Załącznik nr 6 do

Polityki Zarządzenia Systemem Informatycznym

Procedura zarządzania incydentami z zakresu bezpieczeństwa systemów teleinformatycznych i informacji

1. Skróty i definicje.

Administrator Danych (AD) – Starostwo Powiatowe w Wąbrzeźnie reprezentowane przez Starostę Wąbrzeskiego
IOD – Inspektor Ochrony Danych
CSK – Centrum Sieci Komputerowych
CERT – Rządowy Zespół Reagowania na Incydenty Komputerowe
Administrator Systemów Informatycznych (ASI) – pracownik administrujący określonym systemem IT. Rolą ASI jest zapewnienie efektywnego zarządzania operacyjnego danego systemu IT i sprawnej jego pracy. Do typowych zadań administratora należy nadzorowanie pracy powierzonych systemów IT, zarządzanie kontami i uprawnieniami użytkowników (na poziomie systemowym), konfiguracja zasobu, instalowanie i aktualizacja oprogramowania, nadzorowanie, wykrywanie i eliminowanie błędów oraz nieprawidłowości, asystowanie i współpraca z zewnętrznymi specjalistami przy pracach instalacyjnych, konfiguracyjnych i naprawczych, a także zapewnienie aktualności dokumentacji takiego zasobu obejmującego również dokumentację zmian mających bezpośredni wpływ na jego funkcjonalność. ASI odpowiada za właściwą i aktualną informację o systemach.

2. Cel procedury.

Celem Procedury Zarządzania Incydentami Związanymi z Bezpieczeństwem Informacji jest zapewnienie, monitorowania zdarzeń związanych z bezpieczeństwem informacji oraz słabości systemów informacyjnych, a także możliwość zgłaszania i szybkiego podejmowania działań korygujących.

3. Zakres stosowania.

Działania opisane w niniejszej procedurze obowiązują, we wszystkich komórkach organizacyjnych jednostki.

4. Odpowiedzialność.

Odpowiedzialność za prawidłowe zgłoszenie incydentów dotyczących bezpieczeństwa infrastruktury informatycznej spoczywa na pracownikach dokonujących zgłoszeń. ASI odpowiedzialny za rozwiązanie problemu lub zapobieżenie incydentowi działa zgodnie z niniejszą procedurą.

Zespół ds. monitorowania zagrożeń i utrzymania Systemu Zarządzania Bezpieczeństwem Informacji, w którego skład wchodzą ASI oraz IOD jest odpowiedzialny za:

1) Niezwłoczne reagowanie na incydenty bezpieczeństwa informacji w określony i z góry ustalony sposób;
2) Ocenę istniejących i potencjalnych zagrożeń w zakresie bezpieczeństwa informacji;
3) Ocenę przyczyn i skutków incydentów naruszenia bezpieczeństwa informacji w tym gromadzenie materiału dowodowego;

4) Przygotowywanie propozycji działań korygujących i naprawczych oraz nadzór nad ich wprowadzaniem;
5) Dokonywanie okresowego przeglądu i aktualizacji polityk regulujących bezpieczeństwo informacji ;
6) Prowadzenie działań zmierzających do wzrostu świadomości w zakresie zapewnienia bezpieczeństwa informacji wśród pracowników;
7) Współpracę z Rządowym Zespołem Reagowania na Incydenty Komputerowe CERT.

5. Klasyfikacja incydentów.

Podział zdarzeń:

1) **Zdarzenia losowe zewnętrzne** (np.: klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej, ciągłość pracy systemów zostaje zakłócona, nie dochodzi do naruszenia poufności danych.
2) **Zdarzenia losowe wewnętrzne** (np. : niezamierzone pomyłki operatorów, administratorów, awarie sprzętowe, błędy w oprogramowaniu), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych.
3) **Zdarzenia zamierzone, świadome i celowe** stanowią najpoważniejsze zagrożenie naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zdarzenia te możemy podzielić na:
    a) nieuprawniony dostęp do danych z zewnątrz (włamanie do systemu),
    b) nieuprawniony dostęp do danych z sieci wewnętrznej,
    c) nieuprawniony transfer danych,
    d) pogorszenie funkcjonowania sprzętu i oprogramowania (np.: działanie wirusów),
    e) bezpośrednie zagrożenie materialnych składników systemu (np.: kradzież sprzętu).

