BURMISTRZ
MIASTA JAROSŁAWIA
37-500 Jarosław

ZARZĄDZENIE Nr 13/2023

Burmistrza Miasta Jarosławia

z dnia 20 stycznia 2023 r.

w sprawie wprowadzenia procedury zarządzania incydentami związanymi z bezpieczeństwem informacji i cyberbezpieczeństwem w Urzędzie Miasta Jarosławia

Na podstawie art. 30 ust. 1 i art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz.U.2023.40), § 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 (t.j. Dz. U.2017.2247 ze zm.), art. 22 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t. j. Dz. U. 2022. 1863 ze zm.) Burmistrz Miasta Jarosławia

zarządza, co następuje:

§ 1

Wprowadza się Procedurę zarządzania incydentami związanymi z bezpieczeństwem informacji i cyberbezpieczeństwem w Urzędzie Miasta Jarosławia, stanowiącą załącznik do niniejszego Zarządzenia.

§ 2

Wykonanie Zarządzenia powierza się Pełnomocnikowi ds. cyberbezpieczeństwa oraz Zespołowi ds. Systemu Zarządzania Bezpieczeństwem Informacji.

§ 3

Zarządzenie wchodzi w życie z dniem podpisania.

Radca Prawny
mgr Mariusz Rychcom
RZ-P-165

SEKRETARZ MIASTA
mgr Magdalena Kapusta

BURMISTRZ MIASTA
JAROSŁAWIA
mgr Waldemar Paluch

Załącznik do Zarządzenia nr 13/2023
Burmistrza Miasta Jarosławia
z dnia 20 stycznia 2023 r.

Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji i cyberbezpieczeństwem w Urzędzie Miasta Jarosławia

Rozdział I

Postanowienia ogólne

1. Celem Procedury Zarządzania incydentami związanymi z bezpieczeństwem informacji i cyberbezpieczeństwem w Urzędzie Miasta Jarosławia jest podjęcie skutecznych czynności związanych z incydentem, takich jak obsługa, wyszukiwanie powiązań między incydentami, usuwanie przyczyn ich występowania oraz opracowanie wniosków wynikających z obsługi incydentu. Jednocześnie celem dokumentu jest zapewnienie ciągłości operacyjnej oraz ograniczenie wpływu przypadków naruszeń bezpieczeństwa zasobów informacyjnych na działalność jednostki.
2. Podstawą prawną do opracowania i wdrożenia dokumentu 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. Zakres obowiązywania:

   Czynności opisane w niniejszej procedurze obowiązują we wszystkich wydziałach, biurach, wieloosobowych oraz samodzielnych stanowiskach jak również w innych komórkach organizacyjnych Urzędu Miasta Jarosławia korzystających z zasobów Teleinformatycznych Urzędu. Niniejsza procedura jest elementem Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Jarosławia.
4. Odpowiedzialność:
   1) na każdym pracowniku Urzędu Miasta Jarosławia, posiadającym dostęp do zasobów teleinformatycznych spoczywa odpowiedzialność za prawidłowe zgłoszenie dotyczące bezpieczeństwa infrastruktury teleinformatycznej Urzędu Miasta Jarosławia.
   2) każdy pracownik Informatycznego Centrum Zarządzania Miastem odpowiedzialny za rozwiązanie problemu lub zapobieżenie incydentowi działa zgodnie z niniejszą procedurą.
   3) pełnomocnik ds. Cyberbezpieczeństwa oraz Zespół ds. Systemu Zarządzania Bezpieczeństwem Informacji oprócz obowiązków wynikających z Zarządzenia nr 432/2020 Burmistrza Miasta Jarosławia z dnia 17 grudnia 2020 r. w sprawie Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Jarosławia" odpowiedzialni są za:
      a) niezwłoczne reagowanie na incydenty bezpieczeństwa informacji w określony i z góry ustalony sposób,
      b) ocenę istniejących i potencjalnych zagrożeń w zakresie bezpieczeństwa informacji,
      c) ocenę przyczyn i skutków incydentów naruszenia bezpieczeństwa informacji w tym gromadzenie materiału dowodowego,

d) przygotowywanie propozycji działań korygujących i naprawczych oraz nadzór nad ich wprowadzaniem,

e) prowadzenie działań zmierzających do wzrostu świadomości w zakresie zapewnienia bezpieczeństwa informacji w Urzędzie,

f) współpracę z Rządowym Zespołem Reagowania na Incydenty Komputerowe CERT.

