Polityka
Bezpieczeństwa Informacji
Urzędu Miasta Myszków

Opracowali:

Sławomir Matyja – Sekretarz Miasta

Rafał Kupczak – Kierownik Referatu Informatyki

Jacek Orłowski – IDO

Zatwierdził

Burmistrz Miasta – Włodzimierz Żak

Spis treści

Terminy i definicje

Administrator Danych Osobowych (ADO) – Burmistrz Miasta Myszkowa, który decyduje o środkach i celach przetwarzania danych osobowych

Administrator Systemu Informatycznego (ASI) – osoba powołana przez ADO, nadzorująca pracę systemu informatycznego oraz wykonująca w nim czynności wymagające specjalnych uprawnień

Aktywa (zasoby) – wszystko, co ma wartość dla Urzędu Miasta Myszków

Aktywa informatyczne – oprogramowanie, dane, sprzęt, dokumentacja, zasoby administracyjne fizyczne, komunikacyjne lub ludzkie, związane z działalnością informatyczną

Analiza ryzyka – proces dążący do poznania charakteru ryzyka oraz określenia poziomu ryzyka

Audyt bezpieczeństwa – niezależny przegląd i sprawdzenie zapisów oraz funkcji systemu przetwarzania danych w celu sprawdzenia prawidłowości kontroli systemowej, zapewnienia zgodności z przyjętą polityką bezpieczeństwa i procedurami działania w celu wykrycia przełamania bezpieczeństwa oraz zalecenia określonych zmian w kontroli, polityce bezpieczeństwa i procedurach

BI (Bezpieczeństwo Informacji) – zachowanie poufności, integralności i dostępności informacji oraz inne własności, tj. autentyczność, rozliczalność, niezaprzeczalność, niezawodność

BIP – Biuletyn Informacji Publicznej

Ciągłość działania – utrzymanie niezbędnych usług systemu informatycznego po poważnej awarii w centrum informatycznym, która może być spowodowana przyczynami naturalnymi, takimi jak np. pożar, trzęsienie ziemi, lub zdarzeniami wywołanymi umyślnie, np. sabotaż

Cyberprzestrzeń – przestrzeń przetwarzania i wymiany informacji, tworzona przez systemy teleinformatyczne, określone w art.3 pkt 3 ustawy, [1] wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami

Dostępność – właściwość bycia dostępnym i możliwym do wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot

ePUAP – system teleinformatyczny, w którym instytucje publiczne udostępniają usługi przez pojedynczy punkt dostępowy w sieci Internet [2]

Funkcjonalność – zdolność do zapewnienia realizacji funkcji zaspakajających wyznaczone i zakładane potrzeby, podczas używania w określonych warunkach

Gestor zasobu – pełni nadzór nad zasobem i decyduje we wszystkich sprawach merytorycznych dotyczących tego zasobu, zgodnie z Regulaminem organizacyjnym Urzędu Miasta Myszkowa

Incydent naruszenia BI (incydent bezpieczeństwa) – pojedyńcze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń, związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań statutowych organizacji i zagrażają bezpieczeństwu informacji, wymagające podjęcia działania i rozwiązania powstałego problemu w celu utrzymania akceptowanego poziomu ryzyka

1 Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.

2 Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 6 maja 2014 r. w sprawie zakresu i warunków korzystania z elektronicznej platformy usług administracji publicznej.

Inspektor Ochrony Danych (IOD) – osoba, która realizuje zadania określone w art.39 RODO [3]

Integralność – właściwość polegająca na tym, że system realizuje swoją zamierzoną funkcję w nienaruszalny sposób, wolny od nieautoryzowanej manipulacji, celowej lub przypadkowej

Interoperacyjność – zdolność różnych podmiotów oraz używanych przez nie systemów teleinformatycznych i rejestrów publicznych do współdziałania na rzecz osiągnięcia wzajemnie korzystnych i uzgodnionych celów, z uwzględnieniem współdzielenia informacji i wiedzy przez wspierane przez nie procesy biznesowe, realizowane za pomocą wymiany danych za pośrednictwem wykorzystywanych przez te podmioty systemów teleinformatycznych. Osiąganie interoperacyjności następuje poprzez ciągłe doskonalenie w zakresie współdziałania systemów teleinformatycznych

IT – technologia informacyjna, stanowi połączenie zastosowań informatyki i telekomunikacji, obejmuje również sprzęt komputerowy oraz oprogramowanie, a także narzędzia i inne technologie związane ze zbieraniem, przetwarzaniem, przesyłaniem, przechowywaniem, zabezpieczaniem i prezentowaniem informacji

Kontrola dostępu – środki mające na celu zapewnienie, że dostęp do aktywów jest autoryzowany i ograniczony w oparciu o wymagania biznesowe i wymagania bezpieczeństwa

KRI (Krajowe Ramy Interoperacyjności) – stanowią zbiór zasad i sposobów postępowania podmiotów w celu zapewnienia systemom informatycznym interoperacyjności działania, rozumianej jako zdolność tych systemów oraz wspieranych przez nie procesów do wymiany danych oraz do dzielenia się informacjami i wiedzą [4]

Materiały zawierające informacje – wszelkie nośniki, na których we właściwy sposób utrwalono informacje, w szczególności: dokumenty papierowe, dokumenty elektroniczne, katalogi, pliki sieci komputerowej, wydawnictwa książkowe, mapy, sieciowe systemy informatyczne, wszelkie inne nośniki informacji np. płyty CD-ROM, pendrive, zapisy dźwięku lub obrazu, itp.

Niezawodność – właściwość polegająca na zapewnieniu zdolności do wykonywania wymaganych funkcji w określonych warunkach przez określony czas lub dla określonej liczby operacji

Pełnomocnik ds. bezpieczeństwa cyberprzestrzeni - pracownik UM Myszków, który realizuje zadania określone w rozdziale 5 - obowiązki podmiotów publicznych, ustawy [5]

Pełnomocnik ds. ochrony informacji niejawnych (POIN) – osoba powołana do nadzorowania ochrony informacji niejawnych [6]

Plan ciągłości działania (BCP) – plan wznawiania działania w obszarze kluczowych procesów, w przypadku wystąpienia katastrofy. Dotyczy zdarzeń o niskim prawdopodobieństwie wystąpienia, ale o katastrofalnych skutkach, np. pożar, powódź, katastrofa budowlana, skażenie chemiczne, sabotaż, terroryzm itp., których czasu wystąpienia nie można przewidzieć

Podatność – słabość aktywów, która może być wykorzystana przez zagrożenia

---

3 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 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) – RODO /Dz.Urz. UE L 119 z 04.05.2016, str.1 z późn.zm./

4 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.

5 Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa

6 Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych.

