Załącznik do
Zarządzenia nr 5345/2024
Prezydenta Miasta Radomia
z dnia 22 marca 2024r.

Polityka Bezpieczeństwa Informacji w Urzędzie Miejskim w Radomiu

Polityka Bezpieczeństwa Informacji w Urzędzie Miejskim w Radomiu

Spis treści:

1. Postanowienia ogólne

Polityka Bezpieczeństwa Informacji (PBI) jest kluczowym dokumentem określającym zasady ochrony informacji w Urzędzie Miejskim w Radomiu. Jej celem jest określenie zasad bezpieczeństwa informacji na każdym etapie przetwarzania, stosując kompleksowe procedury mające na celu minimalizację ryzyka utraty, ujawnienia lub nieautoryzowanego dostępu do danych.

System Zarządzania Bezpieczeństwem Informacji (SZBI), to systematyczne podejście do ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymania i doskonalenia bezpieczeństwa informacji w organizacji. Strategia ta ma zapewnić ciągłe doskonalenie podjętych działań i procedur w celu optymalizacji ryzyk związanych w szczególności z naruszeniem poufności, integralność, dostępności informacji w organizacji.

Urząd Miejski w Radomiu w celu prawidłowego wykonywania ustawowych zadań związanych z przetwarzaniem i bezpieczeństwem informacji własnych i powierzonych przez inne instytucje czy obywateli oraz w celu utrzymania zgodności z obowiązującymi przepisami prawa ustanawia Politykę Bezpieczeństwa Informacji (PBI). Dąży do utrzymania najwyższych standardów bezpieczeństwa, obejmując zarówno informacje chronione jak i ogólnie dostępne.

Cele Polityki Bezpieczeństwa Informacji:

1) zapewnienie poufności, integralności i dostępności informacji poprzez stosowanie określonych mechanizmów;
2) zminimalizowanie ryzyka poprzez wdrożenie środków technicznych, organizacyjnych i proceduralnych, celem ograniczenia potencjalnych zagrożeń;
3) zapewnienie ciągłości działania w przypadku wystąpienia incydentów bezpieczeństwa, minimalizując wpływ na ciągłość działania Urzędu;
4) podnoszenie świadomości i edukacja pracowników poprzez szkolenia zwiększające kompetencje pracowników w zakresie bezpieczeństwa informacji.

Polityka Bezpieczeństwa Informacji jest nadrzędnym dokumentem w zakresie zarządzania bezpieczeństwem informacji w Urzędzie Miejskim w Radomiu. Jej postanowienia mają pierwszeństwo przed innymi dokumentami systemowymi

związanymi z bezpieczeństwem informacji, zapewniając spójność działań oraz skoordynowaną reakcję w przypadku wystąpienia incydentów.
Wdrażając te postanowienia, Urząd Miejski w Radomiu aktywnie angażuje się w ochronę informacji, umożliwiając jednocześnie efektywne i bezpieczne świadczenie usług dla mieszkańców oraz partnerów zewnętrznych.

Podstawy prawne

Polityka Bezpieczeństwa Informacji (PBI) w Urzędzie Miejskim w Radomiu opiera się na szeregu przepisów prawa, regulujących ochronę danych oraz bezpieczeństwo informacji. Wszystkie jej postanowienia oraz innych dokumentów dotyczących zarządzania bezpieczeństwem informacji są zgodne z obowiązującymi przepisami, spełniającymi wymagania prawne na szczeblu krajowym i unijnym, w szczególności:

1. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2024 r., poz.307);
2. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r., poz. 1781);
3. Ustawa z dnia 06 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2022 r. poz. 902);
4. Ustawa z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego (Dz. U. z 2023 r., poz. 1524);
5. Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z 2021 r., poz. 1797 z późn. zm.);
6. Ustawa z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz. U. z 2023 r., poz. 1440);
7. Ustawa z dnia 19 lipca 2019 r. o zapewnianiu dostępności osobom ze szczególnymi potrzebami (Dz. U. z 2022 r., poz. 2240);
8. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r., poz. 913 z późn. zm.)
9. Ustawa z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (Dz. U. z 2023r., poz.285 z późn. zm.);
10. Rozporządzenie 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. z 2017 r., poz. 2247);

11. Rozporządzenie 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 r., str.73);
12. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 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) (Dz. U. z UE.L.2018.119.1);
13. Norma PN-ISO/IEC 27001:2017-06.

