PROCEDURA ZARZĄDZANIA INCYDENTAMI CYBERBZEPIECZEŃSTWA W URZĘDZIE GMINY W SADKACH

Urząd Gminy w Sadkach

Adres: ul. Strażacka 11

Kod pocztowy: 89-110 Sadki

Powiat nakielski

Telefon..... 52 339 39 30

Fax..... 52 339 39 59

E-mail..... kancelaria@sadki.pl

ePUAP:..... /ugsadki/SkrytkaESP

ROZDZIAŁ 1.

WSTĘP

1. Procedura zarządzania incydentami związanymi z oraz cyberbezpieczeństwem ma na celu zapewnienie ciągłości operacyjnej oraz ograniczenie wpływu przypadków naruszeń bezpieczeństwa zasobów informacyjnych na działalność Urzędu.
2. Podstawą prawną do opracowania i wdrożenia niniejszego Regulaminu jest art. 22 ust.1 pkt. 1 Ustawy o krajowym systemie cyberbezpieczeństwa z dnia 05 lipca 2018r. *(Dz. U. z 2018 r. poz. 1560).*

ROZDZIAŁ 2.

DEFINICJE

1. **Incydent w podmiocie publicznym** - incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny.
3. **Incydent krytyczny** – incydent skutkujący znaczną szkodą dla bezpieczeństwa lub porządku prawnego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw lub wolności obywatelskich lub życia i zdrowia ludzi, klasyfikowany przez właściwy CSIRT NASK.
4. **Osoba pełniącą funkcję odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa**- osoba wyznaczona przez Administratora Danych Osobowych.
5. **Inspektor Ochrony Danych** - osoba wyznaczona przez Administratora Danych Osobowych zwana dalej „IOD".
6. **Administrator Systemów Informatycznych** – osoba wyznaczona przez Administratora Danych Osobowych, odpowiedzialna za sprawność i konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych zwana dalej „ASI".
7. **Administrator Danych Osobowych** – Wójt Gminy Sadki –zwany dalej ADO.
8. **Urząd** – Urząd Gminy Sadki.

9. **Gminne Jednostki Organizacyjne** - Gminna Biblioteka Publiczna w Sadkach, Gminny Ośrodek Kultury w Sadkach, Gminny Ośrodek Pomocy Społecznej w Sadkach, Gminny Zespół Obsługi Oświaty w Sadkach, Przedszkole Gminy Sadki „Dobre Ludki", Straż Gminna w Sadkach, Szkoła Podstawowa im. mjra H. Sucharskiego w Sadkach.

ROZDZIAŁ 3.
KATEGORIE INCYDENTÓW

1. Incydent cyberbezpieczenstwa 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.
2. Przyczyną powstania incydentu cyberbezpieczeństwa może być:
   a) 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 nie powodując naruszenia poufności danych;
   b) zdarzenie losowe wewnętrzne (np. błędy w oprogramowaniu , awarie sprzętu itp.), które mogą powodować zakłócenia ciągłości pracy systemów a także prowadzić do zniszczenia lub utraty danych;
   c) świadome i celowe działania mające na celu naruszenie poufności zasobów informacyjnych, w tym poufności danych.
3. Incydentami cyberbezpieczeństwa w szczególności są takie działania jak:
   a) naruszenie poufności, to jest ujawnienie informacji niepowołanym osobom;
   b) naruszenie integralności, to jest zniszczenie, uszkodzenie lub przekłamanie informacji;
   c) naruszenie dostępności, to jest braku dostępu do danych przez uprawnionych użytkowników.
4. Przyczyny incydentów cyberbezpieczeństwa mogą dotyczyć:

a) niewłaściwego wykorzystywania zasobów informatycznych lub niewłaściwe postępowanie z dokumentacją papierową;
b) działania szkodliwego oprogramowania;
c) próby omijania systemów zabezpieczeń;
d) nieautoryzowanego dostępu do systemów, aplikacji i dokumentów;
e) zniszczenia lub kradzieży urządzeń wykorzystywanych do przetwarzania i przechowywania informacji;
f) zniszczenia lub kradzieży nośników danych;
g) próby wyłudzeń informacji;
h) ataków socjotechnicznych, ataków z wykorzystaniem technik zagrażających poufności;
i) integralności lub dostępności informacji;
j) nieprawidłowości w zakresie zabezpieczenia przechowywania danych, w tym danych osobowych;
k) naruszenia zasad obowiązujących w Urzędzie dotyczących bezpieczeństwa informacji, w tym danych osobowych.

