ZARZĄDZENIE Nr 43/2022
BURMISTRZA PISZA
z dnia 8 marca 2022 r.

w sprawie **wprowadzenia Procedury postępowania z incydentami bezpieczeństwa informacji i cyberbezpieczeństwa**

Na podstawie art. 33 ust. 1 i 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2021 r. poz. 1372 z późn. zm.), w zw. z art. 22 ust. 1 pkt 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369 z późn. zm.), **zarządzam, co następuje:**

§ 1.

W Urzędzie Miejskim w Piszu wprowadzam Procedurę postępowania z incydentami bezpieczeństwa informacji i cyberbezpieczeństwa, stanowiącą Załącznik do niniejszego zarządzenia.

§ 2.

Zobowiązuję wszystkich pracowników Urzędu Miejskiego w Piszu do zapoznania się z Procedurą, o której mowa w § 1 zarządzenia.

§ 3.

Wykonanie zarządzenia powierza się Sekretarzowi Gminy Pisz.

§ 4.

Zarządzenie wchodzi w życie z dniem 9 marca 2022 r.

BURMISTRZ
Andrzej Szymborski

ADWOKAT
Rafał Orłowski

K. Marciniak

Załącznik do Zarządzenia Nr 43/2022
Burmistrza Pisza
z dnia 8 marca 2022 r.

Procedura postępowania

z incydentami bezpieczeństwa informacji i cyberbezpieczeństwa

I. Postanowienia ogólne

Procedura zarządzania incydentami bezpieczeństwa informacji i cyberbezpieczeństwa, zwana dalej „procedurą", ma na celu zapewnienie ciągłości operacyjnej oraz ograniczenie wpływu przypadków naruszeń bezpieczeństwa zasobów informacyjnych, w tym bezpieczeństwa przetwarzania danych osobowych, na działalność Urzędu Miejskiego w Piszu. Z niniejszej procedury wyłączone są informacje niejawne, dla których stosowane są odrębne przepisy.

II. Cel procedury

Celem wprowadzenia do stosowania niniejszej procedury jest zapewnienie właściwego postępowania w zakresie zgłaszania i obsługi incydentów bezpieczeństwa i cyberbezpieczeństwa.

III. Zakres stosowania

Działania opisane w niniejszej procedurze obowiązują pracowników wszystkich wydziałów, samodzielne stanowiska pracy oraz inne podmioty korzystające z sieci komputerowej Urzędu Miejskiego w Piszu, zwanego dalej „Urzędem". Procedura obowiązuje również podmioty zewnętrzne, które dopuszczono do przetwarzania danych, w tym danych osobowych będących zasobami informacyjnymi Urzędu Miejskiego w Piszu.

IV. Definicje

Definicje użyte w niniejszej procedurze oznaczają:

1) **RODO** – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 5 kwietnia 2016 r.);
2) **ustawa o ochronie danych osobowych** – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781);
3) **dane osobowe** – zgodnie z art. 4 ust. 1 pkt 1 RODO oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
4) **dane szczególne** – szczególne kategorie danych osobowych, o których mowa w art. 9 ust. 1 RODO ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne oraz dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby;
5) **incydent bezpieczeństwa** – pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem zasobów informacyjnych;
6) **incydent cyberbezpieczeństwa** – to zdarzenie, którego skutkiem jest lub może być naruszenie bezpieczeństwa aktywów informacyjnych oraz który powoduje lub może

spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez Urząd;

7) **organ nadzorczy** – zgodnie z art. 4 ust. 1 pkt 21 RODO – Prezes Urzędu Ochrony Danych;
8) **osoba nieuprawniona** – oznacza osobę fizyczną lub prawną, jednostkę lub inny podmiot, któremu ujawnia się dane z zasobów informacyjnych z naruszeniem przepisów o ochronie danych osobowych lub poza wyraźnym uprawnionym poleceniem Administratora Danych Osobowych;
9) **osoba wyznaczona do kontaktów w sprawach cyberbezpieczeństwa** – osoba wyznaczona zgodnie z art. 21 ust. 1 ustawy o krajowym systemie cyberbezpieczeństwa;
10) **osoba upoważniona** – osoba wykonująca zadania polegające na przetwarzaniu, w formie tradycyjnej lub elektronicznej, danych osobowych na wyraźne polecenie Administratora Danych Osobowych i jest upoważniona do wykonywania tych czynności;
11) **Administrator Danych Osobowych** – Gmina Pisz reprezentowana przez Burmistrza Pisza, który ustala cele, sposoby przetwarzania danych osobowych, ustanawia system ochrony danych osobowych, tj. zasady oraz zabezpieczenie stosowane podczas przetwarzania danych osobowych.

