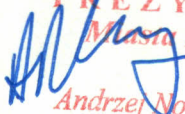


URD: 1555280

ZINTEGROWANY SYSTEM ZARZĄDZANIA – DOKUMENT NADZOROWANY W WERSJI ELEKTRONICZNEJ		
URZĄD MIASTA PŁOCKA	POLITYKA BEZPIECZEŃSTWA INFORMACJI W URZĘDZIE MIASTA PŁOCKA	Wydanie 04 z dnia 21.02.2017 Strona: 1
Kategoria informacji: informacja jawna		

Polityka Bezpieczeństwa Informacji w Urzędzie Miasta Płocka

Opracował: Pełnomocnik ds. Zintegrowanego Systemu Zarządzania Krzysztof Krakowski	Zatwierdził: Prezydent Miasta Płocka Andrzej Nowakowski	PREZYDENT Miasta Płocka  Andrzej Nowakowski
---	--	--

GLÓWNY SPECJALISTA


Anna Domańska

SEKRETARZ MIASTA PŁOCKA


Krzysztof Krakowski

Kategoria informacji: informacja jawna**Spis treści:**

1. Wstęp
2. Terminologia
3. Definicje
4. Podstawy prawne
5. Zakres Systemu Bezpieczeństwa Informacji
6. Deklaracja Najwyższego Kierownictwa w zakresie bezpieczeństwa informacji w Urzędzie Miasta Płocka
7. Organizacja bezpieczeństwa informacji w Urzędzie Miasta Płocka
8. Dokumentacja systemu zarządzania bezpieczeństwem informacji
9. Zasady współpracy ze stronami zainteresowanymi
10. Polityka kontroli dostępu do informacji
11. Klasyfikacja informacji
12. Zarządzanie aktywami i ryzykami
13. Autoryzacja nowych urządzeń
14. Zarządzanie systemami i sieciami
15. Bezpieczeństwo zasobów ludzkich
16. Bezpieczeństwo fizyczne, sprzętu i infrastruktury technicznej
17. Zarządzanie ciągłością działania
18. Zarządzanie zmianami
19. Polityka wymiany informacji między Urzędem Miasta Płocka i miejskimi jednostkami organizacyjnymi
20. Zgodność z wymaganiami prawnymi i innymi
21. Deklaracja ochrony własności intelektualnej
22. Postanowienia końcowe

Opracował:Pełnomocnik ds.
Zintegrowanego Systemu Zarządzania
Krzysztof Krakowski**Zatwierdził:**Prezydent Miasta Płocka
Andrzej Nowakowski

1. Wstęp

O skuteczności działania i rozwoju każdej organizacji świadczy stopień osiągnięcia zamierzonego celu. W procesie tym kluczowe jest stosowanie współczesnych technik i technologii, narzędzi i systemów informatycznych oraz przetwarzania i zarządzania informacją. Informacja jest jednym z najważniejszych zasobów Urzędu Miasta Płocka, dlatego powinna być chroniona na każdym szczeblu organizacji. Urząd Miasta Płocka chroni zarówno informacje własne, jak i powierzone. Poufność, dostępność i integralność informacji ma kluczowe znaczenie dla utrzymania zgodności z przepisami prawa oraz wizerunku Urzędu wobec stron zainteresowanych.

Polityka Bezpieczeństwa Informacji w Urzędzie Miasta Płocka stanowi zestawienie zasad, praw i reguł oraz doświadczeń i dobrych praktyk w zakresie zarządzania i ochrony danych i informacji w naszej organizacji. Polityka określa techniczne i organizacyjne środki służące do osiągnięcia celów stawianych przed systemem zarządzania bezpieczeństwem informacji, jakimi są: zapewnienie spełnienia wymagań prawnych, właściwe zabezpieczenie aktywów informacyjnych, ochrona przetwarzania danych, niezawodność funkcjonowania systemów, zmniejszenie ryzyka utraty informacji oraz systematyczna edukacja użytkowników, a w efekcie pełne zaangażowanie wszystkich pracowników w ochronę informacji. .