5. 2. O możliwości zaistnienia przypadku naruszenia cyberbezpieczeństwa mogą świadczyć:

a) nadmierne, w stosunku do wykonywanych zadań (zakresu upoważnienia), uprawnienia użytkownika do zasobów systemu;
b) niestabilna praca systemu teleinformatycznego;
c) korzystanie z zasobów systemu poza godzinami pracy (bez zgody przełożonego);
d) nowe „podejrzane" (nieznane) konta użytkowników;
e) wysoka aktywność kont, które długo pozostawały niewykorzystane;
f) zanotowanie w krótkim czasie dużej liczby nieudanych prób logowania;
g) anomalie w pracy systemu lub programu (świadczące np. o obecności wirusa komputerowego);
h) naruszenie lub wadliwe funkcjonowanie zabezpieczeń fizycznych w pomieszczeniach, w których następuje przetwarzanie informacji w Urzędzie lub Gminnych Jednostkach Organizacyjnych (uszkodzone zamki, okna, drzwi, naruszone plomby, itp.).

ROZDZIAŁ 4.

ZAKRES OBOWIĄZYWANIA PROCEDURY ZARZĄDZANIA INCYDENTAMI ZWIĄZANYMI Z BEZPIECZEŃSTWEM INFORMACJI ORAZ CYBERBEZPIECZEŃSTWEM

Procedura zarządzania incydentami związanymi z cyberbezpieczeństwem obowiązuje w Urzędzie oraz Gminnych Jednostkach Organizacyjnych.

ROZDZIAŁ 5.

ZGŁASZANIE INCYDENTÓW ZWIĄZANYCH Z BEZPIECZEŃSTWEM INFORMACJI ORAZ CYBERBEZPIECZEŃSTWEM

1. W przypadku ujawnienia incydentu pracownik niezwłocznie powiadamia o tym fakcie Osobę pełniącą funkcję odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, Inspektora Ochrony Danych oraz Administratora Systemów Informatycznych *(w sytuacji gdy, incydent dotyczy bezpośrednio systemów komputerowych).* Zgłoszenie następuje telefonicznie lub mailowo. Dane kontaktowe Osobę pełniącą funkcję odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, IOD oraz ASI znajdują się na stronie internetowej http://www.bip.sadki.pl. Telefoniczne zgłoszenie należy potwierdzić szczegółową notatką służbową, którą przekazuje się IOD poprzez swojego bezpośredniego przełożonego lub bezpośrednio do IOD w przypadku pracowników zatrudnionych na samodzielnych stanowiskach.
2. Notatka musi zawierać następujące informacje:
   a) imię i nazwisko osoby zgłaszającej;
   b) stanowisko oraz komórka organizacyjna Urzędu;
   c) dokładne miejsce oraz datę i godzinę wystąpienia incydentu;

d) opis incydentu w sposób adekwatny do posiadanej wiedzy i umiejętności zgłaszającego;
e) informację o zgromadzonych materiałach dowodowych,
f) informacje dotyczące sposobu postępowania z incydentem.

3. Brak umiejętności poprawnego rozpoznania incydentu przez osobę zgłaszającą nie może być przyczyną zaniechania zgłoszenia.
4. W przypadku dłuższej nieobecności Osobę pełniącej funkcję odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, IOD incydent należy zgłosić do ASI w sposób określony w pkt.1.

ROZDZIAŁ 6.

ZGŁASZANIE INCYDENTÓW ZWIĄZANYCH Z CYBERBEZPIECZEŃSTWEM PRZEZ GMINNE JEDNOSTKI ORGANIZACYJNE

1. W przypadku stwierdzenia incydentu krytycznego lub incydentu w podmiocie publicznym przez Gminne Jednostki Organizacyjne należy niezwłocznie telefonicznie powiadomić o tym fakcie osobę pełniącą funkcję odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa oraz IOD. W dalszej kolejności fakt ten należy zgłosić do IOD mailowo i potwierdzić oficjalnym pismem opatrzonym podpisem kierownika jednostki. Dane kontaktowe IOD znajdują się na stronie internetowej *http://www.bip.sadki.pl*.
2. W zgłoszeniu należy podać wszystkie informacje zgodnie z treścią art. 23 ust. 1 Ustawy o krajowym systemie cyberbezpieczeństwa.
3. W przypadku dłuższej nieobecności osoby pełniącej funkcję odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa lub IOD zgłoszenia należy dokonywać do ASI w sposób opisany w pkt.1. Dane kontaktowe ASI znajdują się na stronie internetowej *http://www.bip.sadki.pl*.

ROZDZIAŁ 7.

PODEJMOWANIE DZIAŁAŃ W ZWIĄZKU ZE ZGŁASZANYMI INCYDENTAMI ZWIĄZANYMI Z BEZPIECZEŃSTWEM INFORMACJI ORAZ CYBERBEZPIECZEŃSTWEM

