ZARZĄDZENIE Nr 11/2023
Wójta Gminy Szczytniki
z dnia 1 marca 2023 r.

w sprawie: wprowadzenia w Urzędzie Gminy w Szczytnikach procedury zarządzania incydentami związanymi z bezpieczeństwem informacji i cyberbezpieczeństwem.

Na podstawie art. 30 ust. 1 i art. 33 ust. 3 i 5 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2023 r., poz. 40) w związku z art. 21 ust. 1 i art. 22 ustawy z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2022 r., poz. 1863 ze zm.) oraz § 20 ust. 2 pkt 13 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r., poz. 2247 ze zm.) **zarządza się, co następuje:**

§ 1. Wprowadza się do użytku służbowego w Urzędzie Gminy w Szczytnikach **„Procedurę zarządzania incydentami związanymi z bezpieczeństwem informacji i cyberbezpieczeństwem”, s**tanowiącą załącznik do niniejszego zarządzenia.

§ 2. Wykonanie zarządzenia powierza się Inspektorowi Ochrony Danych, Administratorowi Systemów Informatycznych, kierownikom komórek organizacyjnych oraz pozostałym pracownikom.

§ 3. Nadzór nad wykonaniem niniejszego zarządzenia powierza się Sekretarzowi Gminy.

§ 4. Zarządzenie wchodzi w życie z dniem podpisania.

Wójt

/-/ Marek Albrecht

Załącznik
do Zarządzenia Nr 11/2023
Wójta Gminy Szczytniki
z dnia 1 marca 2023 r.

PROCEDURA ZARZĄDZANIA INCYDENTAMI ZWIĄZANYMI Z BEZPIECZEŃSTWEM INFORMACJI I CYBERBEZPIECZEŃSTWEM

I. Postanowienia ogólne, definicje

§ 1. Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji oraz cyberbezpieczeństwem ma na celu zapewnienie ciągłości operacyjnej oraz ograniczenie wpływu przypadków naruszeń bezpieczeństwa zasobów informacyjnych na działalność Urzędu Gminy w Szczytnikach.

§ 2. Podstawą prawną do opracowania i wdrożenia procedury jest:

1) art. 22 ust. 1 pkt 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;
2) § 20 ust. 2 pkt. 13 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

§ 3. Użyta terminologia w niniejszej procedurze oznacza:

1. **CSIRT NASK** – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy;
2. **Cyberbezpieczeństwo**– odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy;
3. **Incydent** – zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo;
4. **Incydent cyberbezpieczeństwa**– zbiorcza nazwa obejmująca terminy incydent, incydent w podmiocie publicznym, incydent krytyczny;
5. **Incydent w podmiocie publicznym** – incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny,o którym mowa w art. 4 pkt 7–15 ustawy;
6. **Incydent krytyczny** – incydent skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi, klasyfikowany przez właściwy CSIRT NASK;
7. **Koordynator KSC** – osoba/y odpowiedzialna/e za utrzymanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, o której mowa w art. 21 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2022 r., poz. 1863 ze zm.).
8. **Obsługa incydentu** – czynności umożliwiające wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetyzację, podejmowanie działań naprawczych i ograniczenie skutków incydentu;

9. **Podatność** – właściwość systemu informacyjnego, która może być wykorzystana przez zagrożenie cyberbezpieczeństwa;
10. **System informacyjny** – system teleinformatyczny, o którym mowa w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2023 r., poz. 57) wraz z przetwarzanymi w nim danymi w postaci elektronicznej;
11. **Użytkownik** – osoba posiadająca dostęp do systemu informacyjnego Urzędu służącego do realizacji zadania publicznego;
12. **Ustawa** – ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2022 r., poz. 1863 ze zm.);
13. **Zagrożenie cyberbezpieczeństwa**– potencjalna przyczyna wystąpienia incydentu;
14. **Zarządzanie incydentem** – obsługa incydentu, wyszukiwanie powiązań między incydentami, usuwanie przyczyn ich wystąpienia oraz opracowywanie wniosków wynikających z obsługi incydentu;
15. **Inspektor Ochrony Danych** - osoba wyznaczona przez Administratora Danych Osobowych zwana dalej "IOD";
16. **Administrator Systemów Informatycznych**- osoba wyznaczona przez Administratora Danych Osobowych, odpowiedzialna za sprawność i konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych zwana dalej "ASI";
17. **Administrator Danych Osobowych "ADO"** – Wójt Gminy Szczytniki z siedzibą Urząd Gminy w Szczytnikach.

II. Osoby odpowiedzialne za cyberbezpieczeństwo Urzędu Gminy.

§ 4. 1. Wójt Gminy Szczytniki, ponosząc odpowiedzialność w szczególności za:

1) wyznaczenie osoby odpowiedzialnej za utrzymanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa - Koordynatora KSC;
2) przekazanie do CSIRT NASK w terminie 14 dni od dnia wyznaczenia, danych Koordynatora KSC, a także informacji o zmianie tych danych w terminie 14 dni od dnia ich zmiany. Przekazanie danych Koordynatora KSC odbywa się w sposób następujący:
   a) za pośrednictwem formularza elektronicznego pod adres e-mail: ksc@cert.pl, lub
   b) w formie pisemnej pod adres do korespondencji CSIRT NASK: NASK – Państwowy Instytut Badawczy, ul. Kolska 12, 01-045 Warszawa.

2. Koordynator KSC, który realizuje następujące zadania:

1) przyjmuje od Użytkowników informacje o zdarzeniach mogących stanowić incydent cyberbezpieczeństwa lub podejrzenie ich wystąpienia w organizacji;
2) koordynuje obsługę zgłaszanych incydentów cyberbezpieczeństwa;
3) przygotowuje zgłoszenie incydentu w podmiocie publicznym do CSIRT NASK, zgodnie ze wzorem stanowiącym załącznik nr 1 do niniejszej Procedury;
4) dokonuje zgłoszenia incydentu w podmiocie publicznym do CSIRT NASK. Zgłoszenie incydentu odbywa się za pomocą formularza dostępnego na stronie internetowej https://incydent.cert.pl/;
5) koordynuje wdrażanie działań naprawczych po wystąpieniu incydentu;
6) szkoli i podnosi świadomość Użytkowników oraz pozostałych pracowników organizacji w zakresie incydentów cyberbezpieczeństwa, ich zgłaszania, przeciwdziałania i prewencyjnych sposobach zabezpieczenia przed ich występowaniem;

7) koordynuje prace związane z informowaniem osób, na rzecz których zadanie publiczne jest realizowane w zakresie dostępu do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowania skutecznych sposobów zabezpieczania się przed tymi zagrożeniami;
8) w przypadku wystąpienia incydentu cyberbezpieczeństwa ściśle współpracuje z Użytkownikami, pracownikami organizacji, innymi osobami lub podmiotami świadczącymi organizacji usługi dotyczące obsługi informatycznej, w celu wdrożenia działań naprawczych;
9) wraz z innymi osobami zaangażowanymi przy wystąpieniu zdarzenia, dokonuje oceny danego zdarzenia pod względem możliwości zakwalifikowania go jako incydentów w odniesieniu do przepisów ustawy, w tym ewentualnej konieczności dokonania zgłoszenia wystąpienia incydentu w podmiocie publicznym do właściwego CSIRT;
10) prowadzi rejestr incydentów cyberbezpieczeństwa.

III. Kategorie incydentów bezpieczeństwa informacji oraz cyberbezpieczeństwa

§ 5. 1. Incydent bezpieczeństwa informacji oraz 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 podmiot publiczny. Jego przyczyną mogą być:
1) zdarzenie losowe zewnętrzne (np. klęski żywiołowe, pożary, zakłócenia w dostawie energii elektrycznej, itp), którego wystąpienie może spowodować zniszczenie lub uszkodzenie infrastruktury informatycznej albo dokumentacji papierowej oraz zakłócenie ciągłości pracy systemów informacyjnych nie powodując naruszenia poufności danych;
2) zdarzenie losowe wewnętrzne (np. błędy w oprogramowaniu, awarie sprzętu, błędy użytkowników, itp.), które mogą powodować zakłócenia ciągłości pracy systemów, a także prowadzić do zniszczenia lub utraty danych;
3) świadome i celowe działania mające na celu naruszenie poufności zasobów informacyjnych, w tym poufności danych.

§ 6. Incydentami bezpieczeństwa informacji w szczególności są:
1) naruszenie poufności, to jest ujawnienie informacji niepowołanym osobom;
2) naruszenie integralności, to jest zniszczenie, uszkodzenie lub przekłamanie informacji;
3) naruszenie dostępności, to jest brak dostępu do danych przez uprawnionych użytkowników.

§ 7. Przyczyny incydentów bezpieczeństwa informacji oraz cyberbezpieczeństwa mogą dotyczyć:
1) niewłaściwego wykorzystywania zasobów informatycznych lub niewłaściwego postępowania z dokumentacją papierową;
2) działania szkodliwego oprogramowania;
3) próby omijania systemów zabezpieczeń;
4) nieautoryzowanego dostępu do systemów, aplikacji i dokumentów;
5) zniszczenia lub kradzieży urządzeń wykorzystywanych do przetwarzania i przechowywania informacji;
6) zniszczenia lub kradzieży nośników danych;
7) próby wyłudzeń informacji;
8) ataków socjotechnicznych, ataków z wykorzystaniem technik zagrażających poufności, integralności lub dostępności informacji;
9) nieprawidłowości w zakresie zabezpieczenia przechowywania danych, w tym danych osobowych;

10) naruszenia zasad obowiązujących w Urzędzie Gminy w Szczytnikach dotyczących bezpieczeństwa informacji, w tym danych osobowych.