V. Przyczyny i kategorie incydentów

1. Przyczyną incydentu bezpieczeństwa lub cyberbezpieczeństwa może być:
   1) zdarzenie losowe zewnętrzne (np. klęski żywiołowe, pożary, zakłócenia w dostawie energii elektrycznej itp.), którego wystąpienie może powodować zniszczenie lub uszkodzenie infrastruktury informatycznej albo dokumentacji papierowej oraz zakłócenie ciągłości pracy systemów nie powodując naruszenia poufności danych;
   2) zdarzenie losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratorów, awarie sprzętu, błędy w oprogramowaniu, itp.), które mogą spowodować zniszczenie lub utratę danych, zakłócenia ciągłości pracy systemów, 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,
      d) pogorszenie funkcjonowania sprzętu i oprogramowania (np. działanie wirusów),
      e) bezpośrednie zagrożenie materialnych składników systemu (np. kradzież sprzętu).
2. 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 wilgoć (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 tym samym 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 modyfikację 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 ich obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.;
11) ujawniono istnienie nieautoryzowanych kont dostępu do danych lub do 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 Polityki Bezpieczeństwa Informacji (brak wylogowania się, pozostawienie włączonego komputera po zakończeniu pracy, brak zamknięcia pokoju z komputerem, brak wykonania w ustalonych terminach kopii bezpieczeństwa, prac na danych osobowych w celach prywatnych, itp.;
14) stwierdzenie nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych, w tym także osobowych (otwarte szafy, regały, biurka).

VI. Zgłaszanie incydentów i obsługa incydentów

1. Każdy pracownik oraz współpracownik ma obowiązek zgłosić podejrzenie wystąpienia incydentu bezpieczeństwa lub cyberbezpieczeństwa.
2. Zgłoszenie incydentu bezpieczeństwa należy złożyć w jeden z poniższych sposobów:
   1) drogą elektroniczną na adres: wojciech.jozwik@pisz.home.pl;
   2) pisemnie przekazując zgłoszenie do Punktu Obsługi Interesanta;

3) w formie notatki bezpośredniemu przełożonemu lub osobie wyznaczonej do kontaktów w sprawie cyberbezpieczeństwa.

3. Zgłoszenie o podejrzeniu wystąpienia incydentu bezpieczeństwa powinno zawierać: opis sytuacji wskazującej na potencjalne naruszenie / naruszenie zasad ochrony danych osobowych, datę zdarzenia, konsekwencje zdarzenia (o ile zaistniały), uczestników zdarzenia oraz dotychczasowo podjęte działania w zakresie minimalizacji skutków zdarzenia (o ile zostały podjęte).
4. Zgłaszający incydent nie powinien podejmować żadnych działań na własną rękę, jednak w miarę możliwości powinien zabezpieczyć materiał dowodowy, np. zrzut ekranu monitora, zdjęcie niezabezpieczonych materiałów zawierających dane osobowe itp.).
5. Za obsługę incydentów bezpieczeństwa odpowiada osoba wyznaczona do kontaktów w sprawie cyberbezpieczeństwa.
6. W przypadku nieobecności osoby wyznaczonej do kontaktów w sprawie cyberbezpieczeństwa, obsługę incydentów zapewnia wyznaczony informatyk Urzędu.
7. Osoba odpowiedzialna za obsługę incydentu bezpieczeństwa dokonuje analizy otrzymanego zgłoszenia, tj. przedstawionych informacji i identyfikuje przyczynę wystąpienia zdarzenia oraz wskazuje działania do podjęcia w celu minimalizacji skutków zdarzenia.
8. Działania związane z obsługą zgłoszenia w pierwszej kolejności dotyczą rozpoznania i kwalifikacji zgłoszenia. W przypadku, kiedy zgłoszenie zakwalifikowane zostało jako incydent bezpieczeństwa informacji, dokonywana jest jego ocena istotności.
9. Przy ocenie istotności incydentu pod uwagę brane są następujące czynniki:
   1) powstałe szkody będące wynikiem incydentu;
   2) wpływ incydentu na działanie systemów;
   3) wpływ incydentu na ciągłość działania Urzędu;
   4) koszty usunięcia skutków incydentu;
   5) szacowany czas naprawy skutków wywołanych incydentem;
   6) oszacowanie zasobów koniecznych do przywrócenia ciągłości działania systemów.
10. Zakwalifikowanie zgłoszenia incydentu jako „fałszywy alarm" kończy postępowanie, o czym informuje się zgłaszającego.
11. W przypadku zakwalifikowania zdarzenia jako incydentu związanego z bezpieczeństwem informacji, osoba wyznaczona do kontaktów w sprawie cyberbezpieczeństwa podejmuje działania zabezpieczające i naprawcze zmierzające do zniwelowania szkód powstałych w wyniku incydentu.
12. W przypadku, gdy waga incydentu dotyczy systemów informatycznych i zakwalifikowana jest jako wysoka, o incydencie zawiadamiany jest zespół reagowania na incydenty CSIRT NASK – prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy.
13. Informację o wynikach analizy incydentu oraz podjętych działaniach naprawczych przekazuje się Administratorowi Danych Osobowych.
14. W przypadku stwierdzenia działań zamierzonych, przy jednoczesnym zidentyfikowaniu sprawcy incydentu dotyczącego naruszenia bezpieczeństwa informacji Administrator Danych Osobowych podejmuje decyzję dotyczącą wyciągnięcia ewentualnych konsekwencji dyscyplinarnych wobec sprawcy incydentu.