Definicje:

1. Informacja - to zasób, który podobnie jak inne ważne aktywa biznesowe jest niezbędny dla działalności gospodarczej organizacji i w związku z tym wymaga odpowiedniej ochrony;
2. Bezpieczeństwo informacji - zachowanie poufności, integralności i dostępności Informacji; dodatkowo, mogą być brane pod uwagę inne własności, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność;
3. Aktyw/zasób - wszystko, co ma wartość dla Urzędu Miejskiego w Radomiu i z tego względu wymaga ochrony;
4. Poufność - właściwość zapewniającą, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom fizycznym;
5. Integralność - właściwość polegającą na tym, że zasób systemu teleinformatycznego nie został zmodyfikowany w sposób nieuprawniony;
6. Dostępność - właściwość określającą, że zasób systemu teleinformatycznego jest możliwy do wykorzystania na żądanie, w założonym czasie, przez podmiot uprawniony do pracy w systemie teleinformatycznym;
7. Rozliczalność - właściwość systemu pozwalającą przypisać określone działanie w systemie do osoby fizycznej lub procesu oraz umiejscowić je w czasie;
8. Ryzyko - prawdopodobieństwo wystąpienia zagrożenia oraz potencjalne konsekwencje związane z danym zdarzeniem;
9. Szacowanie ryzyka - całościowy proces identyfikowania ryzyka, analizy ryzyka i oceny ryzyka;

10. Postępowanie z ryzykiem - proces modyfikowania ryzyka;
11. Zarządzanie ryzykiem - systematyczne stosowanie zasad zarządzania, procedur i praktyk na rzecz działań w zakresie informowania, konsultowania, tworzenia kontekstu oraz identyfikowania, analizy, oceny, postępowania z ryzykiem, monitorowania i przeglądania ryzyka związanego z przetwarzaniem informacji;
12. Zdarzenie związane z bezpieczeństwem informacji - stwierdzone wystąpienie stanu systemu, usługi lub sieci, który wskazuje na możliwe naruszenie polityki bezpieczeństwa informacji lub błąd zabezpieczenia, lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem informacji;
13. Incydent bezpieczeństwa informacji - pojedyncze niepożądane lub niespodziewane zdarzenie związane z bezpieczeństwem informacji lub seria takich zdarzeń, które stwarzają znaczne prawdopodobieństwo zakłócenia działań i zagrażają bezpieczeństwu przetwarzanych informacji;
14. Dane osobowe - informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
15. Inspektor Ochrony Danych (IOD) - pracownik wyznaczony przez Prezydenta Miasta oraz podlegający bezpośrednio pod Prezydenta Miasta Radomia w rozumieniu art. 37 i 38 Rozporządzenia Parlamentu Europejskiego i Rady (EU) 2016/679 z dnia 27 kwietnia 2016r. zwanego dalej RODO.

2. Zakres, cele i dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji

System Zarządzania Bezpieczeństwem Informacji (SZBI) w Urzędzie Miejskim w Radomiu zbudowano zgodnie z najwyższymi standardami i oparto na normie PN-ISO/IEC 27001:2017-06. Implementacja SZBI jest kluczowym elementem zapewniającym spójność działań i skoordynowane podejście do zarządzania bezpieczeństwem informacji w całej organizacji.

SZBI obejmuje całą strukturę Urzędu Miejskiego w Radomiu, uwzględniając wszystkie komórki organizacyjne Urzędu, procesy, systemy związane z przetwarzaniem informacji. Podlega regularnym aktualizacjom w celu dostosowania do zmieniającego się otoczenia informacyjnego oraz nowych wyzwań z zakresu bezpieczeństwa.

