REGULAMIN ZARZĄDZANIA INCYDENTAMI

Spis treści:

§ 1.

Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji

1. Wszyscy pracownicy Agencji oraz pracownicy reprezentujący podmiot zewnętrzny, którzy mają dostęp do systemów teleinformatycznych Agencji 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 Agencji dotyczące bezpieczeństwa informacji.
2. Zasady zgłaszania zdarzeń związanych z bezpieczeństwem informacji opisane zostały w Regulaminie użytkownika.
3. Osoba dokonująca zgłoszenia jest informowana przez Inspektora Bezpieczeństwa Informacji/Administratora Zabezpieczeń Fizycznych/Help Desk ARiMR o wyniku obsługi zgłoszenia.
4. Administrator Systemu/Administrator Zabezpieczeń Fizycznych ma obowiązek zareagować na alarm wygenerowany przez moduł automatycznego powiadamiania w systemach wykrywania włamań (systemów teleinformatycznych oraz elektronicznych systemów zabezpieczeń). W razie zidentyfikowania zagrożenia naruszenia bezpieczeństwa ochrony danych osobowych Administrator Systemu/Administrator Zabezpieczeń Fizycznych niezwłocznie informuje Inspektora Ochrony Danych, przy czym sposób poinformowania Inspektora Ochrony Danych powinien nastąpić w sposób zapewniających, iż informacja zostanie odebrana w możliwie najkrótszym czasie od jej przekazania,
5. W przypadku powierzenia obowiązków zarządzania systemami informacyjnymi podmiotom zewnętrznym, powiadamianie Administratora Systemu/Administratora Zabezpieczeń Fizycznych/ Inspektora Bezpieczeństwa Informacji/ Inspektora Ochrony Danych 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, dyrektor komórki właściwej ds. bezpieczeństwa informacji dokonuje:
   1) comiesięcznych analiz z użyciem raportów tworzonych w ramach realizacji umów z podmiotami zewnętrznymi;
   2) przeglądu zdarzeń z wykorzystaniem, udostępnionych przez komórkę właściwą ds. informatyki, narzędzi monitorujących środowisko teleinformatyczne Agencji w czasie rzeczywistym.

§ 2.

Postępowanie z incydentami

1. Administrator Systemu/Administrator Zabezpieczeń Fizycznych lub pracownik Help Desk ARiMR 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 Agencji;

5) incydent średniej kategorii – związany z naruszeniem bezpieczeństwa informacji skutkujący pośrednio lub bezpośrednio zatrzymaniem realizacji jakiegokolwiek procesu ustawowego i/lub stratami finansowymi nie przekraczającymi kwoty 137 tys. € 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 Agencji; skutki tego incydentu powodują uruchomienie PZCD i wznowienie funkcjonowania w Zapasowych Miejscach Pracy; incydentem wysokiej kategorii jest również incydent, którego skutki mogą spowodować straty przekraczające kwotę 137 tys. €.

2. Inspektor Ochrony Danych dokonuje analizy danych dotyczących zdarzenia związanego z naruszeniem zasad ochrony danych osobowych. W toku tego procesu może występować o wszelkie informacje oraz opinie do jednostek i komórek organizacyjnych Agencji, które są zobowiązane do przekazania informacji oraz opinii w wyznaczonym przez Inspektora Ochrony Danych terminie.

3. 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 Agencji (uszkodzone zamki, okna, drzwi, naruszone plomby, itp.).

4. O zdarzeniu noszącym znamiona incydentu Administrator Systemu/Administrator Zabezpieczeń Fizycznych/pracownik Help Desk ARiMR powiadamia niezwłocznie Inspektora Bezpieczeństwa Informacji (IBI), który dokonuje ostatecznej jego klasyfikacji.

5. Inspektor Bezpieczeństwa Informacji, we współpracy z Administratorem Systemu oraz, jeśli zachodzi taka potrzeba, z Administratorem Zabezpieczeń Fizycznych, przeprowadza analizę incydentu.