Polityka Bezpieczeństwa Informacji została wdrożona i jest stale doskonalona w celu:

- 1) zapewnienia poufności, integralności i dostępności danych;
- 2) zapewnienia identyfikowalności czynności i zasobów podczas przetwarzania danych;
- 3) zapewnienia niezawodności działań;
- 4) podejmowania wysiłków prowadzących do poprawy poziomu bezpieczeństwa zasobów informacyjnych w Urzędzie.

Polityka Bezpieczeństwa Informacji jest dokumentem nadrzędnym w stosunku do wszystkich dokumentów systemowych z zakresu zarządzania bezpieczeństwem informacji.

2. Terminologia

Ileokroć w Polityce Bezpieczeństwa Informacji jest mowa o:

- „**Polityce**” - należy przez to rozumieć Politykę Bezpieczeństwa Informacji w Urzędzie Miasta Płocka;
- „**Mieście**” – należy przez to rozumieć Gminę - Miasto Płock;
- „**Prezydencie**” – należy przez to rozumieć Prezydenta Miasta Płocka;
- „**Urzędzie**” - należy przez to rozumieć Urząd Miasta Płocka;

Opracował:

Pełnomocnik ds.
Zintegrowanego Systemu Zarządzania
Krzysztof Krakowski

Zatwierdził:

Prezydent Miasta Płocka
Andrzej Nowakowski

Kategoria informacji: informacja jawna

- „**Systemie informatycznym**” - należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur, narzędzi programowych zastosowanych do przetwarzania informacji i danych;
- „**SZBI**” - należy przez to rozumieć System Zarządzania Bezpieczeństwem Informacji w Urzędzie Miasta Płocka;
- „**Użytkownika**” - należy przez to rozumieć osobę korzystającą z zasobów teleinformatycznych Urzędu.

3. Podstawy prawne:

Polityka Bezpieczeństwa Informacji oraz pozostałe dokumenty ZSZ dotyczące zarządzania bezpieczeństwem informacji w Urzędzie spełniają wymagania prawne i regulacyjne, zawarte w:

- 1) ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. 2014, poz. 1114 ze zmianami);
- 2) ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 2016, poz. 922);
- 3) ustawie z dnia 06 września 2001 r. o dostępie do informacji publicznej (Dz.U. 2016, poz. 1764);
- 4) ustawie z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. 2016, poz. 1579);
- 5) rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. 2004, Nr 100, poz. 1024);
- 6) rozporządzeniu 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 (Dz.U. 2016, poz. 113 ze zmianami);
- 7) rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28 sierpnia 2014, str.73);
- 8) normie PN-ISO/IEC 27001:2014-12.

Opracował:

Pełnomocnik ds.
Zintegrowanego Systemu Zarządzania
Krzysztof Krakowski

Zatwierdził:

Prezydent Miasta Płocka
Andrzej Nowakowski

4. Definicje:

- 1) **Informacja** – wszelkie zapisy w formie papierowej, w systemach komputerowych oraz na innych nośnikach przetwarzane w systemach tradycyjnych, elektronicznych i komunikacyjnych będących własnością Miasta, funkcjonujących w Urzędzie lub tylko administrowanych przez Urząd;
- 2) **Bezpieczeństwo informacji** – zachowanie poufności, integralności i dostępności informacji w wyniku stosowania procesu zarządzania ryzykiem;
- 3) **Aktyw/zasób** – wszystko to, co ma wartość dla organizacji w zakresie informacji (zarówno informacje, jak i środki techniczne oraz organizacyjne do ich przetwarzania).
- 4) **Poufność** – zapewnienie dostępu do informacji tylko osobom upoważnionym.
- 5) **Integralność** – zapewnienie że dokument nie zostanie zmieniony w sposób nieuprawniony.
- 6) **Dostępność** – zapewnienie, że osoby upoważnione będą miały dostęp do informacji zawsze gdy jest to im niezbędne.
- 7) **Ryzyko** – prawdopodobieństwo wystąpienia zagrożenia, które wykorzystując podatność(ci) aktywu, może doprowadzić do jego uszkodzenia lub zniszczenia.
- 8) **Szacowanie ryzyka** – całościowy proces analizy i oceny ryzyka.
- 9) **Postępowanie z ryzykiem** – proces wyboru i wdrażania środków modyfikujących ryzyko.
- 10) **Zarządzanie ryzykiem** – proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych przy zachowaniu akceptowalnego poziomu kosztów.
- 11) **Zdarzenie związane z bezpieczeństwem informacji** – określony stan systemu, usługi lub sieci, który wskazuje na możliwe naruszenie polityki bezpieczeństwa informacji, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem.
- 12) **Incydent bezpieczeństwa informacji** – pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji.
- 13) **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.

Opracował:Pełnomocnik ds.
Zintegrowanego Systemu Zarządzania
Krzysztof Krakowski**Zatwierdził:**Prezydent Miasta Płocka
Andrzej Nowakowski

Kategoria informacji: informacja jawna

- 14) **Administrator Danych (AD)** – organ, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania danych osobowych. Administratorem Danych jest Gmina – Miasto Płock.
- 15) **Administrator Bezpieczeństwa Informacji (ABI)** – powołany przez Administratora Danych pracownik Urzędu, do zadań którego należy zapewnienie przestrzegania przepisów o ochronie danych osobowych oraz prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych.

5. Zakres Systemu Bezpieczeństwa Informacji

SZBI w Urzędzie stanowi część Zintegrowanego Systemu Zarządzania, odnoszącą się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji. SZBI został opracowany, wdrożony i jest utrzymywany w oparciu o normę PN-ISO/IEC 27001:2014-12. Zakres SZBI dotyczy obsługi administracyjnej ludności i podmiotów gospodarczych oraz zarządzania przestrzenią miejską.

Zakresy określone przez dokument Polityki Bezpieczeństwa Informacji mają zastosowanie do całego systemu informacyjnego Urzędu Miasta Płocka, w szczególności do:

- 1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są informacje podlegające ochronie;
- 2) informacji będących własnością Urzędu Miasta Płocka;
- 3) informacji będących własnością klientów Urzędu Miasta Płocka, uzyskanych na podstawie zawartych umów;
- 4) wszystkich lokalizacji Urzędu Miasta Płocka, czyli budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie;
- 5) wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, konsultantów, stażystów i innych osób mających dostęp do informacji podlegających ochronie.

6. Deklaracja Najwyższego Kierownictwa w zakresie bezpieczeństwa informacji w Urzędzie Miasta Płocka

Prezydent Miasta Płocka, stojąc na stanowisku, że informacja jest newralgicznym zasobem Urzędu, wdrożył w ramach Zintegrowanego Systemu Zarządzania w Urzędzie Miasta Płocka system zarządzania bezpieczeństwem informacji i zobowiązuje się do podejmowania wszelkich działań

Opracował:
Pełnomocnik ds.
Zintegrowanego Systemu Zarządzania
Krzysztof Krakowski

Zatwierdził:
Prezydent Miasta Płocka
Andrzej Nowakowski

Kategoria informacji: informacja jawna

prowadzących do kompleksowego zabezpieczenia informacji oraz zapewnienia środków niezbędnych do realizacji niniejszej Polityki.

7. Organizacja bezpieczeństwa informacji w Urzędzie Miasta Płocka

Odpowiedzialność za realizację ochrony informacji w Urzędzie ponoszą wszyscy pracownicy Urzędu – proporcjonalnie do wykonywanych obowiązków i posiadanych uprawnień.

Zakres uprawnień i odpowiedzialności związany z zarządzaniem bezpieczeństwem informacji określony został w procedurach i instrukcjach Zintegrowanego Systemu Zarządzania w Urzędzie Miasta Płocka w procesie „Bezpieczeństwo Informacji w Urzędzie Miasta Płocka”.

Zarządzeniem nr 911/2015 z dnia 11 sierpnia 2015 r. Prezydent Miasta Płocka powołał Administratora Bezpieczeństwa Informacji.

Każdy pracownik Urzędu jest zapoznawany z zasadami bezpieczeństwa oraz z aktualnymi procedurami ochrony informacji w swojej komórce organizacyjnej oraz w Urzędzie Miasta Płocka zawartymi w Instrukcji podstawowych zasad bezpieczeństwa dla pracowników Urzędu. Stażyści oraz praktykanci również są zapoznawani z tymi zasadami. Kierownik komórki organizacyjnej jest odpowiedzialny za ochronę bezpieczeństwa informacji w podległej komórce, a w szczególności za monitorowanie integralności i dostępności posiadanych zasobów informacji, nadzorowanie przestrzegania zasad bezpieczeństwa przez podległych pracowników oraz podejmowanie stosownych działań w razie stwierdzenia wystąpienia incydentu lub sytuacji mogącej prowadzić do wystąpienia incydentu bezpieczeństwa.