SZBI ma zastosowanie w szczególności do:

1) wszelkich informacji przetwarzanych przez Urząd Miejski w Radomiu, obejmujących: dane osobowe, dane finansowe, dokumenty oficjalne, informacje o projektach i inne dane kluczowe dla funkcjonowania Urzędu;
2) wszystkich lokalizacji, w tym siedziby głównej, a także lokalizacji zewnętrznych, w których przetwarzane są informacje;
3) systemów informatycznych oraz tradycyjnych (papierowych) obsługujących zarządzanie dokumentacją, obszar finansów, obsługę stron zainteresowanych oraz inne kluczowe procesy;
4) wszystkich pracowników Urzędu, niezależnie od poziomu dostępu i stanowiska, a także osób trzecich mających dostęp do informacji;
5) systemów dostarczających usługi zewnętrzne, partnerów, instytucji współpracujących oraz innych podmiotów przetwarzających informacje w imieniu i na rzecz Urzędu.

Cele SZBI:

1) ochrona integralności informacji - ochrona przed możliwością zmodyfikowania informacji w sposób nieuprawniony;
2) zapewnienie poufności informacji - ochrona przed udostępnieniem lub wyjawieniem informacji osobom nieupoważnionym;
3) zapewnienie dostępności informacji - zapewnienie dostępu do informacji dla uprawnionego podmiotu, w określonym czasie;
4) zapewnienie rozliczalności informacji – zapewnienie możliwości przypisania określonego działania w procesie przetwarzania informacji osobie fizycznej lub systemowi informatycznemu oraz wskazać, w którym to nastąpiło;
5) zapewnienie autentyczności informacji - zapewnienie braku możliwości zmiany pochodzenia lub zawartość pozyskanych informacji;
6) zapewnienie niezaprzeczalności informacji – zapewnienie braku możliwości zanegowania swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie;
7) zarządzanie Ryzykiem - Identyfikacja, ocena i kontrola ryzyka związanych z przetwarzaniem informacji;
8) świadomość i Szkolenia - podniesienie świadomości pracowników w zakresie bezpieczeństwa informacji oraz zapewnienie szkolenia z tego zakresu.

Dokumentacja SZBI w Urzędzie Miejskim w Radomiu obejmuje:

1) Politykę Bezpieczeństwa Informacji - określa ogólne cele, zasady i zobowiązania związane z bezpieczeństwem informacji w Urzędzie;
2) Deklarację Stosowania - wyraża zobowiązanie Najwyższego Kierownictwa do wdrażania i utrzymania SZBI zgodnie z ustalonymi standardami;
3) Procedury i Instrukcje - określają szczegółowe zasady postępowania oraz procesy związane z bezpieczeństwem informacji;
4) Dokumentację zarządzania ryzykiem - zawiera analizę ryzyka oraz plany działań mające na celu jego minimalizację;
5) Dokumentację informacji chronionych ustawowo (dane osobowe, informacje niejawne, tajemnica skarbowa itp.)

3. Deklaracja Najwyższego Kierownictwa w zakresie bezpieczeństwa informacji w Urzędzie Miejskim w Radomiu

Prezydent Miasta Radomia wprowadza Politykę Bezpieczeństwa Informacji deklarując, że zbudowany System Zarządzania Bezpieczeństwem Informacji będzie podlegał ciągłemu doskonaleniu zgodnie z wymaganiami, które należy oprzeć na podejściu do zarządzania bezpieczeństwem informacji. Prezydent Miasta Radomia deklaruje dostarczenie niezbędnych środków i wsparcia oraz zobowiązuje wszystkich pracowników Urzędu do bezwzględnego przestrzegania ustanowionych zasad ochrony informacji. Celem jest wytyczenie jednolitego kierunku działań, zmierzającego do realizacji i utrzymania SZBI w Urzędzie, poprzez osiągnięcie właściwego poziomu organizacyjnego i technicznego.

4. Organizacja bezpieczeństwa informacji w Urzędzie Miejskim w Radomiu

Zgodnie z założeniami Polityki Bezpieczeństwa Informacji, każdy pracownik Urzędu Miejskiego w Radomiu ponosi indywidualną odpowiedzialność za ochronę informacji.