Jednocześnie, w zależności od wagi incydentu, mogą być zawiadomione organy ścigania.

15. Powyższe działania raportowane są w rejestrze incydentów związanych z bezpieczeństwem informacji, którego wzór stanowi Załącznik Nr 1 do niniejszej procedury.
16. Osoba obsługująca incydent bezpieczeństwa lub cyberbezpieczeństwa zobowiązana jest do monitorowania wdrożenia działań naprawczych, tj. takich, które mają zapobiegać ponownemu zdarzeniu, które naruszyły zasady ochrony danych osobowych.
17. Schemat procedur zarządzania incydentami związanymi z bezpieczeństwem informacji stanowi Załącznik Nr 2 do niniejszej procedury.

VII. Odpowiedzialność za naruszenie ochrony bezpieczeństwa informacji i cyberbezpieczeństwa

1. Odpowiedzialność za prawidłowe zgłoszenie incydentów dotyczących bezpieczeństwa infrastruktury teleinformatycznej w Urzędzie spoczywa na pracownikach, użytkownikach i administratorach systemów oraz podmiotach zewnętrznych współpracujących z Urzędem.
2. Osoba odpowiedzialna za rozwiązanie problemu lub zapobieżenie incydentom w ramach swoich uprawnień działa zgodnie z niniejszą procedurą.
3. Nieprzestrzeganie zasad ochrony bezpieczeństwa informacji i cyberbezpieczeństwa skutkuje sankcjami przewidzianymi w stosownych przepisach prawa.

VIII. Szkolenia

1. 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 podmiocie o zaistniałym incydencie lub podejrzeniu jego wystąpienia.
2. W miarę posiadanych zasobów, co najmniej raz w roku, należy przeprowadzić okresowe szkolenia pracowników Urzędu w zakresie ochrony bezpieczeństwa informacji i cyberbezpieczeństwa.
3. Nowozatrudnionych pracowników osoba wyznaczona do kontaktów w sprawie cybebezpieczeństwa zapoznaje z zasadami prawidłowego zgłaszania incydentów.
4. Wzór oświadczenia o zapoznaniu się pracownika z postanowieniami niniejszej procedury stanowi Załącznik Nr 3.

