Załącznik Nr 1 do zarządzenia Nr 0050.86.2019

Burmistrza Miasta Zambrów

z dnia 23 sierpnia 2019 r.

Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji i cyberbezpieczeństwem

Rozdział 1.
Postanowienia ogólne

§1.1. 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 oraz jednostek organizacyjnych.

2. Podstawą prawną do opracowania i wdrożenia dokumentu jest:

a. art. 22 ust. 1 pkt 1 ustawy o krajowym systemie cyberbezpieczeństwa z dnia 05 lipca 2018 r.

b. §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. Incydent w podmiocie publicznym - incydent, który powoduje lub może powodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny.

4. 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, klasyfikowanych przez właściwy CSIRT NASK.

5. Administrator systemów informatycznych (ASI) - osoba zarządzająca systemami informatycznymi w Urzędzie Miasta Zambrów, osoba odpowiedzialna za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.

6. Inspektor Ochrony Danych - osoba wyznaczona przez Administratora Danych Osobowych, zwany dalej „IOD”.

7. Administratorze danych osobowych - rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, o których mowa w art. 4 pkt. 7 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), decydujący o celach i środkach przetwarzania danych osobowych.

Rozdział 2.
Kategorie incydentów

§ 2. 1. Incydent bezpieczeństwa informacji oraz cyberbezpieczeństwa to zdarzenie, którego skutkiem jest lub może być naruszanie bezpieczeństwa aktywów informacyjnych oraz który powoduje lub może spowodować obniżenie jakości lub przetrwanie realizacji zadania publicznego wykonywanego przez podmiot publiczny. Jego przyczyną może być:

a. zdarzenie losowe zewnętrzne (np. klęski żywiołowe, pożary, zakłócenie 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.

2. Incydentami bezpieczeństwa informacji w szczególności są

a. naruszanie poufności, to jest ujawnienie informacji niepowołanym osobom;

b. naruszanie integralności, to jest zniszczenie, uszkodzenie lub przekłamanie informacji;

c. naruszenie dostępności, to jest brak dostępu do danych przez uprawnionych użytkowników.

3. Przyczyny incydentów bezpieczeństwa informacji oraz cyberbezpieczeństwa mogą dotyczyć:

a. niewłaściwego wykorzystywania zasobów informatycznych lub niewłaściwego postępowania 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, integralności lub dostępności informacji;

i. nieprawidłowości w zakresie zabezpieczenia przechowania danych, w tym danych osobowych;

j. naruszenia zasad dotyczących bezpieczeństwa informacji.

Rozdział 3.
Zakres obowiązywania procedury zarządzania incydentami związanymi z bezpieczeństwem informacji i cyberbezpieczeństwem

§ 3. Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji oraz cyberbezpieczeństwem obowiązuje w Urzędzie Miasta Zambrów oraz we wszystkich jednostkach organizacyjnych Miasta Zambrów.

Rozdział 4.
Zgłaszanie incydentów związanych z bezpieczeństwem informacji oraz cyberbezpieczeństwem

§ 4. W przypadku ujawnienia incydentu pracownik niezwłocznie powiadamia o tym fakcie Inspektora ochrony danych oraz Administratora systemów informatycznych (kiedy incydent dotyczy systemów komputerowych). Zgłoszenie następuje osobiście bądź telefonicznie. Zgłoszenie należy następnie potwierdzić szczegółową notatką służbową.

1) Notatka musi zawierać następujące informacje:
   a. imię i nazwisko osoby zgłaszającej;
   b. stanowisko oraz komórka organizacyjna Urzędu;
   c. dokładne miejsce oraz datę wystąpienia incydentu;
   d. opis incydentu w sposób adekwatny do posiadanej wiedzy i umiejętności zgłoszenia go.
2) Brak umiejętności poprawnego rozpoznania incydentu przez osobę zgłaszającą nie może być przyczyną zaniechania zgłoszenia.

Rozdział 5.
Zgłoszenie incydentów związanych z cyberbezpieczeństwem przez jednostki organizacyjne Miasta Zambrów

§ 5. 1. W przypadku stwierdzenia incydentu krytycznego lub incydentu w podmiocie publicznym przez jednostki organizacyjne Miasta Zambrów należy niezwłocznie telefonicznie powiadomić o tym fakcie pracownika Urzędu Miasta Zambrów odpowiedzialnego za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa (na podstawie Zarządzenia Nr 0050.80.2019 Burmistrza Miasta Zambrów z dnia 5 sierpnia 2019 r.) - Pana Grzegorza Grzeszczuk. W dalszej kolejności należy uzupełnić formularz zgłoszenia incydentów cyberbezpieczeństwa, który stanowi załącznik nr 1 do niniejszej procedury oraz przesłać mailowo na adres informatyk@zambrow.pl. W przypadku dłuższej nieobecności pracownika zgłoszenia należy dokonywać do Inspektora ochrony danych Urzędu Miasta Zambrów.

