśli zachodzi taka potrzeba, to Administrator systemów informatycznych sporządza dodatkowy raport techniczny, stanowiący załącznik do raportu wskazanego w ust. 1 i zawierający co najmniej:
 - 1) rejestr incydentu, zawierający szczegółowe zapisy chronologiczne dotyczące kolejnych zdarzeń i podejmowanych działań,
 - 2) opis incydentu w aspekcie technicznym (zakres incydentu, części systemów dotknięte skutkami incydentu, rozmiar bezpośrednich szkód),
 - 3) kopie dzienników (logów zdarzeń, logów audytu) urządzeń, systemów operacyjnych i aplikacji w części systemów, która była dotknięta skutkami incydentu,
 - 4) kopię dziennika pracy systemu z okresu trwania incydentu,
 - 5) informacje o oryginalnych źródłach dystrybucji oprogramowania oraz kopiach zapasowych wykorzystanych do odtworzenia systemu,
 - 6) zakres informacji technicznych przekazanych Podmiotom zewnętrznym uczestniczącym w działaniach związanych z ograniczaniem skutków incydentu.

3. Administrator systemów informatycznych rekomendacje w zakresie działań zmierzających do zmniejszenia ryzyka powtórzenia incydentu w przyszłości.

VI. Rejestrowanie informacji o incydentach

1. Administrator systemów infromactycznych prowadzi rejestr incydentów zawierający następujące informacje:
 - 1) opis incydentu,
 - 2) datę i godzinę zgłoszenia incydentu,
 - 3) dane identyfikujące osobę zgłaszającą,
 - 4) dane osoby przekazującej informację o incydencie,
 - 5) datę zarejestrowania incydentu,
 - 6) dane identyfikujące osobę rejestrującą incydent,
 - 7) informację o zgromadzonych materiałach dowodowych,
 - 8) informacje dotyczące sposobu postępowania z incydentem.
2. Wójt Gminy zapewnia właściwe wykorzystanie informacji o incydentach związanych z bezpieczeństwem informacji dla celów szkoleniowych i doskonalenia systemu zarządzania bezpieczeństwem informacji.

VII. Gromadzenie materiału dowodowego

1. Na każdym etapie postępowania z incydentem, Administrator systemów informatycznych nadzoruje prawidłowość gromadzenia materiału dowodowego.
2. Każdy element materiału dowodowego – dokument papierowy, dokument elektroniczny, kopia zapasowa bazy danych lub plików systemowych i konfiguracyjnych, obraz dysku, dzienników (logów) zdarzeń, dzienników audytu – jest gromadzony i przechowywany w sposób gwarantujący jego poufność, integralność i kompletność.
3. Każdy element materiału dowodowego jest utrwalany z zachowaniem integralności całego procesu przetwarzania, od utworzenia do ewentualnego przedstawienia jako dowodu w postępowaniu sądowym:
 - 1) dla dokumentów papierowych - oryginał jest bezpiecznie przechowywany wraz z informacją o źródle, czasie i okolicznościach utrwalenia dokumentu,
 - 2) dla zapisów utrwalanych na nośnikach komputerowych – sporządzenie kopii zapasowej lub obrazu dysku wraz z udokumentowaniem procesu kopiowania oraz bezpieczne ich przechowanie (np. poza siedzibą Urzędu Gminy).

3. Zabezpieczenie środków przetwarzania informacji jest przeprowadzane zgodnie z instrukcją zamieszczoną w **załączniku nr 1** do niniejszego regulaminu.
4. Protokół ze sporządzenia elementu materiału dowodowego lub zabezpieczenia środków przetwarzania informacji jest sporządzany zgodnie ze wzorem zamieszczonym w **załączniku nr 2** do niniejszego regulaminu.
5. Wszelkie działania w systemie teleinformatycznym, związane z postępowaniem z incydem, mogą być prowadzone wyłącznie z wykorzystaniem kopii zapasowych, obrazów dysków, kopii plików konfiguracyjnych i systemowych, rejestrów systemowych i aplikacji, plików dokumentów, identycznych ze sporządzonymi uprzednio kopiami przechowywanymi jako materiał dowodowy.