Przykłady zdarzeń, które mogą być zakwalifikowane jako uzasadnione podejrzenie naruszenia bezpieczeństwa informacji:

1) Sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na infrastrukturę teleinformatyczną jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.
2) Niewłaściwe parametry środowiska jak zbyt wysoka temperatura lub nadmierna wilgotność (w szczególności dotyczy to serwerowni).
3) Awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie systemu, a w tym sam fakt pozostawienia serwisantów bez nadzoru.
4) Pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu.
5) Jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikacje w systemie.
6) Nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie.

7) Stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji).
8) Nastąpiła niedopuszczalna manipulacja danymi w systemie.
9) Ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą elementy systemu zabezpieczeń.
10) Praca w systemie lub w sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych, np.: praca w systemie lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.
11) Ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. „bocznej furtki", itp.
12) Podmieniono lub zniszczono nośniki z danymi bez odpowiedniego upoważnienia lub w niedozwolony sposób skasowano lub kopiowano dane osobowe
13) Rażąco naruszono dyscyplinę pracy w zakresie przestrzegania bezpieczeństwa (nie wylogowanie się, pozostawienie włączonego komputera po zakończeniu pracy, nie zamknięcie pokoju z komputerem, nie wykonywanie w ustalonych terminach kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.)
14) Stwierdzenie nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych, w tym także osobowych (otwarte szafy, regały, biurka).

6. Zgłaszanie incydentów

Pracownicy mają obowiązek zgłaszać zauważone przez siebie incydenty oraz notować wszystkie szczegóły związane z incydentem. Incydenty należy zgłaszać do informatyka e-mail: informatyk@wabrzezno.pl lub telefonicznie pod numery **56 6882450**, lub **785699222**. Zgłoszenie musi zawierać (zał. nr 2):

a) imię i nazwisko zgłaszającego,
b) miejsce i datę wystąpienia incydentu,
c) opis zdarzenia.

Zgłaszający incydent nie powinien podejmować żadnych działań na własną rękę jednak w miarę możliwości powinien zabezpieczyć materiał dowodowy, np.: robiąc zdjęcie ekranu komputera, co do którego zaistniało podejrzenie, że jego działanie odbiega od normy. W przypadku podejrzenia zainfekowania komputera wirusa należy niezwłocznie skontaktować się z ASI.

7. Postępowanie z incydentami

Obsługa incydentu rozpoczyna się od jego dokładnego rozpoznania - ustalenia oznak naruszenia bezpieczeństwa, identyfikacji rodzaju incydentu, identyfikacji i zabezpieczenia dowodów oraz poinformowania o zdarzaniu odpowiednich osób.

1) Za obsługę incydentów bezpieczeństwa teleinformatycznego odpowiada ASI, który przyjął zgłoszenie (zał. nr 3), powiadamia niezwłocznie IOD.
2) Po analizie zdarzenia i okoliczności z nim związanych ASI wprowadza dane o incydencie do rejestru incydentów oraz zabezpiecza materiał dowodowy.