Właściciel aktywu odpowiada za bieżące nadzorowanie oraz zarządzanie aktywem.

8. Dokumentacja systemu zarządzania bezpieczeństwem informacji

Dokumentacja SZBI składa się z czterech głównych elementów. Są nimi:

- Polityka Bezpieczeństwa Informacji w Urzędzie Miasta Płocka;
- Deklaracja stosowania;
- Procedury i instrukcje, które określają zasady postępowania;
- Raporty z analizy ryzyka i plany postępowania z ryzykiem.

Uzupełnieniem dokumentacji SZBI jest pozostała dokumentacja Zintegrowanego Systemu Zarządzania oraz Polityka bezpieczeństwa ochrony danych osobowych wraz z instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Opracował:

Pełnomocnik ds.
Zintegrowanego Systemu Zarządzania
Krzysztof Krakowski

Zatwierdził:

Prezydent Miasta Płocka
Andrzej Nowakowski

9. Zasady współpracy ze stronami zainteresowanymi

W Urzędzie Miasta Płocka wdrożono standard bezpieczeństwa fizycznego w odniesieniu do klientów i podmiotów wykonujących prace zlecone na terenie Urzędu. Ponadto instrukcja ogólna w zakresie wymagań dla umów przygotowywanych w Urzędzie Miasta Płocka określa klauzule poufności różnego stopnia szczegółowości, niezbędne przy zawieraniu umów. Celem takiego postępowania jest zapewnienie bezpieczeństwa informacji przed dostępem osób niepowołanych, uszkodzeniem lub innymi zakłóceniami w obiektach oraz systemach Urzędu Miasta Płocka. Wyodrębnione zostały również obszary niedostępne dla klientów i osób trzecich z uwagi na przetwarzane informacje bądź funkcje techniczne. Pomieszczenia komórek organizacyjnych przetwarzających dane osobowe wyposażono w fizyczne bariery (lady) umożliwiające obsługę klientów przy jednoczesnym odseparowaniu ich od zasobów informacyjnych. Ponadto znaczna część klientów jest obsługiwana w Biurze Obsługi Klienta lub na stanowiskach obsługi klienta, co sprawia, że nie mają oni uzasadnionej potrzeby poruszania się po innych obszarach Urzędu Miasta Płocka. Ciągi komunikacyjne pozostają pod stałą obserwacją systemu monitoringu.

10. Polityka kontroli dostępu do informacji

Dostęp do informacji przechowywanych i przetwarzanych w Urzędzie jest poddany kontroli wynikającej z obowiązujących przepisów prawa powszechnego oraz dodatkowych wymagań bezpieczeństwa, przyjętych w normie PN-ISO/IEC 27001:2014-14. Kontrola polega na:

- 1) wydzieleniu obszarów przeznaczonych do przechowywania oraz przetwarzania poszczególnych zbiorów danych i zapewnieniu odpowiednich barier fizycznych przeciwdziałających nieuprawnionemu dostępowi;
- 2) zarządzaniu uprawnieniami poszczególnych użytkowników w sposób zapewniający dostęp wyłącznie do danych wymaganych do wykonywania obowiązków służbowych, jeśli dane te podlegają ochronie z jakiegokolwiek przyczyny;
- 3) stosowaniu bezpiecznych systemów przetwarzania informacji;
- 4) nadzorowaniu działalności stron trzecich, mogących wpłynąć na bezpieczeństwo informacji;
- 5) bieżącym informowaniu pracowników o wszelkich zmianach w zakresie regulacji dotyczących przechowywania, przetwarzania i udostępniania informacji.

Adekwatność i skuteczność stosowanych w Urzędzie środków kontroli dostępu do informacji podlega bieżącej weryfikacji w ramach auditów wewnętrznych, zmian dokumentacji i metod postępowania wynikających z ewolucji uregulowań prawnych oraz systemów przetwarzania danych a także reagowania na zagrożenia ujawnione przez inne strony.