Podmiot publiczny – podmiot, realizujący zadania publiczne, określone w odrębnych ustawach, wskazany w art.2 ust.1 ustawy o informatyzacji

Polityka Bezpieczeństwa Informacji (PBI) – zestaw praw, reguł i praktycznych doświadczeń, regulujących sposób zarządzania, ochrony i dystrybucji informacji wewnątrz określonej organizacji

Poufność – właściwość zapewniająca, że informacja jest udostępniana lub ujawniana tylko osobom lub procesom do tego upoważnionym

Przetwarzanie informacji – wszelkie czynności związane z informacją, takie jak jej: zbieranie, utrwalanie przechowywanie, wytwarzanie, opracowywanie, zmienianie, udostępnianie, kopiowanie, usuwanie (przetwarzanie informacji może występować w systemach obiegu papierowego lub elektronicznego)

Rozliczalność – właściwość systemu, pozwalająca przypisać określone działanie w systemie do osoby fizycznej lub procesu oraz umiejscowić je w czasie

Ryzyko – prawdopodobieństwo, że określone zagrożenie wykorzysta podatność, zasobu lub grupy zasobów, aby spowodować straty lub zniszczenie zasobów

SEKAP – System Elektronicznej Komunikacji Administracji Publicznej, strategiczny dla rozwoju regionu, innowacyjny projekt samorządów gmin i powiatów Województwa Śląskiego

System teleinformatyczny – zespół współpracujących z sobą według określonych reguł urządzeń, oprogramowania, procedur przetwarzania informacji i narzędzi programowych, zastosowanych w celu przetwarzania danych

System zarządzania – system do ustanawiania polityki i celów oraz osiągania tych celów

System zarządzania bezpieczeństwem informacji (SZBI) – część całościowego systemu zarządzania, oparta na podejściu wynikającym z ryzyka biznesowego, odnosząca się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji

Szacowanie ryzyka – szacowanie zagrożeń, ich wpływu, podatności informacji i urządzeń do przetwarzania informacji oraz prawdopodobieństwa ich wystąpienia

Środki komunikacji elektronicznej – rozwiązania techniczne, w tym urządzenia teleinformatyczne współpracujące z nimi narzędzia programowe, umożliwiające porozumiewanie się na odległość przy wykorzystaniu transmisji danych między systemami teleinformatycznymi, a w szczególności pocztę elektroniczną

Usługa elektroniczna – usługa świadczona bez jednoczesnej obecności stron (na odległość), poprzez przekaz danych na indywidualne żądanie usługobiorcy, przesyłanej i otrzymywanej za pomocą urządzeń do elektronicznego przetwarzania i przechowywania danych (na podstawie art.2 pkt 4 ustawy) [7]

Zagrożenie BI – potencjalna przyczyna zdarzenia, incydentu naruszenia BI, którego skutkiem może być szkoda (strata) dla systemu lub organizacji.

7 Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną.

1. Wstęp

Informacja jest jednym z najwartościowszych zasobów każdej organizacji, niezależnie od sposobu jej wykorzystania. Wymagania z zakresu bezpieczeństwa informacji wynikać mogą z:

- z wymagań prawnych (np. ustawa o ochronie danych osobowych, ustawa o ochronie informacji niejawnych, ustawa o dostępie do informacji publicznej, ustawa o rachunkowości)
- z wymagań kontraktowych (klient, dostawca, pracownik)
- z celów statutowych lub biznesowych
- wewnętrznych zasad i procesów
- z analizy ryzyk, odnoszących się do aktywów informacyjnych.

Informacje, podobnie jak inne ważne aktywa, są niezbędne do funkcjonowania każdej organizacji i z tego powodu zaleca się ich odpowiednią ochronę.

Realizacja statutowych zadań każdej organizacji wymaga m.in. efektywnego dostępu do informacji oraz zapewnienia odpowiedniego poziomu bezpieczeństwa informacji. Utrata poufności, integralności i dostępności informacji może mieć negatywny wpływ na bieżącą działalność lub wizerunek organizacji.

Bezpieczeństwo informacji oznacza jej ochronę przed szerokim spektrum zagrożeń w celu zachowania poufności, integralności i dostępności informacji, a także minimalizacji ryzyka oraz zapewnienia ciągłości działania organizacji i realizacji jej zadań statutowych na odpowiednim poziomie.

Bezpieczeństwo informacji można osiągnąć, wdrażając odpowiedni zestaw zabezpieczeń, którymi mogą być polityki, procesy, procedury, zabezpieczenia fizyczne, struktury organizacyjne ora funkcje oprogramowania i sprzętu.

PBI jest zbiorem zasad i procedur, którymi muszą podporządkować się osoby, posiadające dostęp do zasobów informacyjnych. Określa również zasady ochrony infrastruktury, zasobów informatycznych i ludzkich.

2. Cel PBI

Celem PBI jest:

1) zdefiniowanie ogólnych wymagań i zasad ochrony informacji, które będą podstawą dla wszystkich dokumentów związanych z bezpieczeństwem informacji w Urzędzie;
2) zapewnienie bezpieczeństwa i właściwej ochrony zasobów informacyjnych Urzędu poprzez uzyskanie właściwego i zgodnego z wymogami prawa, sposobu przetwarzania informacji, przez pracowników Urzędu oraz osoby będące stronami umów cywilno-prawnych;
3) ochrona aktywów informacyjnych i wzmacnianie pozycji Urzędu oraz jego postrzegania przez petentów (mieszkańców) jako organizacji godnej zaufania;
4) określenie odpowiedzialności za bezpieczeństwo informacji;
5) minimalizowanie ryzyka w obszarze bezpieczeństwa informacji;
6) zaangażowanie wszystkich pracowników Urzędu w ochronę informacji;
7) zapewnienie ciągłości pracy Urzędu i minimalizacja negatywnych skutków wynikających z naruszeń bezpieczeństwa informacji.

3. Deklaracja kierownictwa Urzędu

Kierownictwo Urzędu jest świadome istniejących zagrożeń i ryzyka związanego z przetwarzaniem informacji, tj. ich zbieraniem, utrwalaniem, przechowywaniem, opracowywaniem, zmienianiem, analizowaniem, raportowaniem, aktualizowaniem, udostępnianiem i usuwaniem.

Niniejsza deklaracja stanowi zobowiązanie do podejmowania niezbędnych działań, mających na celu zabezpieczenie informacji, jako aktywu podlegającego ochronie prawnej i niezbędnego do prawidłowego oraz sprawnego funkcjonowania Urzędu.

Niniejszy dokument wyraża również zaangażowanie Kierownictwa Urzędu w zakresie utrzymania odpowiedniego poziomu bezpieczeństwa informacji oraz określa podstawowe przyjęte w tym obszarze cele i strategie. Kierownictwo Urzędu aktywnie wspiera zapewnienie bezpieczeństwa informacji w całej organizacji wskazując kierunki działania, oraz przyjmując odpowiedzialność w zakresie bezpieczeństwa informacji.