Każdy pracownik Urzędu zobowiązany jest do systematycznego zapoznawania się z zasadami bezpieczeństwa oraz ochroną informacji, zgodnie z wytycznymi i procedurami określonymi w Polityce Bezpieczeństwa Informacji.

Kierownicy komórek organizacyjnych odpowiadają nie tylko za ochronę informacji w ich obszarze, ale także za monitorowanie poufności, integralności i dostępności danych. Ich rola

obejmuje zarządzanie zasobem przetwarzanych informacji, nadzór nad przestrzeganiem zasad bezpieczeństwa oraz podejmowanie działań prewencyjnych. W przypadku incydentu bezpieczeństwa, kierownicy są zobowiązani do szybkiego i skoordynowanego reagowania, stosując procedury określone w Polityce Bezpieczeństwa Informacji.

Prezydent Miasta Radomia, wyznaczył Inspektora Ochrony Danych (IOD), którego głównym zadaniem jest monitorowanie i kontrola zgodności działań Urzędu Miejskiego w Radomiu z prawem ochrony danych osobowych, udzielanie informacji i porad dotyczących przetwarzania danych osobowych oraz współpraca z organem nadzorczym ds. ochrony danych osobowych.

5. Zasady współpracy ze stronami zainteresowanymi

W Urzędzie Miejskim w Radomiu zdefiniowano zasady współpracy ze stronami zainteresowanymi, kładąc nacisk na ochronę informacji i bezpieczeństwo interesantów oraz podmiotów wykonujących prace zlecone. Istnieje standard bezpieczeństwa fizycznego dla obszarów dostępnych dla interesantów i kontrahentów, eliminujący ryzyko dostępu osób niepowołanych.

W procesie zawierania umów, stosowane są klauzule o różnym stopniu poufności, gwarantujące ochronę informacji. Bezpieczeństwo informacji przed dostępem osób trzecich jest zapewniane przez wyodrębnienie obszarów niedostępnych dla osób nieuprawnionych. Komórki przetwarzające dane osobowe wyposażone są w bariery fizyczne, które uniemożliwiają dostęp do danych chronionych osobom nieuprawnionym.

6. Polityka kontroli dostępu do informacji

W ramach zobowiązań wynikających z prawa oraz normy PN-ISO/IEC 27001:2017-06, polityka kontroli dostępu do informacji w Urzędzie Miejskim w Radomiu stanowi kluczowy element zapewniający bezpieczeństwo informacji. Specyfika kontroli dostępu obejmuje:

1) określenie i fizyczne wydzielenie obszarów dostępu do różnych rodzajów danych zgodnie z ich klasyfikacją;
2) systematyczna kontrola i aktualizacja uprawnień użytkowników, dostosowująca je do ich aktualnych obowiązków;
3) implementacja środków bezpieczeństwa, takich jak firewall, antywirusy i szyfrowanie, w celu zabezpieczenia teleinformatycznych systemów przetwarzania informacji;

4) ustanowienie procedur nadzoru i kontroli dostępu dla podmiotów trzecich, które przetwarzają informacje w imieniu Urzędu;
5) systematyczne informowanie pracowników o zmianach w regulacjach dotyczących kontroli dostępu do informacji oraz przeprowadzanie odpowiednich szkoleń;
6) przeprowadzanie regularnych audytów wewnętrznych w celu oceny skuteczności i zgodności z założeniami Polityki Bezpieczeństwa Informacji.

Stosowanie polityki kontroli dostępu do informacji stanowi fundament dla zapewnienia poufności, integralności i dostępności informacji w Urzędzie Miejskim w Radomiu, zabezpieczając jednocześnie przed nieautoryzowanym dostępem oraz zagrożeniami związanymi z przetwarzaniem danych.

7. Klasyfikacja informacji

W ramach Polityki Bezpieczeństwa Informacji w Urzędzie Miejskim w Radomiu, wprowadzono system klasyfikacji informacji, mający na celu skategoryzowanie różnych rodzajów danych, stanowiących kluczowy zasób organizacji. Celem klasyfikacji jest uporządkowanie postępowania z informacjami, zwłaszcza tymi, których ujawnienie mogłoby narazić Urząd Miejski w Radomiu na szkodę.

