ZARZĄDZENIE NR 628/2023
BURMISTRZA MIASTA I GMINY CHMIELNIK

z dnia 27 stycznia 2023 r.

w sprawie Polityki Bezpieczeństwa Informacji w Urzędzie Miasta i Gminy w Chmielniku

Na podstawie art. 33 ust. 3 i 5 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz. U. z 2023 r. poz. 40) zarządzam, co następuje:

§ 1. Wprowadza się Politykę Bezpieczeństwa Informacji w Urzędzie Miasta i Gminy w Chmielniku załącznika do zarządzenia.

§ 2. Zarządzenie wchodzi w życie z dniem wydania.

Burmistrz Miasta i Gminy
Chmielnik

Paweł Wójcik

Załącznik do zarządzenia Nr 628/2023
Burmistrza Miasta i Gminy Chmielnik
z dnia 27 stycznia 2023 r.

Polityka Bezpieczeństwa Informacji w Urzędzie Miasta i Gminy w Chmielniku

1. **Deklaracja stosowania**

Jednym z głównych celów Urzędu Miasta i Gminy w Chmielniku jest zapewnienie ochrony przetwarzanych danych z zachowaniem gwarancji należytego bezpieczeństwa i poufności powierzonych informacji.

W celu spełnienia powyższej deklaracji Burmistrz Miasta i Gminy Chmielnik przyjmuje następującą Politykę Bezpieczeństwa Informacji:

1) Jesteśmy świadomi ważności przetwarzanych w Urzędzie informacji i będziemy stwarzać odpowiednie warunki dla ich ochrony, w tym także poprzez zabezpieczenie odpowiednich zasobów finansowych i ludzkich.
2) Zobowiązujemy się do spełnienia wymogów prawnych, w szczególności w zakresie wymagań Ustawy o ochronie danych osobowych (UODO), Rozporządzenia 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)), ustawy o ochronie informacji niejawnych (UoOIN), Ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (UodoZP) oraz Rozporządzenia 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 (DODO)).
3) Działania Urzędu oparte są również o przepisy rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (RKRI) i Ustawę o krajowym systemie cyberbezpieczeństwa (UKSC).

Zakresem ochrony objęte są wszystkie informacje przetwarzane w Urzędzie, niezależnie od miejsca i sposobu ich przetwarzania.

4) Za bezpieczeństwo informacji w Urzędzie odpowiada każdy na swoim stanowisku pracy.
5) Na podstawie niniejszej Polityki sformułowano poszczególne cele realizowane w oparciu o odpowiednie polityki, procedury i inne zabezpieczenia.
6) Przyjęto metodę szacowania i oceny ryzyka oraz wyznaczono kryteria akceptacji ryzyka. W stosunku do zidentyfikowanych ryzyk wprowadzono stosowne zabezpieczenia.
7) Obowiązkiem pracowników Urzędu jest przestrzeganie zasad postępowania opisanych w niniejszej Polityce Bezpieczeństwa Informacji oraz wszystkich funkcjonujących w Urzędzie polityk i procedur związanych z bezpieczeństwem.
8) Wdrożony system zarządzania bezpieczeństwem informacji będzie doskonalony.

Niniejsza Polityka została ogłoszona w Urzędzie Miasta i Gminy w Chmielniku i jest dostępna dla wszystkich pracowników.
Burmistrz Miasta i Gminy Chmielnik deklaruje pełne zaangażowanie w realizację postanowień niniejszej Polityki.

2. **Definicje i wyrażenia**

Ilekroć w niniejszym dokumencie mowa o:

1) Burmistrzu – należy przez to rozumieć Burmistrza Miasta i Gminy Chmielnik .
2) Urzędzie - należy przez to rozumieć Urząd Miasta i Gminy w Chmielniku.

3) Straży – należy przez to rozumieć Straż Miejską w Chmielniku.

3) Komórce organizacyjnej – należy przez to rozumieć: Wydziały, Urząd Stanu Cywilnego, Straż Miejską, pracowników na samodzielnych stanowiskach.

4) Niniejszej Polityce –należy przez to rozumieć: Politykę Bezpieczeństwa Informacji.

5) Polityce Bezpieczeństwa Urzędu (PBPDU) – należy przez to rozumieć Politykę Bezpieczeństwa Przetwarzania Danych Osobowych Urzędu Miasta i Gminy w Chmielniku.

- *wprowadzonej jako załącznik nr 1 zarządzeniem nr 29/2019 Burmistrza Miasta i Gminy Chmielnik z dnia 22 stycznia 2019 r., zamiana zarządzenie nr 232/2020 z 3 czerwca 2020 r.*

6) Polityce Bezpieczeństwa Straży (PBDS)– należy przez to rozumieć Politykę Bezpieczeństwa danych osobowych w Straży Miejskiej w Chmielniku.

- *wprowadzonej załącznikiem do zarządzenia nr 190/2020 Burmistrza Miasta i Gminy Chmielnik z dnia 26 lutego 2020 r., przy kontrasygnacie Komendanta Straży Miejskiej w Chmielniku.*

7) Instrukcję Zarządzania (IZSI) – należy przez to rozumieć Instrukcję zarządzania system informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta i Gminy w Chmielniku.

- *wprowadzonej jako załącznik nr 2 zarządzeniem nr 29/2019 Burmistrza Miasta i Gminy Chmielnik z dnia 22 stycznia 2019 r., zamiana zarządzenie nr 232/2020 z 3 czerwca 2020 r.*

7) Administrator Danych Osobowych – Burmistrz Miasta i Gminy Chmielnik

8) Administrator Danych Osobowych w Straży Miejskiej – Komendant Straży Miejskiej w Chmielniku

9) IOD – Inspektor Ochrony Danych, osoba fizyczna powołana przez administratora danych w celu nadzoru nad prawidłowym, zgodnym z RODO przetwarzaniem danych osobowych.

10) ASI – Administrator Systemów Informatycznych.

11) Bezpieczeństwo informacji – zachowanie poufności, integralności i dostępności informacji.

3. **Analiza ryzyka**

Proces dążący do poznania charakteru ryzyka oraz określenia poziomu ryzyka.

3.1. Metoda szacowania ryzyka

Szacowanie ryzyka oparte zostało na klasyfikacji ważności informacji. Za informacje przetwarzane w Urzędzie uznano wszystkie informacje związane z działalnością Urzędu, które są tu przetwarzane, w tym przechowywane.

3.1.1. Klasyfikacja Aktywów Informacyjnych
Informacje przetwarzane w Urzędzie są dzielone na trzy podstawowe grupy ważności i podgrupy:

Ze względu na zarządzanie informacją:
1) informacje ważne ze względu na poufność:
- informacja jawna – informacja publicznie dostępna,
- informacja wewnętrzna – informacja, której przetwarzanie podlega dodatkowym obwarowaniom przez wzgląd na szczególne znaczenie dla pracy Urzędu,
- informacje dostępne – informacje dostępne dla wszystkich pracowników Urzędu,
- informacje poufne – informacje udostępniane jedynie grupie pracowników właściwych ze względu na realizowane zadania,
- informacje stanowiące tajemnicę służbową – informacje, których udostępnianie może narazić Urząd na szkody,
- informacje niejawne – informacje do których stosuje się przepisy ustawy o ochronie informacji niejawnych, ustawy o ochronie danych osobowych lub innych odrębnych aktów prawnych;

2) informacje ważne ze względu na integralność:

- informacje przetwarzane tradycyjnie,

- informacje przetwarzane elektronicznie;

3) informacje ważne ze względu na spójność:

- informacje samodzielne: w odniesieniu do realizowanego celu/zadania
- informacje powiązane:w odniesieniu do wielu celów i zadań realizowanych równolegle lub w konsekwencji.
  Informacja należąca do więcej niż jednej grupy przypisywana jest zawsze do najważniejszej z grup, do których należy. Przypisanie informacji do grupy wykonywane jest w następujący sposób:
- przeprowadzenie inwentaryzacji informacji,
- analiza strat, które mogą być efektem utraty integralności, poufności lub dostępności,
- przypisanie informacji do grupy z najwyższą stratą.

W niniejszym dokumencie Polityki wskazano jedynie stosowane metody oraz zidentyfikowano podstawowe czynniki brane pod uwagę. W niniejszej Polityce nie jest prowadzona szczegółowa analiza ryzyka wraz z niezbędnymi wyliczeniami i dokumentacją.

3.2. Lista aktywów informacyjnych

W Urzędzie prowadzi się zarówno w wersji elektronicznej jak i papierowej, rejestr czynności przetwarzania danych.

3.3. Obszar przetwarzania informacji

Obszar przetwarzania informacji w Urzędzie zlokalizowany jest w budynkach pod adresami:
- Plac Kościuszki 7, 26-020 Chmielnik,
- ul. Dygasińskiego 12, 26-020 Chmielnik (wyodrębniony Wydział: Straż Miejska w Chmielniku).