IV. Zakres obowiązywania procedury zarządzania incydentami związanymi z bezpieczeństwem informacji oraz cyberbezpieczeństwem

§ 8. Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji oraz cyberbezpieczeństwem obowiązuje w Urzędzie Gminy w Szczytnikach.

V. Zgłaszanie incydentów związanych z bezpieczeństwem informacji oraz cyberbezpieczeństwem

§ 9. 1. Każdy Użytkownik i/lub pracownik Urzędu, który zaobserwuje zdarzenie mogące stanowić incydent cyberbezpieczeństwa lub podejrzewa, iż wystąpił incydent cyberbezpieczeństwa w Urzędzie - w tym, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez Urząd – zobowiązany jest poinformować o w/w okolicznościach Koordynatora KSC.

2. Poinformowanie Koordynatora KSC, o którym mowa w ust. 1, winno nastąpić niezwłocznie, jednak nie później niż w terminie 2 godzin od wystąpienia zdarzenia lub podejrzenia jego wystąpienia oraz winno być potwierdzone w formie pisemnej za pośrednictwem poczty elektronicznej e-mail.

3. W przypadku nieobecności w pracy Koordynatora KSC informacje, o których mowa w ust. 1 należy przekazać do drugiej osoby wyznaczonej do kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. Odpowiednio mają zastosowanie postanowienia ust. 2.

4. Osoba zgłaszająca odpowiada za wyczerpujący opis incydentu odpowiednio do posiadanej wiedzy
i umiejętności. O zaistniałym zdarzeniu informowany jest również ASI.

5. Zgłoszenie musi zawierać następujące informacje:

1) imię i nazwisko osoby zgłaszającej;
2) jednostka organizacyjna lub nazwa podmiotu zewnętrznego;
3) stanowisko oraz komórka organizacyjna;
4) dokładne miejsce oraz datę wystąpienia incydentu;
5) opis incydentu w sposób adekwatny do posiadanej wiedzy i umiejętności zgłaszającego.

6. Po otrzymaniu zgłoszenia Koordynator KSC lub osoba, o której mowa w ust. 3 we współpracy z ASI dokonuje wstępnej weryfikacji otrzymanych informacji pod względem przesłanek identyfikujących zaistnienie incydentu cyberbezpieczeństwa, w tym czy stanowi on incydent w podmiocie publicznym podlegający zgłoszeniu do CSIRT NASK.

7. Brak umiejętności poprawnego rozpoznania incydentu przez osobę zgłaszającą nie może być przyczyną zaniechania zgłoszenia.

VI. Podejmowanie działań w związku ze zgłaszanymi incydentami związanymi z bezpieczeństwem informacji oraz cyberbezpieczeństwem

§ 10. 1. Zgłoszenie incydentu rejestrowane jest przez Koordynatora KSC i przechowywane w teczce ”Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji cyberbezpieczeństwem”.

2. Osoba zgłaszająca incydent powinna w miarę możliwości zabezpieczyć materiał dowodowy (np. zrzut ekranu monitora, zdjęcie niezabezpieczonych materiałów zawierających dane osobowe itp.).

3. Działania związane z obsługą zdarzenia w pierwszej kolejności dotyczą rozpoznania i kwalifikacji zgłoszenia.

4. W przypadku kiedy zgłoszenie zakwalifikowane zostało jako incydent bezpieczeństwem informacji lub cyberbezpieczeństwa, Koordynator KSC wraz z ASI dokonuje oceny jego istotności.

5. Przy ocenie istotności incydentu pod uwagę brane są następujące czynniki:

1) powstałe szkody będące wynikiem incydentu;
2) wpływ incydentu na działanie systemów informacyjnych;
3) wpływ incydentu na ciągłość realizacji zadań publicznych z wykorzystaniem systemów informacyjnych,
4) wpływ zdarzenia na dostępność, integralność, poufność oraz autentyczność danych wykorzystywanych do realizacji zadań publicznych,;
5) szacowany czas naprawy skutków wywołanych incydentem;
6) oszacowanie zasobów koniecznych do przywrócenia ciągłości działania systemów.

6. Koordynator KSC wspólnie z osobami zaangażowanymi w zarządzanie i obsługę incydentu cyberbezpieczeństwa weryfikują zgromadzone o zdarzeniu informacje, w tym w szczególności informacje:

1) opisujące wpływ incydentu w podmiocie publicznym na realizowane zadanie publiczne, w tym:
   a) wskazanie zadania publicznego, na które incydent cyberbezpieczeństwa miał wpływ,
   b) liczbę osób, na które incydent miał wpływ,
   c) moment wystąpienia i wykrycia incydentu cyberbezpieczeństwa oraz czas jego trwania,
   d) zasięg geograficzny obszaru, którego dotyczy incydent,
   e) przyczynę zaistnienia incydentu i sposób jego przebiegu oraz skutki jego oddziaływania na systemy informacyjne podmiotu publicznego;
2) informacje o przyczynie i źródle incydentu;
3) informacje o podjętych działaniach zapobiegawczych.

