OPIS POSTĘPOWANIA

1. Za przekazanie informacji o incydencie odpowiedzialny jest pracownik, który zauważył zaistnienie incydentu. Incydent powinien zostać niezwłocznie zgłoszony do Kierownika Oddziału Teleinformatyki (Kierownika IT).
2. Za prowadzenie rejestru incydentów bezpieczeństwa oraz jego przeglądy odpowiada Kierownik IT, który ustala zakres informacji objętych incydentem oraz przekazuje informacje o incydencie właścicielom informacji.
3. Kierownik IT wyznacza operatora incydentu.
4. Operator incydentu podejmuje działanie niezwłocznie po zgłoszeniu incydentu i przekazaniu mu informacji.
5. Właściciel informacji w czasie nie dłuższym niż 2 godziny od powzięcia informacji dokonują oceny istotności incydentu i przekazują tą informację do Operatora Incydentu.
6. Właściciele informacji objętych incydentem są odpowiedzialni za podjęcie zaplanowanie i podjęcie działań mających na celu ograniczenie wpływu incydentu.
7. Informacja o zaplanowanych i podjętych działania jest przekazywana do Kierownika IT.
8. W przypadku incydentów poważnych i krytycznych Kierownik IT w raz z zainteresowanymi właścicielami informacji tworzy plan działań mających na celu ograniczenie możliwości powstania incydentu podobnego typu w przyszłości. Za realizację planu odpowiedzialny jest Kierownk IT.
9. W razie konieczności Kierownik IT wdraża działania związane z reagowaniem na naruszenie przepisów prawa, zgodnie ze stosowną instrukcją.
10. Zamknięcia incydentu dokonuje Pełnomocnik ds. ZSZ, zarządzając w razie potrzeby audit odpowiedniego obszaru działania.
11. Przeglądu rejestru dokonuje sie nie rzadziej niż raz na 6 miesięcy, przy czym w przypadku wystąpienia incydentu skutkującego utratą poufności bądź integralności danych przegląd przeprowadza się niezwłocznie. Celem przeglądu jest ustalenie czy wszystkie działania mjące na celu złagodzenie skutków incydentów oraz mające na celu ograniczenie incydentów w przyszłości zostały podjęte zgodnie z planem.

KLASYFIKACJA INCYDENTÓW

1. Sposób obliczenia wagi incydentu bazuje na zakresie naruszenia poufności integralności i dostępności informacji, których dotyczy incydent
2. Współczynnik obliczony jest na podstawie następującego wzoru:

Współczynnik=2*Poufność + Integralność_1 + Integralność_2 + Dostępność - 5

Klasyfikacja incydentu	Wartość współczynnika
Krytyczny	8 i powyżej
Poważny	7-9
Istotny	3-6

Tabela 1.Definicje wskaźników bezpieczeństwa wykorzystanych klasyfikacji informacji.

Naruszenie Poufności (P)	1	Ujawniono informacje, do których dostęp mogą mieć wszyscy pracownicy Urzędu Miasta Płocka.
	2	Ujawniono informacje wymagające ochrony przed nieautoryzowanym dostępem. Dostęp do nich ma tylko wybrana grupa pracowników Urzędu Miasta Płocka.
	3	Ujawniono informacje niezwykle ważne, wymagające szczególnej ochrony. Dostęp do dokumentów jest ściśle nadzorowany.
Naruszenie Integralności_1 (I1)	1	W wyniku nieautoryzowanej zmiany informacji jej odtworzenie nie zajmie więcej niż 3 dni. Odtworzenie informacji będzie możliwe przy nikłym nakładzie zasobów ludzkich i finansowych.
	2	W wyniku nieautoryzowanej zmiany informacji jej odtworzenie nie zajmie więcej niż dwa tygodnie. Odtworzenie informacji będzie możliwe przy znacznym wykorzystaniu zasobów ludzkich i finansowych.
	3	W wyniku nieautoryzowanej zmiany nie będzie możliwe odtworzenie informacji lub jej odtworzenie pochłonie bardzo duże zasoby ludzkie i finansowe.
Naruszenie Integralności_2 (I2)	1	Nieautoryzowana zmiana informacji nie pociąga za sobą odpowiedzialności prawej oraz nie wiąże się z zauważalną utratą reputacji Urzędu.
	2	Nieautoryzowana zmiana informacji pociąga za sobą ewentualną odpowiedzialność prawną oraz wiąże się z zauważalną utratą reputacji Urzędu.
	3	Nieautoryzowana zmiana informacji pociąga za sobą automatyczną odpowiedzialność prawną oraz wiąże się z istotną utratą reputacji Urzędu.
Naruszenie Dostępności (D)	1	W wyniku incydentu nastąpi opóźnienie w dostępności informacji w wyskości 50% wymaganego czasu dostępności
	2	W wyniku incydentu nastąpi opóźnienie w dostępności informacji w wyskości 50%-100% wymaganego czasu dostępności
	3	W wyniku incydentu nastąpi opóźnienie w dostępności informacji w wyskości powyżej 100% wymaganego czasu dostępności