3.4. Ryzyka

W Urzędzie zostały zidentyfikowane podstawowe ryzyka występujące w kontekście procesu przetwarzania informacji wraz z oszacowaniem ich wielkości. Analiza ryzyka jest dokonywana corocznie.

4. Zbiory danych osobowych i systemy informatyczne używane do ich przetwarzania

Poniższy fragment dokumentu zawiera identyfikację zbiorów danych osobowych funkcjonujących w Urzędzie oraz systemów informatycznych, w tym programów, wykorzystywanych do ich przetwarzania.

Zawartość wymienionych poniżej Wykazów stanowi część Rejestru Czynności Przetwarzania i rejestrów Administratora Systemów Informatycznych.

Wykaz zbiorów danych osobowych i metod ich przetwarzania

Część wykazanych zbiorów przetwarzana jest w sposób rozproszony logicznie i podzielony strukturalnie i użytkowo.

Wykaz systemów informatycznych wykorzystywanych do przetwarzania informacji

Wykaz systemów informatycznych, w których przetwarza się informacje został uporządkowany z wymienieniem systemów i przypisaniem programów wchodzących w skład tych systemów. Ponadto wskazano jakie zbiory przetwarzane są jakimi systemami.

Opis przepływu danych

Niniejszy fragment dokumentów zawiera opis przepływów danych w zbiorach danych osobowych.
W pierwszej części opisane zostały przepływy danych w ramach każdego ze zbiorów, w drugiej zaś przepływy danych pomiędzy zbiorami.
Przepływ danych w ramach zbiorów
Wprowadzanie danych do systemów realizowane jest we wszystkich zbiorach, których dane są przetwarzane. Zbiory danych posiadają przepływy danych osobowych w formie elektronicznej wszędzie tam gdzie przepływy takie są możliwe technicznie.

Przepływ danych pomiędzy zbiorami

W Urzędzie występują przepływy danych między zbiorami z wykorzystaniem programów komputerowych jedynie w zakresie realizowanych przez Urząd zadań.

Opis struktur danych

Opis struktur danych stosowanych w poszczególnych programach wykorzystywanych do przetwarzania danych osobowych przez Urząd pochodzi od producentów oprogramowania. Urząd dopuszcza program do wykorzystania po otrzymaniu od producenta opisu struktur danych.

5. Organizacja bezpieczeństwa informacji

Niniejszy fragment dokumentu opisuje zasady organizacji bezpieczeństwa informacji, zarówno od strony wewnętrznej jak i zewnętrznej.

5.1. Organizacja wewnętrzna

5.1.1. Zaangażowanie kierownictwa w bezpieczeństwo informacji

Burmistrz odpowiada za całokształt bezpieczeństwa informacji Urzędu. W związku z powołaniem IOD oraz z przekazaniem zadań z zakresu obsługi informatycznej do Wydziału Administracji, Burmistrz podejmuje część działań związanych z bezpieczeństwem informacji organizacji, część zleca IOD, a część ASI.
Burmistrz:

1) zapewnia, by cele bezpieczeństwa informacji były włączane do wszystkich działań, które są z tym związane;
2) określa i zatwierdza obowiązującą w Urzędzie Niniejszą Politykę oraz poddaje ją okresowym przeglądom;
3) podejmuje działania mające na celu zapewnienie środków niezbędnych do realizacji zadań związanych z bezpieczeństwem informacji;
4) koordynuje wdrożenie zabezpieczeń w całej organizacji;
5) poddaje okresowym przeglądom skuteczność wdrożenia Polityki bezpieczeństwa;
6) przydziela i zatwierdza poszczególne role i zakresy odpowiedzialności związane z bezpieczeństwem informacji;
7) inicjuje plany i programy utrzymujące właściwą świadomość problematyki bezpieczeństwa informacji;
8) wspiera inicjatywy z zakresu bezpieczeństwa informacji.

5.1.2. Koordynacja bezpieczeństwa informacji

W Urzędzie dopuszcza się tworzenie zespołu koordynującego bezpieczeństwo informacji. Za całokształt działań koordynacyjnych odpowiada Burmistrz, a z jego ramienia Sekretarz.
Wszyscy pracownicy, a w szczególności kierownicy komórek organizacyjnych i pracownicy na samodzielnych stanowiskach są zobowiązani do współpracy przy koordynacji bezpieczeństwa informacji.
Wszyscy pracownicy na swoich stanowiskach pracy są zobowiązani do realizacji zadań zgodnie z obowiązującą Polityką Bezpieczeństwa Informacji. W przypadku zidentyfikowania działań niezgodnych z obowiązującymi politykami, pracownik jest zobowiązany zgłosić ten fakt swojemu bezpośredniemu przełożonemu lub Sekretarzowi, a w przypadku naruszeń dotyczących systemów informatycznych: do ASI, w przypadku danych osobowych do IOD.

W przypadku zidentyfikowania okoliczności znacząco zmieniających zagrożenia bądź wpływających na adekwatność zastosowanych środków zabezpieczających do istniejących zagrożeń każdy pracownik, który powziął tego typu informację jest zobowiązany do jej przekazania ASI i IOD, a w przypadku braku takiej możliwości swojemu bezpośredniemu przełożonemu.

Pracownicy pełniący funkcje kierownicze (zarządzający pracownikami) są zobowiązani do utrzymania wśród podległych sobie pracowników świadomości potrzeb i obowiązków z zakresu bezpieczeństwa informacji.

Zatwierdzanie stosowanych metod i procesów związanych z bezpieczeństwem informacji znajduje się w wyłącznej kompetencji Burmistrza.

5.1.3. Przypisanie odpowiedzialności w zakresie bezpieczeństwa informacji

Za bezpieczeństwo informacji odpowiedzialny jest każdy pracownik Urzędu na swoim stanowisku pracy. Za całokształt realizacji niniejszej Polityki odpowiada Burmistrz. Za realizację poszczególnych elementów niniejszej Polityki odpowiadają IOD oraz ASI (zależnie od zakresu obowiązków przypisanych poszczególnym stanowiskom).

5.1.4. Proces autoryzacji środków przetwarzania informacji

Do przetwarzania informacji w Urzędzie mogą być wykorzystywane wyłącznie środki autoryzowane przez ASI i IOD.

Składając zapotrzebowanie na środek przetwarzania informacji, kierownik komórki organizacyjnej uwzględnia w specyfikacji środka jego cechy mające wpływ na bezpieczeństwo przetwarzanych informacji.

Poprawność działania nowego środka przetwarzania informacji zapewnia i koordynuje kierownik komórki organizacyjnej, dla której środek jest przyjmowany.

Dopuszcza się poprzez autoryzację, nowe środki przetwarzania informacji do wykorzystania w Urzędzie, jeżeli ich używanie nie narusza obowiązujących zasad niniejszej Polityki i PBPDU. Przed podjęciem decyzji o autoryzacji Burmistrz lub IOD, może zwrócić się o opinię do ASI, lub osób realizujących konfigurację przyjmowanego środka. ASI wydając opinię ma na uwadze w szczególności kompatybilność sprzętu i oprogramowania z innymi komponentami systemu. W razie zaistnienia potrzeby Burmistrz lub IOD zwracają się do właściwych dla danego rodzaju środka specjalistów, o modyfikację środka tak by spełniał on wymogi bezpieczeństwa opisane w niniejszej Polityce.

5.1.5. Umowy o zachowaniu poufności

Urząd ze względu na charakter swojej działalności nie stosuje powszechnie umów o zachowaniu poufności. Ewentualną decyzję o zastosowaniu umowy o zachowaniu poufności, w konkretnym przypadku, każdorazowo podejmuje Burmistrz.

5.1.6. Kontakty z organami władzy

W Urzędzie nie tworzy się specjalnych uregulowań dotyczących kontaktów z organami władzy. Kontakty ze służbami ratowniczymi zawarte są w odrębnych od niniejszej Polityki uregulowaniach.

5.1.7. Kontakty z grupami zaangażowanymi w zapewnienie bezpieczeństwa

Burmistrz utrzymuje regularne kontakty z Prezydentami/ Wójtami/ Burmistrzami w podobnych miejscowościach, w szczególności w celu wymiany doświadczeń, informacji o nowych technologiach oraz otrzymywania wczesnych ostrzeżeń o potencjalnych zagrożeniach.

5.1.8. Niezależny przegląd bezpieczeństwa informacji

Funkcjonujący w Urzędzie system zarządzania bezpieczeństwem informacji jest poddawany okresowym przeglądom przeprowadzanym przez Podmiot zewnętrzny.

Przeglądy powinny być wykonywane nie rzadziej niż raz do roku, a także dodatkowo w sytuacjach, gdy nastąpiły znaczące zmiany w organizacji mające wpływ na politykę Urzędu lub z nią związane. Przeglądy takie mogą być inicjowane przez Sekretarza lub IOD.