7. Na podstawie informacji, o których mowa w ust. 6 dokonywana jest ostateczna ocena incydentu cyberbezpieczeństwa pod względem przesłanek stanowiących o zaistnieniu incydentu w podmiocie publicznym podlegającemu zgłoszeniu do CSIRT NASK.

8. Ustalenia dotyczące incydentu cyberbezpieczeństwa winny zostać odnotowane w dokumencie „Raport incydentu cyberbezpieczeństwa", stanowiącym załącznik nr 2 do niniejszej Procedury.

9. Po sporządzeniu Raportu incydentu cyberbezpieczeństwa – w przypadku gdy zdarzenie zakwalifikowano jako incydent w podmiocie publicznym – Urząd zobowiązany jest do dokonania zgłoszenia do właściwego CSIRT.

10. Incydent cyberbezpieczeństwa, każdorazowo należy odnotować w „Rejestrze incydentów cyberbezpieczeństwa", stanowiącym załącznik nr 3 do niniejszej Procedury.

11. Koordynator KSC niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia zdarzenia, dokonuje zgłoszenia incydentu w podmiocie publicznym do CSIRT NASK NASK (Naukowa i Akademicka Sieć Komputerowa - Państwowy Instytut Badawczy ul. Kolska 12, 01-045 Warszawa) zgodnie z dyspozycją przepisu art. 23 Ustawy.

12. Zgłoszenia do CSIRT NASK przekazywane są w sposób elektroniczny. Procedura zgłoszeń opisana jest pod adresem internetowym: https://incydent.cert.pl/. W przypadku braku możliwości przekazania zgłoszenia w sposób elektroniczny należy dokonać go przy użyciu innych dostępnych środków komunikacji (np. telefon +48 223808274 lub fax).

13. Dokonując zgłoszenia incydentu w podmiocie publicznym zgodnie z ust. 11, dla wiadomości CSIRT NASK należy uwzględnić oznaczenie wszystkich informacji prawnie chronionych, w tym stanowiących tajemnicę przedsiębiorstwa jeśli takie informacje są zostaną zawarte w zgłoszeniu.

14. Po dokonaniu zgłoszenia o incydencie do CSIRT NASK, Koordynator KSC gromadzi dodatkowe informacje o incydencie cyberbezpieczeństwa na podstawie analizy systemów

monitorujących, systemów zabezpieczeń, urządzeń sieciowych, logów oraz baz wiedzy (szczególnie z uwzględnieniem przesłanek i powiązań z wcześniejszymi analogicznymi zdarzeniami lub incydentami cyberbezpieczeństwa, o ile takie występowały).

15. W przypadku powzięcia nowych informacji dotyczących obsługiwanego incydentu cyberbezpieczeństwa, Koordynator KSC informuje o tych okolicznościach CSIRT NASK, uzupełniając wcześniejsze zgłoszenie. Sposób informowana na zasadach określonych w ust. 11.

16. Koordynator KSC wdraża działania naprawcze i zabezpieczające mające na celu ograniczenie skutków incydentu cyberbezpieczeństwa, w szczególności incydentu w podmiocie publicznym, polegające w szczególności na:

1) przywróceniu pełnej funkcjonalności systemu informacyjnego;
2) zapewnienie bezpieczeństwa dla systemu informacyjnego np. zmiana haseł, wzmacnianie bezpieczeństwa instalacji i ustawień systemów (hardening), włączanie innych, wymaganych zabezpieczeń (na przykład zabezpieczeń firewall, dodatkowej kontroli dostępu, zmiany reguł w systemach IPS itp.);
3) usunięcie z systemów śladów incydentów cyberbezpieczeństwa (min. poprzez usunięcie szkodliwego oprogramowania, odblokowanie kont użytkowników zablokowanych wskutek wystąpienia incydentu itp.);
4) przeglądu, aktualizacji lub wdrożenia planów ciągłości działania, wpływających na realizację zadania publicznego;
5) przeglądu oraz aktualizacji procedur i/lub polityk związanych z bezpieczeństwem informacji oraz danych osobowych;
6) analizie incydentów cyberbezpieczeństwa, które wystąpiły w Urzędzie lub jednostkach o podobnym profilu działania;
7) po zakończeniu obsługi incydentu cyberbezpieczeństwa, w terminie nieprzekraczającym 21 dni od zakończenia obsługi incydentu, Koordynator KSC lub firma zewnętrzna przeprowadza szkolenie dla wszystkich Użytkowników;
8) w przypadku gdy do incydentu doszło z winy umyślnej Użytkownika, przechodzi on szkolenie indywidualne z zakresu cyberbezpieczeństwa zakończone testem wiedzy.

17. W celu potwierdzenia skuteczności przeprowadzonych w Urzędzie działań naprawczych i zapobiegawczych incydentom cyberbezpieczeństwa, mogą zostać przeprowadzone dodatkowe działania weryfikacyjne do których należą: przeprowadzenie testów podatności systemu IT, jeżeli incydent spowodowany został podatnością tego systemu lub inne czynności analityczne i sprawdzające.

18. Zakwalifikowanie zgłoszenia jako „fałszywy alarm” kończy postępowanie, o czym ASI informuje zgłaszającego.

19. W przypadku stwierdzenia działań zamierzonych, przy jednoczesnym zidentyfikowaniu sprawcy incydentu dotyczącego naruszenia bezpieczeństwa informacji oraz cyberbezpieczeństwa, ADO podejmuje decyzję dotyczącą wyciągnięcia ewentualnych konsekwencji dyscyplinarnych wobec sprawcy incydentu. Jednocześnie w zależności od wagi incydentu może powiadomić organy ścigania.

VII. Podejmowanie działań w związku ze zgłaszanymi incydentami naruszenia bezpieczeństwa przetwarzania danych osobowych.

§ 11. 1.W przypadku naruszenia ochrony danych osobowych mają zastosowanie przepisy art. 33-34 Rozporządzenia 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 - RODO) (Dz. Urz. UE L 119 z dnia 05 kwietnia 2016 r).

2. W przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego lub

zaistnienia sytuacji, które mogą wskazywać na naruszenie ochrony danych osobowych tj.:

a) przypadkowe lub niezgodne z prawem zniszczenie danych;
b) przypadkowa lub niezgodna z prawem utrata danych;
c) przypadkowa lub niezgodna z prawem modyfikacja danych;
d) nieuprawnione ujawnienie danych;
e) nieuprawniony dostęp do danych osobowych.

każdy pracownik zatrudniony przy przetwarzaniu danych osobowych (pracownik, stażysta, praktykant itp.) jest zobowiązany przerwać przetwarzania danych osobowych i niezwłocznie powiadomić o tym fakcie swojego bezpośredniego przełożonego oraz Inspektora Ochrony Danych oraz ASI w Urzędzie (jeżeli naruszenie ma związek z systemami informatycznymi).

3. Fakt naruszenia lub podejrzenia naruszenia ochrony danych osobowych należy potwierdzić pisemnie poprzez niezwłoczne sporządzenie zgłoszenia w którym umieszcza się informację o dacie, czasie, miejscu, okolicznościach zdarzenia. Notatkę przekazuje się Inspektorowi Ochrony Danych oraz Administratorowi Danych Osobowych.

4. Notatka jest rejestrowana przez IOD i przechowywana w teczce „Rejestr naruszeń ochrony danych osobowych".

VIII. Reagowanie na awarię

§ 12. 1. Jeśli awaria dotyczy systemu krytycznego i może mieć wpływ na wydajność systemów teleinformatycznych, ASI informuje ADO.

2. W przypadku gdy awarię można usunąć samodzielnie, ASI dokonuje naprawy.

3. Do podstawowych działań w takim wypadku zaliczyć można:

1) wymianę stacji roboczej;
2) wymianę podzespołów w stacji roboczej;
3) wymianę urządzenia sieciowego;
4) odtworzenie danych z kopii zapasowej.

4. Jeżeli ASI podejmie decyzję, iż nie może samodzielnie usunąć awarii, decyzję tę oraz wszelkie dodatkowe informacje dotyczące awarii eskaluje do producenta sprzętu lub oprogramowania.

5. Jeżeli naprawa dotyczy sprzętu, producent naprawy dokonuje w obecności ASI.

6. Jeżeli naprawa dotyczy oprogramowania, wgrywana poprawka powinna zostać pozytywnie zweryfikowana w środowisku testowym.

IX. Reagowanie na błędy w oprogramowaniu

§ 13. 1. Po otrzymaniu zgłoszenia dotyczącego wystąpienia błędu systemowego lub aplikacyjnego w oprogramowaniu, ASI diagnozuje przyczyny błędu oraz podejmuje działania zmierzające do rozwiązania problemu. Do podstawowych działań w tym zakresie zaliczyć można:

1) wykorzystanie bazy wiedzy o błędach w oprogramowaniu;
2) zmianę konfiguracji oprogramowania;
3) ponowną instalację oprogramowania;
4) instalację nowej wersji oprogramowania.

2. Jeśli ASI, nie jest w stanie samodzielnie naprawić błędu w oprogramowaniu, przekazuje tę informację do producenta oprogramowania (pracownik powinien w tym przypadku postępować zgodnie z umowami serwisowymi lub licencjami).

3. Jeśli zaistnieje powód wskazujący na to, że przyczyną błędu w oprogramowaniu było naruszenie bezpieczeństwa, ASI informuje o tym fakcie ADO.