Klasyfikacja informacji: informacja wewnętrzna dostępna

Lista incydentów bezpieczeństwa informacji objętych obowiązkiem rejestracji (lista otwarta)

1. Identyfikacja złośliwego oprogramowania
2. Niezgodna ze specyfikacją praca systemu informatycznego, wpływająca na procesy pracy
3. Niedostępność systemu informatycznego
4. Niedostępność danych
5. Utrata danych (zniszczenie)
6. Utrata kontroli nad danymi (naruszenie poufności bądź integralności)
7. Utrata sprzętu przetwarzającego informacje bądź jej nośnika
8. Uszkodzenie sprzętu przetwarzającego informacje bądź jej nośnika
9. Awaria sprzętu bądź oprogramowania przetwarzającego informacje, uniemożliwiająca pracę bądź prowadząca do niewłaściwych wyników.
10. Przebywanie osób nieuprawnionych w obszarze wyłączonym z dostępu z przyczyn bezpieczeństwa.
11. Penetracja sieci LAN
12. Brak kopii bezpieczeństwa bądź jej nieskuteczne odtworzenie
13. Upublicznienie danych chronionych przez organizację.
14. Brak stosownych zabezpieczeń w umowach ze stronami trzecimi (klauzula poufności)
15. Pozostawienie bez nadzoru strony trzeciej w obszarze wyłączonym z dostępu z przyczyn bezpieczeństwa
16. Brak oświadczenia o poufności i upoważnienia do przetwarzania danych przez pracownika do trakiej pracy dopuszczonego
17. Niewłaściwe fizyczne zabezpieczenie danych na stanowisku pracy
18. Naruszenie polityki haseł
19. Naruszenie zasad postępowania z kluczami do pomieszczeń
20. Skierowanie wydruku do drukarki innej niż bezposrednio nadzorowana przez drukującego lub osoby z nim współpracujące
21. Zalanie, pożar bądź inna awaria o charakterze destrukcyjnym pomieszczenia, w którym znajdują się dane lub środki przetwarzania danych
22. Nieautoryzowane wykonanie lub udostępnienie klucza do pomieszczenia biurowego lub innego, związanego z przetwarzaniem danych.
23. Użycie niezinwentaryzowanego bądź niedopuszczonego do użytkowania nośnika danych
24. Użycie niezinwentaryzowanego bądź niedopuszczonego do użytkowania oprogramowania
25. Instalacja niedopuszczonego do uzycia oprogramowania
26. Fizyczne bądź logiczne obejście / złamanie zabezpieczeń teleinformatycznych w Urzędzie (także uzyskanie dostępu do zawartości sieci www objętej blokadą w UMP)
27. Wykorzystanie publicznych serwisów pocztowych w celach służbowych (dotyczy także wysyłania korespondencji służbowej na adresy umieszczone w takich domenach).
28. Wykorzystanie poczty służbowej do celów nie związanych z powierzonymi obowiązkami
29. Wykonywanie pracy zdalnej niezgodnie ze stosowną instrukcją
30. Przesłanie danych do niewłaściwego odbiorcy

Klasyfikacja informacji: informacja wewnętrzna dostępna

Wzór listy incydentów bezpieczeństwa informacji objętych obowiązkiem rejestracji

lp/data	Zgłasza	Rodzaj incydentu	Operator obsługi incydentu	Podjęte czynności	Efekt podjętych czynności	Data zamknięcia incydentu	Zatwierdził zamknięcie incydentu

Wzór raportu z przeglądu incydentów

Raport z przeglądu incydentów

Nr i data przeglądu:

Dokonujący przeglądu:

Podsumowanie przeglądu:

Spostrzeżenia:

Załączniki:

Rozdzielnik:

Sporządził: Zatwierdził: