Załącznik nr 1 do
Zarządzenia Nr 286/17 Burmistrza Czarnej Białostockiej
z dnia 22 listopada 2017 r.

Polityka bezpieczeństwa informacji
w Urzędzie Miejskim w Czarnej Białostockiej

Spis treści:

1. Definicje

Bezpieczeństwo Informacji - zapewnienie podstawowych usług ochrony informacji (tj. poufności, integralności i dostępności) informacjom przetwarzanym przez Urząd,

Poufność – właściwość polegająca na zapewnieniu dostępu do informacji tylko osobom do tego upoważnionym,

Integralność –, właściwość zapewniająca, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
Dostępność – zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów zawsze wtedy, gdy jest to potrzebne,

Incydent – zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji ,które stwarzają ryzyko zakłócenia funkcjonowania Urzędu i zagrażają bezpieczeństwu informacji,

Ryzyko – jest zbiorczą miarą prawdopodobieństwa i wagi sytuacji, w której dane zagrożenie wykorzystuje określoną słabość , powodując stratę lub uszkodzenie aktywów systemu, a zatem pośrednią lub bezpośrednią szkodę dla organizacji

Rozliczalność – właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,

System informatyczny – zespół współpracujących urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,

Polityka Bezpieczeństwa Informacji (PBI) –Polityka Bezpieczeństwa Informacji w Urzędzie Miejskim w Czarnej Białostockiej'

Aktywa – zasoby informacyjne, zdefiniowane jako mające wartość dla organizacji i podlegające ochronie,
ABI - Administrator Bezpieczeństwa Informacji,

SZBI – System Zarządzania Bezpieczeństwem Informacji w Urzędzie Miejskim w Czarnej Białostockiej, część całościowego systemu zarzadzania, na który składa się zbiór dokumentów odnoszących się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji

Urząd – Urząd Miasta w Czarnej Białostockiej

2 .Wstęp

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, między innymi, efektywnego dostępu do informacji oraz zapewnienia odpowiedniego poziomu bezpieczeństwa informacji. Utrata poufności, integralności, dostępności, autentyczności lub niezawodności 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 oraz funkcje oprogramowania i sprzętu.

Polityka bezpieczeństwa informacji jest zbiorem zasad i procedur, którym muszą podporządkować się osoby posiadające dostęp do zasobów informacyjnych. Określa również zasady ochrony infrastruktury, zasobów informatycznych i ludzkich

3. Cel polityki bezpieczeństwa informacji

1. Celem Polityki Bezpieczeństwa Informacji jest określenie zasad przetwarzania informacji będących w zasobach Urzędu Miejskiego w Czarnej Białostockiej w celu zapewnienia im właściwej ochrony w sposób zapewniający odpowiedni poziom bezpieczeństwa, zgodnie z obowiązującymi przepisami prawa oraz stworzenie podstaw do wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).
2. Wdrożenie Polityki Bezpieczeństwa Informacji polega na opracowaniu i wprowadzeniu zasad bezpieczeństwa informacji w Urzędzie zgodnie z wytycznymi zawartymi w niniejszym dokumencie, procedurami operacyjnymi i narzędziami wspierającymi funkcjonowanie SZBI, zgodnie z wymaganiami normy PN-ISO/IEC 27001:2014.

4. Zakres obowiązywania

1. Polityka Bezpieczeństwa Informacji obejmuje systemy informatyczne i infrastrukturę teleinformatyczną Urzędu, przetwarzanie dokumentów papierowych, archiwizację informacji na dowolnych nośnikach.
2. PBI obejmuje swym zakresem Urząd Miejski w Czarnej Białostockiej
3. Niniejszy dokument nie dotyczy innych jednostek podległych Urzędowi Miasta i Gminy takich jak: oświata, pomoc społeczna, etc.
4. Do przestrzegania zapisów PBI zobowiązani są wszyscy pracownicy Urzędu, zgodnie z zasadami ochrony dostępnych i/lub powierzonych im aktywów.
5. W celu zapewnienia jak najwyższego poziomu bezpieczeństwa informacji, będącej w posiadaniu lub przetwarzaniu przez Urząd, do zasad wynikających z Polityki Bezpieczeństwa Informacji powinni również stosować się wszyscy dostawcy, audytorzy i konsultanci, którzy mają dostęp do informacji, dokumentów papierowych oraz zasobów i systemów informatycznych. Obowiązki odnoście podmiotów zewnętrznych wynikające z Polityki Bezpieczeństwa Informacji zostały przedstawione w paragrafie 8 „Zasady współpracy z osobami trzecimi i stronami zewnętrznymi”.