Rozdział 6.
Podejmowanie działań w związku ze zgłaszanymi incydentami związanymi z bezpieczeństwem informacji oraz cyberbezpieczeństwem

§6.1. Zgłoszenie incydentu rejestrowane jest przez osobę wyznaczoną do utrzymywania kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. 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.

1) 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 lub jednostek organizacyjnych;
   d. koszty usunięcia skutków incydentu;
   e. szacowany czas naprawy skutków wywołanych incydentem;
   f. oszacowanie zasobów koniecznych do przywrócenia ciągłości działania systemów.
2) Zakwalifikowanie zgłoszenia incydentu jako „fałszywy alarm" kończy się postępowanie, o czym osoba wyznaczona informuje zgłaszającego.
3) W przypadku zakwalifikowania zdarzenia jako incydentu związanego z bezpieczeństwem informacji lub cyberbezpieczeństwem, osoba wyznaczona (ASI) podejmuje działania zabezpieczające i naprawcze zmierzające do zniwelowania szkód powstałych w wyniku incydentu.
4) Jednostki organizacyjne Miasta Zambrów we własnym zakresie podejmują działania naprawcze zmierzające do zniwelowania szkód powstałych w wyniku incydentu.
5) W przypadku stwierdzenia incydentu w podmiocie publicznym lub incydentu krytycznego osoba wyznaczona 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).
6) 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).
7) W zgłoszeniu przekazuje się informacje zgodnie z formularzem oraz zgodnie z treścią art. 23 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.
8) 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 7.
Podejmowanie działań w związku ze zgłaszanymi incydentami naruszenia bezpieczeństwa przetwarzania danych osobowych

§7.1. 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 2016r).

1. 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 przetwarzanie 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).

2. Fakt naruszenia lub podejrzenia naruszenia ochrony danych osobowych należy potwierdzić pisemnie poprzez niezwłoczne sporządzenie notatki służbowej, w której umieszcza się informacje o dacie, czasie, miejscu,

okolicznościach zdarzenia. Notatkę przekazuje się Inspektorowi ochrony danych za pośrednictwem swojego przełożonego lub bezpośrednio w przypadku osób zatrudnionych na samodzielnych stanowiskach. O zdarzeniu IOD niezwłocznie powiadamia ADO.

3. 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 naruszenie;

d. możliwe konsekwencje naruszenia ochrony danych osobowych;

e. wpływ incydentu na ciągłość działania Urzędu;

f. koszty usunięcia skutków incydentu;

g. szacowany czas naprawy skutków wywołanych incydentem.

4. Zakwalifikowanie zgłoszenia incydentu jako „fałszywy alarm” kończy postępowanie o czym IOD informuje zgłaszającego.

5. Sprawdzenie naruszenia lub podejrzenia naruszenia ochrony danych osobowych kończy się sprawozdaniem, które przekazywane jako ADO. Sprawozdanie wykonuje IOD wraz z ASI.

6. W przypadku zakwalifikowania zdarzenia jako naruszenie ochrony danych osobowych, które skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych, ADO bez zbędnej zwłoki, nie później niż w terminie 72 godzin od stwierdzenia naruszenia powiadamia Urząd Ochrony Danych Osobowych.

7. Zgłoszenia do UODO przekazywane są w sposób elektroniczny. Procedura zgłoszeń opisana jest pod adresem internetowym https://uodo.gov.pl/pl/134/233

8. IOD wraz z ASI podejmuje również działania zabezpieczające i naprawcze zmierzające do niwelowania skutków powstałych w wyniku incydentu, jak również działania zaradcze dla uniknięcia wystąpienia podobnych incydentów w przyszłości.

9. Jeżeli zgłoszony incydent naruszenia ochrony danych osobowych może spowodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, a stosowane w Urzędzie techniczne i organizacyjne środki ochrony danych nie eliminują tego ryzyka, IOD bez zbędnej zwłoki informuje ADO o konieczności zawiadomienia osób, których dane dotyczą o takim naruszeniu.