5.2. Strony zewnętrzne

Charakter działalności Urzędu wymaga kontaktów z podmiotami zewnętrznymi. W trakcie kontaktów z podmiotami zewnętrznymi pracownicy Urzędu mają szczególnie na uwadze obowiązujące zasady bezpieczeństwa informacji.

W każdym przypadku współpracy z podmiotem zewnętrznym, która wymaga przekazania dostępu do środków przetwarzania informacji lub do informacji należących do Urzędu, konieczna jest analiza ryzyka związanego z tą współpracą.

Szacowanie ryzyka, o którym mowa powyżej odbywa się metodą intuicyjną. Ze względów ekonomicznych nie stosuje się w tym przypadku metodologii szacowania ryzyka opisanej w początkowej części niniejszego dokumentu. Oszacowania ryzyka w poszczególnych przypadkach współpracy z podmiotami zewnętrznymi dokonuje Burmistrz lub upoważniona osoba. W szczególnych przypadkach Burmistrz może podjąć decyzję o zastosowaniu wybranej metodyki szacowania ryzyka.

Przy szacowaniu ryzyka współpracy z podmiotami zewnętrznymi należy brać pod uwagę w szczególności:

- środki przetwarzania informacji, do których ma być zrealizowany dostęp strony zewnętrznej,
- sposób dostępu strony zewnętrznej do informacji oraz środków przetwarzania informacji,
- wartość i wrażliwość udostępnianych informacji oraz ich krytyczność dla realizowanych procesów,

- zabezpieczenia potrzebne dla ochrony informacji, które z założenia nie są dostępne dla podmiotu zewnętrznego,
- sposób identyfikacji organizacji i personelu uprawnionego do dostępu,
- zabezpieczenia wprowadzane przez podmiot zewnętrzny do przechowywania, przekazywania, współużytkowania i wymiany informacji,
- skutki braku dostępu podmiotu zewnętrznego, gdy jest on wymagany oraz wprowadzanie lub otrzymywanie niepoprawnych lub wprowadzających w błąd informacji,
- wymagania prawne, regulacje wewnętrzne oraz inne zobowiązania umowne, właściwe dla strony zewnętrznej, które należy wziąć pod uwagę.

W każdym przypadku, gdy podmiot zewnętrzny otrzymuje dostęp do informacji lub środków przetwarzania informacji należących do Urzędu należy upewnić się, że jest on świadom i akceptuje odpowiedzialności i zobowiązania z tym związane.

6. **Zarządzanie aktywami**

Urząd posiada lub dysponuje szeregiem aktywów posiadających wartość. W zakresie niezbędnym dla zapewnienia ochrony tym aktywom prowadzi się ich inwentaryzację oraz dąży do wskazania dla każdego z aktywów jego właściciela odpowiedzialnego za nie.

Użyte powyżej pojęcie „właściciel" odnosi się do osoby lub podmiotu, który ma zatwierdzoną kierowniczą odpowiedzialność za określone aktywa, w tym za ich bezpieczeństwo. W tym znaczeniu pojęcie to nie oznacza faktycznego posiadania praw własności do aktywów.

6.1. Inwentaryzacja aktywów

W Urzędzie zidentyfikowano następujące typy aktywów:
- informacyjne,
- aktywa fizyczne,
- usługi,
- kadra,
- wartości niematerialne (w tym oprogramowanie).

Aktywa informacyjne funkcjonujące w Urzędzie zostały zidentyfikowane w rozdziale 3 niniejszej Polityki.

Inwentaryzacja wykorzystywanego oprogramowania prowadzona jest odrębnie. W Polityce Bezpieczeństwa wskazano jedynie oprogramowanie wykorzystywane do przetwarzania Informacji.

Spis aktywów fizycznych prowadzony jest w ramach Inwentarza, tworzonego i obsługiwanego na podstawie odrębnych przepisów prawa.

Prowadzi się wyodrębnioną ewidencję aktywów usługowych. Częściowo funkcja ewidencyjna w zakresie tego typu aktywów realizowana jest umowach
Ewidencję aktywów ludzkich prowadzi się wraz z ewidencją kadrową.
Prowadzi się ewidencję aktywów niematerialnych.

6.2. Własność aktywów

Przypisanie własności aktywów w Urzędzie następuje na podstawie ogólnie obowiązujących przepisów prawa.

6.3. Akceptowalne użycie aktywów

Wszelkie aktywa wykorzystywane przez pracowników Urzędu mogą być wykorzystywane wyłącznie zgodnie ze swoim przeznaczeniem i dla realizacji celów Urzędu.
Pracownicy są odpowiedzialni za wykorzystywane przez siebie aktywa oraz sposób ich wykorzystywania. Dotyczy to również działań prowadzonych pod ich nadzorem.

6.4. Dostęp do aktywów

Niektóre aktywa wskazane w części Lista aktywów informacyjnych, są dostępne w trybie Ustawy o dostępie do informacji publicznej. Część wyżej wymienionych aktywów jest publikowana (BIP, strony www, materiały

prasowe). Decyzję o publikacji konkretnych informacji podejmują właściwi dla rodzaju aktywa pracownicy Urzędu.

7. **Bezpieczeństwo zasobów ludzkich**

Mając na względzie potencjalne zagrożenia wynikające z działań ludzi podejmuje się kroki służące redukcji ryzyka i zabezpieczeniu przed negatywnymi działaniami lub ich skutkami.
Urząd zatrudnia pracowników. W związku z tym w poniższej części dokumentu opisane zostały zasady postępowania związane z nawiązaniem, trwaniem i ustaniem zatrudnienia.

7.1. Przed zatrudnieniem

7.1.1. Role i zakresy odpowiedzialności

W trakcie prowadzenia procesu rekrutacji pracowników zwraca się uwagę na zagadnienia bezpieczeństwa informacyjnego Urzędu. Opis stanowiska pracy przedstawiany kandydatom powinien zawierać role i odpowiedzialności związane z danym stanowiskiem pracy.

Role i odpowiedzialności związane z danym stanowiskiem pracy uwzględniają:
- ogólne założenia niniejszej Polityki,
- zagadnienie ochrony aktywów przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem,
- realizację konkretnych działań i procesów bezpieczeństwa,
- konieczność zapewnienia odpowiedzialności osoby za jej działania,
- obowiązki i drogę raportowania zdarzeń związanych z bezpieczeństwem.

Zdefiniowane role i zakresy odpowiedzialności przedstawia się w trakcie procesu rekrutacyjnego osobom ubiegającym się o dane stanowisko.
Analogicznie postępuje się w przypadku dopuszczania do pracy osób trzecich, niezatrudnionych bezpośrednio przez Urząd (na przykład pracownicy firm realizujących usługi).
Każdy nowo zatrudniany pracownik musi zostać również przeszkolony przez IOD w zakresie procedur bezpieczeństwa danych osobowych, przed przystąpieniem do obowiązków.

7.1.2. Postępowanie sprawdzające

W Urzędzie zatrudnia się pracowników na stanowiskach, dla których obowiązujące przepisy obligowały zatrudniającego do przeprowadzenia postępowania sprawdzającego opisanego w ustawie o pracownikach samorządowych.

W trakcie określania formy i zakresu weryfikacji kandydatów do pracy należy brać pod uwagę w szczególności:

- dostępność satysfakcjonujących referencji, uwzględniających referencje formalne (np. świadectwo pracy), jak i referencje osobiste,
- kompletność i dokładność przedstawionego życiorysu (zwłaszcza historii zatrudnienia),
- rzetelność deklaracji w zakresie wykształcenia i kwalifikacji zawodowych,
- niezależne potwierdzenie tożsamości.

Szczególną uwagę zwraca się na kwestię postępowania sprawdzającego w przypadku weryfikacji kandydata na stanowisko, którego zakres obowiązków obejmuje przetwarzanie danych podlegających szczególnej ochronie, zwłaszcza tak zwanych danych szczególnych kategorii w rozumieniu przepisów o ochronie danych osobowych oraz danych o wynagrodzeniach. Postępowanie sprawdzające jest prowadzone z poszanowaniem wszystkich obowiązujących przepisów prawa polskiego, w szczególności przepisów o ochronie danych osobowych.
Decyzję o formie i zakresie prowadzenia weryfikacji podejmuje osoba odpowiedzialna za proces rekrutacji na dane stanowisko lub Burmistrz.

Postępowanie sprawdzające może być również prowadzone wobec podmiotów trzecich realizujących zadania na rzecz Urzędu. Zasady prowadzenia takiego postępowania stosuje się odpowiednio.

7.1.3. Zasady i warunki zatrudnienia

Jeżeli tylko jest to formalnie możliwe, częścią zobowiązań kontraktowych pracowników, wykonawców i współpracowników (bez względu na rodzaj nawiązywanego stosunku prawnego) są zasady i warunki zatrudnienia lub współpracy precyzujące obowiązki i odpowiedzialność w zakresie bezpieczeństwa informacji.