Opracował:

Pełnomocnik ds.
Zintegrowanego Systemu Zarządzania
Krzysztof Krakowski

Zatwierdził:

Prezydent Miasta Płocka
Andrzej Nowakowski

11. Klasyfikacja informacji

Klasyfikacja została wprowadzona w celu uporządkowania w Urzędzie postępowania z różnymi rodzajami informacji, które są głównym zasobem naszej organizacji. W szczególności sposób potraktowano informację, której ujawnienie może narazić pracodawcę na szkodę.

Podstawowym elementem klasyfikacji są grupy informacji. W grupach informacji zebrane zostały dokumenty logicznie ze sobą powiązane o podobnych wymaganiach związanych z bezpieczeństwem. Do określenia poziomu bezpieczeństwa danej grupy informacji przyjęto wskaźniki definiujące poufność, integralność oraz dostępność danej grupy informacji, wymagane w Urzędzie.

Przez poufność rozumiemy zapewnienie, iż dostęp do informacji mają tylko i wyłącznie osoby uprawnione. Przez integralność rozumiemy zapewnienie, iż informacje nie zostały zmienione lub zniszczone w nieautoryzowany sposób (niezgodny z wewnętrznymi regulacjami Urzędu).

Przez dostępność rozumiemy możliwość dostępu do informacji w takim czasie, jaki jest oczekiwany przez użytkownika. Ze względu na charakter pracy Urzędu i cel jego funkcjonowania do określenia wskaźników bezpieczeństwa największy nacisk położono na parametr integralności. Zdefiniowano trzy poziomy dla każdego z powyższych wskaźników po to, aby możliwe było powiązanie danej grupy informacji z określonym poziomem zdefiniowanego wskaźnika w skali 1-3.

Struktura klasyfikacji informacji w Urzędzie Miasta Płocka opiera się na założeniu istnienia trzech poziomów postrzegania informacji:

- 1) **informacje jawne** – informacje publicznie dostępne,
- 2) **informacje wewnętrzne** – informacje, których przetwarzanie i udostępnianie podlega restrykcjom z uwagi na szczególne znaczenie dla pracodawcy (właściciela informacji):
 - a) informacje **wewnętrzne dostępne** – informacje dostępne dla wszystkich pracowników Urzędu Miasta Płocka,
 - b) informacje **wewnętrzne wrażliwe** – informacje dostępne dla grupy pracowników upoważnionych z uwagi na realizowane zadania regulaminowe,
 - c) informacje **stanowiące tajemnicę pracodawcy** – informacje, których przetwarzanie i udostępnianie może narazić pracodawcę na szkodę;
- 3) **informacje ustawowo chronione** – tajemnice określone w odrębnych przepisach.

Opracował:

Pełnomocnik ds.
Zintegrowanego Systemu Zarządzania
Krzysztof Krakowski

Zatwierdził:

Prezydent Miasta Płocka
Andrzej Nowakowski

12. Zarządzanie aktywami i ryzykami

Urząd zarządza swoimi aktywami informacyjnymi poprzez zapewnienie im wymaganego poziomu bezpieczeństwa. Identyfikowane są aktywa informacyjne i klasyfikowane zgodnie ze stawianymi im wymaganiami w zakresie ochrony. Ważnym elementem zarządzania aktywami i bezpieczeństwem informacji jest przeprowadzanie okresowej analizy ryzyka i opracowywanie planów postępowania z ryzykiem. Analiza wyników stanowi podstawę podejmowania wszelkich działań w zakresie doskonalenia ochrony zasobów Urzędu. Na podstawie wyników analizy ryzyka opracowywane są plany postępowania z ryzykiem dla aktywów o ryzykach większych niż ustalony poziom ryzyka akceptowalnego. Ryzyka są przeglądane na przeglądach kierownictwa oraz po zmianach mających wpływ na system bezpieczeństwa informacji.