VIII. Zgłaszanie incydem do CSIRT.GOV.PL

1. Jeżeli istotność incydem jest wysoka, należy zawiadomić Rządowy Zespół Reagowania na Incydenty Komputerowe CSIRT.GOV.PL pełniący rolę głównego zespołu CSIRT w obszarze administracji rządowej. Wyznaczony przez Wójta Gminy pracownik wypełnia formularz zgłoszenia incydem, pobrany ze strony www.csirt.gov.pl oraz wysyła go do CSIRT zgodnie z informacją zamieszczoną na tej stronie. Incydem zgłaszany jest dwutorowo, faksem na numer +48 22 58 58 833 oraz pocztą elektroniczną na adres incydent@csirt.gov.pl. Dalsza korespondencja z CSIRT w sprawie tego incydem odbywa się za pomocą szyfrowanej poczty elektronicznej.
2. W przypadku, gdy zgłoszone zdarzenie nie zostało zaklasyfikowane jako incydem bezpieczeństwa informacji, ma charakter fałszywego alarmu Administrator systemów informatycznych powiadamia zgłaszającego o zdarzeniu, że zdarzenie nie stanowi incydem bezpieczeństwa.
3. W przypadku stwierdzenia działań umyślnych i ustaleniu sprawcy incydem Administrator systemów informatycznych przekazuje wyniki analizy w raz z zabezpieczonym materiałem dowodowym Wójtowi Gminy w celu wyciągnięcia konsekwencji dyscyplinarnych wobec sprawcy, ewentualnego zawiadomienia organów ścigania lub podjęcia kroków prawnych wobec osób trzecich.
4. Administrator systemów informatycznych inicjuje działania naprawcze zmierzające do zniwelowania szkód wyrządzonych przez incydem, wyciąga wnioski z każdego incydem i określa, jeśli to możliwe działania korygujące i zapobiegawcze w celu uniknięcia ponownego wystąpienia incydem.
5. Administrator systemów informatycznych na bieżąco dokumentuje swoje działania na każdy z etapów procesu zarządzania incydemem w formie notatki.

INSTRUKCJA ZABEZPIECZANIA KOMPUTERÓW

1. Odsuń w sposób zdecydowany, ale taktowny całą obsługę od komputerów (mogą później być przydatni). Na czas zabezpieczenia zabroń im korzystania z urządzeń komputerowych i łączności.
2. Jeśli urządzenie jest wyłączone, **NIE WŁĄCZAJ GO**.
3. Jeśli urządzenie jest włączone, **NIE** próbuj zamykać programów ani wyłączać komputera. Nie przerywaj drukowania, zabezpiecz, jeśli to możliwe, wykonane wydruki. Zanotuj dokładnie wszystkie wiadomości, jakie pojawiają się na ekranie. Zanotuj wszystkie parametry połączeń komputera:
 - 1) w przypadku połączenia modemowego, zanotuj numer telefoniczny, adres IP komputera, adresy bramki wychodzącej oraz serwera DNS,
 - 2) w przypadku połączenia po sieci kablowej, zanotuj typ połączenia, adres IP komputera, adresy bramki wychodzącej oraz serwera DNS,
 - 3) w przypadku połączenia po sieci bezprzewodowej, zanotuj ustawienia zabezpieczenia sieci adres IP komputera, adresy bramki wychodzącej oraz serwera DNS.
4. Przed zabezpieczeniem zanotuj, w jaki sposób poszczególne części stanowiska są ze sobą połączone. Zrób zdjęcia, wykonaj szkic (plan połączeń z opisem wyposażenia). Oznacz odpowiednio wszystkie przewody i połączenia.
5. Następnie **ODŁĄCZ WSZYSTKIE KABLE ZEWNĘTRZNE KOMPUTERA**. Zanotuj czas odłączenia kabli.
6. Zabezpiecz jednostkę centralną (komputer) oraz inne urządzenia z zainstalowaną na stałe pamięcią masową w wytrzymałych mechanicznie workach foliowych. **ZAPŁOMBUIJ WOREK I WYPEŁNIJ METRYCZKĘ**. Metryczka powinna zawierać typ, numer seryjny urządzenia i numer inwentarzowy nadany przez jednostkę albo opis jego indywidualnych cech. Wpisz do **PROTOKOŁU** wykonane czynności (Załącznik nr 2 do Regulaminu zarządzania incydentami).
7. Pakuj ostrożnie okablowanie i sprzęt (klawiatury, monitory, drukarki, plotery, skanery, czytniki kart i pamięci, napędy zewnętrzne itp.).
8. Zabezpiecz wszystkie wymienne nośniki komputerowe: pamięci flash, dyskietki, dyskietki ZIP, JAZZ, taśmy streamera, płyty CD, DVD, MO oraz niezamontowane dyski twarde (także uszkodzone). Grupy nośników pakuj zbiorczo (dyskietki, płyty CD itp.). **PAKUJ**,