Zasady i warunki, o których mowa powyżej konstruuje się uwzględniając:

- konieczność zachowania poufności informacji, do których pracownik bądź współpracownik uzyskuje dostęp,
- prawa i obowiązki pracowników bądź współpracowników związane z realizowanymi przez nich zadaniami,
- odpowiedzialność pracowników bądź współpracowników związaną z przetwarzaniem informacji pochodzących zarówno z wewnątrz Urzędu, jak i od stron zewnętrznych,
- odpowiedzialność za działania prowadzone poza siedzibą Urzędu.,
- działania podejmowane w sytuacji, gdy pracownik lub współpracownik nie przestrzega wymagań bezpieczeństwa.

W dokumentacji związanej z wdrożeniem zasad i warunków, o których mowa powyżej powinno znaleźć się oświadczenie pracownika bądź współpracownika potwierdzające akceptację przyjętych ustaleń.

Zaleca się, by w każdym przypadku rozważać sensowność rozszerzenia odpowiedzialności zawartej w zasadach i warunkach zatrudnienia lub współpracy na określony czas po ustaniu stosunku pracy lub współpracy.

7.2. Nadanie uprawnień

Nadanie uprawnień następuje w sposób zintegrowany z PBPDU. Kierownik komórki organizacyjnej wnioskuje o nadanie upoważnienia dla nowego pracownika a IOD przeprowadza proces szkolenia i wydania upoważnienia w porozumieniu z ASI. Na podstawie upoważnienia ASI nadaje dostęp do systemów informatycznych.

7.2.1. Odpowiedzialność kierownictwa

Burmistrz wymaga od wszystkich pracowników i współpracowników stosowania zasad bezpieczeństwa, zgodnie z wprowadzonymi i obowiązującymi w Urzędzie politykami i procedurami, w szczególności z niniejszą Polityką.

Zadaniem Burmistrz jest podejmowanie wobec pracowników i współpracowników działań mających na celu:

- zapewnienie właściwego sposobu wprowadzania ich w obowiązki i odpowiedzialność związaną z bezpieczeństwem informacji, zwłaszcza ochroną danych osobowych.

Działania te powinny być podejmowane przed przyznaniem tym osobom dostępu do danych lub narzędzi ich przetwarzania:

- przekazywanie im zaleceń określających wymagania związane z bezpieczeństwem informacji, związane z ich obowiązkami w Urzędzie,
- osiągnięcie poziomu świadomości problematyki bezpieczeństwa informacji, a zwłaszcza ochrony danych osobowych, adekwatnego do realizowanych przez nich obowiązków w Urzędzie,
- zapewnienie wypełniania zaleceń i warunków zatrudnienia, uwzględniających niniejszą Politykę, uregulowania w zakresie ochrony danych osobowych oraz właściwe metody pracy,
- ciągłe utrzymanie odpowiednich umiejętności i kwalifikacji.

7.2.2. Uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji

W miarę posiadanych możliwości ekonomicznych i organizacyjnych Urząd podejmuje działania zmierzające do tego, by wszyscy pracownicy Urzędu zostali odpowiednio przeszkoleni oraz byli regularnie informowani o uaktualnieniach obowiązujących w Urzędzie polityk i procedur, w szczególności niniejszej Polityki, które są związane z wykonywaną przez nich pracą.

Szkolenia przeprowadza się przed podjęciem pracy, a w szczególności przed uzyskaniem przez pracownika dostępu do danych podlegających ochronie.
Szkolenie powinno obejmować w szczególności:

- wymagania bezpieczeństwa funkcjonujące w Urzędzie,

- zabezpieczania wynikające z uregulowań prawnych,
- naukę korzystania ze środków przetwarzania informacji, z którymi pracownik będzie miał do czynienia,
- informacje o środkach dyscyplinarnych i karnych związanych z naruszeniami zasad bezpieczeństwa stosowanych w organizacji.

Szkolenia prowadzi IOD i/lub ASI.

7.2.3. Postępowanie dyscyplinarne

Naruszenie bezpieczeństwa przez pracownika, zwłaszcza rażące przypadki, powinny wiązać się z przeprowadzeniem formalnego procesu dyscyplinarnego w stosunku do tego pracownika.

Formalne postępowanie dyscyplinarne jest rozpoczynane dopiero w momencie przeprowadzenia weryfikacji potwierdzającej fakt naruszenia bezpieczeństwa przez daną osobę.

Formalne postępowanie dyscyplinarne powinno zapewniać poprawne i obiektywne traktowanie pracowników, którzy dopuścili się naruszenia bezpieczeństwa.

Postępowanie to powinno być adekwatne i uwzględniać w szczególności takie czynniki jak: rodzaj i waga naruszenia, jego wpływ na działalność Urzędu, informacje, czy jest to pierwsze naruszenie czy kolejne wykonane przez tego samego pracownika, właściwe przepisy prawne i inne stosowne czynniki.
W postępowaniu dyscyplinarnym bierze udział IOD, a w sytuacjach dotyczących systemów informatycznych również ASI.

7.3. Zakończenie lub zmiana zatrudnienia

Zakończenie pracy przez pracowników lub współpracowników, związane zarówno z odejściem z organizacji, jak i istotną zmianą stanowiska powinny odbywać się w sposób zorganizowany. Zaleca się, by w przypadku istotnej zmiany stanowiska pracy wewnątrz Urzędu było traktowane jako zakończenie pracy na danym stanowisku i rozpoczęcie nowej po zmianie. W związku z tym zapisy bieżącego rozdziału powinny wówczas być stosowane odpowiednio.

7.3.1 Odpowiedzialność związana z zakończeniem zatrudnienia

Burmistrz, pracownik odpowiedzialny za prowadzenie ewidencji kadrowej lub upoważniona przez nich osoba są zobowiązani do zarządzania odejściem pracowników lub współpracowników z Urzędu, w tym za doprowadzenie do zwrotu wszelkiego sprzętu i odebranie wszystkich praw dostępu. W swoich działaniach osoba ta współpracuje z bezpośrednim przełożonym pracownika kończącego zatrudnienie. Przekazywanie obowiązków przy zakończeniu zatrudnienia powinno odnosić się w swojej formie, treści i zakresie do istniejących wymagań bezpieczeństwa, uregulowań i zobowiązań prawnych, a także odpowiedzialności z tytułu umów (np. o zachowaniu poufności) i warunków zatrudnienia, zwłaszcza tych, które obowiązują jeszcze po momencie zakończenia zatrudnienia. Obowiązki i zakresy odpowiedzialności, które pozostają w mocy po ustaniu zatrudnienia lub współpracy powinny być zawarte w umowach lub innych dokumentach formalnych. Każdorazowo należy rozważyć konieczność poinformowania pozostałego personelu o zmianach w zatrudnieniu i podjąć stosowne działania. Wszelkie decyzje w tej sprawie podejmuje Burmistrz.

7.3.2. Zwrot aktywów

Pracownik lub współpracownik kończący zatrudnienie w Urzędzie jest zobowiązany do zwrotu wszystkich aktywów, które są własnością Urzędu.

Do aktywów tych zaliczają się m.in:
1) dokumenty,
2) sprzęt,
3) oprogramowanie,
4) inne urządzenia do przetwarzania danych, w tym przenośne,
5) karty dostępu,
6) podręczniki,
7) informacje przechowywane na nośnikach elektronicznych,
8) inne aktywa.

W przypadku, gdy pracownik lub współpracownik korzysta z własnego sprzętu należy upewnić się, że wszystkie informacje podlegające ochronie w Urzędzie, a zwłaszcza dane osobowe zostały bezpiecznie zwrócone oraz trwale usunięte ze sprzętu.

Jeżeli pracownicy lub współpracownicy dysponują wiedzą istotną z punktu widzenia bieżącej działalności Urzędu, wiedza ta powinna zostać przed ustaniem zatrudnienia udokumentowana i przekazana Urzędowi.

7.3.3. Odebranie praw dostępu

Dział Kadr zobowiązany jest przekazać IOD i ASI informacje o zakończeniu zatrudnienia pracownika co najmniej na dzień przed jego zakończeniem. W momencie zakończenia zatrudnienia wszelkie prawa dostępu do informacji i środków przetwarzania informacji, które posiadała osoba kończąca zatrudnienie powinny zostać odebrane.

W indywidualnych sytuacjach należy rozważyć odebranie lub ograniczenie praw dostępu przed zakończeniem lub zmianą zatrudnienia. Decyzję o takim działaniu podejmuje Burmistrz lub ASI w porozumieniu z IOD.

Przy rozważaniu powyższej decyzji należy wziąć pod uwagę między innymi takie czynniki ryzyka jak:

1) czy zakończenie lub zmiana zatrudnienia jest inicjowana przez pracownika, czy przez kierownictwo i jakie są tego przyczyny,

2) aktualny zakres odpowiedzialności pracownika,

3) wartość aktualnie dostępnych dla niego aktywów.