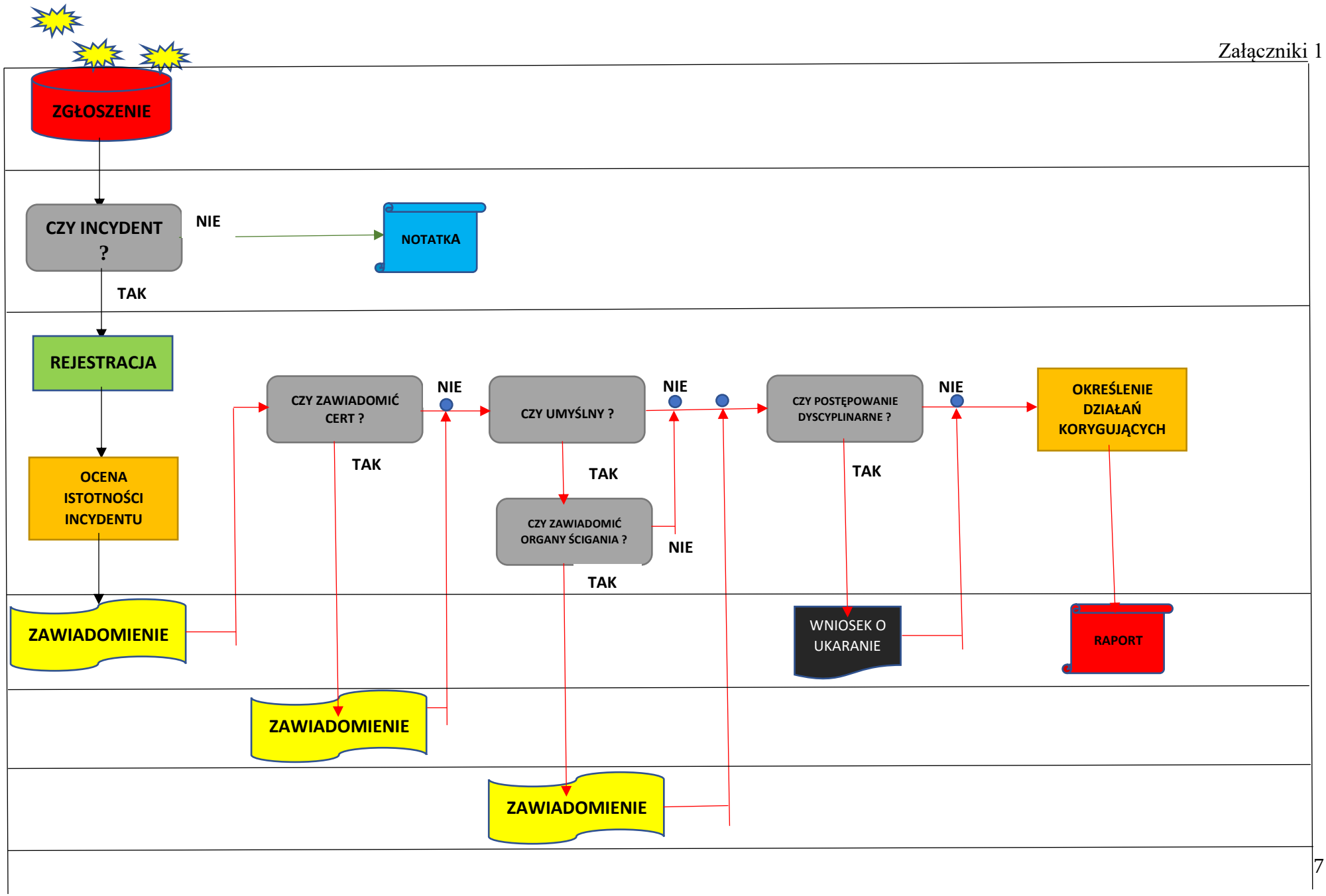
3) Zespół zbiera się niezwłocznie, dokonuje analizy materiału dowodowego i podejmuje decyzję o sposobie dalszego postępowania. Gromadzenie materiału dowodowego:
    a) dla dokumentów papierowych: oryginał jest bezpiecznie przechowywany wraz z informacją, kto znalazł dokument, gdzie, kiedy i kto by był świadkiem tego zdarzenia; każde śledztwo może wykazać, że oryginał nie został naruszony
    b) dla dokumentów na nośnikach komputerowych zaleca się: utworzenie obrazu lub kopii (zależnie od stosownych wymagań) wszelkich nośników wymiennych; zaleca się zapisanie informacji znajdujących się na dyskach twardych lub w pamięci komputera, aby zapewnić ich dostępność, zaleca się zachowanie zapisów wszelkich działań podczas procesu kopiowania oraz aby proces ten odbywał się w obecności świadków; zaleca się przechowywanie oryginalnego nośnika i dziennika zdarzeń w sposób bezpieczny i nienaruszony (jeśli to niemożliwe, to co najmniej jeden obraz lustrzany lub kopię).
4) W przypadku, gdy zgłoszone zdarzenie zostało uznane za incydent bezpieczeństwa informacji, Zespół dokonuje oceny istotności incydentu oraz zawiadamia AD o zaistnieniu incydentu oraz poziomie zagrożenia dla bezpieczeństwa informacji. Zespół ds. monitorowania zagrożeń i utrzymania Systemu Zarządzania Bezpieczeństwem Informacji ocenia poziom istotności incydentu dla jednostki kierując się następującymi kryteriami:
    a) wpływ incydentu na ciągłość działania jednostki i wypełnianie jego zadań statutowych;
    b) krytyczność systemów dotkniętych skutkami incydentu bezpieczeństwa;
    c) wrażliwość informacji, których poufność, integralność czy dostępność naruszono (na przykład czy naruszono bezpieczeństwo informacji prawnie chronionej — np.: danych osobowych, informacji niejawnych);
    d) rozległość wpływu incydentu na działanie systemów (nie działa jeden komputer, cała sieć itp.);
    e) rozmiar szkód powstałych skutkiem incydentu;
    f) koszt usunięcia i naprawy skutków incydentu bezpieczeństwa;
    g) szacowany czas przywrócenia ciągłości działania dotkniętego incydentem bezpieczeństwa systemu;
    h) zasoby wymagane do przywrócenia ciągłości działania systemu (personel, wsparcie firm zewnętrznych, wymagane dodatkowe czy zamienne urządzenia oraz oprogramowanie, czas odtwarzania systemów z kopii zapasowych itp.);
5) Jeżeli istotność incydentu jest wysoka, należy zawiadomić Rządowy Zespół Reagowania na Incydenty Komputerowe **CERT.GOV.PL** pełniący rolę głównego zespołu CERT w obszarze administracji rządowej. Wyznaczony przez przewodniczącego członek zespołu wypełnia formularz zgłoszenia incydentu, ściągnięty ze strony www.cert.gov.pl oraz wysyła go do CERT zgodnie z informacją zamieszczoną na tej stronie. Incydent zgłaszany jest dwutorowo, faksem na numer **+48 22 58 58 833** oraz pocztą elektroniczną na adres incydent@cert.gov.pl .Dalsza korespondencja z CERT w sprawie tego incydentu odbywa się za pomocą szyfrowanej poczty elektronicznej.
6) W przypadku, gdy zgłoszone zdarzenie nie zostało zaklasyfikowane jako incydent bezpieczeństwa informacji, ma charakter fałszywego alarmu ASI powiadamia zgłaszającego o zdarzeniu, że zdarzenie nie stanowi incydent bezpieczeństwa.

7) W przypadku stwierdzenia działań umyślnych i ustaleniu sprawcy incydentu zespół przekazuje wyniki analizy wraz z zabezpieczonym materiałem dowodowym AD w celu wyciągnięcia konsekwencji dyscyplinarnych wobec sprawcy, ewentualnego zawiadomienia organów ścigania lub podjęcia kroków prawnych wobec osób trzecich.
8) Zespół ds. monitorowania zagrożeń i utrzymania Systemu Zarządzania Bezpieczeństwem Informacji inicjuje działania naprawcze zmierzające do zniwelowania szkód wyrządzonych przez incydent, wyciąga wnioski z każdego incydentu i określa, jeśli to możliwe działania korygujące i zapobiegawcze w celu uniknięcia ponownego wystąpienia incydentu.
9) Zespół na bieżąco dokumentuje swoje działania na każdym z etapów procesu zarządzania incydentem w formie notatki. Obsługa incydentu kończy się raportem zatwierdzonym przez AD zawierającym opis incydentu oraz wnioski co do działań na przyszłość. (zał. nr 1)

8. Szkolenia.

Brak wiedzy i umiejętności poprawnego rozpoznania i klasyfikacji oraz oceny poziomu istotności incydentu po stronie zgłaszającego nie może być przyczyną zaniechania powiadomienia osób odpowiedzialnych w jednostce o zaistniałym incydencie lub podejrzeniu jego wystąpienia. Dlatego w miarę posiadanych zasobów, co najmniej raz do roku należy przeprowadzać okresowe szkolenia pracowników w zakresie bezpieczeństwa teleinformatycznego i zarządzania incydentami. Niezależnie od prowadzonych szkoleń wskazane jest przeprowadzanie szkolenia każdego nowozatrudnionego pracownika celem zapewnienia znajomości zasad prawidłowego zgłaszania incydentów. (zał. nr 4)

Załączniki:
1. Schemat postępowania z incydentami związanymi z bezpieczeństwem informacji
2. Zgłoszenie wstępne z naruszenia ochrony danych osobowych
3. Dziennik Ewidencji Incydentów Bezpieczeństwa TI
4. Dziennik Ewidencji Szkoleń w Zakresie Bezpieczeństwa TI
5. Wykaz przykładowych incydentów