X. Reagowanie na wykrycie złośliwego kodu mobilnego

§ 14. 1. Po otrzymaniu zgłoszenia dotyczącego pojawienia się złośliwego kodu mobilnego na stacji roboczej, serwerze lub samodzielnemu wejściu w posiadanie wiedzy o takim zdarzeniu, ASI w pierwszej kolejności powinien:

1) odłączyć komputer od sieci komputerowej;
2) sprawdzić aktualność baz danych wirusów (jeżeli są nieaktualne należy dokonać ich aktualizacji);
3) sprawdzić poprawność działania oprogramowania antywirusowego (jeżeli oprogramowanie nie działa poprawnie należy je odinstalować i zainstalować ponownie);
4) uruchomić pełne skanowanie komputera i nośników informacji, z jakimi mógł mieć styczność.

2. Jeżeli atak złośliwego kodu mobilnego nie został zneutralizowany przez oprogramowanie antywirusowe to ASI nakazuje użytkownikowi przerwanie pracy. Następnie dokonuje ponownej instalacji systemu operacyjnego i oprogramowania oraz odzyskania danych z kopii zapasowych. Kopie zapasowe należy sprawdzić programem antywirusowym przed wgraniem do komputera.

3. Jeśli istnieje powód wskazujący na to, że przyczyną ataku złośliwego kodu mobilnego było naruszenie bezpieczeństwa, to ASI informuje o tym fakcie ADO.

XI. Szkolenia

§ 15. 1. Każdy Użytkownik i pracownik Urzędu Gminy w Szczytnikach winien być przeszkolony z zakresu ustawy oraz informacji o zagrożeniach cyberbezpieczeństwa.

2. Koordynator KSC z własnej inicjatywy lub na wniosek Wójta Gminy Szczytniki przeprowadza wewnętrzne szkolenia, o którym mowa w ust. 1.

3. Szkolenia, o których mowa w ust. 1 może również przeprowadzić firma zewnętrzna na zlecenie kierownictwa Urzędu.

4. Dodatkowo szkolenia winny zostać przeprowadzone w przypadku każdej istotnej zmiany zasad lub przepisów dotyczących ustawy w zakresie odnoszącym się do podmiotu publicznego. Przepis ust. 2 stosuje się odpowiednio.

5. W przypadku zaistnienia incydentu cyberbezpieczeństwa – po zakończeniu obsługi tego incydentu – Koordynator KSC winien przeprowadzić w terminie 21 dni od zakończenia obsługi incydentu szkolenie dla pracowników Urzędu, mające na celu przekazanie informacji o zaistniałym incydencie cyberbezpieczeństwa i prewencyjnych sposobach zabezpieczenia Urzędu przed podobnymi incydentami.

6. Każde szkolenie wewnętrzne powinno być udokumentowane poprzez sporządzenie dokumentów potwierdzających uczestnictwo w takim szkoleniu przez jego uczestników (lista obecności lub zaświadczeń/certyfikat imienny dla osoby uczestniczącej w szkoleniu).

XII. Dystrybucja oraz aktualizacja Procedury

§ 16. 1. Niniejsza Procedura podlega regularnym (nie rzadziej niż raz na rok) przeglądom dokonywanym przez Koordynatora KSC.

2. W zależności od potrzeb mogą zostać przeprowadzone także dodatkowe przeglądy po stwierdzeniu istotnego naruszenia bezpieczeństwa, pojawieniu się zasadniczych zmian w Urzędzie, jego strukturze lub jego otoczeniu (nowe zagrożenia, technologie).

3. Każdy Użytkownik, który wykorzystuje system informacyjny do realizacji zadań publicznych pozostających w jego zakresie obowiązków, jest zobowiązany do zapoznania się z obowiązkami związanymi z przepisami wynikającymi z Ustawy.

4. Wójt Gminy Szczytniki zapewnia dostęp do niniejszej Procedury każdemu Użytkownikowi i pracownikowi Urzędu.

5. Każdy Użytkownik oraz pracownik Urzędu zobowiązany jest zapoznać się z niniejszą Procedurą potwierdzając tę okoliczność własnoręcznym podpisem w dokumencie „Wykaz osób zapoznanych z Procedurą zarządzania incydentami cyberbezpieczeństwa", stanowiącym załącznik nr 4 do niniejszej Procedury.

XIII. Wykaz załączników

Załącznik nr 1 – Formularz zgłaszania incydentów cyberbezpieczeństwa Gminy Szczytniki do CSIRT NASK,
Załącznik nr 2 – Wzór raportu incydentu cyberbezpieczeństwa,
Załącznik nr 3 – Rejestr incydentów cyberbezpieczeństwa.
Załącznik Nr 4 – Wykaz osób zapoznanych z Procedurą zarządzania incydentami cyberbezpieczeństwa,
Załącznik Nr 5 – Raport z naruszenia ochrony danych osobowych.