Jeżeli prawa dostępu są przyznane większej grupie osób niż odchodzący pracownik, należy usunąć tego pracownika z każdej grupowej listy dostępu oraz należy poinformować pozostałych pracowników, będących członkami tych grup, o zakazie dzielenia się informacjami z osobą odchodzącą z pracy.

8. **Bezpieczeństwo fizyczne i środowiskowe**

8.1. Obszary bezpieczne

Jednym ze środków zapewnienia bezpieczeństwa w Urzędzie jest ochrona przed nieautoryzowanym dostępem fizycznym, uszkodzeniami lub zakłóceniami w odniesieniu do wszelkich aktywów, zarówno fizycznych, jak i informacyjnych.

W związku z tym w Urzędzie stosuje się obszar bezpieczny oraz dodatkowo obszar przetwarzania danych osobowych, który może być tożsamy z obszarem bezpiecznym.

8.1.1. Fizyczne granice obszaru bezpiecznego

Za obszar bezpieczny uważa się całą siedzibę Urzędu, łącznie z zewnętrznymi siedzibami komórek Urzędu (Straż Miejska). Dodatkowo, mając na względzie przetwarzanie informacji i szczególny charakter ich ochrony, wyznacza się obszar przetwarzania informacji (w tym danych osobowych).

8.1.2. Fizyczne i proceduralne zabezpieczenie obszaru przetwarzania informacji

Wejścia do obszaru bezpiecznego podlegają zabezpieczeniom fizycznym.

Wykorzystywane wejścia operacyjne chronione są za pomocą:
1) Zamykanych na klucz drzwi do pomieszczeń,
2) Ewidencjonowania kluczy do pomieszczeń pracowniczych,
3) Osobnej ewidencji kluczy do pomieszczeń i szaf metalowych/sejfów,
4) Zamykanych na zamek szyfrowy bądź magnetyczny pomieszczeń wybranych komórek organizacyjnych,
6) Sejfów i szaf pancernych w pomieszczeniach wybranych komórek organizacyjnych,
7) Zabezpieczenia w postaci 24 godzinnego dozoru.
8) Zabezpieczenia w postaci rejestracji wejść i wyjść pracowników a w przypadku Interesantów identyfikacja przy pomocy monitoringu,
9) Zabezpieczenia w postaci alarmu oraz alarmu przeciwpożarowego,
11) Zabezpieczenia w postaci Monitoringu wizyjnego pomieszczenia monitoringu miejskiego i terenu zalewu Andrzejówka,
12) Zabezpieczenia w postaci monitoringu wizyjnego siedziby Urzędu

Wyjścia zapasowe zabezpieczone są fizycznie w sposób trwały i wykorzystywane wyłącznie w sytuacjach awaryjnych.

W Urzędzie wykonuje się regularne przeglądy stanu zabezpieczenia wejść i wprowadza ewentualne korekty.

8.1.3. Zabezpieczanie pomieszczeń

Pomieszczenia, w których przetwarza się (w tym przechowuje) informacje podlegające ochronie w Urzędzie zabezpiecza się przed dostępem osób niepowołanych.

Podstawowym stosowanym sposobem zabezpieczania jest zamykanie pomieszczeń z użyciem kluczy, drzwiami wyposażonymi w zamki.

Pomieszczenia oznacza się w stopniu minimalnym, wymaganym prawem lub niezbędnym dla sprawnego funkcjonowania Urzędu. Nie stosuje się zbędnych oznaczeń, które mogłyby obniżać poziom bezpieczeństwa informacji przetwarzanych w danych pomieszczeniach.

8.1.4. Ochrona przed zagrożeniami zewnętrznymi i środowiskowymi

W przypadku Urzędu w kontekście zagrożeń zewnętrznych i środowiskowych rozpatruje się jedynie zagrożenie pożarem. W związku z tym budynek będący siedzibą Urzędu wyposaża się w sprzęt przeciwpożarowy i gaśniczy oraz wprowadza się inne oznaczenia (instrukcje przeciwpożarowe, drogi ewakuacyjne itp.) zgodnie z odrębnymi, obowiązującymi przepisami w zakresie ochrony przeciwpożarowej.

W Urzędzie nie przechowuje się materiałów niebezpiecznych i wybuchowych w ilościach, które mogłyby stanowić zagrożenie.

Prawdopodobieństwo wystąpienia powodzi, trzęsienia ziemi, wybuchu, niepokojów społecznych oraz innych form naturalnych lub spowodowanych przez człowieka katastrof, uznaje się za bardzo małe i nie tworzy się specjalnych uregulowań niniejszej Polityki związanych z tymi zdarzeniami.

8.1.5. Praca w obszarach bezpiecznych

Praca w obszarach bezpiecznych powinna być wykonywana ze zwracaniem szczególnej uwagi na zagadnienie bezpieczeństwa informacji, w szczególności powinna uwzględniać wszystkie wskazówki, zalecenia i uregulowania obowiązujące w Urzędzie, zwłaszcza niniejszą Politykę.

Personel wykonujący pracę w obszarach bezpiecznych powinien zostać uświadomiony w zakresie istnienia takich obszarów oraz poinstruowany w zakresie sposobu prowadzenia tam działań. Należy unikać prowadzenia prac w obszarach bezpiecznych przez przedstawicieli stron trzecich, gdy praca ta wykonywana jest bez nadzoru ze strony uprawnionego przedstawiciela Urzędu (zarówno ze względów bezpieczeństwa, jak i z uwagi na uniemożliwienie złośliwych działań).

Obszary bezpieczne, w których nie pracują i nie przebywają ludzie powinny być zamykane i okresowo sprawdzane. Używanie urządzeń fotograficznych, wideo, audio i innych urządzeń nagrywających jest dopuszczalne jedynie wtedy, gdy jest to niezbędne dla realizacji zadań realizowanych przez poszczególne komórki organizacyjne lub gdy osoba używająca takie urządzenie posiada odpowiednie, indywidualne upoważnienie Burmistrza.

8.1.6. Obszary publicznie dostępne

W Urzędzie wyznacza się obszary publicznie dostępne. Obszarem publicznie dostępnym jest taki obszar, do którego osoba trzecia może wejść bez przejścia przez dowolny wykorzystywany proces autoryzacji. Obszary publicznie dostępne stosowane są w celach organizacyjnych, mając na uwadze specyfikę funkcjonowania Urzędu, ułatwiających funkcjonowanie organizacji.

Obszar publicznie dostępny w siedzibie Urzędu stanowi teren wokół budynku z wyznaczonymi drogami dla pieszych i pojazdów oraz: hol wejściowy, obszar BOK, sala ślubów, korytarze (w tym toalety) i klatki schodowe budynku, pokoje pracowników.

8.2. Bezpieczeństwo sprzętu

Sprzęt będący w posiadaniu lub użytkowaniu Urzędu podlega ochronie w celu zapobiegania jego utracie, uszkodzeniu, kradzieży i innych zdarzeń mogących zakłócić lub przerwać działalność Urzędu.

8.2.1. Lokalizacja i ochrona sprzętu

Sprzęt w Urzędzie umieszczany i lokowany jest w sposób minimalizujący ryzyko związane z bezpieczeństwem jego funkcjonowania oraz bezpieczeństwem informacji.

Komputery i inne środki przetwarzania informacji lokalizowane są w taki sposób, aby zapewnić im poprawne funkcjonowanie (np. w zakresie wentylacji), a jednocześnie utrudnić potencjalne działania mające na celu naruszenie zasad bezpieczeństwa.

Monitory komputerowe i inne wyświetlacze, na których przetwarzane są dane podlegające ochronie, a w szczególności dane osobowe, umieszczane są w sposób uniemożliwiający podejrzenie danych na nich wyświetlanych przez osoby nieuprawnione lub postronne.

Urządzenia kluczowe z punktu widzenia funkcjonowania Urzędu w miarę posiadanych możliwości lokalowych i organizacyjnych umieszczane są w odrębnych pomieszczeniach, przystosowanych do pracy tego typu urządzeń.

Dla zapewnienia optymalnych warunków pracy regularnie monitoruje się warunki środowiskowe, takie jak temperatura czy wilgotność, aby wykrywać ich potencjalny negatywny wpływ na środki przetwarzania informacji.

Każdy użytkownik, który stwierdzi, iż warunki środowiskowe, w których pracują nośniki przetwarzania informacji mogą negatywnie wpłynąć na ich funkcjonowanie jest zobowiązany zgłosić ten fakt swojemu bezpośredniemu przełożonemu lub ASI, a w przypadku ich niedostępności bezpośrednio Burmistrzowi.

Dla zapewnienia optymalnych warunków pracy oraz niezawodności urządzeń na stanowiskach pracy z urządzeniami przetwarzania informacji, w szczególności na stanowiskach komputerowych w Urzędzie wszystkich użytkowników obowiązuje zakaz spożywania posiłków, napojów.
Budynki Urzędu są wyposażone w instalację odgromową.