ZGŁOSZENIE
CZY INCYDENT ?
NIE
NOTATKA
TAK
REJESTRACJA
OCENA ISTOTNOŚCI INCYDENTU
ZAWIADOMIENIE
CZY ZAWIADOMIĆ CERT ?
NIE
TAK
ZAWIADOMIENIE
CZY UMYŚLNY ?
NIE
TAK
CZY ZAWIADOMIĆ ORGANY ŚCIGANIA ?
NIE
TAK
ZAWIADOMIENIE
CZY POSTĘPOWANIE DYSCYPLINARNE ?
NIE
TAK
WNIOSEK O UKARANIE
OKREŚLENIE DZIAŁAŃ KORYGUJĄCYCH
RAPORT

Załączniki 2

1. Data ……..……. Godzina ……
2. Osoba powiadamiająca o naruszeniu oraz inne osoby zaangażowane lub odpytane w związku z naruszeniem (imię, nazwisko, stanowisko służbowe,):
   ……
   ……..……
   ……
   ……
3. Lokalizacja zdarzenia (nr. pokoju, nazwa pomieszczenia, określenie komputerowego stanowiska roboczego, nazwa programu lub aplikacji itp.):
   ……
   ……..……
   ……
   ……
4. Rodzaj naruszenia i określenie okoliczności towarzyszących naruszeniu:
   ……
   ……
   ……
   ……
   ……
5. Podjęte działania:
   ……
   ……
   ……
   ……
   ……
   ……
   ……
6. Wstępna ocena przyczyn wystąpienia naruszenia:
   ……
   ……
   ……
   ……
   ……
7. Postępowanie wyjaśniające i naprawcze:
   ……
   ……
   ……
   ……
   ……
   ……
   ……
   ……
   ……

……
(podpis zgłaszającego)

Załącznik 3

DZIENNIK EWIDENCJI INCYDENTÓW BEZPIECZEŃSTWA TI

Lp.	Imię i nazwisko oraz funkcja osoby zgłaszającej incydent	Opis incydentu, data oraz okoliczności jego wykrycia	Opis dalszego postępowania	Imię i nazwisko osoby dokonującej zapisu	Uwagi
1.	2.	3.	4.	5.	6.

Załącznik 4

DZIENNIK EWIDENCJI SZKOLEŃ W ZAKRESIE BEZPIECZEŃSTWA TI

Lp.	Data szkolenia	Zakres szkolenia	Uczestnik/cy szkolenia	Uwagi/ podpis prowadzącego szkolenie
1.				
2.				
3.				
4.				
5.				
6.				
6.				
8.				

Załącznik 5

Wykaz przykładowych incydentów

FORMY NARUSZEŃ	SPOSOBY POSTĘPOWANIA
W ZAKRESIE WIEDZY	
Ujawnianie sposobu działania aplikacji i systemu oraz jej zabezpieczeń osobom niepowołanym.	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. **Bezzwłocznie powiadomić inspektora ochrony danych osobowych (IOD).**
Ujawnianie informacji o sprzęcie i pozostałej infrastrukturze informatycznej.	
Dopuszczanie i stwarzanie warunków, aby ktokolwiek taką wiedzę mógł pozyskać np. z obserwacji lub dokumentacji.	
W ZAKRESIE SPRZĘTU I OPROGRAMOWANIA	
Opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji umożliwiającej dostęp do bazy danych osobowych.	Niezwłocznie zakończyć działanie aplikacji.
Dopuszczenie do korzystania z aplikacji umożliwiającej dostęp do bazy danych osobowych przez jakiekolwiek inne osoby niż osoba, której identyfikator został przydzielony.	Wezwać osobę bezprawnie korzystającą z aplikacji do opuszczenia stanowiska przy komputerze.
Pozostawienie w jakimkolwiek niezabezpieczonym, a w szczególności w miejscu widocznym, zapisanego hasła dostępu do bazy danych osobowych lub sieci.	Natychmiast zabezpieczyć notatkę z hasłami w sposób uniemożliwiający odczytanie.
Dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania umożliwiającego dostęp do bazy danych osobowych osobom nieuprawnionym.	Wezwać osobę nieuprawnioną do opuszczenia stanowiska. Ustalić, jakie czynności zostały przez osoby nieuprawnione wykonane. Przerwać działające programy.
Samodzielne instalowanie jakiegokolwiek oprogramowania.	Pouczyć osobę popełniającą wymienioną czynność, aby jej zaniechała. Wezwać Informatyka w celu odinstalowania programów. **Bezzwłocznie powiadomić administratora systemu informatycznego (ASI).**
Modyfikowanie parametrów systemu i aplikacji.	Wezwać osobę popełniającą wymieniona czynność, aby jej zaniechała. **Bezzwłocznie powiadomić administratora systemu informatycznego (ASI).**