13. Autoryzacja nowych urządzeń

Każde nowe lub zmienione urządzenie służące do przetwarzania informacji lub mogące w jakikolwiek inny sposób wpływać na bezpieczeństwo informacji jest weryfikowane na zgodność z wymaganiami systemu bezpieczeństwa informacji i zaakceptowane przez uprawnioną osobę. Szczegółowy opis postępowania zawiera właściwa instrukcja ZSZ.

Urządzenia służące do przetwarzania informacji nie będące własnością Urzędu mogą być używane (po sprawdzeniu sprzętu pod względem kryteriów bezpieczeństwa) wyłącznie za zgodą osoby upoważnionej.

14. Zarządzanie systemami i sieciami

Urząd dba o przestrzeganie zasad związanych z utrzymywaniem i użytkowaniem systemów informatycznych i sieci. Celem takiego postępowania jest zapewnienie poufności, integralności i dostępności przetwarzanej przez nie informacji własnych. Skuteczna realizacja postawionego celu możliwa jest dzięki:

- 1) kompetencjom i świadomości pracowników oraz podpisanym umowom ze specjalistycznymi firmami administrującymi zasobami informatycznymi;
- 2) opracowanym zasadom konserwacji urządzeń w celu zapewnienia ich ciągłej pracy;
- 3) kontrolowaniu wprowadzania wszelkich zmian do infrastruktury technicznej,
- 4) prowadzeniu prac rozwojowych i testowych na oddzielnych urządzeniach lub środowiskach w celu zapewnienia bezpieczeństwa systemów produkcyjnych;
- 5) nadzorowaniu usług dostarczanych przez strony trzecie, w szczególności odbieraniu ich i akceptowaniu w sposób świadomy uwzględniający jego wpływ na istniejący system bezpieczeństwa;

Opracował:

Pełnomocnik ds.
Zintegrowanego Systemu Zarządzania
Krzysztof Krakowski

Zatwierdził:

Prezydent Miasta Płocka
Andrzej Nowakowski

Kategoria informacji: informacja jawna

- 6) wdrożeniu zabezpieczeń chroniących przed oprogramowaniem złośliwym i mobilnym;
- 7) systematycznemu tworzeniu i testowaniu kopii bezpieczeństwa;
- 8) przestrzeganiu opracowanych zasad postępowania z nośnikami;
- 9) bieżącemu monitorowaniu aktywów informacyjnych.

Urząd monitoruje możliwość wystąpienia incydentów bezpieczeństwa i posiada mechanizmy reagowania w przypadkach ich wystąpienia. Szczegółowy sposób postępowania zawiera właściwa instrukcja ZSZ.

15. Bezpieczeństwo zasobów ludzkich

Urząd zapewnia kompetentną kadrę pracowniczą do realizacji wyznaczonych zadań. Celem takiego postępowania jest ograniczenie ryzyka błędu ludzkiego, kradzieży, nadużycia lub niewłaściwego użytkowania zasobów. Realizacja postawionego celu możliwa jest dzięki ustanowionym praktykom i podziałowi odpowiedzialności związanemu z weryfikacją kandydatów do pracy podczas naboru, zasadom zatrudniania pracowników oraz ustalonej procedurze rozwiązywania umów o pracę.

16. Bezpieczeństwo fizyczne, sprzętu i infrastruktury technicznej

W Urzędzie określono następujące kierunkowe standardy:

- standard bezpieczeństwa fizycznego;
- standard bezpieczeństwa sprzętu i okablowania;
- standard konfiguracji i eksploatacji sieci.

Z uwagi na to, że standardy zawierają informacje, których ujawnienie nieuprawnionym stronom trzecim mogłoby w istotnym stopniu obniżyć poziom bezpieczeństwa informacji, są udostępnione tylko pracownikom Urzędu wykonującym zadania określone w standardach.