8.2.2. Systemy wspomagające

W celu ochrony systemów przetwarzających informacje w Urzędzie przed awarią lub zakłóceniami spowodowanymi awariami systemu zasilania stosuje się stosowne zabezpieczenia.

Systemy przetwarzające informacje, w tym w szczególności sprzęt komputerowy, a zwłaszcza ten, za pomocą, którego przetwarzane są dane osobowe zabezpiecza się przed awarią lub zakłóceniami spowodowanymi utratą zasilania za pomocą awaryjnych zasilaczy bezprzerwowych (UPS).

Dokonuje się regularnego przeglądu stosowanych zasilaczy awaryjnych (UPS) oraz ich testowania, zgodnie z zaleceniami producentów, aby zapewnić ich skuteczność i odpowiednią pojemność na wypadek awarii.

Szczegółowe zasady stosowania zasilaczy awaryjnych opisane są w dokumencie Instrukcja zarządzania systemami informatycznymi w części Zabezpieczenia systemów przed skutkami utraty zasilania.

Urządzenia, dla których stosowanie zasilaczy awaryjnych nie jest wymagane zabezpiecza się przed uszkodzeniem spowodowanym przepięciem w sieci elektroenergetycznej za pomocą filtrów przeciwprzepięciowych. Systemy wspomagające takie jak dodatkowe zasilanie, zaopatrzenie w wodę, kanalizacja, ogrzewanie, wentylacja oraz klimatyzacja poddaje się okresowym przeglądom serwisowym celem zapewnienia ich bezawaryjnej i skutecznej pracy.

8.2.3. Bezpieczeństwo okablowania

Okablowanie zasilające, telekomunikacyjne i teleinformatyczne wykorzystywane w Urzędzie jest prowadzone zgodnie z obowiązującymi wymogami prawnymi, obowiązującymi dobrymi praktykami w tym zakresie oraz uregulowaniami niniejszego dokumentu.
Uregulowania zawarte poniżej obejmują przede wszystkim to okablowanie, które będzie prowadzone w przyszłości w stosunku do ogłoszenia niniejszego dokumentu.

Okablowanie już funkcjonujące w Urzędzie w momencie wejścia w życie niniejszej Polityki a niespełniające wskazanych poniżej zaleceń będzie dostosowywane do tych regulacji sukcesywnie, w miarę posiadanych możliwości finansowych, organizacyjnych i w sytuacji istnienia jednoznacznego ekonomicznego uzasadnienia prowadzenia takich prac.

Zalecenia dotyczące okablowania:

1) okablowanie powinno być prowadzone z sposób uniemożliwiający lub silnie utrudniający dostęp do niego przez osoby niepowołane (pod ziemią, pod tynkiem, w specjalnych kanałach kablowych itp.),

2) okablowanie nie powinno być prowadzone przez obszary publicznie dostępne,

3) okablowanie zasilające powinno być oddzielone od okablowania telekomunikacyjnego i teleinformatycznego w celu uniknięcia interferencji,

4) kable i inny sprzęt związany z okablowaniem powinny być wyraźnie oznakowane w sposób umożliwiający ich jednoznaczną identyfikację,

5) struktura okablowania powinna być udokumentowana,

6) powinna być prowadzona ponadto dokumentacja wykonanych połączeń kablowych,

7) kluczowe elementy infrastruktury kablowej (np. koncentratory) powinny być dodatkowo zabezpieczane fizycznie przed nieuprawnionym dostępem.

8.2.4. Konserwacja sprzętu

W celu zapewnienia ciągłej dostępności i integralności sprzętu prowadzi się jego regularną konserwację. Przy organizacji i realizacji działań konserwacyjnych bierze się pod uwagę:

- zalecenia producenta lub dostawcy sprzętu, w kwestii częstotliwości i zakresu konserwacji,
- realizacje napraw i czynności serwisowych przez kompetentny (autoryzowany – jeżeli dotyczy) personel,
- wdrożenie stosownych zabezpieczeń w trakcie prowadzenia naprawy lub konserwacji, w tym w szczególności z uwzględnieniem miejsca realizacji tych działań (w siedzibie Urzędu lub poza nim),
- konieczność zapewnienia zgodności z wymaganiami nakładanymi przez uregulowania umów gwarancyjnych lub polis ubezpieczeniowych.

Przy realizacji działań konserwacyjnych mają ponadto zastosowanie wszystkie uregulowania zawarte w dokumencie Instrukcja zarządzania systemami informatycznymi.

8.2.5. Bezpieczeństwo sprzętu poza siedzibą

W zakresie bezpieczeństwa sprzętu poza siedzibą stosuje się uregulowania z dokumentu Instrukcja zarządzania systemami informatycznymi.

8.2.6. Bezpieczne zbywanie sprzętu lub przekazywanie do ponownego użycia

Przed zbyciem lub przekazaniem do ponownego użycia sprzęt powinien zostać sprawdzony pod kątem dostępności na nim jakichkolwiek informacji podlegających ochronie w Urzędzie, a zwłaszcza danych osobowych. Szczególnie w tym kontekście zwraca się uwagę na sprzęt komputerowy i inne narzędzia przetwarzania informacji zawierające nośniki danych.

Przed zbyciem lub przekazaniem do ponownego użycia wszelkie informacje podlegające ochronie, zwłaszcza dane osobowe, a także licencjonowane oprogramowanie są trwale usuwane.

Jeżeli jest to możliwe w przypadku likwidacji nośników informacji dąży się do ich fizycznego niszczenia.

8.2.7. Wynoszenie mienia

Zabrania się wynoszenia sprzętu, informacji oraz oprogramowania poza siedzibę Urzędu. Każdy przypadek wynoszenia mienia będącego własnością Urzędu lub tu użytkowanego wymaga zezwolenia.

Zezwolenia na wynoszenie mienia udziela Burmistrz lub upoważniona osoba.

W przypadku wynoszenia sprzętu poza siedzibę Urzędu sprawdza się czas zwrotu oraz stan sprzętu po zwrocie.

Burmistrz wprowadzi obowiązek rejestrowania, kiedy i przez kogo sprzęt jest wynoszony oraz zwracany.

9. Zarządzanie systemami i sieciami

Zasady obowiązujące w zakresie zarządzania systemami i sieciami w Urzędzie zostały opisane w odrębnym dokumencie, zatytułowanym Instrukcja zarządzania systemami informatycznymi.

10. Kontrola dostępu

10.1. Wymagania wobec kontroli dostępu

Dostęp do informacji lub środków ich przetwarzania w Urzędzie jest ograniczany i kontrolowany. Stosowane zasady przyznawania uprawnień, ich kontroli oraz odbierania uwzględniają przedmiot i specyfikę działalności Urzędu.
Zagadnienia kontroli dostępu odnoszące się do systemów informatycznych zostały uregulowane w dokumencie Instrukcja zarządzania systemami informatycznymi. W niniejszej polityce zebrane zostały zalecenia i zasady ogólne oraz szczegółowe odnoszące się do innych obszarów niż systemy informatyczne.

10.1.1. Polityka kontroli dostępu

Tworzona i stosowana w Urzędzie polityka kontroli dostępu uwzględnia:

- wymagania bezpieczeństwa poszczególnych aplikacji,
- identyfikację wszystkich informacji związanych z aplikacjami oraz ryzyka, na które te informacje mogą być narażone,
- obowiązujące w Urzędzie zasady rozpowszechniania informacji,
- odpowiednie przepisy prawa, w tym w szczególności przepisy o ochronie danych osobowych, a także zobowiązania wynikające z zawartych umów,
- standaryzowane profile praw dostępu dla użytkowników na typowych stanowiskach,
- w miarę posiadanych możliwości finansowo-organizacyjnych rozdzielenie ról związanych z kontrolą dostępu,
- wymagania formalnej autoryzacji wniosku o przyznanie dostępu,
- wymagania okresowych przeglądów zabezpieczeń,
- odbieranie praw dostępu.

W trakcie określania, zarówno ogólnych, jak i szczegółowych, zasad kontroli dostępu rozważa się następujące zagadnienia:
- rozróżnienie pomiędzy zasadami, które muszą obowiązywać zawsze, a zasadami wprowadzanymi wariantowo lub warunkowo,
- przyjęcie przy ustalaniu zasad założenia, że „wszystko jest zabronione, dopóki nie jest wyraźnie dozwolone” (alternatywnie do założenia „dozwolone jest wszystko, co nie jest zabronione”),
- określenie zasad, które przed wprowadzeniem wymagają uzyskania odpowiedniej zgody i takich, które jej nie wymagają.

10.2. Zarządzanie dostępem użytkowników

10.2.1. Dostęp do systemów informatycznych

Zasady zarządzania dostępem użytkowników do wykorzystywanych w Urzędzie systemów informatycznych zostały uregulowane w dokumencie Instrukcja zarządzania systemami informatycznymi.

10.2.2. Dostęp do budynku

Dostęp do budynku jest ograniczony zgodnie z zasadami wskazanymi w niniejszym dokumencie w rozdziale 8. Bezpieczeństwo fizyczne i środowiskowe w części 8.1. Obszary bezpieczne w punkcie 8.1.2.

