## ZARZĄDZENIE NR

# **PREZYDENTA MIASTA POZNANIA**

**z dnia 4 października 2018r.**

|  |  |
| --- | --- |
| w sprawie | **zarządzania incydentami w zakresie zadań publicznych zależnych od systemu informacyjnego.** |

Na podstawie art. 22 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2018 r. poz. 1560), w związku z art. 33 ust. 1, 3 i 5 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2018 r. poz. 994 ze zm.) zarządza się, co następuje:

**§ 1**

Ilekroć w zarządzeniu i załączniku do zarządzenia jest mowa o:

1) Prezydencie – należy przez to rozumieć Prezydenta Miasta Poznania;

2) kierowniku miejskiej jednostki organizacyjnej – należy przez to rozumieć kierownika miejskiej jednostki organizacyjnej w rozumieniu określonym w Regulaminie Organizacyjnym Urzędu Miasta Poznania;

3) dyrektorze wydziału – należy przez to rozumieć dyrektora w rozumieniu określonym w Regulaminie Organizacyjnym Urzędu Miasta Poznania;

4) Mieście – należy przez to rozumieć Miasto Poznań jako jednostkę samorządu terytorialnego;

5) Urzędzie – należy przez to rozumieć Urząd Miasta Poznania;

6) wydziale – należy przez to rozumieć wydział w rozumieniu określonym w Regulaminie Organizacyjnym Urzędu Miasta Poznania;

7) miejskiej jednostce organizacyjnej (m.j.o.) – należy przez to rozumieć miejską jednostkę organizacyjną w rozumieniu określonym w Regulaminie Organizacyjnym Urzędu Miasta Poznania;

8) ustawie – należy przez to rozumieć ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;

9) CSIRT NASK – należy przez to rozumieć Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy;

10) cyberbezpieczeństwie – należy przez to rozumieć odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy;

11) poufności danych lub usług – należy przez to rozumieć dane lub usługi, które są dostępne wyłącznie dla uprawnionych osób;

12) integralności danych lub usług – należy przez to rozumieć dane lub usługi, które są prawdziwe i nie zostały w sposób nieuprawniony („złośliwie”) zmienione;

13) dostępności danych lub usług – należy przez to rozumieć dane lub usługi, do których uprawnione osoby mają dostęp w ustalonym z góry czasie (np. w czasie godzin pracy);

14) autentyczności danych lub usług – należy przez to rozumieć dane lub usługi, co do których mamy pewność ich pochodzenia (treści i autorstwa);

15) incydencie – należy przez to rozumieć zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo, występujące w zakresie realizowanych zadań publicznych zależnych od systemu informacyjnego;

16) podatności – należy przez to rozumieć właściwość systemu informacyjnego, która może spowodować zagrożenie cyberbezpieczeństwa;

17) zagrożeniu cyberbezpieczeństwa – należy przez to rozumieć potencjalną przyczynę wystąpienia incydentu;

18) systemie informacyjnym – należy przez to rozumieć system teleinformatyczny, o którym mowa w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne wraz z przetwarzanymi w nim danymi w postaci elektronicznej.

**§ 2**

1. Za zapewnienie adekwatności, skuteczności i jednolitości zarządzania incydentami w Urzędzie Miasta Poznania oraz w miejskich jednostkach organizacyjnych odpowiedzialny jest Przewodniczący Zespołu ds. Bezpieczeństwa Informacji lub osoba przez niego upoważniona.

2. Przewodniczący Zespołu ds. Bezpieczeństwa Informacji lub osoba przez niego upoważniona wykonują swoje czynności przy pomocy członków Zespołu ds. Bezpieczeństwa Informacji.

3. Zarządzanie incydentami w szczególności dotyczy koordynacji zgłaszania i obsługi incydentów.

4. Prezydent wyznacza Przewodniczącego Zespołu ds. Bezpieczeństwa Informacji do utrzymywania kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.

5. Do zadań Zespołu ds. Bezpieczeństwa Informacji w zakresie koordynacji zarządzania incydentami należy w szczególności:

1) zapewnienie obsługi incydentu poprzez:

a) przeprowadzanie postępowań wyjaśniających okoliczności wystąpienia incydentu,

b) przygotowanie projektu szczegółowych wyjaśnień przekazywanych do CSIRT NASK, w tym informacji uzupełniających do pierwotnego zgłoszenia,

c) przygotowanie projektu rekomendacji dla dyrektorów wydziałów oraz kierowników m.j.o. w celu minimalizacji bądź usunięcia skutków wystąpienia incydentu oraz zapobiegania ich wystąpieniu w przyszłości;

2) prowadzenie rejestru incydentów dla Miasta Poznania;

3) podejmowanie czynności zmierzających do zapewnienia dostępu do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa.