Przedmiot poszczególnych standardów:

- 1) standard bezpieczeństwa fizycznego: parametr bezpieczeństwa fizycznego, kontrola fizycznych wejść, zabezpieczenie biur, pokoi i urzędzeń, ochrona przed zagrożeniami zewnętrznymi i środowiskowymi, praca w obszarach zabezpieczonych, obszary ogólnie dostępne, obszary dostaw i załadunku;
- 2) standard bezpieczeństwa sprzętu i okablowania: rozmieszczenie i ochrona sprzętu, urządzenia wspomagające, bezpieczeństwo okablowania, utrzymanie sprzętu, bezpieczeństwo sprzętu znajdującego się poza terenem organizacji, bezpieczne usuwanie sprzętu, wynoszenie majątku;

Opracował:

Pełnomocnik ds.
Zintegrowanego Systemu Zarządzania
Krzysztof Krakowski

Zatwierdził:

Prezydent Miasta Płocka
Andrzej Nowakowski

Kategoria informacji: informacja jawna

3) standard konfiguracji i eksploatacji sieci: środki kontroli przeciwko kodowi złośliwemu i mobilnemu, środki kontroli sieci, bezpieczeństwo usług sieciowych, polityki i procedury dotyczące wymiany informacji, przesyłanie wiadomości drogą elektroniczną, korzystanie z usług sieciowych, identyfikacja sprzętu w sieciach, ochrona portu służącego do zdalnego diagnozowania i konfiguracji, segregacja w sieciach, kontrola połączeń sieci, routing, nadzorowanie słabości technicznych.

17. Zarządzanie ciągłością działania

Urząd dba o zapewnienie ciągłości funkcjonowania usług związanych z przetwarzaniem danych. Celem takiego postępowania jest przeciwdziałanie przerwom w działalności oraz ochrona krytycznych procesów przed rozległymi awariami lub katastrofami. Realizacja postawionego celu możliwa jest dzięki ustanowionym praktykom i podziałowi odpowiedzialności związanemu z zarządzaniem ciągłością działania tak, aby ograniczyć do akceptowalnego poziomu skutki wypadków i awarii. Zasady reagowania na zdarzenia mogące prowadzić do zaburzenia procesów przetwarzania informacji są przedmiotem „Strategii ciągłości działania w Urzędzie Miasta Płocka” oraz instrukcji i planów awaryjnych. Plany awaryjne podlegają systematycznemu testowaniu.

18. Zarządzanie zmianami

Urząd, mając na uwadze konieczność szybkiego dostosowywania się do wymagań stron zainteresowanych, ciągle zmiany przepisów prawnych oraz dążenie do wzrostu efektywności i wydajności pracy, zapewnia metody postępowania dla skutecznej i terminowej obsługi zmian w infrastrukturze teleinformatycznej przy utrzymaniu pożądanego poziomu bezpieczeństwa przetwarzanych danych i ograniczeniu ryzyka negatywnego wpływu zmiany na obsługę teleinformatyczną organizacji.

Proces zarządzania zmianą w Urzędzie Miasta Płocka przebiega w następujących etapach:

- 1) ustalenie celu zmiany;
- 2) rozważenie wielkości i ważności zmiany dla organizacji;
- 3) określenie momentów krytycznych we wdrożeniu zmiany;
- 4) zainicjowanie zmiany, przeprowadzenie testów, wdrożenie w systemie produkcyjnym;
- 5) aktywne włączenie pracowników Urzędu w proces zmiany;
- 6) monitorowanie i raportowanie kolejnych kroków wdrożenia zmiany.

Szczegółowy sposób postępowania zawarty jest w instrukcji ZSZ „Zarządzanie zmianami w Urzędzie Miasta Płocka”.

Opracował:

Pełnomocnik ds.
Zintegrowanego Systemu Zarządzania
Krzysztof Krakowski

Zatwierdził:

Prezydent Miasta Płocka
Andrzej Nowakowski

Kategoria informacji: informacja jawna

19. Polityka wymiany informacji między Urzędem a miejskimi jednostkami organizacyjnymi

Urząd oraz miejskie jednostki organizacyjne posiadają własne rozłączne zbiory danych, którymi administrują. Zbiory danych przechowywane są na rozdzielonych logicznie serwerach w serwerowniach Urzędu oraz miejskich jednostek organizacyjnych.

W celu zapewnienia bezpieczeństwa danych, pomiędzy zbiorami danych Urzędu i miejskich jednostek organizacyjnych nie występuje bezpośrednia wymiana danych. W komunikacji między Urzędem a miejskimi jednostkami organizacyjnymi, biorącymi udział w projekcie „Płocka Platforma Teleinformatyczna e-Urząd” pośredniczy Obszar Wymiany Danych, w szczególności pracownicy poszczególnych miejskich jednostek organizacyjnych i Urzędu nie mają bezpośredniego dostępu do baz danych innych jednostek. Dane przesyłane za pomocą Płockiej Platformy Teleinformatycznej e-Urząd przesyłane są siecią wewnętrzną.