Rozdział II

Klasyfikacja i przyczyny incydentów

1. Incydent bezpieczeństwa informacji i cyberbezpieczeństwa możemy zdefiniować, jako każde bezprawne, nieautoryzowane lub nieakceptowalne działanie w systemie komputerowym lub innym urządzeniu elektronicznym (np. telefonie), którego efektem jest naruszenie poufności, integralności lub dostępności systemu lub danych.
2. 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. Obsługa incydentu to czynności umożliwiające wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetyzację, podejmowanie działań naprawczych i ograniczenie skutków incydentu.
5. Przyczyną incydentu bezpieczeństwa informacji oraz cyberbezpieczeństwa mogą być:
   1) zdarzenia losowe zewnętrzne (np.: klęski żywiołowe, przerwy w zasilaniu itp.), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia, uszkodzenia infrastruktury technicznej, ciągłość pracy systemów zostaje zakłócona, nie dochodzi jednak 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).

4) incydentami bezpieczeństwa informacji w szczególności są:
   a) naruszenie poufności, tzn. ujawnienie informacji niepowołanym osobom;
   b) naruszenie integralności, tzn. zniszczenie, uszkodzenie lub przekłamanie informacji;
   c) naruszenie dostępności, tzn. brak dostępu do danych przez uprawnionych użytkowników.
5) przykłady zdarzeń, które mogą być zakwalifikowane jako uzasadnione podejrzenie naruszenia bezpieczeństwa informacji i cyberbezpieczeństwa:
   a) 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.,
   b) niewłaściwe parametry środowiska jak zbyt wysoka temperatura lub nadmierna wilgotność (w szczególności dotyczy to serwerowni),
   c) 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,
   d) pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,
   e) jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikacje w systemie,
   f) nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,
   g) stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
   h) nastąpiła niedopuszczalna manipulacja danymi w systemie,
   i) ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą elementy systemu zabezpieczeń,
   j) 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.,
   k) ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki", itp.,
   l) podmieniono lub zniszczono nośniki z danymi bez odpowiedniego upoważnienia lub w niedozwolony sposób skasowano lub kopiowano dane osobowe,
   m) rażąco naruszono dyscyplinę pracy w zakresie przestrzegania PBT (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.),

n) stwierdzenie nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych, w tym także osobowych (otwarte szafy, regały, biurka).

6. W sytuacji, gdy nie mamy pewności, co do tego, czy zdarzenie stanowi incydent bezpieczeństwa, każdą podejrzaną aktywność zawsze należy traktować, jako potencjalny incydent, który trzeba zbadać i ewentualnie udowodnić, że nim nie jest.

Rozdział III
Zgłoszenie incydentu

1. Pracownicy Urzędu Miasta Jarosławia mają obowiązek niezwłocznie zgłaszać zauważone przez siebie incydenty oraz notować wszystkie szczegóły związane z incydentem. Punktem kontaktowym jest Inspektor Ochrony Danych tel. 16 624 8731 email: iod@um.jaroslaw.pl, Administrator Systemu Informatycznego wyznaczony z wydziału Informatycznego Centrum Zarządzania Miastem tel. 16 624 8713 email: it@um.jaroslaw.pl oraz pełnomocnik ds. cyberbezpieczeństwa tel. 16 624 8703 email: dariusz.tracz@um.jaroslaw.pl. Incydenty można zgłaszać również za pomocą e-zgłoszeń dostępnych z każdej stacji roboczej. W pilnych sprawach incydenty można zgłaszać pod nr telefonów 16 624 8776, 16 624 8791, 16 624 8771.
2. Zgłoszenie musi zawierać:
   1) miejsce i datę wystąpienia incydentu,
   2) imię i nazwisko zgłaszającego,
   3) opis incydentu w sposób adekwatny do posiadanej wiedzy i umiejętności zgłaszającego. Wzór zgłoszenia incydentu stanowi załącznik nr 1 do procedury
3. Zgłoszenia telefoniczne należy następnie potwierdzić szczegółową notatką służbową wg wzoru zgłoszenia incydentu, którą przekazuje się IOD lub jednej z osób wskazanych w ust. 1, poprzez swojego bezpośredniego przełożonego lub bezpośrednio w przypadku pracowników zatrudnionych na samodzielnych stanowiskach.
4. Pracownik 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.
5. Brak umiejętności poprawnego rozpoznania incydentu przez osobę zgłaszającą nie może być przyczyną zaniechania zgłoszenia.