10. Jeżeli zawiadomienie osób, których dane dotyczą wymagałoby niewspółmiernie dużego wysiłku, IOD przygotowuje publiczny komunikat lub wybiera inny stosowny środek, za pomocą którego zawiadomienie zostanie tym osobom przekazane.

11. Szczegółową instrukcję postępowania z incydentem dotyczącym danych osobowych zawiera "Polityka zarządzania ryzykiem utraty bezpieczeństwa danych w Urzędzie Miasta Zambrów."

12. W przypadku stwierdzenia działań zamierzonych, przy jednoczesnym zidentyfikowaniu sprawcy incydentu dotyczącego naruszenia bezpieczeństwa przetwarzania danych osobowych ADO podejmuje decyzję dotyczącą wyciągnięcia ewentualnych konsekwencji dyscyplinarnych wobec sprawcy incydentu. Jednocześnie, w zależności od wagi incydentu, mogą być powiadomione organa ścigania.

Załącznik Nr 1 do Załącznika Nr 1

FORMULARZ ZGŁASZANIA INCYDENTÓW CYBERBEZPIECZEŃSTWA JEDNOSTEK ORGANIZACYJNYCH MIASTA ZAMBRÓW

CZĘŚĆ A: DANE GMINY		
1 .Nazwa podmiotu zgłaszającego	MIASTO ZAMBRÓW	
2.Siedziba i adres zgłaszającego	UL. FABRYCZNA 3, 18-300 ZAMBRÓW	
3.NIP zgłaszającego	723-162-22-31	
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, w której wystąpił incydent)		
ó.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*		Dostępności podanego numeru: o7:30-15:30 o w godzinach: o24h
9.Adres poczty elektronicznej osoby z jednostki organizacyjnej, zgłaszającej incydent*		
CZĘŚĆ D: OSOBA UPRAWNIONA DO SKŁADANIA WYJAŚNIEŃ W SPRAWIE INCYDENTU		
10. Imię i nazwisko osoby uprawionej do składania wyjaśnień dotyczących zgłaszanych informacji		
11 .Numer telefonu służbowego osoby uprawnionej do składania wyjaśnień dotyczących zgłaszania informacji		
12.Adres poczty elektronicznej osoby uprawnionej do składania wyjaśnień dotyczących zgłaszania informacji		
CZĘŚĆ E: OPIS INCYDENTU (uzupełnia osoba zgłaszająca z jednostki organizacyjnej w której wystąpił incydent)		
13.Data wystąpienia incydentu* Orientacyjny czas incydentu	Podany czas jest o przybliżony o dokładny	
14.Data wykrycia incydentu* Oraz stan incydentu Incydent nadal trwa/wygasł/został obsłużony	o nadal trawa o wygasł o został obsłużony	
15.Zadanie publiczne, na które incydent miał wpływ*		
16. Liczba osób, na które incydent miał wpływ*	ol-50 O51-500 O501-1.000 ol.000 - 10.000 o >10.000 o brak danych	
17.Zasięg geograficzny obszaru, którego dotyczy incydent*	o lnstytucja o Miasto/Województwo o Polska o Unia Europejska o Świat o brak danych	
18.Rodzaj działania*	O Celowe o Niecelowe	

Celowe-świadome /Niecelowe-nieświadome	
19.Kategoria zdarzenia*	□Podejrzana wiadomość e-mail np. podejrzane załączniki, phishing, szantaż □Zbieranie informacji np. skanowanie, podsłuch, SPAM, inżynieria społeczna □Treści obraźliwe np. obrażanie, pornografia dziecięca, przemoc i inne nielegalne treści □Oprogramowanie złośliwe 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 □Bezpieczeństwo informacji np. nieuprawniony dostęp do informacji, nieuprawniona zmiana informacji lub jej skasowanie □Oszustwo np. nieuprawnione wykorzystanie zasobów, naruszenie praw autorskich, podszywanie się, kradzież tożsamości □Podatność np. błędna konfiguracja, wykrycie podatności □Cyberterroryzm zdarzenie o charakterze terrorystycznym popełnione w cyberprzestrzeni □Inne zdarzenia nie mieszczące się w powyższych kategoriach
20.Skutki oddziaływania incydentu na systemy informacyjne jednostki organizacyjnej*	□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*	
24.1nne istotne informacje	
Pola oznaczone * są polami wymaganymi. Wypełniony formularz należy niezwłocznie wysyłać w postaci załącznika do wiadomości e-mail na adres: informatyk@zambrow.pl Jeśli pojawią się nowe informacje dotyczące incydentu należy niezwłocznie je przekazać uzupełniając formularz i przekazując go ponownie na ww. adres.	