ZARZĄDZENIE NR 95
BURMISTRZA MIASTA RAWA MAZOWIECKA

z dnia 1 listopada 2021 r.

w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji w Urzędzie Miasta Rawa Mazowiecka

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2021 r. poz.1372) oraz § 20 ust. 1 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 roku 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) zarządza się, co następuje:

§ 1. Wprowadza się do stosowania Politykę Bezpieczeństwa Informacji w Urzędzie Miasta Rawa Mazowiecka w brzmieniu stanowiacym załącznik do zarządzenia.

§ 2. Wykonanie zarządzenia powierza się Sekretarzowi Miasta Rawa Mazowiecka.

§ 3. Zarządzenie wchodzi w życie z dniem podpisania.

Załącznik do zarządzenia Nr 95

Burmistrza Miasta Rawa Mazowiecka

z dnia 1 listopada 2021 r.

z dnia 1 listopada 2021 roku
w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji w Urzędzie Miasta Rawa Mazowiecka

POLITYKA BEZPIECZEŃSTWA INFORMACJI W URZĘDZIE MIASTA RAWA MAZOWIECKA

HISTORIA DOKUMENTU

Wersja i data utworzenia	Podmiot wprowadzający zmiany	Opis zmian	Data zatwierdzenia / data wejścia w życie	Osoba zatwierdzająca
1.0 11.2021 r.	Miasto Rawa Mazowiecka	Pierwsza wersja dokumentu	11.2021	Burmistrz Miasta

Spis treści

Wstęp

O skuteczności działania i rozwoju każdej organizacji świadczy stopień osiągania 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 Rawa Mazowiecka, dlatego powinna być chroniona na każdym szczeblu organizacji. Urząd Miasta Rawa Mazowiecka 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 Rawa Mazowiecka stanowi zestawienie zasad, praw i reguł oraz doświadczeń i dobrych praktyk w zakresie zarządzania i ochrony danych i informacji w naszej jednostce.

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.

Terminologia

Ilekroć w Polityce Bezpieczeństwa Informacji jest mowa o:

„Polityce” - należy przez to rozumieć Politykę Bezpieczeństwa Informacji w Urzędzie Miasta Rawa Mazowiecka;

„Mieście” – należy przez to rozumieć Gminę - Miasto Rawa Mazowiecka;

„Burmistrzu” – należy przez to rozumieć Burmistrza Miasta Rawa Mazowiecka;

„Urzędzie” - należy przez to rozumieć Urząd Miasta Rawa Mazowiecka;

„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 Rawa Mazowiecka;

„Użytkowniku” - należy przez to rozumieć osobę korzystającą z zasobów teleinformatycznych Urzędu.

Podstawy prawne

Polityka Bezpieczeństwa Informacji oraz pozostałe dokumenty 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;
2) ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych;
3) ustawie z dnia 06 września 2001 r. o dostępie do informacji publicznej;
4) ustawie z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej;
5) ustawie z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych;
6) ustawie z dnia 19 lipca 2019 r. o zapewnianiu dostępności osobom ze szczególnymi potrzebami;
7) 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;
8) 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);

9) rozporządzeniu 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. UE. L.2018.119.1);
10) normie PN-ISO/IEC 27001:2017-06.

Nazwy

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 i zagrażają bezpieczeństwu informacji.
13) Dane osobowe – wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"). Osoba fizyczna możliwa do zidentyfikowania 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.
14) Administrator – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania.
15) Inspektor Ochrony Danych (IOD) – wyznaczony przez Administratora pracownik Urzędu, do zadań którego należy zapewnienie przestrzegania przepisów o ochronie danych osobowych

Zakres Systemu Bezpieczeństwa Informacji

SZBI w Urzędzie stanowi część 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/IEC27001:2017-06. 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 Rawa Mazowiecka, 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 Rawa Mazowiecka;
3) informacji będących własnością klientów Urzędu Miasta Rawa Mazowiecka, uzyskanych na podstawie zawartych umów;
4) wszystkich lokalizacji Urzędu Miasta Rawa Mazowiecka, 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.