Rozdział IV

Postępowanie z incydentami

1. Obsługa incydentu rozpoczyna się od jego dokładnego rozpoznania - ustalenia oznak naruszenia bezpieczeństwa, identyfikacji rodzaju incydentu, identyfikacji i zabezpieczenia dowodów oraz poinformowania o zdarzeniu odpowiednich osób. Osoba, która przyjęła zgłoszenie, powiadamia niezwłocznie członków Zespołu ds. Systemu Zarządzania Bezpieczeństwem Informacji oraz pełnomocnika ds. cyberbezpieczeństwa o fakcie i treści zgłoszenia.
2. Zespołu ds. Systemu Zarządzania Bezpieczeństwem Informacji dokonuje rozpoznania, jakiego typu incydent wystąpił. W przypadku incydentu bezpieczeństwa informacji związanego z naruszeniem danych osobowych postępuje zgodnie z zapisami § 11 Polityki Bezpieczeństwa Informacji stanowiącej załącznik nr 1 do Zarządzenia nr 432/2020 Burmistrza Miasta Jarosławia z dnia 17 grudnia 2020 r. w sprawie Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Jarosławia, zaś w przypadku incydentu dotyczącego cyberbezpieczeństwa po analizie zdarzenia i okoliczności z nim związanych pełnomocnik ds. cyberbezpieczeństwa wprowadza dane o incydencie do rejestru incydentów stanowiącego załącznik nr 2 do niniejszej procedury oraz zabezpiecza materiał dowodowy i deponuje go w wydzielonym pomieszczeniu, które zlokalizowane jest w budynku Rynek 6, pok. 25. Wskazane pomieszczenie objęte jest elektroniczną kontrolą dostępu.
3. Dla dokumentów na nośnikach komputerowych należy utworzyć obraz lub kopię (zależnie od stosownych wymagań), aby zapewnić ich dostępność oraz należy prowadzić zapisy wszelkich działań podczas procesu kopiowania jak również, 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. Po ww. czynnościach pełnomocnik ds. cyberbezpieczeństwa zawiadamia członków Zespołu ds. Systemu Zarządzania Bezpieczeństwem Informacji. Zespół zbiera się niezwłocznie, dokonuje analizy materiału dowodowego i podejmuje decyzję o sposobie dalszego postępowania.
5. W przypadku, gdy zgłoszone zdarzenie zostało uznane za incydent bezpieczeństwa informacji, Zespół dokonuje oceny istotności incydentu oraz zawiadamia Administratora danych osobowych o zaistnieniu incydentu oraz poziomie zagrożenia dla bezpieczeństwa informacji.
6. Zespół ocenia poziom istotności incydentu dla Urzędu kierując się następującymi kryteriami:
   1) wpływ incydentu na ciągłość działania Urzędu i wypełnianie jego zadań statutowych;
   2) krytyczność systemów dotkniętych skutkami incydentu bezpieczeństwa;
   3) wrażliwość informacji, których poufność, integralność czy dostępność naruszono (np czy naruszono bezpieczeństwo informacji prawnie chronionej - np.: danych osobowych, informacji niejawnych, itp.);
   4) rozległość wpływu incydentu na działanie systemów (nie działa jeden komputer, cała sieć, itp.);

5) rozmiar szkód powstałych skutkiem incydentu;
6) koszt usunięcia i naprawy skutków incydentu bezpieczeństwa;
7) szacowany czas przywrócenia ciągłości działania dotkniętego incydentem bezpieczeństwa systemu;
8) 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.);