Załącznik Nr 1
do Procedury zarządzania
incydentami cyberbezpieczeństwa

FORMULARZ ZGŁASZANIA INCYDENTÓW CYBERBEZPIECZEŃSTWA GMINY SZCZYTNIKI		
CZĘŚĆ A: DANE GMINY SZCZYTNIKI		
1. Nazwa podmiotu zgłaszającego	Gmina Szczytniki	
2. Siedziba i adres zgłaszającego	62-865 Szczytniki 139	
3. NIP zgłaszającego		
CZĘŚĆ B: DANE ZGŁASZAJĄCEJ JEDNOSTKI ORGANIZACYJNEJ (uzupełnia osoba zgłaszająca z jednostki organizacyjnej, w której wystąpił incydent)		
4. Pełna nazwa jednostki organizacyjnej, w której wystąpił incydent*		
5. Siedziba i adres jednostki organizacyjnej, w której wystąpił incydent*		
CZĘŚĆ C: DANE OSOBY ZGŁASZAJĄCEJ Z JEDNOSTKI ORGANIZACYJNEJ (uzupełnia osoba zgłaszająca z jednostki organizacyjnej, której wystąpił incydent)		
6. Imię i nazwisko osoby z jednostki organizacyjnej, zgłaszającej incydent*		
7. Stanowisko służbowe osoby z jednostki organizacyjnej, zgłaszającej incydent *		
8. Numer telefonu służbowego osoby z jednostki organizacyjnej, zgłaszającej incydent *		Dostępność podanego numeru: ☐ 7:00 – 15:00 ☐ w godzinach: ☐ 24h
9. Adres poczty elektronicznej osoby z jednostki organizacyjnej, zgłaszającej incydent *		
D: OSOBA UPRAWNIONA DO SKŁADANIA WYJAŚNIEŃ W SPRAWIE INCYDENTU		
10. Imię i nazwisko osoby uprawnionej do składania wyjaśnień dotyczących zgłaszanych informacji	Pan **Dariusz Wawrzyniak** – Sekretarz Gminy Szczytniki oraz Pan **Mirosław Kowalski** – Starszy inspektor w Urzędzie Gminy w Szczytnikach	
11. Numer telefonu służbowego osoby uprawnionej do składania wyjaśnień dotyczących zgłaszanych informacji	tel. **62/ 7625001 lub 7625015** dostępny w godzinach **7:00 – 15:00**	
12. Adres poczty elektronicznej osoby uprawnionej do składania wyjaśnień dotyczących zgłaszanych informacji	sekretariat@szczytniki,ug.gov,pl	
CZĘŚĆ E: OPIS INCYDENTU (uzupełnia osoba zgłaszająca z jednostki organizacyjnej, w której wystąpił incydent)		
13. Data wystąpienia incydentu * orientacyjny czas trwania incydentu	podany czas jest: ☐ przybliżony ☐ dokładny	
14.Data wykrycia incydentu * oraz stan incydentu	☐ nadal trwa ☐ wygasł ☐ został obsłużony	

incydent nadal trwa/wygasł/został obsłużony	
15. Zadanie publiczne/usługa na które incydent miał wpływ *	
16. Liczba osób, na które incydent miał wpływ *	☐ 1-50 ☐ 51-500 ☐ 501 – 1.000 ☐ 1.000-10.000 ☐ > 10.000 ☐ brak danych
17. Zasięg geograficzny obszaru, którego dotyczy incydent *	☐ Instytucja ☐ Miejscowość/Gmina/Województwo ☐ Polska ☐ Unia Europejska ☐ Świat ☐ brak danych
18. Rodzaj działania * Celowe-świadome/Niecelowe-nieświadome	☐ Celowe ☐ Niecelowe
19. Kategoria zdarzenia *	☐ Podejrzana wiadomość e-mail/ np. podejrzane załączniki, phishing, szantaż ☐ Zbieranie informacji/ np. skanowanie, podsłuch, SPAM, inżynieria społeczna ☐ Treści obraźliwe / np. obrażanie, przemoc i inne nielegalne treści/zgłoszenia przeznaczone dla Zespołu Dyżurnet,pl ☐ Oprogramowanie złośliwe /np. wirus, trojan, banker, spyware, ransomware, zagrożenia mobilne ☐ 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 ☐ Naruszenia bezpieczeństwa informacji /np. nieuprawniony dostęp do informacji, nieuprawniona zmiana informacji lub jej skasowanie ☐ Oszustwa internetowe /np. nieuprawnione wykorzystanie zasobów, Naruszenie praw autorskich, podszywanie się, kradzież tożsamości ☐ Podatności/błędy w oprogramowaniu lub aplikacjach /np. błędna konfiguracja, wykrycie podatności ☐ Cyberterroryzm/zdarzenie o charakterze terrorystycznym popełnione w cyberprzestrzeni, w sieci ☐ Inne/ zdarzenia niemieszczące się w powyższych kategoriach