Odczytywanie wymiennych nośników danych przed sprawdzeniem ich programem antywirusowym.	Pouczyć osobę popełniającą wymienioną czynność, aby zaczęła stosować się do wymogów bezpieczeństwa pracy w systemie. Wezwać Administratora Systemu Informatycznego lub informatyka w celu wykonania kontroli antywirusowej. Sporządzić raport.
W ZAKRESIE DOKUMENTÓW I OBRAZÓW ZAWIERAJĄCYCH DANE OSOBOWE	
Pozostawienie dokumentów w otwartych pomieszczeniach bez nadzoru.	Zabezpieczyć dokumenty.
Przechowywanie dokumentów niewłaściwie zabezpieczonych przed dostępem osób niepowołanych.	Powiadomić przełożonych. Spowodować poprawienie zabezpieczeń.
Wyrzucanie dokumentów w stopniu zniszczenia umożliwiającym ich odczytanie.	Zabezpieczyć niewłaściwie zniszczone dokumenty. **Bezzwłocznie powiadomić Inspektora ochrony danych osobowych (IOD).**
Dopuszczanie do kopiowania dokumentów i utraty kontroli nad kopią.	Zaprzestać kopiowania. Odzyskać i zabezpieczyć wykonaną kopię. Powiadomić przełożonych.
Dopuszczanie, aby inne osoby odczytywały zawartość ekranu monitora, na którym wyświetlane są dane osobowe.	Wezwać nieuprawnioną osobę odczytującą dane do zaprzestania czynności, wyłączyć monitor.
Sporządzanie kopii danych na nośnikach danych w sytuacjach nie przewidzianych procedurą.	Spowodować zaprzestanie kopiowania. Podjąć próbę odzyskania oraz zabezpieczyć wykonaną kopię. **Bezzwłocznie powiadomić (ASI).**
Utrata kontroli nad kopią danych osobowych.	Podjąć próbę odzyskania kopii. **Bezzwłocznie powiadomić (ASI).**
W ZAKRESIE POMIESZCZEŃ I INFRASTRUKTURY SŁUŻĄCYCH DO PRZETWARZANIA DANYCH OSOBOWYCH	
Opuszczanie i pozostawianie bez dozoru nie zamkniętego pomieszczenia, w którym zlokalizowany jest sprzęt komputerowy używany do przetwarzania danych osobowych, co stwarza ryzyko dokonania na sprzęcie lub oprogramowaniu modyfikacji zagrażających bezpieczeństwu danych osobowych.	Zabezpieczyć pomieszczenie.
Wpuszczanie do pomieszczeń osób nieznanych i dopuszczanie do ich kontaktu ze sprzętem komputerowym.	Wezwać osoby bezprawnie przebywające w pomieszczeniach do ich opuszczenia, próbować ustalić ich tożsamość.
Dopuszczanie, aby osoby spoza służb informatycznych i telekomunikacyjnych podłączały jakiekolwiek urządzenia do sieci	Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania. Postarać się ustalić ich tożsamość. **Powiadomić (ASI).**

komputerowej, demontowały elementy obudów gniazd i torów kablowych lub dokonywały jakichkolwiek manipulacji.	
W ZAKRESIE POMIESZCZEŃ, W KTÓRYCH ZNAJDUJĄ SIĘ KOMPUTERY CENTRALNE I URZĄDZENIA SIECI	
Dopuszczenie lub ignorowanie faktu, że osoby spoza służb informatycznych i telekomunikacyjnych dokonują jakichkolwiek manipulacji przy urządzeniach lub okablowaniu sieci komputerowej w miejscach publicznych (hole, korytarze, itp.).	Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania i ew. opuszczenia pomieszczeń. Postarać się ustalić ich tożsamość. **Bezzwłocznie powiadomić inspektora ochrony danych osobowych (IOD).**
Dopuszczanie do znalezienia się w pomieszczeniach komputerów centralnych lub węzłów sieci komputerowej osób spoza służb informatycznych i telekomunikacyjnych.	Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania i opuszczenia chronionych pomieszczeń. Postarać się ustalić ich tożsamość. **Bezzwłocznie powiadomić inspektora ochrony danych osobowych (IOD).**