7. W przypadku zakwalifikowania zdarzenia, jako incydentu związanego z bezpieczeństwem informacji lub cyberbezpieczeństwem, informatycy urzędu podejmują działania zabezpieczające i naprawcze zmierzające do zniwelowania szkód powstałych w wyniku incydentu.
8. W przypadku, gdy waga incydentu dotyczy systemów informatycznych i zakwalifikowana została, jako wysoka, o incydencje zawiadamiany jest właściwy CSIRT NASK (Naukowa i Akademicka Sieć Komputerowa - Państwowego Instytutu Badawczego ul. Kolska 12, 01-045 Warszawa).
9. Zgłoszenia do CSIRT NASK przekazywane są w sposób elektroniczny. Pełnomocnik ds. cyberbezpieczeństwa wypełnia formularz zgłoszenia incydentu dostępnego pod adresem https://incydent.cert.pl/ oraz wysyła go do CERT zgodnie z informacją zamieszczoną na tej stronie. Dalsza korespondencja z CERT w sprawie tego incydentu odbywa się zgodnie z wytycznymi CERT. W przypadku braku możliwości przekazania go w sposób elektroniczny można zgłaszać przy użyciu innych dostępnych środków komunikacji (np. na numer telefonu +48223808274).
10. W zgłoszeniu przekazuje się informacje zgodnie z formularzem oraz zgodnie z treścią art. 23 ust. 1 ustawy z dnia 05 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.
11. Zgłoszenie do CSIRT NASK obejmuje również wszelkie kwestie związane ze zmianą lokalizacji jednostki organizacyjnej, danych kontaktowych, itp.
12. W przypadku, gdy zgłoszone zdarzenie nie zostało zaklasyfikowane jako incydent bezpieczeństwa informacji, ale wyłącznie jako mające charakter „fałszywego alarmu" pełnomocnik ds. cyberbezpieczeństwa powiadamia zgłaszającego o fakcie, że zdarzenie nie stanowi incydentu bezpieczeństwa i tym samym postępowanie zostaje zakończone.
13. W przypadku stwierdzenia działań zamierzonych, umyślnych i ustaleniu sprawcy incydentu Zespół przekazuje wyniki analizy wraz z zabezpieczonym materiałem dowodowym Administratora Danych Osobowych celem wyciągnięcia konsekwencji dyscyplinarnych wobec sprawcy, ewentualnego zawiadomienia organów ścigania lub podjęcia kroków prawnych wobec osób trzecich.
14. Zespół ds. 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. Zespół na bieżąco dokumentuje swoje działania na każdym z etapów procesu zarządzania incydentem w formie notatki.

15. Rejestr incydentów przechowywany jest u pełnomocnika ds. cyberbezpieczeństwa. Rejestr może być prowadzony w formie cyfrowej. Wzór załącznika stanowi załącznik do niniejszej procedury.
16. Obsługa incydentu kończy się raportem zatwierdzonym przez Przewodniczącego Zespołu, ds. Systemu Zarządzania Bezpieczeństwem Informacji, który winien zawierać opis incydentu oraz wnioski, co do działań na przyszłość.

Załącznik nr 1 do procedury

Wzór zgłoszenia incydentu

Wstępny opis incydentu

1. Data ..... godzina .....
2. Osoba powiadamiająca o incydencie oraz inne osoby zaangażowane w związku z incydentem *(imię, nazwisko, stanowisko służbowe, dane kontaktowe)*.....
   .....
   .....
3. Lokalizacja zdarzenia *(nr pokoju, nazwa pomieszczenia, określenie roboczego stanowiska komputerowego, nazwa programu lub aplikacji itp.)*
   .....
   .....
   .....

.....

(podpis osoby/osób zgłaszających incydent)

Wstępna analiza incydentu

1. Zadanie publiczne, którego dotyczy zgłoszenie:
   .....
   .....
2. Liczba osób, na które miłą wpływ incydent:
   .....
3. Moment wystąpienia i wykrycia incydentu oraz czas jego trwania:
   .....
   .....
4. Zasięg geograficzny obszaru, którego dotyczy incydent:
   .....
   .....
5. Przyczyna zaistnienia incydentu:
   1) podejrzana wiadomość email*
   2) próba oszustwa*,
   3) nielegalne treści*,
   4) podatności*,

5) złośliwe oprogramowanie*,

6) inny (*należy opisać*).....

6. źródło incydentu:

.....

7. Sposób przebiegu incydentu:

.....

8. Skutki oddziaływania incydentu na systemy informacyjne podmiotu publicznego:

.....

.....

9. Informacja o podjętych działaniach zapobiegawczych:

.....

.....

10. Czy doszło do naruszenia danych osobowych:

tak/nie*

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

.....

(podpisy osób obsługujących incydent)

**- proszę zaznaczyć prawidłową odpowiedź*

Załącznik nr 2 do procedury

Rejestr incydentów cyberbezpieczeństwa

Lp.	Data zgłoszenia	Kategoria (incydent bezpieczeństwa/cyberbezpieczeństwa, naruszenie ochrony danych osobowych)	Opis incydentu (zdarzenia)	Osoba zgłaszająca	Przyczyna lub potencjalna przyczyna wystąpienia incydentu	Opis działań podjętych w związku z incydentem	Data zamknięcia incydentu