6. Zawarte w niniejszej Polityce zapisy są oparte na wytycznych zawartych w normie PN-ISO/IEC 27001:2014.

5. Deklaracja Kierownictwa.

1. Z punktu widzenia działalności Urzędu informacja jest cennym aktywem mającym wpływ na utrzymanie zgodności z obowiązującym prawem, możliwości prowadzenia powierzonych zadań oraz dobrego wizerunku zarówno Gminy jak i Urzędu.
2. Burmistrz Czarnej Białostockiej będąc świadomym istniejących zagrożeń i ryzyka związanego z tworzeniem, przechowywaniem, przetwarzaniem i przesyłaniem informacji w tym Danych Osobowych podjął decyzje o wdrożeniu Systemu Zarządzania Bezpieczeństwem Informacji i zobowiązuje się do :
    1) zapewnienia ,że informacje przetwarzane w Urzędzie będą chronione, tak aby była zapewniona ich poufność, integralność, dostępność i rozliczalność oraz przetwarzane w sposób adekwatny do ich klasyfikacji,
    2) opieraniu się na wynikach procesu zarządzania ryzykiem bezpieczeństwa informacji przy w prowadzaniu zmian w procesach przetwarzania informacji oraz podejmowaniu decyzji o wdrażaniu mechanizmów kontrolnych,
    3) zabezpieczania infrastruktury informatycznej odpowiednio do zidentyfikowanego ryzyka,
    4) zapewnienia koniecznych zasobów materialnych , osobowych i informacyjnych, które są niezbędne do skutecznego funkcjonowania SZBI,
    5) zaangażowania wszystkich pracowników Urzędu w ochronę informacji oraz ciągłego podnoszenia ich świadomości o zagrożeniach związanych z ich bezpieczeństwem ,
    6) ciągłego doskonalenia Systemu,
    7) zapewnienia bieżącego funkcjonowania zasad bezpieczeństwa informacji w codziennej pracy Urzędu.
3. Niniejsza Polityka Bezpieczeństwa Informacji jest adresowana do wszystkich pracowników Urzędu.
4. Polityka Bezpieczeństwa Informacji jest kluczowym elementem Systemu Zarządzania Bezpieczeństwem Informacji

6. Cele Systemu Zarządzania Bezpieczeństwem Informacji

Głównymi celami stawianymi przed SZBI są:

1) zapewnienie zgodności działań z obowiązującymi wymaganiami prawnymi dotyczącymi ochrony informacji,

2) ochrona systemów przetwarzania informacji przed nieuprawnionym dostępem, atakami , błędami, awariami ,działaniami sił natury,
3) zapewnienie poufności, integralności, dostępności i rozliczalności informacji,
4) zapewnienie aktywom należytej ochrony w celu minimalizowania strat i ograniczaniu ryzyka,
5) zapewnienie skutecznej i bezzwłocznej reakcji na wypadek wystąpienia wszelkiego rodzaju incydentów bezpieczeństwa informacji,
6) uświadomienie pracownikom możliwych zagrożeń bezpieczeństwa informacji w celu przestrzegania zasad bezpieczeństwa i stosowania niezbędnych zabezpieczeń,
7) przekazanie pracownikom wiedzy dotyczącej procesu przetwarzania informacji w Urzędzie , w szczególności w zakresie utrzymania zgodności z wymaganiami rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowym Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2012 r. poz.526, z 2014 r. poz.1671), normy PN-ISO/IEC 27001.
8) zaangażowanie wszystkich pracowników Urzędu w ochronę informacji.

7. Zakres Systemu Bezpieczeństwa Informacji

System Zarządzania Bezpieczeństwem Informacji w Urzędzie Miejskim jest elementem sytemu zarządzania i odnosi się do ustanawiania, wdrażania ,eksploatacji, monitorowania,, utrzymywania, i doskonalenia bezpieczeństwa informacji. SZBI został opracowany, wdrożony i utrzymywany w oparciu o normę PN-ISO/IEC 27001:2007.
Zakres SZBI ma zastosowanie do całego systemu informacyjnego Urzędu Miejskiego w Czarnej Białostockiej a w szczególności dotyczy następujących grup zasobów:

1) wszystkich istniejących , wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są informacje podlegające ochronie z wyjątkiem systemów w których przetwarzane są informacje niejawne ;
2) wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy , stażystów , a także innych osób mających dostęp do informacji podlegających ochronie (np. pracowników firm zewnętrznych realizujących prace na rzecz Urzędu);
3) informacji będących własnością Urzędu Miejskiego oraz będących własnością klientów , które zostały uzyskane na podstawie zawartych umów;
4) infrastruktura – wszystkie zasoby sprzętowe takie jak: łącza teleinformatyczne , przyłącza internetowe, infrastruktura energetyczna, budynki, pomieszczenia z infrastrukturą wspomagającą oraz inne zasoby istotne z punktu widzenia wymagań bezpieczeństwa informacji ;
5) sprzęt i oprogramowanie informatyczne takie jak: komputery stacjonarne i przenośne, serwery , urządzenia sieciowe, systemy operacyjne, aplikacje ,licencje oraz inne urządzenia elektroniczne lub systemy przechowujące, przetwarzające, przesyłające lub prezentujące informacje;