4. Zakres obowiązywania PBI

1. PBI stanowi najwyższej rangi dokument dotyczący bezpieczeństwa informacji w Urzędzie, obejmuje swoim zakresem Urząd Miasta Myszkowa.
2. Dokument ma zastosowanie do wszystkich zasobów informacyjnych Urzędu, niezależnie od formy w jakiej są przechowywane (papierowej, elektronicznej i innej).
3. Dokument ten dotyczy wszystkich pracowników w rozumieniu w szczególności ustawy o służbie cywilnej oraz przepisów Kodeksu pracy, a także innych osób, mających dostęp do zasobów informacyjnych Urzędu, np. pracowników firm zewnętrznych, realizujących prace w Urzędzie.
4. Dokument dotyczy również wszystkich systemów informatycznych, zlokalizowanych w budynkach Urzędu.
5. PBI nie obejmuje swoim zakresem informacji niejawnych w rozumieniu ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych. [8]

5. Organizacja SZBI

Zgodnie z § 20 ust. 1 rozporządzenia 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, Urząd jest zobowiązany ustanowić, wdrożyć, eksploatować, monitorować, przeglądać, utrzymywać i doskonalić SZBI zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

Mając powyższe na uwadze, w Urzędzie Miasta Myszkowa wprowadzona zostaje do stosowania niniejsza PBI (zawierająca niezbędne elementy SZBI wg. kryteriów normy PN-ISO/IEC 27001) aby zapewnić adekwatne i proporcjonalne zabezpieczenia, które odpowiednio chronią aktywa informacyjne Urzędu oraz aby uzyskać zaufanie petentów (mieszkańców) i innych zainteresowanych podmiotów.

8 Obszar ochrony informacji niejawnych posiada własne regulacje prawne i stosowane mechanizmy ochronne, posiada także struktury organizacyjne dedykowane do ochrony informacji niejawnych wytwarzanych, przetwarzanych oraz przechowywanych w wydzielonych systemach teleinformatycznych.

Każdy pracownik Urzędu jest zapoznawany (za pisemnym potwierdzeniem) z regułami oraz z aktualnymi procedurami ochrony informacji, obowiązującymi w Urzędzie.

W Urzędzie za bezpieczeństwo informacji, a w szczególności za zorganizowanie i zapewnienie funkcjonowania PBI, odpowiada Burmistrz Miasta Myszkowa.

Sekretarz Miasta, IOD, ASI, Pełnomocnik ds. ochrony informacji niejawnych, Pełnomocnik ds. bezpieczeństwa cyberprzestrzeni oraz pracownik odpowiedzialny za bezpieczeństwo Urzędu Miasta, tworzą zespół ds. monitorowania zagrożeń i utrzymania:

- „Polityki Bezpieczeństwa Informacji"
- „Polityki ochrony danych osobowych"
- „Polityki zarządzania incydentami związanymi z bezpieczeństwem informacji".

IOD, ASI, Pełnomocnik ds. ochrony informacji niejawnych oraz Pełnomocnik ds. bezpieczeństwa cyberprzestrzeni, zobowiązani są do natychmiastowego podjęcia działań, określonych w odpowiednich procedurach w przypadku naruszenia zasad bezpieczeństwa informacji.

Audytor wewnętrzny odpowiada za coroczne przeprowadzenie audytu w zakresie bezpieczeństwa informacji, zgodnie z:

- § 20 ust.2 pkt 14 rozporządzenia 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
- rozporządzeniem Ministra Finansów z dnia 4 września 2015 r. w sprawie audytu wewnętrznego oraz informacji o pracy i wynikach tego audytu.

5.1. Procesy zarządzania bezpieczeństwem

SZBI wprowadzony w Urzędzie uwzględnia procesy utrzymania odpowiedniego poziomu bezpieczeństwa, w tym:

a) zarządzania ryzykiem;
b) monitorowania i przeglądu SZBI;
c) utrzymania i doskonalenia SZBI;
d) nadzoru nad dokumentacją;

e) zarządzania dostępem do zasobów;

f) zarządzania incydentami.

Zarządzeniem Nr 25/ON/2016 Burmistrza Miasta Myszkowa z dnia 2 lutego 2016 r. wprowadzono kartę audytu wewnętrznego w Urzędzie Miasta Myszkowa i jednostkach organizacyjnych.

W zarządzeniu NR 121/RI/2020 Burmistrza Miasta Myszkowa z dnia 18 czerwca 2020 r. w sprawie wprowadzenia Polityki ochrony danych osobowych Urzędu Miasta Myszkowa oraz instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta Myszkowa- wprowadzono:

- podstawowe zasady bezpieczeństwa informacji,
- podstawowe zasady bezpieczeństwa danych.

5.1.1 Zarządzanie ryzykiem

Utrzymanie bezpieczeństwa przetwarzanych przez Urząd Miasta Myszkowa informacji rozumie się jako zapewnienie ich poufności, integralności i dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka związanego z zasobem stanowiącym przedmiot niniejszej Polityki.

Audytor wewnętrzny, opracowując roczny plan audytu wewnętrznego w zakresie bezpieczeństwa informacji, przeprowadza analizę ryzyka, zgodnie z kartą audytu uwzględniającą sposób zarządzania ryzykiem w Urzędzie. Wynik analizy ryzyka, stanowi lista wszystkich zidentyfikowanych obszarów działalności Urzędu, uwzględniająca ich kolejność, wynikającą z oceny ryzyka.

5.1.2 Monitorowanie i przegląd SZBI

Dokumentacja PBI jest przeglądana i weryfikowana:

- na polecenie Burmistrza Miasta Myszkowa;
- w przypadku wystąpienia poważnych incydentów, związanych z bezpieczeństwem informacji;
- w celu realizacji zaleceń, wynikających z przeprowadzonych audytów i kontroli;

- w przypadku wejścia w życie nowych przepisów dot. bezpieczeństwa informacji;
- w przypadku poważnych modyfikacji infrastruktury teleinformatycznej;
- w przypadku zawarcia umów, z których wynikają zobowiązania związane z bezpieczeństwem informacji;
- okresowo, nie rzadziej niż raz w roku.

5.1.3 Utrzymanie i doskonalenie SZBI

Działanie (utrzymywanie) poszczególnych elementów SZBI w Urzędzie jest procesem ciągłym, stale doskonalonym i dostosowywanym do zmieniających się okoliczności, poprzez ich bieżące monitorowanie i regularny przegląd.

Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo Urzędu warunków, umożliwiających realizację i egzekwowanie następujących działań:

1) zapewnienia aktualizacji regulacji wewnętrznych (aktów normatywnych);
2) utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji;
3) przeprowadzania okresowych analiz ryzyka;
4) nadawania i zmiany uprawnień osobom zaangażowanym w proces przetwarzania informacji;
5) zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji;
6) zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami;
7) ustanowienia zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;
8) zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;
9) zawierania w umowach serwisowych, podpisanych ze stronami trzecimi, zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;
10) ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;
11) zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych;

12) bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób;
13) zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

W celu doskonalenia i utrzymania odpowiedniego poziomu bezpieczeństwa informacji ważne jest systematyczne szkolenie oraz podnoszenie kwalifikacji zawodowych wszystkich pracowników Urzędu.

5.1.4 Nadzór nad dokumentacją

Nadzór nad dokumentacją w Urzędzie określają:

1) **Rozporządzenie Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych**, określa dla organów Gminy:
    a) instrukcję kancelaryjną;
    b) sposób klasyfikowania i kwalifikowania dokumentacji w formie jednolitych rzeczowych wykazów akt;
    c) instrukcję w sprawie organizacji i zakresu działania archiwów zakładowych, zwaną „Instrukcją archiwalną".

Zadania w zakresie postępowania z dokumentacją i wykonywania czynności kancelaryjnych realizuje Burmistrz Miasta Myszkowa.

Instrukcja kancelaryjna, określa szczegółowe zasady i tryb wykonywania czynności kancelaryjnych w Urzędzie. Dokumentacja powstająca w Urzędzie i do niego napływająca jest klasyfikowana i kwalifikowana na podstawie jednolitego rzeczowego wykazu akt, zwanego „wykazem akt", przez oznaczenie rejestrację i łączenie dokumentacji w akta spraw albo jej grupowanie jako dokumentacji nie tworzącej akt spraw.

Instrukcja archiwalna, określa organizację, zadania i zakres działania archiwum zakładowego oraz szczegółowe zasady i tryb postępowania z dokumentacją w archiwum zakładowym.

2) **Regulamin organizacyjny Urzędu Miasta Myszkowa (zarządzenie NR 224/ON/2020 Burmistrza Miasta Myszkowa z dnia 9 listopada2020 r.)** określający m.in.:

a) zasady kierowania Urzędem;
b) strukturę organizacyjną Urzędu;
c) zasady i tryb pracy Urzędu;
d) zakres działania wydziałów;
e) tryb realizacji zadań wynikających z działalności Rady Miasta;
f) zasady postępowania przy załatwianiu spraw indywidulanych;
g) obieg dokumentów;
h) zasady podpisywania pism;
i) zasady opracowywania i wydawania aktów prawnych;
j) organizację działalności kontrolnej.

5.1.5 Zarządzanie dostępem do zasobów

Zasoby materialne takie jak służbowe narzędzia pracy oraz niematerialne w postaci informacji, mogą być wykorzystywane przez pracowników wyłącznie do realizacji celów statutowych Urzędu.

Zasoby materialne i niematerialne Urzędu przechowywane są w sposób zapobiegający ich utracie, uszkodzeniu, czy też kradzieży.

Dostęp do zasobów niematerialnych Urzędu regulują:

a) Konstytucja RP
b) ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (tryb wnioskowy)
c) rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 stycznia 2007 r. w sprawie Biuletynu Informacji Publicznej (tryb bezwnioskowy)
d) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 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) – RODO /Dz.Urz. UE L 119 z 04.05.2016, str.1 z późn.zm./ - (upoważnienie)
e) ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (upoważnienie, poświadczenie bezpieczeństwa, zaświadczenie)
f) ustawa z dnia 21 listopada 2008 r. o pracownikach samorządowych

g) ustawa z dnia 29 września 1994 r. o rachunkowości

h) Regulamin organizacyjny Urzędu Miasta Myszkowa (zarządzenie NR 224/ON/2020 Burmistrza Miasta Myszkowa z dnia 9 listopada 2020 r.).

5.1.6 Zarządzanie incydentem

Zarządzenie Nr 21/ON/2019 Burmistrza Miasta Myszkowa z dnia 14 lipca 2019 r. w sprawie powołania i określenia zadań pełnomocnika do spraw cyberbezpieczeństwa w Urzędzie Miasta Myszkowa.

Zarządzeniem NR 121/RI/2020 Burmistrza Miasta Myszkowa z dnia r. wprowadzono Instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych w Urzędzie Miasta Myszkowa.

5.2. Struktura dokumentacji SZBI

Dokumentacja SZBI ma strukturę hierarchiczną, gdzie PBI jest dokumentem nadrzędnym nad wszystkimi innymi dokumentami dot. bezpieczeństwa informacji.

Szczegółowe regulacje dot. bezpieczeństwa informacji, w tym kwestie korzystania z aktywów informacyjnych, a także użytkowania systemów informatycznych Urzędu, opracowuje się i doskonali poprzez tworzenie polityk szczegółowych, zasad, procedur, instrukcji, regulaminów i wydawanie innych aktów normatywnych.

Poszczególne rodzaje dokumentacji opisują obszar bezpieczeństwa informacji na różnych poziomach szczegółowości.

5.3. Odpowiedzialność za bezpieczeństwo informacji

Do przestrzegania zapisów PBI oraz innych regulacji dot. bezpieczeństwa informacji, zawartych w procedurach, instrukcjach i innych dokumentach Polityki, zobowiązani są zarówno Kierownictwo jak i wszyscy pracownicy Urzędu, a także stażyści, praktykanci i inne osoby, mające mieć dostęp do zasobów informacyjnych Urzędu, w tym pracownicy dostawców usług i oprogramowania, oraz jednostek zewnętrznych, itp.

W zawieranych przez Urząd Miasta Myszkowa umowach cywilno-prawnych należy stosować odpowiednie zapisy dot.:

- zachowania w tajemnicy danych osobowych (zawarcie odrębnej umowy o powierzeniu przetwarzania danych osobowych);
- zachowania poufności i ochrony informacji (zawarcie odrębnej umowy o zachowaniu poufności);
- odpowiedzialności za przekazane/udostępnione informacje;
- zasad dostępu do zasobów informatycznych oraz pomieszczeń Urzędu (upoważnienie, zapoznanie się z PBI Urzędu);
- zasad przekazywania i zwrotu informacji (postępowanie z nośnikami informacji w trakcie trwania umowy oraz po jej zakończeniu);
- dbałości o mienie Urzędu ;
- przeprowadzenia szkolenia (w uzasadnionych przypadkach) w zakresie PBI Urzędu;
- zobowiązania wykonawcy zewnętrznego, świadczącego usługi na rzecz Urzędu, do zgłaszania incydentów (do rejestru prowadzonego przez Urząd), stwierdzonych podczas wykorzystywania infrastruktury Urzędu.

Ponadto wszyscy pracownicy są zobowiązani do zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić Urząd na szkodę, a także przestrzegać tajemnicy określonej w odrębnych przepisach dot. np. danych osobowych, informacji niejawnych, tajemnic zawodowych.

Nieprzestrzeganie unormowań, o jakich mowa powyżej może stanowić naruszenie:

a) obowiązków pracowniczych i może być podstawą do zastosowania odpowiedzialności porządkowej, z odpowiedzialnością dyscyplinarną włącznie, czy też wypowiedzenia umowy o pracę lub rozwiązania umowy o pracę bez wypowiedzenia z winy pracownika,
b) postanowień umowy i może być podstawą do odpowiedzialności cywilnej i karnej.

Rola i odpowiedzialność za bezpieczeństwo informacji w Urzędzie wynika z indywidualnego zakresu obowiązków służbowych pracownika Urzędu i uprawnień ustawowych, określonych dla osób funkcyjnych, tj. ADO, IOD, ASI, Pełnomocnik ds. ochrony informacji niejawnych, Pełnomocnik ds. bezpieczeństwa cyberprzestrzeni.

Odpowiedzialność za bezpieczeństwo zasobów informatycznych Urzędu obejmuje nie tylko siedzibę Urzędu, ale także wszelkie sytuacje, w których informacje związane z działalnością Urzędu są przetwarzane poza jej siedzibą. Obejmuje to w szczególności zdalny dostęp do sieci komputerowej Urzędu.

Za całokształt obsługi informatycznej i utrzymania sieci komputerowej Urzędu, w tym inwentaryzację sprzętu i oprogramowania informatycznego (licencje na oprogramowanie) oraz zasobów teleinformatycznych (rejestr), odpowiada osoba zatrudniona na stanowisku Kierownika Referatu Informatyki Urzędu.

Nieprzestrzeganie zasad zawartych w dokumentach PBI jest naruszeniem obowiązków pracowniczych, wynikających w szczególności z ustawy o pracownikach samorządowych oraz Kodeksu pracy i może pociągnąć za sobą skutki dyscyplinarne oraz spowodować pociągnięcie do odpowiedzialności wynikającej z przepisów prawa.

Naruszenie zasad ochrony informacji może spowodować pociągnięcie do odpowiedzialności administracyjnej, cywilnej, karnej wynikającej z przepisów:

- ustawy o ochronie danych osobowych;
- rozporządzenia RODO;
- ustawy o ochronie informacji niejawnych;
- kodeku karnego (rozdział XXXIII. Przestępstwa przeciwko ochronie informacji);
- przepisów dot. innych tajemnic prawnie chronionych, w tym tajemnic zawodowych.

6. Zarządzanie aktywami (zasobami)

Urząd w swym działaniu wykorzystuje zasoby ludzkie, finansowe, informacyjne, materialne, które są przedmiotem zarządzania.

Urząd jest właścicielem wszystkich zasobów, związanych ze środkami przetwarzania informacji w poszczególnych komórkach organizacyjnych.

Informacje przetwarzane i przechowywane w systemie informatycznym Urzędu w jakiejkolwiek formie nie są objęte prawem do prywatności, jakie przewiduje Konstytucja RP, ze szczególnym uwzględnieniem zasobów gromadzonych na komputerach użytkowników oraz poczty elektronicznej.

Korzystanie z zasobów informacyjnych innych niż wytworzone w Urzędzie wymaga posiadania do nich przez Urząd praw autorskich, licencji, dowodów zakupu, aktów darowizny, itp. W szczególny sposób dotyczy to oprogramowania, baz danych petentów.

Za każdy z zasobów informacyjnych Urzędu odpowiada Gestor zasobu, stosownie do swoich kompetencji, wynikających z Regulaminu organizacyjnego Urzędu Miasta Myszkowa.

Zasoby informacyjne będące własnością Urzędu lub przez niego wykorzystywane podlegają rejestracji i przeglądowi.

Dostęp do określonych zasobów informatycznych jest przydzielany na podstawie udokumentowanych potrzeb użytkowników (pisemne upoważnienie).

Jednostki zewnętrzne mają dostęp do zasobów informacyjnych Urzędu na podstawie odrębnych przepisów, czy też upoważnień.

6.1. Autoryzacja nowych informatycznych środków przetwarzania informacji

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.

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

Zarządzeniem NR 121/RI/2020 Burmistrza Miasta Myszkowa 18 czerwca 2020 r. wprowadzono Regulamin korzystania z oprogramowania i sprzętu komputerowego w Urzędzie Miasta Myszkowa.

7. Zarządzanie aktywami informacyjnymi

Wszystkie zasoby informacyjne, będące własnością Urzędu lub przez Urząd wykorzystywane, podlegają klasyfikacji. Klasyfikacja zasobu informacyjnego określa jego znaczenie dla Urzędu, w szczególności odzwierciedla ewentualne zagrożenia, wynikające z naruszenia bezpieczeństwa zasobu informacyjnego. Klasyfikowanie zasobów ma na celu zapewnienie właściwego poziomu ich bezpieczeństwa.

Do podstawowych zadań związanych z zarządzaniem informacjami należą:

a) sterowanie przepływami informacji w sieci komunikacyjnej Urzędu;
b) eksploatacja systemów informatycznych i telekomunikacyjnych, wykorzystywanych w Urzędzie (utrzymywanie ich w stanie sprawności technicznej – niezawodności);
c) zarządzanie jakością informacji;
d) zapewnienie bezpieczeństwa informacyjnego Urzędu;
e) konserwacja strategicznych zasobów informacyjnych (utrzymywanie ich w gotowości do efektywnego wykorzystania przez użytkowników w pożądanej przez nich formie, miejscu i czasie);
f) rozwój systemu informacyjnego Urzędu (racjonalne planowanie środków inwestycyjnych na projektowanie i wdrażanie systemów);
g) tworzenie racjonalnych strategii informacyjnych Urzędu.

Dokumenty stanowiące zasoby informacyjne są oznaczane, przetwarzane, przechowywane oraz niszczone zgodnie z zapisami Instrukcji kancelaryjnej oraz rzeczowego wykazu akt.

7.1. Zasady zarządzania aktywami informacyjnymi w Urzędzie

Skuteczna ochrona zasobów informatycznych Urzędu wymaga wspólnego działania i zaangażowania wszystkich pracowników.

Pracownicy w szczególności zobowiązani są do przestrzegania podstawowych zasad bezpieczeństwa informacji, zasad bezpieczeństwa danych, czy też procedur, opisujących zasady korzystania z oprogramowania i sprzętu komputerowego.

Pracownicy Urzędu zobowiązani są do używania zasobów informacyjnych Urzędu wyłącznie do celów służbowych, chyba, że regulacje szczególne stanowią inaczej. W związku z tym wszyscy użytkownicy zasobów informacyjnych podlegają kontroli dostępu do nich.

Obowiązek ochrony zasobów Urzędu, w przypadku współpracy z kontrahentami i jednostkami zewnętrznymi, określany jest w ramach umów cywilno-prawnych, zawartych z tymi podmiotami (stosowanie zapisów o zachowaniu poufności, czy też odrębnej umowy o zachowaniu poufności).

7.2. Rodzaje informacji przetwarzanych w Urzędzie i sposób ich ochrony

Informacje występują w formie ustnej lub w formie aktywów.

O uznaniu informacji za informację niepodlegającą udostępnieniu – informacje prawnie chronione oraz każda informacja, której utrata, modyfikacja, zniszczenie, ujawnienie lub udostępnienie osobie/podmiotowi nieuprawnionemu mogłoby spowodować zauważalną szkodę materialną lub niematerialną dla Urzędu Miasta Myszkowa lub naruszyć prawnie chroniony interes innych osób/podmiotów – decyduje Administrator Danych lub upoważniona przez niego osoba.

Sposób ochrony informacji uzależniony jest od kategorii informacji – dane osobowe, tajemnice prawnie chronione, tajemnice Urzędu, informacje jawne – i wynika on z przepisów prawa oraz wydanych (obowiązujących) w Urzędzie wewnętrznych aktów normatywnych.

7.3. Zasady klasyfikacji informacji

Zasady klasyfikacji informacji wynikają z przepisów prawa.

Wszystkie informacje w Urzędzie dzielimy na:

a) **PUBLICZNE** – czyli takie, które nie wymagają dodatkowych zabezpieczeń przed dostępem osób nieupoważnionych, ich utrata nie spowoduje istotnych szkód i strat;

b) **WEWNĘTRZNE** – informacje są dostępne wszystkim pracownikom Urzędu, ale udostępnienie ich na zewnątrz wymaga zgody właściciela informacji;

c) **CHRONIONE** – są to informacje o istotnym znaczeniu dla funkcjonowania Urzędu, dostęp do nich mają tylko upoważnieni pracownicy.

Wszyscy pracownicy Urzędu obowiązani są do:

a) przeprowadzenia inwentaryzacji aktywów;

b) przeprowadzenia klasyfikacji informacji;

c) uaktualniania w trybie ciągłym inwentaryzacji aktywów i klasyfikacji informacji oraz utrzymywania ich ewidencji.

7.4. Zasady ochrony informacji klasyfikowanych

Zasady ochrony informacji klasyfikowanych wynikają z przepisów prawa, tj. w szczególności ustawa o ochronie danych osobowych, rozporządzenie RODO, ustawa o dostępie do informacji publicznej, ustawa o ochronie informacji niejawnych, ustawa o rachunkowości.

Urząd dobiera cele stosowania zabezpieczeń i poszczególne zabezpieczenia odpowiednio do wymagań prawnych i wyników analizy ryzyka, określenia poziomu zagrożeń dla bezpieczeństwa informacji.

Zabezpieczenia fizyczne, techniczne i organizacyjne powinny uzupełniać się wzajemnie zapewniając wspólnie wymagany poziom bezpieczeństwa informacji. W doborze celów stosowania zabezpieczeń należy kierować się zaleceniami polskich norm z rodziny ISO 27000.

7.5. Zasady postępowania z informacjami klasyfikowanymi

Zasady postępowania z informacjami klasyfikowanymi wynikają z przepisów prawa tj. w szczególności ustawa o ochronie danych osobowych, rozporządzenie RODO, ustawa o dostępie do informacji publicznej, ustawa o ochronie informacji niejawnych, ustawa o rachunkowości oraz wydanych (obowiązujących) w Urzędzie wewnętrznych aktów normatywnych.

Przy postępowaniu z informacją decyduje zasada nadrzędności przepisów prawa i umów nad regułami postępowania obowiązującymi w Urzędzie.

8. Bezpieczeństwo zasobów ludzkich

Zarządzeniem NR 2/ON/2013 Burmistrza Miasta Myszkowa z dnia 8 stycznia 2013 r. wprowadzono Regulamin naboru na wolne stanowiska urzędnicze, w tym kierownicze urzędnicze w Urzędzie Miasta Myszkowa oraz na stanowiska kierowników jednostek organizacyjnych Gminy Myszków.

8.1. Obsada stanowisk odpowiedzialnych za bezpieczeństwo informacji i systemów

Osoby funkcyjne, do których należą IOD, ASI, Pełnomocnik ds. ochrony informacji niejawnych, Pełnomocnik ds. bezpieczeństwa cyberprzestrzeni, posiadają wykształcenie oraz niezbędną wiedzę i umiejętności w zakresie bezpieczeństwa informacji i systemów, potwierdzone dyplomem, certyfikatem, zaświadczeniem, itp.

8.2. Szkolenia pracowników

Zarządzeniem NR 189/ON/2020 Burmistrza Miasta Myszkowa z dnia 28 września 2020 r. wprowadzono regulamin podnoszenia kwalifikacji zawodowych pracowników Urzędu Miasta Myszkowa.

8.3. Zarządzanie bezpieczeństwem zasobów ludzkich

Polityka kadrowa Urzędu wynika z bieżących potrzeb oraz głównie z przechodzenia pracowników na emeryturę.

9. Bezpieczeństwo fizyczne i środowiskowe

Zabezpieczenie budynku, pomieszczeń, urządzeń IT.

Na bezpieczeństwo fizyczne składa się system powiązanych ze sobą przedsięwzięć organizacyjnych, osobowych, technicznych i fizycznych służących ochronie.

Z uwagi na publiczny charakter działania Urzędu w czasie jego godzin pracy nie obowiązuje eskorta interesantów, czy też system przepustek, ani też inny sformalizowany system określający uprawnienia do wejścia, przebywania i wyjścia z budynku Urzędu Miasta.

Ochronę Urzędu realizuje się przy wykorzystaniu systemu zabezpieczeń technicznych, takich jak:

- budowlanych;
- mechanicznych;
- zabezpieczenia mienia i obiektu;
- zabezpieczenia życia (sprzęt gaśniczy);
- zabezpieczenia infrastruktury krytycznej (zarządzanie kryzysowe).

System ochrony Urzędu wspomaga się środkami technicznymi, takimi jak:

- systemy i urządzenia alarmowe oraz monitorujące;
- środki łączności (przewodowa, bezprzewodowa);
- oświetlenie obiektu;
- zabezpieczenia mechaniczne.

Budynek Urząd Miasta Myszkowa podlega dozorowi i ochronie, polegającej na całodobowym monitorowaniu poprzez system telewizji dozorowanej (monitoring wizyjny) .

Fizyczne zabezpieczenie wejścia do budynku, pomieszczeń, urządzeń IT – odbywa się poprzez zastosowanie zabezpieczeń fizycznych i proceduralnych, tj.:

- alarmy z kodami (budynek , pomieszczenie serwerowni, kancelaria materiałów niejawnych);
- zamki w drzwiach;
- zamykane na klucz szafy, szafki, itp.

W Urzędzie obowiązuje:

a) **zarządzenie nr 136/2020/ON Burmistrza Miasta Myszkowa z dnia 13 lipca 2020 r. w sprawie wprowadzenia Instrukcji postępowania z kluczami oraz zabezpieczenia pomieszczeń i obiektu Urzędu Miasta w Myszkowie –„ Polityka Kluczy”.**

b) **„Instrukcja bezpieczeństwa pożarowego opracowana dla budynku Urzędu Miasta Muszkowa z grudnia 2017 r.”**

Urządzenia podtrzymujące napięcie.

Sprzęt jest chroniony przed awariami zasilania i innymi zakłóceniami elektrycznymi poprzez:

- zapewnienie odpowiednich warunków atmosferycznych w pomieszczeniu, w którym znajduje się serwer poprzez zastosowanie klimatyzatora;
- urządzenie podtrzymujące zasilanie UPS, o ile jest to wskazane;
- listwy przeciwprzepięciowe przy każdym stanowisku komputerowym;
- urządzenie podtrzymujące UPS w serwerowni.

Bezpieczeństwo okablowania.

Kable zasilające i sieciowe są schowane, tak aby zabezpieczyć je przed uszkodzeniem. Są stosowane oznaczenia kabli, gniazdek oraz jest zachowana rozdzielność kabli sieciowych, zasilających i telekomunikacyjnych.

Zabezpieczenie sprzętu poza siedzibą Urzędu.

Obowiązuje zasada, że sprzęt i nośniki nie są wynoszone poza siedzibę Urzędu. W szczególnie uzasadnionych przypadkach, sprzęt IT może być użytkowany poza siedzibą Urzędu – wymagana jest pisemna zgody Burmistrza Miasta Myszkowa oraz uzgodnienie z informatykiem, który określi zasady postępowania w celu zapewnienia bezpieczeństwa informacji.

1) Osoba używająca komputer przenośny, zawierający dane osobowe, zobowiązana jest zachować szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych osobowych w Urzędzie.

2) Osoba używająca komputer przenośny, zawierający dane osobowe w szczególności powinna:
   a) stosować ochronę kryptograficzną wobec danych osobowych przetwarzanych na komputerze przenośnym;
   b) zabezpieczyć dostęp do komputera na poziomie systemu operacyjnego – identyfikator i hasło;
   c) nie zezwalać na używanie komputera osobom nieupoważnionym do dostępu do danych osobowych;
   d) nie wykorzystywać komputera przenośnego do przetwarzania danych osobowych w obszarach użyteczności publicznej;
   e) zachować szczególną ostrożność przy podłączaniu do sieci publicznych poza obszarem przetwarzania danych osobowych.

3) W przypadku podłączenia komputera przenośnego do sieci publicznej poza siecią Urzędu należy zastosować firewall, zainstalowany bezpośrednio na tym komputerze oraz system antywirusowy.

4) Użytkownik powinien zachować wyjątkową ostrożność podczas korzystania z zasobów sieci publicznej.

5) Za wszelkie działania wykonywane na komputerze przenośnym odpowiada jego faktyczny użytkownik.

Zarządzeniem NR 121/RI/2020 Burmistrza Miasta Myszkowa z dnia 18 czerwca 2020 r. w sprawie Polityki ochrony danych osobowych wprowadzono do stosowania podstawowe zasady bezpieczeństwa informacji oraz podstawowe zasady bezpieczeństwa danych osobowych w Urzędzie Miast Myszkowa.

10. Zarządzanie systemami i sieciami

Zarządzeniem nr 239/RI/2020 Burmistrza Miasta Myszkowa z dnia 07 grudnia 2020 r. wprowadzono Regulamin korzystania z oprogramowania i sprzętu komputerowego w Urzędzie Miasta Myszkowa.

Wydano zarządzenie nr 121/RI/2020 Burmistrza Miasta Myszkowa z dnia 18 czerwca 2020 r. w sprawie d

opuszczenia do pracy w Urzędzie Miasta Myszkowa systemów informatycznych służących do przetwarzania danych, przy użyciu komputera.

11. Kontrola dostępu

Wszyscy użytkownicy uzyskujący dostęp do zasobów sieci komputerowej Urzędu, jak również użytkownicy stanowisk nie podłączonych do sieci ale zainstalowanych na terenie Urzędu, odpowiedzialni są za przestrzeganie zasad opisanych w:

- **zarządzeniu nr 121/RI/2020 Burmistrza Miasta Myszkowa z dnia 18 czerwca 2020 r. w sprawie Polityki ochrony danych osobowych;**
- **zarządzeniu nr 239/RI/2020 Burmistrza Miasta Myszkowa z dnia 07 grudnia 2020 r. w sprawie wprowadzenia Regulamin korzystania z oprogramowania i sprzętu komputerowego w Urzędzie Miasta Myszkowa;**
- **zarządzeniu nr 121/RI/2020 Burmistrza Miasta Myszkowa z dnia 18 czerwca 2020 r. w sprawie dopuszczenia do pracy w Urzędzie Miasta Myszkowa systemów informatycznych służących do przetwarzania danych, przy użyciu komputera.**

ASI odpowiedzialny jest za zakładanie i usuwanie kont w systemie, przydzielanie i odbieranie dostępu do zasobów użytkownikom stanowisk, generowanie użytkownikom pierwszych haseł dostępowych, przechowywanie wniosków o uruchomienie stanowiska.

12. Pozyskiwanie, rozwój i utrzymanie systemów teleinformacyjnych

Pozyskiwanie i rozwój systemów teleinformatycznych wynika z bieżących potrzeb Urzędu, a utrzymanie funkcjonujących systemów teleinformatycznych z zapisów zawartych w obowiązujących umowach cywilno-prawnych, z dostawcami usług IT.

13. Zarządzanie incydentami związanymi z bezpieczeństwem informacji

Zarządzeniem nr 21/ON2019 Burmistrza Miasta Myszkowa z dnia 14.02.2019 r. wprowadzono Politykę zarządzania incydentami, związanymi z bezpieczeństwem informacji w Urzędzie Miasta Myszkowa.

Zarządzeniem nr 121/ON/2020 Burmistrza Miasta Myszkowa z dnia 18.06.2020 r. wprowadzono Instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych w Urzędzie Miasta Myszkowa.

14. Zarządzanie ciągłością działania

Funkcjonujący w Urzędzie sprzęt jest chroniony przed awariami zasilania i innymi zakłóceniami elektrycznymi poprzez:

- zapewnienie odpowiednich warunków atmosferycznych w pomieszczeniu, w którym znajduje się serwer poprzez zastosowanie klimatyzatora
- urządzenie podtrzymujące zasilanie UPS, o ile jest to wskazane
- listwy przeciwprzepięciowe przy każdym stanowisku komputerowym
- urządzenie podtrzymujące UPS w serwerowni.

ASI odpowiedzialny jest za tworzenie kopii zapasowych i ich przechowywanie (okresowe sprawdzanie jakości kopii zapasowych) oraz bieżącą współpracę z dostawcami usług IT, w tym nadzór nad wywiązywaniem się dostawcy usług ze zobowiązań zawartych w umowie.