Wszystkie zdarzenia wymiany danych pomiędzy bazami danych są rejestrowane w logach systemów wysyłających i odbierających.

20. Zgodność z wymaganiami prawnymi i regulacyjnymi

Urząd dba o zapewnienie zgodności postępowania z przepisami obowiązującego prawa, przyjętych uwarunkowań umownych i normatywnych oraz wypracowanych własnych standardów. Celem takiego postępowania jest unikanie naruszania jakichkolwiek przepisów prawnych, zobowiązań wynikających z ustaw, zarządzeń lub umów oraz wymagań bezpieczeństwa. Realizacja postawionego celu możliwa jest dzięki ustanowionym praktykom i podziałowi odpowiedzialności związanemu z identyfikacją wymagań prawnych w zakresie bezpieczeństwa informacji. Prowadzone są audyty wewnętrzne i zewnętrzne funkcjonowania systemu.

21. Deklaracja ochrony własności intelektualnej

W Urzędzie Miasta Płocka zostały wdrożone w ramach ZSZ mechanizmy zapobiegające naruszeniom przepisów prawa powszechnego związanych z ochroną własności intelektualnej. Przede wszystkim zabezpieczono stacje robocze przed możliwością instalacji oprogramowania z naruszeniem właściwej licencji. Sieć podlega ciągłemu monitorowaniu, a dostęp do stron oraz usług internetowych, co do których zachodzi podejrzenie naruszania własności intelektualnej lub ryzyko infekcji systemu złośliwym oprogramowaniem, może zostać zablokowany.

W ramach usług domeny wprowadzono filtrowanie plików użytkownika, blokując te z formatów, które nie będąc z założenia wynikającego z funkcjonalności przydatnymi w pracy zawodowej, mogłyby zarazem być nośnikami treści naruszających prawa autorskie i pokrewne. Prowadzona jest bieżąca ewidencja licencji oprogramowania, co zapewnia, że pracownicy upoważnieni do instalacji

Opracował:

Pełnomocnik ds.
Zintegrowanego Systemu Zarządzania
Krzysztof Krakowski

Zatwierdził:

Prezydent Miasta Płocka
Andrzej Nowakowski

ZINTEGROWANY SYSTEM ZARZĄDZANIA – DOKUMENT NADZOROWANY W WERSJI ELEKTRONICZNEJ**URZĄD MIASTA PŁOCKA****POLITYKA BEZPIECZEŃSTWA INFORMACJI W
URZĘDZIE MIASTA PŁOCKA**Wydanie 04
z dnia 21.02.2017
Strona: 14**Kategoria informacji: informacja jawna**

oprogramowania działają w granicach praw nabytych przez Gminę - Miasto Płock. Nadzorowana jest także własność intelektualna powierzona lub przekazana przez osoby trzecie, zarówno klientów, jak i kontrahentów.

22. Postanowienia końcowe

Najwyższe kierownictwo Urzędu zapoznaje pracowników Urzędu, stażystów i praktykantów z dokumentem Polityki Bezpieczeństwa Informacji oraz Instrukcją podstawowych zasad bezpieczeństwa dla pracowników Urzędu Miasta Płocka. Kierownik każdej komórki organizacyjnej Urzędu jest odpowiedzialny za zebranie od podległych pracowników oświadczeń o zapoznaniu się z instrukcją i przyjęciu jej do stosowania. Naruszenia świadome, bądź przypadkowe niniejszej Polityki Bezpieczeństwa Informacji (wraz z wszystkimi dokumentami operacyjnymi) powodują skutki prawne zgodnie z Regulaminem Pracy, a w przypadkach zastrzeżonych przez ustawodawcę – karne wynikające z odpowiedzialności określonej przez przepisy prawa.

Opracował:Pełnomocnik ds.
Zintegrowanego Systemu Zarządzania
Krzysztof Krakowski**Zatwierdził:**Prezydent Miasta Płocka
Andrzej Nowakowski