10.2.3. Dostęp do kluczy

Dostęp do kluczy został uregulowany w PBPDU.

10.3. Odpowiedzialność użytkowników

Za bezpieczeństwo informacyjne, w tym za bezpieczeństwo przetwarzanych danych osobowych w Urzędzie odpowiedzialny jest każdy na swoim stanowisku pracy.

Skuteczność wdrożonych środków bezpieczeństwa w dużej mierze zależy od współdziałania uprawnionych użytkowników. W związku z tym uświadamia się ten fakt użytkownikom, a użytkownicy są zobowiązani do współpracy w zakresie bezpieczeństwa informacji w Urzędzie.

W szczególny sposób każdy z pracowników lub współpracowników Urzędu jest odpowiedzialny za utrzymanie skutecznej kontroli dostępu i zapewnienie bezpieczeństwa w odniesieniu do swojego stanowiska pracy, zwłaszcza wykorzystywanego sprzętu i haseł, którymi się posługuje.

10.3.1. Polityka czystego biurka i czystego ekranu

Wprowadza się w Urzędzie politykę czystego biurka dla dokumentów papierowych i nośników oraz czystego ekranu dla elektronicznych środków przetwarzania informacji.

W trakcie realizacji polityki czystego biurka i czystego ekranu zwraca się szczególną uwagę na:

1) przechowywanie pod zamknięciem nośników zawierających informacje podlegające ochronie (zarówno nośników elektronicznych, jak i dokumentów papierowych), szczególnie, gdy pomieszczenie jest opuszczane,
2) blokowanie urządzeń przetwarzających informacje, zwłaszcza komputerów, gdy pozostawiane są bez opieki lub czasowo nieużywane,
3) ochronę punktów przyjmowania i wysyłania korespondencji (np. faksów),
4) autoryzowane użycie kopiarek lub innych technik kopiowania,
5) niezwłoczne usuwanie z drukarek dokumentów zawierających informacje podlegające ochronie, a zwłaszcza dane osobowe.

10.4. Kontrola dostępu do sieci

Uregulowania dotyczące zasad dostępu do sieci znajdują się w dokumencie IZSI.

11. **Pozyskiwanie, rozwój i utrzymanie systemów informacyjnych**

Urząd, ze względu na specyfikę swojej działalności, korzysta z gotowych rozwiązań informatycznych nabywanych na rynku. Ponadto zadania z zakresu obsługi informatycznej oraz obowiązek zaopatrzenia Urzędu w sprzęt IT zostały przekazane Wydziałowi Administracji.

W przypadku, gdy sytuacja Urzędu ulegnie zmianie i w ramach organizacji będzie tworzone, rozwijane bądź utrzymane oprogramowanie, Burmistrz zobowiązuje się do aktualizacji niniejszej Polityki i Polityki bezpieczeństwa o uregulowania z tym związane. Za określanie kierunków rozwoju i ewaluacji oprogramowania odpowiedzialny jest ASI.

12. **Zarządzanie incydentami związanymi z bezpieczeństwem informacji**

12.1. Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji i słabości

Aby zapewnić skuteczność funkcjonowania systemu bezpieczeństwa informacji w Urzędzie wprowadza się zasady zgłaszania zdarzeń związanych z bezpieczeństwem informacji oraz słabości systemów. Wszyscy pracownicy Urzędu są zobowiązani do postępowania zgodnie z uregulowaniami niniejszego dokumentu.

12.1.1. Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji

W przypadku zauważenia jakiegokolwiek zdarzenia mogącego wpłynąć negatywnie na bezpieczeństwo informacji w Urzędzie każdy pracownik bądź współpracownik jest zobowiązany podjąć działania opisane w niniejszym dokumencie, w szczególności zgłosić ten fakt do ASI oraz IOD.

Kwalifikacji zdarzenia jako mogącego wpłynąć na bezpieczeństwo informacji dokonuje osoba obserwująca to zdarzenie. Za tego typu zdarzenia uważa się w szczególności:
1) utratę usługi, urządzenia lub funkcjonalności,
2) przeciążenie lub niepoprawne działanie systemu,
3) błędy ludzkie,
4) niezgodność z politykami lub zaleceniami,
5) naruszenia ustaleń związanych z bezpieczeństwem fizycznym, w tym nieuprawniony dostęp do danych lub obszaru przetwarzania, kradzież sprzętu bądź nośników danych,
6) niekontrolowane zmiany systemu lub zabezpieczeń, w tym wszelkie próby naruszenia poufności, integralności i rozliczalności systemu bądź danych,
7) niepoprawne działanie sprzętu lub oprogramowania,
8) naruszenia dostępu,
9) zdarzenia losowe.

W przypadku zauważenia zdarzenia wpływającego bądź mogącego mieć wpływ na bezpieczeństwo informacji osoba, która powzięła taką informację powinna:
1) zawiadomić o tym fakcie Burmistrza lub swojego bezpośredniego przełożonego, ASI oraz IOD. Zawiadomienie powinno nastąpić tak szybko, jak jest to możliwe,
2) zapamiętać lub zanotować wszystkie ważne szczegóły dotyczące zdarzenia (np. typ niezgodności lub naruszenia, błąd działania, wiadomość z ekranu, dziwne zachowanie itp.),
3) nie podejmować żadnych dalszych działań do czasu interwencji wyznaczonych pracowników, zwłaszcza wówczas, gdy dalsze działania mogłyby pogłębić ujawnione problemy lub zatrzeć ślady związane ze zidentyfikowanym wcześniej naruszeniem,
4) jeżeli naruszenie spowodowało sytuację, w której istnieje zagrożenie dostępu do chronionych danych, a w szczególności danych osobowych, przez osoby nieuprawnione, wówczas niezależnie od oczekiwania na interwencję wyznaczonych pracowników każdy pracownik jest zobowiązany do zabezpieczenia danych w celu uniemożliwienia dostępu do nich przez niepowołane osoby.
Zawiadomienie powinno zostać przeprowadzone w formie, która umożliwia najszybsze przekazanie informacji. Jeżeli jednak naruszenie dotyczy zagadnień ochrony danych osobowych informacja o naruszeniu powinna być dostarczona również w formie pisemnej do IOD.

Niezgłaszanie zauważonych naruszeń będzie traktowane jako naruszenie systemu bezpieczeństwa i może podlegać odpowiedzialności dyscyplinarnej bądź karnej.

12.1.2. Zgłaszanie słabości systemu bezpieczeństwa

W przypadku, gdy użytkownik zaobserwował lub podejrzewa istnienie słabości w systemie bezpieczeństwa jest zobowiązany zgłosić ten fakt Burmistrzowi i lub swojemu bezpośredniemu przełożonemu oraz ASI i IOD.

Jednocześnie użytkownicy nie są uprawnieni do testowania zabezpieczeń systemu. W związku z tym niedopuszczalne jest dowodzenie istnienia podejrzewanej słabości, a obowiązek dotyczy jedynie zgłoszenia podejrzenia jej występowania.

12.2. Zarządzanie incydentami związanymi z bezpieczeństwem informacji oraz udoskonaleniami

12.2.1. Odpowiedzialność i procedury

Burmistrz dokłada wszelkich starań, by reakcja na incydenty związane z bezpieczeństwem informacji przebiegała w sposób szybki, skuteczny i uporządkowany.

Pozostałe procedury funkcjonujące w Urzędzie muszą być zgodne pod kątem zachowania bezpieczeństwa informacji z niniejszą polityką.

Dopuszcza się możliwość ustanawiania osobnych procedur w ramach rozwoju systemu zarządzania bezpieczeństwem informacji w przyszłości. Procedury awaryjne tworzone są w sposób możliwie prosty i skrócony. Za tworzenie procedur związanych z takimi zdarzeniami jak atak terrorystyczny, pożar, katastrofy, groźne zjawiska meteorologiczne odpowiedzialny jest Pracownik na Samodzielnym Stanowisku ds. Dowodów Osobistych i Ewidencji Ludności mający w swym zakresie czynności zadania z zakresu zarządzania kryzysowego.

Tworzeniem nowych i weryfikacją (oraz uzupełnianiem) już funkcjonujących procedur zarządza IOD w porozumieniu i przy udziale komórek organizacyjnych Urzędu.

W przypadku pojawienia się incydentu związanego z bezpieczeństwem informacji podejmuje się właściwe działania, uwzględniając:
1) analizę i identyfikację przyczyny incydentu,
2) ograniczanie zasięgu naruszenia bezpieczeństwa,
3) planowanie i wdrażanie działań naprawczych w celu uniknięcia powtórnego wystąpienia incydentu,
4) komunikację z podmiotami związanymi z incydentem i zaangażowanymi w jego usunięcie,
5) dokumentację prowadzonych działań,
6) gromadzenie ewentualnych dowodów,
7) utrzymanie ciągłości działania Urzędu.