6. 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 Agencji, zakres zasobów dotkniętych incydentem;
   4) identyfikację zasobów potrzebnych przy dalszych działaniach w ramach postępowania z incydentem związanym z bezpieczeństwem informacji;
   5) możliwości rozszerzania się incydentu 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 incydentu zostaną zlikwidowane, jeżeli nie ma możliwości natychmiastowego usunięcia stanu naruszenia bezpieczeństwa informacji;
   9) skutki organizacyjne i prawne (wstępny szacunek).
7. W przypadku, gdy incydent ma skutki przekładające się na możliwość zakłócenia działalności ustawowej bądź statutowej Agencji, dyrektor komórki właściwej ds. bezpieczeństwa informacji informuje niezwłocznie Prezesa Agencji.
8. W przypadku, gdy zasięg i szacunkowy czas trwania powoduje zakwalifikowanie incydentu jako incydentu wysokiej kategorii, dyrektor komórki właściwej ds. bezpieczeństwa informacji powiadamia niezwłocznie Prezesa Agencji.
9. W przypadku, gdy zasięg incydentu wykracza poza system teleinformatyczny Agencji, Administrator Systemu, w porozumieniu z dyrektorem komórki właściwej ds. bezpieczeństwa informacji 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.
10. W przypadku, gdy rodzaj i zasięg incydentu, zidentyfikowany na którymkolwiek z etapów postępowania, uzasadnia potrzebę powiadomienia organów ścigania, to decyzję o sposobie i terminie powiadomienia podejmuje Prezes Agencji.

§ 3.

Postępowania Inspektora Ochrony Danych w toku obsługi incydentów

1. Inspektor Ochrony Danych dokonuje analizy danych dotyczących zdarzenia związanego z naruszeniem zasad ochrony danych osobowych. W toku tego procesu może

występować o wszelkie informacje oraz opinie do jednostek i komórek organizacyjnych Agencji, które są zobowiązane do niezwłocznego przekazania informacji oraz opinii.

2. W wyniku analizy Inspektor Ochrony Danych stwierdza czy jest prawdopodobne, że stwierdzony incydent skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych oraz szacuje ryzyko z tym związane.
3. W przypadku stwierdzenia wysokiego ryzyka naruszenia praw i wolności osób fizycznych Inspektor Ochrony Danych informuje o tym Prezesa ARiMR.
4. Inspektor Ochrony Danych odpowiada za dokonanie czynności zgłoszenia stwierdzonego incydentu naruszenia ochrony danych osobowych, w którym wystąpiło wysokie ryzyko naruszania praw i wolności osób fizycznych, do Urzędu Ochrony Danych Osobowych.
5. Inspektor Ochrony Danych pełni nadzór nad właściwym dokonaniem procesu poinformowania właścicieli danych osobowych, których dotyczy incydent, przez odpowiednie jednostki, komórki organizacyjne Agencji. Informacje z pełnionego nadzoru przekazuje Prezesowi ARiMR oraz Komitetowi Sterowania Bezpieczeństwem Informacji.
6. Inspektor Ochrony Danych prowadzi Rejestr incydentów naruszeń ochrony danych osobowych, o których mowa w ust. 3.

§ 4.

Ograniczanie skutków incydentu

1. Administrator Systemu/Administrator Zabezpieczeń Fizycznych prowadzi bieżącą dokumentację incydentu. 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 incydentem 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 Systemu/Administrator Zabezpieczeń Fizycznych 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 Agencji, Administrator Systemu/Administrator Zabezpieczeń Fizycznych przedstawia decyzję do akceptacji Prezesa Agencji, wraz z rekomendacją dyrektora komórki właściwej ds. bezpieczeństwa informacji.