Deklaracja Najwyższego Kierownictwa w zakresie bezpieczeństwa informacji w Urzędzie Miasta Rawa Mazowiecka

Burmistrz Miasta Rawa Mazowiecka, stojąc na stanowisku, że informacja jest newralgicznym zasobem Urzędu, wdrożył w ramach systemu zarządzania w Urzędzie Miasta Rawa Mazowiecka system zarządzania bezpieczeństwem informacji i zobowiązuje się do podejmowania wszelkich działań prowadzących do kompleksowego zabezpieczenia informacji oraz zapewnienia środków niezbędnych do realizacji niniejszej polityki.

Organizacja bezpieczeństwa informacji w Urzędzie Miasta Rawa Mazowiecka

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 SZBI w Urzędzie Miasta Rawa Mazowiecka. Zarządzeniem nr 4310/2018 z dnia 20 czerwca 2018 r. Burmistrz Miasta Rawa Mazowiecka wyznaczył Inspektora Ochrony Danych. Każdy pracownik Urzędu jest zapoznawany z zasadami bezpieczeństwa oraz z aktualnymi procedurami ochrony informacji w swojej komórce organizacyjnej oraz w Urzędzie Miasta Rawa Mazowiecka zawartymi w takich dokumentach jak: „SZBI-PBT – Instrukcja Zarządzania Zasobami Informatycznymi (Polityka Bezpieczeństwa Teleinformatycznego)”, „SZBI-PBT-Zał. 0 - Regulamin

korzystania z zasobów informatycznych”, „Polityka ochrony danych osobowych”. Stażyści oraz praktykanci również są zapoznawani z tymi zasadami. Kierownicy komórek Urzędu są odpowiedzialni 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.

Dokumentacja systemu zarządzania bezpieczeństwem informacji

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

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

Uzupełnieniem dokumentacji SZBI jest pozostała dokumentacja w tym Polityka ochrony danych osobowych wraz z Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Zasady współpracy ze stronami zainteresowanymi

W Urzędzie Miasta Rawa Mazowiecka wdrożono standard bezpieczeństwa fizycznego w odniesieniu do klientów i podmiotów wykonujących prace zlecone na terenie Urzędu. Wprowadzono dokument pod nazwą „SZBI-PBI-Zał. 2 Współpraca z podmiotami zewnętrznymi” regulujący zasady współpracy w zakresie wymagań dla umów przygotowywanych w Urzędzie Miasta Rawa Mazowiecka określający 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 Rawa Mazowiecka. 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. 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 Rawa Mazowiecka. Ciągi komunikacyjne pozostają pod stałą obserwacją.

Polityka kontroli dostępu do informacji

1. 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 27001:2017-06.

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 jakiejkolwiek przyczyny;
3) stosowaniu bezpiecznych systemów przetwarzania informacji;
4) nadzorowaniu działalności innych podmiotów, 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 audytów wewnętrznych, zmian dokumentacji i metod postępowania wynikających z ewolucji uregulowań prawnych oraz systemów przetwarzania danych a także reagowania na zagrożenia ujawnione przez inne strony.

2. Procedura wydania zgody na przebywanie w obszarze przetwarzania danych osobowych
    - W przypadku osób, które są zatrudnione w organizacji zgodnie z kodeksem pracy, ale z racji zajmowanego stanowiska pracy nie mogą przetwarzać danych osobowych, co nie zmienia faktu, że istnieje uzasadniona konieczność by przebywały w obszarach przetwarzania danych osobowych, Administrator wydaje ,,Upoważnienie do przebywania w obszarze przetwarzania danych" stanowiącą dokument nr: ,,SZBI-PBl-Zał. 16" tj. załącznik nr 16 do Polityki Bezpieczeństwa lnformacji.
    - Procedura zgody na przebywanie w obszarze przetwarzania zawiera zobowiązanie osoby, której dotyczy do zachowania w poufności wszelkiego rodzaju powziętych informacji o osobach, których dane osobowe organizacja przetwarza.
    - Administrator zaznacza, iż względem każdej osoby zatrudnionej w organizacji, która narusza zasady bezpieczeństwa informacji, również względem osoby, która nie jest upoważniona do przetwarzania danych osobowych, a tylko uzyskała od Administratora zgodę na przebywanie w obszarze przetwarzania danych osobowych, może być prowadzone postępowanie dyscyplinarne w trybie art. 52 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy.
    - Administrator prowadzi ewidencję osób, względem których wydano zgodę na przebywanie w obszarze przetwarzania zawierającą imię i nazwisko, stanowisko oraz datę wydania zgody. ,,Ewidencja osób upoważnionych do przebywania w obszarze przetwarzania danych" stanowi dokument nr: ,,SZBI-PBl-Zał. 17." tj. załącznik nr 17 do Polityki Bezpieczeństwa Informacji.

Klasyfikacja informacji

Klasyfikacja została wprowadzona w celu uporządkowania w Urzędzie postępowania z różnymi rodzajami informacji, które są głównym zasobem naszego urzędu. W szczególny 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 identyfikujące poufność, integralność oraz dostępność danej grupy informacji, wymaganej 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.
Struktura klasyfikacji informacji w Urzędzie Miasta Rawa Mazowiecka opiera się na założeniu istnienia czterech kategorii informacji:

- stanowiące dane osobowe, oznaczone jako „dane osobowe”
- informacje ogólnodostępne - publikowane
- informacje wewnętrzne urzędu w tym informacje stanowiące tajemnice urzędu
- informacje prawnie chronione – tajemnice określone w odrębnych przepisach

Zarządzanie aktywami i ryzykiem.

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.

Autoryzacja nowych urządzeń

Przed zakupem 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 ASI. Urządzenia służące do przetwarzania informacji nie będące własnością Urzędu mogą być używane (po sprawdzeniu sprzętu pod względem kryteriów bezpieczeństwa) wyłącznie za zgodą Administratora, IOD, ASI.

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) zasadom konserwacji urządzeń w celu zapewnienia ich ciągłej pracy;
3) kontrolowaniu wprowadzania wszelkich zmian do infrastruktury technicznej,
4) nadzorowaniu usług dostarczanych przez inne podmioty, w szczególności odbieraniu ich i akceptowaniu w sposób świadomy uwzględniający jego wpływ na istniejący system bezpieczeństwa;
5) wdrożeniu zabezpieczeń chroniących przed oprogramowaniem złośliwym;
6) systematycznemu tworzeniu i testowaniu kopii bezpieczeństwa;
7) przestrzeganiu opracowanych zasad postępowania z nośnikami;
8) bieżącemu monitorowaniu aktywów informacyjnych - urząd monitoruje możliwość wystąpienia incydentów bezpieczeństwa i posiada mechanizmy reagowania w przypadkach ich wystąpienia. Szczegółowy sposób postępowania zawiera właściwa instrukcja SZBI.

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. Pracownicy są zobowiązani stale podnosić swoje kwalifikacje oraz przestrzegać niniejszych zasad.

Bezpieczeństwo fizyczne, sprzętu i infrastruktury technicznej

W urzędzie określono następujące kierunkowe standardy:

- standard bezpieczeństwa fizycznego określone w dokumencie („SZBI-PBI-Zał.12 Polityka Bezpieczeństwa Fizycznego")
- standard bezpieczeństwa sprzętu i okablowania (określany i realizowany przez IT)
- standard konfiguracji i eksploatacji sieci (określany i realizowany przez IT)

Z uwagi na to, że standardy zawierają informacje, których ujawnienie nieuprawnionym podmiotom 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 urządzeń, 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 urzędu, bezpieczne usuwanie sprzętu, wynoszenie majątku;
3) standard konfiguracji i eksploatacji sieci: środki kontroli przeciwko kodowi złośliwemu, 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.

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 zarządzeniem 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 ciągłości działania w Urzędzie Miasta Rawa Mazowiecka.

Zarządzanie zmianami

Urząd, mając na uwadze konieczność szybkiego dostosowywania się do wymagań stron zainteresowanych, ciągłe 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 urzędu. Proces zarządzania zmianą w Urzędzie Miasta Rawa Mazowiecka 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 „SZBI-PBI-Zał. 10 - Zarządzanie zmianą”.

Polityka wymiany informacji między Urzędem a miejskimi jednostkami organizacyjnymi

Urząd oraz miejskie jednostki organizacyjne posiadają własne rozłączne zasoby informacyjne, którymi administrują. Zasady wymiany informacji miedzy Urzędem a innymi podmiotami opisuje dokument „SZBI-PBI-Zał. 6 Wymiana informacji z podmiotami zewnętrznymi”.

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.

Deklaracja ochrony własności intelektualnej

W Urzędzie Miasta Rawa Mazowiecka zostały wdrożone w ramach SZBI 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. Prowadzona jest bieżąca ewidencja licencji oprogramowania, co zapewnia, że pracownicy upoważnieni do instalacji oprogramowania działają w granicach praw nabytych przez Gminę Miasto Rawa Mazowiecka. Nadzorowana jest także własność intelektualna powierzona lub przekazana przez inne podmioty.

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 Rawa Mazowiecka. 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 wszystkim i dokumentami operacyjnymi) powodują skutki prawne zgodnie z Regulaminem Pracy, a w przypadkach zastrzeżonych przez ustawodawcę – karne wynikające z odpowiedzialności określonej przez przepisy prawa.

WAŻNE

Przedstawione poniżej dokumenty wewnętrzne nie stanowią katalogu zamkniętego dokumentacji składającej się na Politykę Bezpieczeństwa Informacji. Każda dodatkowa, nowa procedura, instrukcja czy wytyczna Administratora dotycząca obszaru ochrony bezpieczeństwa informacji stanowi integralną część niniejszej Polityki, a ich dodanie nie wymaga jej zmiany.

Załączniki:

1. SZBI-PBI-Zał. 0 - Deklaracja stosowania UM Rawa Mazowiecka
2. SZBI-PBI-Zał. 1 - Polityka BEZPIECZEŃSTWA INFORMACJI
3. SZBI-PBI-Zał. 2 Współpraca z podmiotami zewnętrznymi
4. SZBI-PBI-Zał. 3 - Obiegowa Karta Uprawnień
5. SZBI-PBI-Zał. 4 - Zarządzanie ciągłością działania
6. SZBI-PBI-Zał. 5 - PAW-SZAC - Procedura Analiza Ryzyka Ogólnego i DPIA
7. SZBI-PBI-Zał. 6 Wymiana informacji z podmiotami zewnętrznymi
8. SZBI-PBI-Zał. 7 Ewidencja obszarów przetwarzania
9. SZBI-PBI-Zał. 8 - Deklaracja stosowania podmiotu przetwarzającego
10. SZBI-PBI-Zał. 9 Formularz zgłoszenia naruszenia bezpieczeństwa informacji
11. SZBI-PBI-Zał. 10 - Zarządzanie zmianą
12. SZBI-PBI-Zał.11 Klasyfikacja incydentów i zdarzeń
13. SZBI-PBI-Zał.12 Polityka Bezpieczeństwa Fizycznego
14. SZBI-PBI-Zał.13 Informacje sklasyfikowane
15. SZBI-PBI-Zał.14 Klauzula Poufności
16. SZBI-PBI-Zał.15 Ewidencja Klauzul Poufności
17. SZBI-PBI-Zał.16 Upoważnienie do przebywania w obszarach przetwarzania