12.2.2. Postępowanie wyjaśniające

Burmistrz wyznacza jako osoby odpowiedzialne za prowadzenie postępowań wyjaśniających w przypadku incydentów związanych z bezpieczeństwem informacji ASI i IOD.

W przypadku otrzymania informacji o incydencie związanym z bezpieczeństwem informacji, osoba odpowiedzialna za prowadzenie postępowań wyjaśniających:

1) udaje się na miejsce wystąpienia incydentu,
2) dokonuje przeglądu i oceny sytuacji zastanej, ze szczególnym uwzględnieniem stanu urządzeń i pomieszczeń w momencie przybycia,
3) odbiera relację dotyczącą zdarzeń związanych z incydentem od osoby zgłaszającej incydent, a także jeśli jest taka konieczność od innych osób, których wiedza może być pomocna przy ustalaniu okoliczności incydentu,
4) wydaje polecenia i podejmuje decyzje w zakresie prowadzenia dalszych działań. Wszyscy pracownicy, których działania mogą mieć związek z incydentem bądź jego usuwaniem są zobowiązani do bezwzględnej realizacji tych poleceń,
5) jeżeli naruszenie jest wynikiem niezastosowania się przez pracowników bądź współpracowników Urzędu do obowiązujących przepisów prawa lub uregulowań wewnętrznych dotyczących bezpieczeństwa informacji lub ochrony danych osobowych, osoba prowadząca postępowanie wyjaśniające wnioskuje do Burmistrza o wyciągnięcie stosownych konsekwencji. Do wniosku dołącza się zgromadzony w wyniku postępowania wyjaśniającego materiał dowodowy,
6) w zależności od sytuacji i potrzeb z postępowania wyjaśniającego może być sporządzony protokół. Jeśli naruszenie dotyczyło ochrony bądź przetwarzania danych osobowych, osoba prowadząca postępowanie wyjaśniające jest zobowiązana do sporządzenia protokołu z prowadzonego postępowania i po jego zakończeniu przekazania go Burmistrzowi. Protokół ten powinien zawierać co najmniej:
   a) informacje o czasie – prawdopodobnym zaistnienia zdarzenia, zgłoszenia incydentu oraz przybycia na miejsce osoby prowadzącej postępowanie wyjaśniające,
   b) informacje o osobach związanych z incydentem, w szczególności o zgłaszającym oraz prowadzącym postępowanie,
   c) opis sytuacji zastanej po przybyciu na miejsce wystąpienia incydentu, w tym opis stanu systemów, urządzeń i pomieszczeń,
   d) opis podjętych działań,
   e) opis efektów uzyskanych w wyniku podjętych działań,
   f) opis przyczyny lub prawdopodobnej przyczyny zaistnienia incydentu,
   g) ewentualne wnioski ogólne, mające na celu zmniejszenie prawdopodobieństwa wystąpienia podobnego incydentu w przyszłości.

12.2.3.Wyciąganie wniosków z incydentów związanych z bezpieczeństwem informacji

Regularnie prowadzi się analizę występujących incydentów oraz wyciąga wnioski z tej analizy. W uzasadnionych przypadkach wnioski z analizy, o której mowa powyżej, stanowią podstawę do wnioskowania zmian w obowiązującej Polityce i PBPDU.

12.2.4. Gromadzenie materiału dowodowego

W przypadku, gdy naruszenie może powodować kroki prawne (natury dyscyplinarnej, cywilnoprawnej lub karnej), w szczególności, gdy naruszenie dotyczy ochrony danych osobowych, w ramach czynności związanych z obsługą incydentu powinien być gromadzony, zachowywany, a na właściwym etapie przedstawiany materiał dowodowy.

13. **Zarządzanie ciągłością działania**

W Urzędzie na chwilę wprowadzenia w życie niniejszej Polityki nie tworzy się odrębnych planów ciągłości działania.

Zakłada się, iż rozwój systemu zarządzania bezpieczeństwem informacji w Urzędzie w przyszłości może zakładać poszerzenie go o szczegółowe uregulowania w zakresie zarządzania ciągłością działania, w szczególności o plany ciągłości działania.

14. **Zgodność**

14.1. Zgodność z przepisami prawnymi

Działalność Urzędu opiera się na obowiązującym prawie polskim. W związku z tym wszelkie działania organizacji jako całości oraz poszczególnych pracowników, w tym działania w zakresie bezpieczeństwa informacji, mają odzwierciedlenie w obowiązujących przepisach prawa.

14.1.1. Prawo własności intelektualnej

W Urzędzie wykorzystuje się jedynie legalne, licencjonowane oprogramowanie oraz inne utwory chronione prawem autorskim.

W celu zapewnienia skutecznej realizacji powyższego wymogu:
1) wszyscy użytkownicy mają świadomość zasad wykorzystywania oprogramowania oraz innych utworów chronionych prawem autorskim,
2) pozyskuje się oprogramowanie tylko z zaufanych źródeł,
3) naruszenie przez pracowników praw własności intelektualnej sankcjonowane jest dyscyplinarnie,
4) przechowuje się dowody własności licencji, a także oryginalne dyski instalacyjne i dokumentację,
5) prowadzi się regularne kontrole zainstalowanego oprogramowania pod kątem jego legalności i zgodności z licencją.

14.1.2.Ochrona danych osobowych

Szczegółowe uregulowania dotyczące ochrony danych osobowych znajdują się w PBPDU.

14.1.3. Zapobieganie nadużywaniu środków przetwarzania informacji

Zasady wykorzystywania środków przetwarzania informacji do celów innych niż realizacja obowiązków służbowych zostały uregulowane w dokumencie Instrukcja zarządzania systemami informatycznymi.

14.1.4. Regulacje dotyczące zabezpieczeń kryptograficznych

W Urzędzie wykorzystuje się sprzęt i oprogramowanie realizujące funkcje kryptograficzne.

Za prawidłowe działanie sprzętu i oprogramowania odpowiada ASI, który określa procedury jego wykorzystania.

14.2. Zgodność z politykami bezpieczeństwa i standardami

Burmistrz dokłada wszelkich starań, by Polityki Bezpieczeństwa i inne uregulowania związane z bezpieczeństwem informacji w Urzędzie były realizowane prawidłowo.

W tym celu prowadzi się regularne przeglądy zgodności przetwarzania informacji z obowiązującymi uregulowaniami i standardami. W przypadku wykrycia niezgodności:
1) określa się przyczyny niezgodności,
2) ocenia się potrzebę podjęcia działań zapewniających, że niezgodność nie wystąpi ponownie,
3) określa się i wprowadza odpowiednie działania korygujące,
4) poddaje się przeglądowi podjęte działania korygujące i ich efekty.
Prowadzenie przeglądów oraz wnioski z nich płynące są dokumentowane i ewidencjonowane.

15. Bezpieczeństwo danych osobowych

Dane osobowe są kategorią danych podlegających ochronie. W Urzędzie przykłada się szczególną wagę do bezpieczeństwa przetwarzania danych osobowych.

W zakresie przetwarzania danych osobowych obowiązują uregulowania PBPDU, chyba że odrębne uregulowania (np. prawne) nakładają obowiązek stosowania dalej idącej ochrony – wówczas zastosowanie mają te uregulowania.

Przy przetwarzaniu danych osobowych stosuje się dodatkowo uregulowania następujących kwestii:

1) Wymogi prawne,

2) Dopuszczenie do przetwarzania danych osobowych,

3) Ewidencja upoważnionych do przetwarzania danych osobowych,

4) Powierzanie przetwarzania danych osobowych,

16. Przeglądy Polityki i audyty systemu bezpieczeństwa

W celu utrzymania odpowiedniego, wysokiego poziomu bezpieczeństwa informacji w Urzędzie dokonuje się regularnych przeglądów niniejszej Polityki i ewentualnie audytów systemu bezpieczeństwa informacyjnego Urzędu.

Przeglądu dokonuje się nie rzadziej niż jeden raz w ciągu roku. IOD koordynuje realizację przeglądów i w zależności od potrzeb zaleca ich wykonanie wewnątrz Urzędu lub na zewnątrz. Przeprowadzenie przeglądu bądź audytu jest dokumentowane w formie protokołu lub raportu, który dołącza się do dokumentacji związanej z bezpieczeństwem i ochroną danych.

Ponadto prowadzi się dodatkowe przeglądy Polityki bezpieczeństwa i stosowanych zabezpieczeń w sytuacji, gdy nastąpiły znaczące zmiany mogące wpływać na system bezpieczeństwa. W szczególności dotyczy to sytuacji:

- przekazania do eksploatacji nowego, kluczowego systemu informatycznego,
- znaczących zmian organizacyjnych w funkcjonowaniu Urzędu,
- zmian w obowiązującym prawie.

Polityka wprowadzana jest do użytku Zarządzeniem Burmistrza i przekazywana jest do wiadomości wszystkich pracowników.