6. Do zadań Przewodniczącego Zespołu ds. Bezpieczeństwa Informacji należy w szczególności:

1) zatwierdzanie kwalifikacji zdarzenia jako incydent;

2) zatwierdzanie wyjaśnień przekazywanych do CSIRT NASK, w tym informacji uzupełniających do pierwotnego zgłoszenia;

3) zatwierdzanie rekomendacji dla dyrektorów wydziałów oraz kierowników m.j.o. w celu minimalizacji bądź usunięcia skutków wystąpienia incydentu oraz zapobiegania ich wystąpieniu w przyszłości;

4) decydowanie o przekazaniu do CSIRT NASK w niezbędnym zakresie (gdy jest to konieczne do realizacji zadań CSIRT NASK) informacji stanowiących tajemnice prawnie chronione, w tym stanowiących tajemnicę przedsiębiorstwa oraz oznaczanie ich w przekazywanej treści informacji.

7. W celu sprawnego przyjmowania zawiadomień o wystąpieniu incydentów z wydziałów i m.j.o. oraz zgłaszania ich do CSIRT NASK wyznacza się pracowników dyżurujących w Centrum Zarządzania Kryzysowego Wydziału Zarządzania Kryzysowego i Bezpieczeństwa.

8. Dyrektor Wydziału Zarządzania Kryzysowego i Bezpieczeństwa zobowiązany jest do zapewnienia wykonania zadania, o którym mowa w ust. 6, zgodnie z Procedurą stanowiącą załącznik do niniejszego zarządzenia.

9. Wszyscy pracownicy wydziałów i m.j.o. zobowiązani są w trybie pilnym do zgłaszania incydentów zgodnie z Procedurą stanowiącą załącznik do niniejszego zarządzenia.

10. Zobowiązuje się dyrektorów wydziałów oraz kierowników m.j.o. do przyjęcia i wdrożenia rekomendacji, o których mowa w ust. 6 pkt 3, lub w przypadku niemożności ich realizacji – do przekazania do Przewodniczącego Zespołu ds. Bezpieczeństwa Informacji pisemnych informacji wraz z uzasadnieniem o konieczności odstąpienia od nich.

**§ 3**

1. Zespół ds. Bezpieczeństwa Informacji jest odpowiedzialny za prowadzenie rejestru incydentów związanych z naruszeniem cyberbezpieczeństwa, występujących w wydziałach i m.j.o.

2. Za utrzymywanie aktualności danych, o których mowa w ust. 1, odpowiada Przewodniczący Zespołu ds. Bezpieczeństwa Informacji.

3. Osoby koordynujące zarządzanie incydentami związanymi z naruszeniem cyberbezpieczeństwa, o których mowa w § 2 ust. 5 załącznika, są odpowiedzialne za przedstawienie Przewodniczącemu Zespołu ds. Bezpieczeństwa Informacji szczegółowych danych wymaganych w rejestrze incydentów.

4. Osoby, o których mowa w ust. 3, mają także obowiązek zgłoszenia ryzyka z obszaru bezpieczeństwa informacji w przypadku braku możliwości zastosowania działań doskonalących, eliminujących przyczyny i skutki incydentu. Zasady zarządzania ryzykiem z obszaru bezpieczeństwa informacji zostały określone odrębnym zarządzeniem.

**§ 4**

Zgodnie z art. 37 ust. 1 ustawy, do informacji o podatnościach, incydentach i zagrożeniach cyberbezpieczeństwa oraz o ryzyku wystąpienia incydentu nie stosuje się ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej.

**§ 5**

Wykonanie zarządzenia powierza się Zastępcom Prezydenta, Sekretarzowi, Skarbnikowi oraz dyrektorom wydziałów i kierownikom miejskich jednostek organizacyjnych.

**§ 6**

Zarządzenie wchodzi w życie z dniem podpisania.

PREZYDENT MIASTA POZNANIA

(-) Jacek Jaśkowiak