5. Rekomendacja dyrektora komórki właściwej ds. bezpieczeństwa informacji uwzględnia:
   1) uzależnienie Agencji od systemu teleinformatycznego (jak długo Agencja może funkcjonować przy całkowitym lub częściowym wyłączeniu systemu);
   2) stopień narażenia informacji przetwarzanych w systemach teleinformatycznych Agencji 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 Agencji, jakie są tego koszty).
6. Przy ograniczaniu skutków incydentu Administrator Systemu/Administrator Zabezpieczeń Fizycznych, w uzgodnieniu z dyrektorem komórki właściwej ds. bezpieczeństwa informacji, może korzystać z konsultantów zewnętrznych, jeśli Agencja wcześniej zawarła w umowach z tymi podmiotami stosowne zapisy o przekazywaniu i ochronie informacji Agencji.

§ 5.

Odtwarzanie systemu informacyjnego

1. Z zastrzeżeniem ust. 4, Administrator Systemu przystępuje do odtworzenia systemu po zidentyfikowaniu i usunięciu lub zablokowaniu źródła incydentu.
2. W przypadku zaistnienia sytuacji, kiedy nastąpiło uruchomienie Planu Zapewnienia Ciągłości Działania ARiMR, odtwarzanie systemu jest realizowane w oparciu o procedury opisane w tym planie.
3. Odtwarzanie systemu odnosi się do punktu odtworzenia, co do którego Administrator Systemu ma uzasadnioną pewność, że nie zawiera źródła incydentu.
4. Zasoby w postaci oprogramowania oraz danych są odtwarzane z oryginalnych źródeł dystrybucji oprogramowania oraz kopii zapasowych.
5. Prezes Agencji, po zasięgnięciu opinii dyrektora komórki właściwej ds. bezpieczeństwa informacji i Administratora Systemu, może podjąć decyzję o podjęciu przetwarzania mimo braku pewności usunięcia źródła incydentu, jeśli szacowane negatywne skutki braku przetwarzania przewyższają potencjalne ryzyko podjęcia działania.

§ 6.

Działania po zakończeniu incydentu

1. Dyrektor komórki właściwej ds. bezpieczeństwa informacji, przy wsparciu Administratora Systemu, Właścicieli Procesów / Właścicieli Zasobów, Administratora

Zabezpieczeń Fizycznych, sporządza raport z incydentu, zgodnie ze wzorem zamieszczonym w załączniku nr 3 do niniejszego regulaminu, oraz przedstawia go Komitetowi.

2. Jeśli zachodzi taka potrzeba, to Administrator Systemu/ Administrator Zabezpieczeń Fizycznych 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. Dyrektor komórki właściwej ds. bezpieczeństwa informacji przedkłada Prezesowi Agencji rekomendacje w zakresie działań zmierzających do zmniejszenia ryzyka powtórzenia incydentu w przyszłości.

§ 7.

Rejestrowanie informacji o incydentach

1. Dyrektor komórki właściwej ds. bezpieczeństwa informacji 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. Dyrektor komórki właściwej ds. bezpieczeństwa informacji prowadzi analizy i statystyki incydentów.
3. Dyrektor komórki właściwej ds. bezpieczeństwa informacji zapewnia właściwe wykorzystanie informacji o incydentach związanych z bezpieczeństwem informacji dla celów szkoleniowych i doskonalenia systemu zarządzania bezpieczeństwem informacji.

§ 8.

Gromadzenie materiału dowodowego

1. Na każdym etapie postępowania z incydentem, dyrektor komórki właściwej ds. bezpieczeństwa informacji 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 Agencji).
4. Zabezpieczenie środków przetwarzania informacji jest przeprowadzane zgodnie z instrukcją zamieszczoną w załączniku nr 1 do niniejszego regulaminu.
5. Protokół ze sporządzenia elementu materiału dowodowego lub zabezpieczenia środków przetwarzania informacji jest sporządzany zgodnie ze wzorem zamieszczonym w załączniku nr 2 do niniejszego regulaminu.
6. Wszelkie działania w systemie teleinformatycznym, związane z postępowaniem z incydentem, 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.