Klasyfikacja oparta jest na grupach informacji, gdzie dokumenty o podobnych wymaganiach związanych z bezpieczeństwem zostały logicznie ze sobą powiązane. Wskaźniki poufności, integralności oraz dostępności stanowią fundament określania poziomu bezpieczeństwa dla każdej grupy informacji, co jest istotne w kontekście funkcjonowania Urzędu Miejskiego.

Zdefiniowano cztery poziomy dla każdego wskaźnika bezpieczeństwa, umożliwiając powiązanie grupy informacji z określonym poziomem wskaźnika.

Klasyfikacja obejmuje cztery poziomy informacji:

a) IPD - Informacja publicznie dostępna,

b) IWD - Informacja wewnętrzna - dostępna dla wszystkich pracowników urzędu,

c) IWZ - Informacja wewnętrzna zastrzeżona - dostępna dla uprawnionych pracowników urzędu,

d) IUC - Informacja ustawowo chroniona (np. informacje niejawne, dane osobowe, tajemnica skarbowa, itp.)

8. Zarządzanie aktywami i ryzykami

W ramach Polityki Bezpieczeństwa Informacji w Urzędzie Miejskim w Radomiu, zarządzanie aktywami informacyjnymi skupia się na utrzymaniu wymaganego poziomu bezpieczeństwa dla identyfikowanych aktywów umożliwiając skuteczne zarządzanie nimi. Proces polega na bieżącej identyfikacji aktywów zgodnie z przyjętą klasyfikacją.

Proces zarządzania aktywami obejmuje regularne przeprowadzanie analizy ryzyka, identyfikując potencjalne zagrożenia oraz opracowane plany postępowania z ryzykiem. Wyniki analizy stanowią podstawę dla działań doskonalących ochronę zasobów Urzędu Miejskiego.

W przypadku zagrożeń niosących większe ryzyko niż akceptowalne, wymagane jest stworzenie szczegółowych planów postępowania. W sytuacjach awaryjnych plany postępowania powinny określać konieczne do podjęcia kroki oraz strategie zarządzania ryzykiem w celu wyeliminowania go lub sprowadzenia do akceptowalnego poziomu.

Przeglądy prowadzone przez kadrę kierowniczą oraz analizę ryzyka zaleca się przeprowadzać regularnie. Powinny one obejmować okresowe oceny skuteczności i adekwatności środków bezpieczeństwa. Ponadto, przeglądy te powinny być realizowane po każdej istotnej zmianie, która mogłaby wpłynąć na bezpieczeństwo informacji.

9. Bezpieczeństwo zasobów ludzkich

Zapewnienie bezpieczeństwa zasobów ludzkich w ramach Polityki Bezpieczeństwa Informacji w Urzędzie Miejskim w Radomiu opiera się na posiadaniu kompetentnej kadry pracowniczej do wykonywania powierzonych zadań. Cel ten realizowany jest poprzez zastosowanie skutecznych praktyk rekrutacyjnych, weryfikację kandydatów oraz określone zasady zatrudniania pracowników.

Proces Rekrutacji i Weryfikacji Kandydatów - W celu zapewnienia bezpieczeństwa zasobów ludzkich, Urząd Miejski w Radomiu stosuje określone praktyki rekrutacyjne. Proces rekrutacji obejmuje weryfikację kwalifikacji i doświadczenia zgodnie z obowiązującym

regulaminem dotyczącym naboru na wolne stanowiska urzędnicze, wolne kierownicze stanowiska urzędnicze w Urzędzie Miejskim w Radomiu oraz wolne stanowiska kierowników jednostek podległych Prezydentowi Miasta Radomia.

Zasady Zatrudniania Pracowników - Podjęcie decyzji o zatrudnieniu i podpisanie umowy o pracę odbywa się zgodnie z obowiązującym regulaminem dotyczącym naboru na wolne stanowiska urzędnicze, wolne kierownicze stanowiska urzędnicze w Urzędzie Miejskim w Radomiu oraz wolne stanowiska kierowników jednostek podległych Prezydentowi Miasta Radomia.