Załącznik Nr 1 do procedury

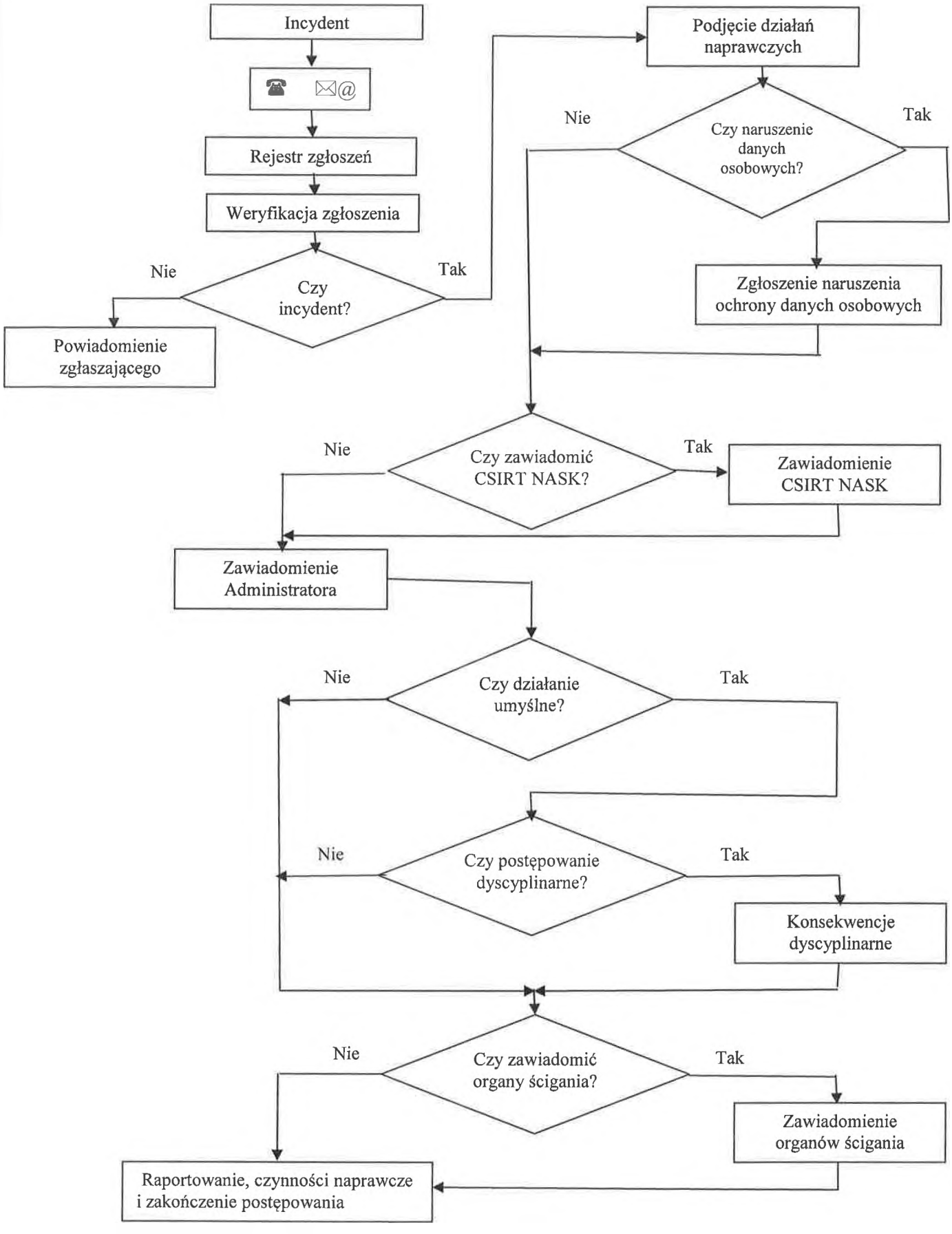
REJESTR INCYDENTÓW BEZPIECZEŃSTWA i CYBERBEZPIECZEŃSTWA

- wzór –

Lp.	Data zgłoszenia	Kategoria zgłoszenia (incydent bezpieczeństwa/ cyberbezpieczeństwa lub naruszenie bezpieczeństwa informacji)	Opis incydentu (zdarzenia)	Osoba zgłaszająca	Wykaz dokumentów dołączonych w sprawie	Przyczyna lub potencjalna przyczyna wystąpienia incydentu	Opis działań podjętych w związku z incydentem/ Czy dołączono dokumenty w sprawie	Data zamknięcia incydentu

Załącznik Nr 2 do procedury

Schemat procedur zarządzania incydentami związanymi z bezpieczeństwem informacji



Załącznik Nr 3 do procedury

..... Pisz, dnia .....

(imię i nazwisko)

.....

(stanowisko)

Oświadczenie

Oświadczam, że zapoznałem/łam się z postanowieniami Procedury postępowania z incydentami bezpieczeństwa informacji i cyberbezpieczeństwa oraz zobowiązuję się do ich bezwzględnego stosowania.

.....

(podpis)