NUMERUJ poszczególne paczki, PLOMBUJ I OPISZ W PROTOKOLE. Wpisz do PROTOKOŁU wykonane czynności.

9. Zażądaj od użytkownika spisu oprogramowania zainstalowanego na komputerze, a następnie zgodnie ze spisem - okazania licencji i oryginalnych nośników oprogramowania lub wskazania miejsca przechowywania lub osoby upoważnionej, która zarządza licencjami i oryginalnymi nośnikami oprogramowania. Jeśli użytkownik nie ma spisu oprogramowania, to zażądaj okazania wszystkich posiadanych przez niego licencji i oryginalnych nośników oprogramowania. Oznaczenia licencji i nośników wpisz do protokołu, a następnie zabezpiecz jako materiał porównawczy. Wpisz do protokołu wykonane czynności.
10. Zażądaj od użytkownika przekazania instrukcji programów pisanych na zamówienie lub programów nietypowych (np. FK). Zabezpiecz jako materiał porównawczy i wpisz do protokołu wykonane czynności.
11. Zażądaj od użytkowników i administratora podania parametrów dostępu do BIOS-u, systemu operacyjnego i oprogramowania (kont, haseł, identyfikatorów, itp.), a następnie zabezpiecz je przed osobami postronnymi za pomocą bezpiecznej koperty. Wpisz czynność przejścia parametrów dostępu do protokołu.
12. Przechowuj zabezpieczone materiały (nośniki i sprzęt) w miejscach suchych i chłodnych z daleka od urządzeń emitujących pole elektromagnetyczne, a bezpieczne koperty w sejfie.

Uwagi końcowe:

1. Sprawdź przed odesłaniem zgodność numerów zabezpieczonych materiałów i dowodów z treścią protokołu (zwróć uwagę na puste pudełka i nośniki pozostawione w napędach komputerowych i innych urządzeniach),
2. Skontaktuj się z odpowiednią komórką organizacyjną w celu zorganizowania przewozu i badań zabezpieczonych materiałów.

Pamiętaj:

NIE PRÓBUJ SAMODZIELNIE BADAĆ KOMPUTERA, ANI ZAWARTOŚCI
NOŚNIKÓW DANYCH.

KAŻDE TWOJE WŁĄCZENIE KOMPUTERA PO ZAKOŃCZENIU ZABEZPIECZENIA
WYWOŁUJE POWSTANIE ŚLADÓW WSKAZUJĄCYCH NA NARUSZENIE
INTEGRALNOŚCI MATERIAŁU BADAWCZEGO.

PROTOKÓŁ ZABEZPIECZENIA MATERIAŁU DOWODOWEGO

Wykonano w dniu o godzinie w obecności:

Świadek 1:
(imię i nazwisko, stanowisko, komórka organizacyjna)

Świadek 2:
(imię i nazwisko, stanowisko, komórka organizacyjna)

Świadek 3:
(imię i nazwisko, stanowisko, komórka organizacyjna)

I. Rodzaj materiału dowodowego

(zaznaczyć właściwe kwadraty i wpisać odpowiednie nazwy i oznaczenia)

Dokument papierowy	<input type="checkbox"/>	Rodzaj i Nazwa dokumentu:			
Dokument elektroniczny	<input type="checkbox"/>	Rodzaj i Nazwa dokumentu:			
Kopia zapasowa	<input type="checkbox"/>	System operacyjny Nazwa i wersja systemu:	<input type="checkbox"/>	Aplikacja Nazwa i wersja aplikacji:	<input type="checkbox"/>
	<input type="checkbox"/>	Baza danych Nazwa i wersja bazy:	<input type="checkbox"/>	Oznaczenie nośnika	<input type="checkbox"/>
Obraz dysku	<input type="checkbox"/>	Lokalizacja dysku (adres IP/IPX): Typ i nr seryjny dysku:			
Pliki konfiguracyjne i/lub systemowe	<input type="checkbox"/>	System operacyjny Nazwa i wersja systemu:	<input type="checkbox"/>	Aplikacja Nazwa i wersja aplikacji:	<input type="checkbox"/>
	<input type="checkbox"/>	Baza danych Nazwa i wersja bazy:	<input type="checkbox"/>	Nazwa(y) Pliku(ów)	<input type="checkbox"/>
Kopie zawartości dzienników (logów) zdarzeń	<input type="checkbox"/>	System operacyjny Nazwa i wersja systemu:	<input type="checkbox"/>	Aplikacja Nazwa i wersja aplikacji:	<input type="checkbox"/>
	<input type="checkbox"/>	Baza danych Nazwa i wersja bazy:	<input type="checkbox"/>	Nazwa(y) Pliku(ów)	<input type="checkbox"/>
Kopia zawartości skrzynki pocztowej	<input type="checkbox"/>	zewnętrzna	<input type="checkbox"/>	wewnętrzna	<input type="checkbox"/>
	<input type="checkbox"/>	Nazwa skrzynki pocztowej:		Za okres od:	

II. Opis czynności

(opisać kolejne czynności z zaznaczeniem Wykonawcy(ów))

III. Wytworzony materiał dowodowy

Wykonano kopie materiału dowodowego w 2 egzemplarzach, którym nadano etykiety:

„....., Egzemplarz nr 1”

„....., Egzemplarz nr 2”

(wprowadzić krótkie oznaczenie zabezpieczonego materiału dowodowego, zgodnie z kategorią wskazaną w pkt. I, datą i godziną wykonania)

IV. Zabezpieczenie materiału dowodowego

(opisać sposób zabezpieczenia jednego z egzemplarzy)

.....
.....
.....

Protokół sporządził:

Podpisano:

Świadek 1

Świadek 2

Świadek 3

Miejscowość, data

RAPORT O INCYDENCIE BEZPIECZEŃSTWA INFORMACJI

A. ZGŁOSZENIE INCYDENTU (wypełnia osoba zgłaszająca zdarzenie/incydent)

DANE OSOBY ZGŁASZAJĄCEJ

Imię i nazwisko.....Stanowisko służbowe

Adres

Nr telefonue-mail

OPIS INCYDENTU:

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Komu zgłoszono:

Data i godzina zgłoszenia:

Podpis osoby zgłaszającej:

B. DZIAŁANIA PO ZAISTNIENIU INCYDENTU

(wypełnia osoba rozpatrująca zgłoszenie incydentu)

DANE OSOBY, KTÓRA PRZYJĘŁA ZGŁOSZENIE INCYDENTU

Imię i nazwisko..... Stanowisko

Adres

Nr telefonu e-mail

INFORMACJE O INCYDENCIE

Data i czas zajścia incydentu

Data i czas wykrycia incydentu

Data i czas zgłoszenia incydentu

Czy incydent jest zakończony? TAK ☐ NIE ☐

Jeśli tak, to jak długo trwał (dni/godziny/minuty)?