Minimalizacja Ryzyka Błędów Ludzkich i Nadużyć - Polityka Bezpieczeństwa Informacji ma na celu minimalizację ryzyka związanego z błędami ludzkimi, kradzieżą, nadużyciem lub niewłaściwym użytkowaniem zasobów. W ramach tego celu, systematyczne szkolenia pracowników oraz regularne przeglądy procedur służą podniesieniu świadomości i skuteczności personelu w obszarze bezpieczeństwa informacji. Ważnym elementem jest również zdobywanie lub uzupełnianie wiedzy i umiejętności przez pracowników zgodnie z obowiązującym regulaminem określającym zasady i warunki podnoszenia kwalifikacji zawodowych pracowników samorządowych zatrudnionych w Urzędzie Miejskim w Radomiu.

10. Zarządzanie ciągłością działania

W ramach Polityki Bezpieczeństwa Informacji w Urzędzie Miejskim w Radomiu, zarządzanie ciągłością działania polega na nieprzerwanej dostępności usług związanych z przetwarzaniem danych. Celem jest przeciwdziałanie przerwom w funkcjonowaniu oraz ochrona kluczowych procesów przed awariami lub katastrofami.

Ustanowione praktyki i odpowiedzialności związane z zarządzaniem ciągłością działania obejmują ograniczanie skutków wypadków do akceptowalnego poziomu. Opisują je zasady reagowania na zakłócenia procesów przetwarzania informacji wraz z instrukcjami i planami awaryjnymi.

Regularne testowanie planów awaryjnych stanowi kluczowy element systematycznego utrzymania gotowości do reakcji na ewentualne incydenty, zapewniając ciągłość funkcjonowania usług i ochronę kluczowych procesów w Urzędzie Miejskim w Radomiu.

11. Polityka wymiany informacji między Urzędem, a miejskimi jednostkami organizacyjnymi

Wymiana informacji z miejskimi jednostkami organizacyjnymi odbywa się w formie papierowej i elektronicznej. Wymiana w wersji papierowej odbywa się zgodnie z wymaganiami prawnymi w tym regulacjami wewnętrznymi zapewniając wymagany poziom bezpieczeństwa informacji.

Wymiana informacji elektronicznych z miejskimi jednostkami organizacyjnymi opiera się wyłącznie przy wykorzystaniu wymaganych zabezpieczeń logicznych chroniących przed nieuprawnionym dostępem, w szczególności takich jak ochrona kryptograficzna. Bezpieczeństwo danych jest skutecznie utrzymane poprzez stosowanie mechanizmu silnego szyfrowania połączenia VPN w procesie komunikacji do zasobów informacyjnych Urzędu. Wszelkie zdarzenia związane z wymianą danych są systematycznie rejestrowane w logach uczestniczących w tym procesie systemów, co zapewnia pełną kontrolę i umożliwia monitorowanie bezpieczeństwa informacji.

12. Postanowienia końcowe

Najwyższe kierownictwo Urzędu Miejskiego w Radomiu zobowiązuje wszystkich pracowników do ścisłego przestrzegania Polityki Bezpieczeństwa Informacji oraz pozostałych dokumentów SZBI. Kierownicy komórek organizacyjnych pełnią kluczową rolę w tym procesie, odpowiadając za zbieranie oświadczeń od pracowników, potwierdzających ich zapoznanie się i akceptację zasad bezpieczeństwa.
Naruszenia Polityki Bezpieczeństwa Informacji, niezależnie od ich charakteru wiążą się z konsekwencjami prawno-regulaminowymi, zgodnie z obowiązującym Regulaminem Pracy oraz innymi aktami prawnymi. Naruszenia te mogą prowadzić do odpowiedzialności karnej, określonej przez przepisy prawa.

Urząd Miejski w Radomiu aktywnie dba o zgodność działania z obowiązującymi przepisami prawa, warunkami umownymi i normatywnymi oraz własnymi standardami. Działania te mają na celu zapobieganie naruszeń przepisów prawa poprzez identyfikację wymagań prawnych w zakresie bezpieczeństwa informacji. W celu monitorowania i oceny funkcjonowania systemu zgodności prowadzone są audyty wewnętrzne i zewnętrzne.