15. Zgodność z przepisami prawa i dokumentami związanymi

Niniejsza Polityka stoi w zgodzie z przepisami prawa i dokumentami związanymi – obowiązującymi w Urzędzie Miasta Myszkowa.

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 funkcjonowania systemu bezpieczeństwa informacji.

16. Zasady rozpowszechniania dokumentu PBI oraz tryb wprowadzania zmian

Do zapoznania się z niniejszą Polityką i dokumentami związanymi, zobligowani są kierownictwo Urzędu oraz wszyscy pracownicy. Niniejszy dokument winien być udostępniony również

uprawnionym podmiotom zewnętrznym, w celu zapoznania się i postępowania w zgodzie z postanowieniami PBI Urzędu Miasta Myszkowa.

Komórka odpowiedzialna za sprawy kadrowe Urzędu, przekazuje do zapoznania się, nowo zatrudnionym pracownikom oraz stażystom i praktykantom, PBI Urzędu wraz z dokumentami związanymi. Nowo zatrudniony pracownik oraz stażysta, czy praktykant jest zobowiązany zapoznać się i złożyć pisemne oświadczenie, potwierdzające znajomość zasad, reguł i postanowień zawartych w w/wym. dokumentach.
Zmiany w dokumentach wprowadza Sekretarz Miasta w porozumieniu z IOD, ASI, Pełnomocnikiem ds. ochrony informacji niejawnych oraz Pełnomocnikiem ds. bezpieczeństwa cyberprzestrzeni na podstawie okresowych przeglądów, a zmieniony dokument zatwierdza Burmistrz Miasta Myszkowa i wprowadza w drodze zarządzenia.

17. Postanowienia uzupełniające

17.1. Odstępstwa od reguł ochrony

W szczególnie uzasadnionych przypadkach dopuszcza się stosowanie odstępstw od postanowień niniejszej Polityki i dokumentów z niej wynikających. Każde odstępstwo powinno zostać uzasadnione i udokumentowane.

Odstępstwa mogą być podyktowane ważnymi względami i powinny wynikać z konieczności realizacji istotnych celów Urzędu. Odstępstwa od wymagań, zawartych w niniejszej Polityce oraz w dokumentach powołanych nie mogą prowadzić do naruszalności zdefiniowanych celów bezpieczeństwa informacji.

Decyzję o odstępstwie podejmuje Administrator Danych lub osoba przez niego upoważniona.

17.2. Nadzór nad SZBI

Burmistrz Miasta Myszkowa lub osoba przez niego upoważniona sprawuje nadzór nad realizacją zadań, określonych w Polityce Bezpieczeństwa Informacji Urzędu Miasta Myszkowa.

18. Lista dokumentów związanych

Należą do nich następujące dokumenty:

1) Polityka ochrony danych osobowych;
2) Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych;
3) Polityka zarządzania incydentami związanymi z bezpieczeństwem informacji;
4) Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych w Urzędzie Miasta Myszkowa.
5) Instrukcja postępowania z kluczami oraz zabezpieczenia pomieszczeń i obiektu Urzędu Miasta Myszkowa;
6) Zarządzenie Burmistrza nr 280/2018/SM z dnia 3.10.2018 r. w sprawie monitoringu wizyjnego na terenie Urzędu Miasta Myszkowa;
7) Regulamin organizacyjny Urzędu Miasta Myszkowa;
8) Regulamin korzystania z oprogramowania i sprzętu komputerowego;
9) Zarządzenie w sprawie przyjęcia zasad bezpieczeństwa informacji
10) Zarządzenie w sprawie obowiązku przestrzegania zasad bezpieczeństwa informacji
11) Zarządzenie w sprawie przyjęcia zasad bezpieczeństwa danych
12) Zarządzenie w sprawie dopuszczenia do pracy w Urzędzie Miasta Myszkowa systemów informatycznych służących do przetwarzania danych, przy użyciu komputera;
13) Zarządzenie w sprawie zasady rejestrowania procedur kontroli zarządczej w Urzędzie Miasta Myszkowa;
14) Zarządzenie w sprawie zasady wydawania i rejestracji upoważnień w Urzędzie Miasta Myszkowa;
15) Kodeks etyki pracowników Urzędu Miasta Myszkowa;
16) Instrukcja postępowania w zakresie przeciwdziałania wprowadzeniu do obrotu finansowego wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł oraz przeciwdziałaniu finansowania terroryzmu;
17) Instrukcja postepowania na wypadek informacji o podłożeniu ładunku wybuchowego, otrzymania podejrzanej przesyłki lub innego miejscowego zagrożenia wprowadzona zarządzeniem Burmistrza Miasta Myszkowa NR 215/ON/2020 z dnia 30 października 2020 r. ;

19. Przepisy prawne i polskie normy

1. Informacje w Urzędzie podlegają ochronie, w szczególności zgodnie z następującymi aktami prawa:
    1) Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny;
    2) Ustawa z dnia 26 czerwca 1974 r. – Kodeks pracy;
    3) Ustawa z dnia 06 czerwca 1997 r. – Kodeks karny;
    4) Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych;
    5) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.;
    6) Ustawa z dnia 05 sierpnia 2010 r. o ochronie informacji niejawnych;
    7) Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia;
    8) Ustawa z dnia 29 września 1994 r. o rachunkowości;
    9) Ustawa z dnia 21 listopada 2008 r. o pracownikach samorządowych;
    10) Ustawa z dnia 06 września 2001 r. o dostępie do informacji publicznej;
    11) Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym;
    12) Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne;
    13) Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych;
    14) Ustawa z dnia 04 lutego 1994 r. o prawie autorskim i prawach pokrewnych;
    15) Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2001 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego;
    16) 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;
    17) Rozporządzenie Ministra Finansów z dnia 04 września 2015 r. w sprawie audytu wewnętrznego oraz informacji o pracy i wynikach tego audytu;
    18) Rozporządzenie Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych;
    19) Rozporządzenie Ministra Pracy i Polityki Socjalnej w z dnia 01 grudnia 1998 r. w sprawie bezpieczeństwa i higieny pracy na stanowiskach wyposażonych w monitory ekranowe;

2. Podstawą normalizacyjną SZBI i dokumentu PBI są, w szczególności, niżej wymienione polskie normy:

   1) PN-ISO/IEC 27000:2014 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Przegląd i terminologia;
   2) PN-ISO/IEC 27001 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania;
   3) PN-ISO/IEC 27002:2014 Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zabezpieczania informacji;
   4) PN-ISO/IEC 27005:2014 Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji;
   5) PN-ISO/IEC 17799:2007 Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zarządzania bezpieczeństwem informacji;
   6) PN-ISO/ICE 24762 Technika informatyczna – Techniki bezpieczeństwa – Wytyczne dla usług odtwarzania techniki teleinformatycznej po katastrofie.

ZAŁĄCZNIKI:

- wzór oświadczenia o zapoznaniu się z PBI Urzędu Miasta Myszkowa