Jeśli nie, należy określić jak długo już trwa?

Kogo powiadomiono z KIEROWNICTWA?

OPIS WSTĘPNY / PODJĘTE DZIAŁANIA / ZABEZPIECZENIE MATERIAŁU DOWODOWEGO

.....
.....
.....
.....
.....

Załączniki (materiał dowodowy):

1.
2.
3.

OPIS ROZWIĄZANIA PROBLEMU / KOSZTY ODTWORZENIA

.....
.....
.....
.....

Imię i Nazwisko.....

Data

Podpis

C. POSTĘPOWANIE WYJAŚNIAJĄCE/ ZAKOŃCZENIE INCYDENTU

(wypełnia osoba prowadząca postępowanie wyjaśniające)

Data rozpoczęcia postępowania ws. incydentu

Data zakończenia incydentu (jeśli jest zakończony)

Data zamknięcia skutków incydentu

Data zakończenia postępowania ws. incydentu

USTALENIA – OPIS POSTĘPOWANIA - SPRAWCY INCYDENTU

(w tym opis postępowania dyscyplinarnego, jeśli takie ma miejsce)

.....
.....
.....
.....
.....
.....
.....
.....

WNIOSKI I REKOMENDACJE

(w tym zalecenia dotyczące zmian w procedurach wewnętrznych)

.....
.....
.....
.....
.....
.....
.....
.....

WYKAZ DOŁĄCZONYCH DOKUMENTÓW

.....
.....
.....
.....

DANE OSÓB PROWADZĄCYCH POSTĘPOWANIE WYJAŚNIAJĄCE

Imię i Nazwisko.....	Imię i Nazwisko.....
Stanowisko	Stanowisko
Data	Data
Podpis	Podpis

DANE ADRESOWE

1. Nazwa instytucji*	<input type="text"/>		
2. Nazwa skrócona	<input type="text"/>		
2. Adres*	<input type="text"/>		
3. Kod pocztowy	<input type="text"/>	4. Miasto*	<input type="text"/>
5. NIP	<input type="text"/>		
6. tel.*	<input type="text"/>	7. fax.*	<input type="text"/>
8. e-mail*	<input type="text"/>		

ADRESACJA IP

9. NETNAME	<input type="text"/>	10. CIDR	<input type="text"/>
11. Zakres IP	<input type="text"/>		

OSOBY WYZNACZONE DO KONTAKTU

Imię i Nazwisko / Nazwa*	<input type="text"/>				
Stanowisko / Funkcja*	<input type="text"/>				
tel.*	<input type="text"/>	dostępność	<input type="radio"/> 8-16	<input type="radio"/> 8-22	<input type="radio"/> 24h
tel. kom.*	<input type="text"/>	dostępność	<input type="radio"/> 8-16	<input type="radio"/> 8-22	<input type="radio"/> 24h
e-mail*	<input type="text"/>				

Imię i Nazwisko / Nazwa*	<input type="text"/>				
Stanowisko / Funkcja*	<input type="text"/>				
tel.*	<input type="text"/>	dostępność	<input type="radio"/> 8-16	<input type="radio"/> 8-22	<input type="radio"/> 24h
tel. kom.*	<input type="text"/>	dostępność	<input type="radio"/> 8-16	<input type="radio"/> 8-22	<input type="radio"/> 24h
e-mail*	<input type="text"/>				

Wypełniony formularz należy wysłać w postaci załącznika do wiadomości e-mail na adres: **incydent@csirt.gov.pl**. Pola oznaczone * są polami wymaganymi.
W przypadku konieczności zgłoszenia większej ilości osób / komórek wyznaczonych do kontaktów z CSIRT GOV, należy wypełnić dodatkowy formularz.