Załącznik nr 1 do Regulaminu zarządzania incydentami - 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 WSZYSTIE 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. ZAPLOMBUJ WOREK I WYPEŁNIJ METRYCZKĘ. Metryczka powinna zawierać typ, numer seryjny urządzenia i numer inwentarzowy nadany przez Agencję 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 protokółu, 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 przejęcia 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:

a) 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),
b) Skontaktuj się z odpowiednią komórką organizacyjną Agencji 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.

Załącznik nr 2 do Regulaminu zarządzania incydentami - Wzór protokołu zabezpieczenia materiału dowodowego

PROTOKÓŁ ZABEZPIECZENIA MATERIAŁU DOWODOWEGO

Wykonano w dniu ..... o godzinie ..... w obecności:

Świadek 1: <imię i nazwisko, stanowisko, komórka organizacyjna Agencji>

Świadek 2: <imię i nazwisko, stanowisko, komórka organizacyjna Agencji>

Świadek 3: <imię i nazwisko, niezależny ekspert>

I. Rodzaj materiału dowodowego

(zaznaczyć właściwe kwadraty i wpisać odpowiednie nazwy i oznaczenia)

Dokument papierowy	☐	*Rodzaj i Nazwa dokumentu:*			
Dokument elektroniczny	☐	*Rodzaj i Nazwa dokumentu:*			
Kopia zapasowa	☐	System operacyjny *Nazwa i wersja systemu:*		Aplikacja *Nazwa i wersja aplikacji:*	☐
		Baza danych *Nazwa i wersja bazy*:	☐	Oznaczenie nośnika	
Obraz dysku	☐	Lokalizacja dysku (adres IP/IPX): ..... Typ i nr seryjny dysku:			
Pliki konfiguracyjne i/lub systemowe	☐	System operacyjny *Nazwa i wersja systemu:*	☐	Aplikacja *Nazwa i wersja aplikacji:*	☐
		Baza danych *Nazwa i wersja bazy*:	☐	Nazwa(y) Pliku(ów)	
Kopie zawartości dzienników (logów) zdarzeń	☐	System operacyjny *Nazwa i wersja systemu:*	☐	Aplikacja *Nazwa i wersja aplikacji:*	☐
		Baza danych *Nazwa i wersja bazy*:	☐	Nazwa(y) Pliku(ów)	
Kopia zawartości skrzynki pocztowej	☐	zewnętrzna	☐	wewnętrzna	☐
		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 . . . . . .

Załącznik nr 3 do Regulaminu zarządzania incydentami - Wzór raportu z incydentu

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 telefonu ……e-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 - ADMINISTRATOR SYSTEMU/ ADMINISTRATOR ZABEZPIECZEŃ FIZYCZNYCH/ IBI

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 – IBI w Centrali/OR)

Data rozpoczęcia postępowania ws. incydentu ……

Data zakończenia incydentu (jeśli jest zakończony) ……

Data zamknięcia skutków incydentu ……

Data zakończenia postępowania ws. incydentu ……

Data przedstawienia incydentu na KSBI ……

USTALENIA – OPIS POSTĘPOWANIA - SPRAWCY INCYDENTU

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

……
……
……
……
……
……
……

WNIOSKI I REKOMENDACJE

(w tym zalecenia dotyczące zmian w SZBI)

……
……
……
……
……
……
……
……
……

WYKAZ DOŁĄCZONYCH DOKUMENTÓW

……
……
……
……

DANE OSÓB PROWADZĄCYCH POSTĘPOWANIE WYJAŚNIAJĄCE

Imię i Nazwisko ……. Imię i Nazwisko ……

Stanowisko …….. Stanowisko ……

Data ……..…… Data ……..

Podpis …… Podpis ……..……