1. Zgłoszenie incydentu rejestrowane jest przez IOD i przechowywane w teczce „Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji oraz cyberbezpieczeństwem dla Urzędu Gminy Sadki". Osoba zgłaszająca incydent powinna w miarę możliwości zabezpieczyć materiał dowodowy *(np. zrzut ekranu monitora, zdjęcie niezabezpieczonych materiałów zawierających dane osobowe itp.).* Działania związane z obsługą zdarzenia w pierwszej kolejności dotyczą rozpoznania i kwalifikacji zgłoszenia. W przypadku, kiedy zgłoszenie zakwalifikowane zostało jako incydent bezpieczeństwa informacji lub cyberbezpieczeństwa, dokonywana jest jego ocena istotności. Powyższe działania – ocena istotności - wykonuje osoba pełniąca funkcję odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa lub IOD w porozumieniu z ASI oraz informatykami, których łączy umowa dotycząca obsługi informatycznej w Gminnych Jednostkach Organizacyjnych *(w sytuacji gdy, zgłoszenie dotyczy naruszenia cyberbezpieczeństwa w tych jednostkach).*
2. Przy ocenie istotności incydentu pod uwagę brane są następujące czynniki:
   a) powstałe szkody będące wynikiem incydentu;
   b) wpływ incydentu na działanie systemów;
   c) wpływ incydentu na ciągłość działania Urzędu;
   d) koszty usunięcia skutków incydentu;
   e) szacowany czas naprawy skutków wywołanych incydentem;
   f) oszacowanie zasobów koniecznych do przywrócenia ciągłości działania systemów.
3. Zakwalifikowanie zgłoszenia incydentu jako „fałszywy alarm" kończy postępowanie, o czym osoba pełniąca funkcję odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa lub IOD informuje zgłaszającego.

4. W przypadku zakwalifikowania zdarzenia jako incydentu związanego z bezpieczeństwem informacji lub cyberbezpieczeństwem, osobę pełniąca funkcję odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa lub IOD wspólnie z ASI podejmuje działania zabezpieczające i naprawcze zmierzające do zniwelowania szkód powstałych w wyniku incydentu.
5. Gminne Jednostki Organizacyjne we własnym zakresie podejmują działania naprawcze zmierzające do zniwelowania szkód powstałych w wyniku incydentu.
6. Poinformowany o wynikach analizy incydentu oraz podjętych działaniach naprawczych: osoba pełniąca funkcję odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa lub IOD informuje ADO.
7. W przypadku stwierdzenia incydentu w podmiocie publicznym lub incydentu krytycznego osoba pełniąca funkcję odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa lub IOD nie później niż w ciągu 24 godzin od momentu wykrycia zgłasza incydent do właściwego CSIRT NASK (Naukowa i Akademicka Sieć Komputerowa - Państwowego Instytutu Badawczego ul. Kolska 12, 01-045 Warszawa).
8. 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 go w sposób elektroniczny można zgłaszać przy użyciu innych dostępnych środków komunikacji (np. na numer telefonu +48223808274).
9. W zgłoszeniu przekazuje się informacje zgodnie z formularzem oraz zgodnie z treścią art. 23 ust. 1 Ustawy o krajowym systemie cyberbezpieczeństwa z dnia 05 lipca 2018 r. *(Dz. U. z 2018 r. poz. 1560).*
10. 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 mogą być powiadomione organy ścigania.

ROZDZIAŁ 8.

PODEJMOWANIE DZIAŁAŃ W ZWIĄZKU ZE ZGŁASZANYMI INCYDENTAMI NARUSZENIA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH

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.
3. 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 i Administratora Systemów Informatycznych *(jeżeli naruszenie ma związek z systemami informatycznymi)*.
4. Fakt naruszenia lub podejrzenia naruszenia ochrony danych osobowych należy potwierdzić pisemnie poprzez niezwłoczne sporządzenie notatki służbowej w której umieszcza się informację o dacie, czasie, miejscu, okolicznościach zdarzenia. Notatkę przekazuje się IOD za pośrednictwem swojego przełożonego lub bezpośrednio w przypadku osób zatrudnionych na samodzielnych stanowiskach. O zdarzeniu IOD niezwłocznie powiadamia ADO.
5. Zgłoszenia są rejestrowane w „Rejestrze naruszeń ochrony danych osobowych" prowadzonym zgodnie z art.33 ust. 5 RODO.
6. Przy ocenie istotności incydentu pod uwagę brane są następujące czynniki:

a. charakter naruszenia ochrony danych osobowych;

b. kategorię i przybliżoną liczbę osób których dane dotyczą;

c. kategorię i przybliżoną liczbę wpisów danych osobowych, których dotyczy.

Załącznik nr 1
PROCEDURY ZARZĄDZANIA
INCYDENTAMI CYBERBZEPIECZEŃSTWA
W URZĘDZIE GMINY W SADKACH

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:
    a) w przypadku połączenia modemowego, zanotuj numer telefoniczny, adres IP komputera, adresy bramki wychodzącej oraz serwera DNS,
    b) w przypadku połączenia po sieci kablowej, zanotuj typ połączenia, adres IP komputera, adresy bramki wychodzącej oraz serwera DNS,
    c) 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 Urząd albo opis jego indywidualnych cech. Zapisz wszystkie wykonane czynności

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. Zabezpiecz jako materiał porównawczy i wpisz do protokołu wykonane czynności.
11. Zażądaj od użytkowników i administratora podania parametrów dostępu do 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.
13. 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 Urzędu 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.