	☐ Test/ kategoria ćwiczebna	
20. Skutki oddziaływania incydentu na systemy informacyjne instytucji*	☐ utrata dostępności danych/usługi ☐ utrata poufności danych/usługi ☐ utrata integralności danych/usługi ☐ próba infekcji oprogramowaniem złośliwym ☐ próba uzyskania nieuprawnionego dostępu ☐ inne	
Dodatkowe informacje		
21. Przebieg incydentu oraz możliwa przyczyna jego wystąpienia *		
22. Podjęte działania zapobiegawcze*		
23. Podjęte działania naprawcze *		
24. Inne istotne informacje *		
25. Pola stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa (podaj nr pól po przecinku lub w przedziale np. 16. – 24.)		

Pola oznaczone* są polami wymaganymi.
Wypełniony formularz należy niezwłocznie wysłać w postaci załącznika do wiadomości e-mail na adres: cert@cert.pl lub faksem pod numer (22) 380 83 99
Jeśli pojawią się nowe informacje dotyczące incydentu należy niezwłocznie je przekazać uzupełniając formularz i przekazując go również na adres cert@cert.pl

Załącznik Nr 2
do Procedury zarządzania
incydentami cyberbezpieczeństwa

RAPORT INCYDENTU CYBERBEZPIECZEŃSTWA

I. OPIS INCYDENTU

1. Data ..... Godzina .....

2. Osoba powiadamiająca o incydencie oraz inne osoby zaangażowane lub odpytane w związku z incydentem (imię, nazwisko, stanowisko służbowe, dane kontaktowe):

….....

3. Lokalizacja zdarzenia *(nr. pokoju, nazwa pomieszczenia, określenie komputerowego stanowiska roboczego, nazwa programu lub aplikacji itp.):*

.....

II ANALIZA INCYDENTU

1. Zadanie publiczne, którego dotyczy zgłoszenie:

……..……...…

…….....

2. Liczba osób na które incydent miał wpływ

.....

3. Moment wystąpienia i wykrycia incydentu oraz czas jego trwania

.....

4. Zasięg geograficzny obszaru którego incydent dotyczy

….....

5. Przyczyna zaistnienia incydentu:

☐ Podejrzana wiadomość e-mail ☐ Podatności

☐ Próba oszustwa ☐ Złośliwe oprogramowanie

☐ Nielegalne treści ☐ Inny …….

6. Sposób przebiegu incydentu

……...

7. Skutki oddziaływania incydentu na systemy informacyjne podmiotu publicznego

…….

8. Przyczyna i źródło incydentu

…….

9. Informacja o podjętych działaniach zapobiegawczych

……..……

10. Informacja o podjętych lub planowanych działaniach naprawczych

……..……

11. Czy doszło do naruszenia danych osobowych

☐ TAK ☐ NIE

W przypadku naruszenia danych osobowych należy dodatkowo uruchomić procedurę zgłaszania naruszeń związanych z ochroną danych osobowych.

W przypadku naruszenia danych osobowych podać nr zgłoszenia z rejestru naruszeń ochrony danych osobowych ……

W przypadku informacji dotyczącej nielegalnych treści zgłoszenie należy przesłać do zespołu Dyżurnet.pl

.....
(podpisy osób obsługujących incydent)

***** Do Raportu należy dołączyć kopię zgłoszenia do CSIRT NASK.

Załącznik Nr 3
do Procedury zarządzania
incydentami cyberbezpieczeństwa

REJESTR INCYDENTÓW CYBERBEZPIECZEŃSTWA

Lp.	Data zgłoszenia	Zadanie publiczne, którego dotyczy zgłoszenie	Opis zdarzenia	Kategoria incydentu	Podjęte działania zapobiegawcze	Podjęte działania naprawcze
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						

Kategorie incydentu:
A – Podejrzana wiadomość e-mail
B – Próba oszustwa
C – Podatności
D – Złośliwe oprogramowanie
E – Nielegalne treści
F – Inny incydent

Załącznik Nr 4
do Procedury zarządzania
incydentami cyberbezpieczeństwa

Wykaz osób zapoznanych z Procedurą zarządzania incydentami cyberbezpieczeństwa

Lp.	Imię i nazwisko pracownika	Podpis
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		
16.		
17.		
18.		
19.		
20.		
21.		
22.		
23.		
24.		
25.		
26.		
27.		
28.		
29.		
30.		
31.		
32.		
33.		
34.		
35.		
36.		
37.		
38.		
39.		
40.		

Załącznik Nr 5
do Procedury zarządzania
incydentami cyberbezpieczeństwa

RAPORT Z NARUSZENIA OCHRONY DANYCH

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 pracownika) (data i podpis ADO/Inspektora ochrony danych)