8. Organizacja Bezpieczeństwa Informacji

1. W Urzędzie odpowiedzialność za bezpieczeństwo informacji ponoszą wszyscy pracownicy przetwarzający informacje, zgodnie z posiadanymi zakresami obowiązków.
2. Szczególne role w funkcjonowaniu SZBI pełnią:
    1) Burmistrz Czarnej Białostockiej w zakresie ustalania celów i zakresu SZBI, zatwierdzania zmian organizacyjnych i budżetu związanego z funkcjonowaniem SZBI, zatwierdzania dokumentacji SZBI w tym wyników analizy ryzyka i planów postępowania z ryzykiem oraz przeglądów SZBI i wyników audytów;
    2) Pełnomocnik ds. Bezpieczeństwa Informacji ponosi odpowiedzialność za przeprowadzenie oceny ryzyka i przygotowanie sprawozdania podsumowującego wyniki oceny ryzyka, przewodniczy spotkaniom Zespołu ds. monitorowania bezpieczeństwa informacji , podejmuje decyzje związane z incydentami bezpieczeństwa informacji;
    3) Sekretarz opiniuje zmiany w treści dokumentów SZBI pod kątem zgodności z wymaganiami wewnętrznymi Urzędu, zapewnia potrzebne zasoby w zakresie funkcjonowania Urzędu.
    4) Administrator Bezpieczeństwa Informacji /Inspektor Bezpieczeństwa Informacji odpowiada za nadzór nad przestrzeganiem zasad ochrony przetwarzanych danych osobowych oraz za opracowanie i aktualizacje dokumentacji przetwarzania tych danych;
    5) Informatyk pełniący funkcje Administratora Systemów Informatycznych odpowiada za funkcjonowanie systemów i sieci teleinformatycznej , realizację zadań związanych z zarządzaniem systemem informatycznym Urzędu w tym za zabezpieczenie sieci komputerowej w celu zabezpieczenia danych przed nieuprawniona modyfikacją , zniszczeniem, dostępem i ujawnieniem a także utratą, opracowanie , aktualizację procedur lub instrukcji systemów;
    6) Zespół ds. monitorowania bezpieczeństwa informacji - odpowiada za monitorowanie funkcjonowania mechanizmów bezpieczeństwa informacji, właściwe postępowanie z incydentami, dokonywanie przeglądu naruszeń bezpieczeństwa informacji , dokonywanie corocznych przeglądów PBI i SZBI i opracowywanie zmian w stosownych dokumentach, procedurach, infrastrukturze technicznej, podejmowanie przedsięwzięć zmierzających do podniesienia poziomu bezpieczeństwa informacji. Zespół powoływany jest zarządzeniem Burmistrza.
    7) Kierownicy komórek organizacyjnych Urzędu , którzy wykonują zadania takie, jak udział w procesie zarządzania ryzykiem w zakresie nadzoru zadań realizowanych w podległych komórkach, nadzoru nad przestrzeganiem zasad SZBI przez podwładnych, udział w spotkaniach Zespołu ds. monitorowania bezpieczeństwa informacji w charakterze doradczym , nadzór nad uprawnieniami podległych pracowników

3. Dostawcy są zobowiązani do przestrzegania przepisów prawa, zasad bezpieczeństwa wynikających z umów oraz umożliwienia prowadzenia kontroli w zakresie dotyczącym bezpieczeństwa informacji w ramach świadczonych usług

9. Zasady bezpieczeństwa

1. System Zarządzania Bezpieczeństwem Informacji powinien zapewnić wprowadzenie i stosowanie niżej wymienionych podstawowych zasad bezpieczeństwa informacji:
    1) zasada poufności , polegająca na tym, że informacje stanowiące tajemnicę Urzędu w tym dane osobowe oraz dane techniczne dotyczące infrastruktury informatycznej i jej zabezpieczenia, nie mogą być przekazywane nieupoważnionym osobom;
    2) zasada wiedzy koniecznej , polegająca na tym, że pracownik Urzędu posiada dostęp tylko do informacji , których zakres jest ograniczony do potrzeb wynikających z wykonywanych zadań służbowych ;
    3) zasada rozliczalności polegająca na zapewnieniu jednoznacznej odpowiedzialności pracowników za powierzone im zasoby w celu wykonywania zadań służbowych w ramach usług świadczonych przez Urząd; wszyscy użytkownicy zasobów informacyjnych ponoszą odpowiedzialność za wykonywanie swoich obowiązków w sposób niezgodny z zachowaniem bezpieczeństwa informacji;
    4) zasada czystego biurka - polegająca na unikaniu pozostawiania dokumentów na biurku bez nadzoru . Po zakończeniu pracy należy uprzątnąć biurko z dokumentów papierowych oraz informatycznych nośników danych. Dokumenty i nośniki powinny być przechowywane w zamykanych szafach .
    5) zasada czystego ekranu – polegająca na blokowania komputera i terminala pozostawionego bez opieki lub czasowo nieużywanego za pomocą mechanizmu blokowania ekranu i klawiatury kontrolowanego hasłem, tokenem lub innym podobnym mechanizmem. Po zakończonym dniu pracy komputer powinien być wyłączony.

2. Zarządzanie bezpieczeństwem informacji jest procesem obejmującym dokonywanie analiz zmian w wymaganiach bezpieczeństwa , wdrażanie zabezpieczeń zgodnie z wynikami analizy ryzyka, przestrzegania przyjętych harmonogramów czynności zapewniających funkcjonowanie systemu, nadzorowanie stosowania mechanizmów kontrolnych wdrażanych w wyniku rekomendacji audytowych i przeglądów SZBI.
3. Bezpieczeństwo informacji zapewnia się poprzez implementacje zasad bezpieczeństwa w procesy realizowane w Urzędzie oraz przez prawidłowe wykonywanie zadań w zakresie bezpieczeństwa przez właścicieli informacji, osoby funkcyjne , administratorów systemów informatycznych oraz bezpośrednich użytkowników przetwarzających informacje.
4. Dostęp pracownika do systemów informatycznych i informacyjnych powinien być nadawany z uwzględnieniem wiedzy koniecznej za zgodą i na wniosek właściwych kierowników komórek organizacyjnych Urzędu, w sposób zapewniający monitorowanie dostępu i rozliczalność .
5. Dostęp do budynków, oraz pomieszczeń w tym w szczególności do pomieszczeń specjalnie chronionych powinien być nadzorowany, rejestrowany i umożliwiający udokumentowane wyjaśnianie ewentualnych incydentów.

6. Właściwy poziom bezpieczeństwa fizycznego i środowiskowego obiektów Urzędu powinien być zapewniony zgodnie z wymaganiami prawa oraz wymaganiami technicznymi dla pomieszczeń specjalnych.
7. Zasady eksploatacji i utrzymania systemów informatycznych powinny być zgodne z wymaganiami określonymi w Rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowym Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2012 r. poz.526, z 2014 r. poz.1671) oraz zaleceniami normy PN-ISO/IEC 27001:2014.
8. Bezpieczeństwo systemów informatycznych powinno być zapewnione poprzez bieżące analizowanie bezpieczeństwa infrastruktury teleinformatycznej i bezzwłocznym wdrażaniu niezbędnych poprawek .
9. Współpraca z dostawcami powinna być oparta na umowie , która musi zawierć zapisy o poufności i w przypadkach uzasadnionych , umowie powierzenia przetwarzania danych osobowych. Umowa powinna zapewniać przetwarzanie informacji zgodnie z niniejszą Polityką oraz umożliwiać przeprowadzanie kontroli bezpieczeństwa informacji na zgodność z wymaganiami.

10. Zarządzanie ryzykiem

1. Jednym z kluczowych elementów SZBI jest prowadzenie regularnej oceny ryzyka w zakresie bezpieczeństwa informacji i przetwarzających ją systemów. Na tej podstawie opracowuje się plany postępowania z ryzykiem, w celu ograniczenia ich do poziomu akceptowalnego przez kierownictwo Urzędu.

2. Zarządzanie ryzykiem bezpieczeństwa informacji odnosi się do obszaru bezpieczeństwa informacji przetwarzanych w systemach informatycznych. Uwzględnia też w szczególności ryzyka związane z podatnościami teleinformatycznymi. Metodykę i zasady zarządzania ryzykiem w Urzędzie określa „Procedura zarządzania ryzykiem w bezpieczeństwie informacji” stanowiąca załącznik nr 3 do Polityki Bezpieczeństwa .

3. Analiza ryzyka w obszarze bezpieczeństwa informacji wykonywana jest przez kierowników referatów w ramach prowadzonej w Urzędzie kontroli zarządczej, którzy powinni uwzględnić zagrożenia związane z bezpieczeństwem informacji. jako element ochrony zasobów.

4. Analiza ryzyka dokonywana jest przez kierowników referatów w odniesieniu do zasobów informacyjnych . których są właścicielami . Szacowania i oceny ryzyka na podstawie sporządzonych analiz dokonuje Zespół ds. monitorowania bezpieczeństwa informacji, który analizuje wyniki i wyciąga wnioski z wykrytych słabości, incydentów i wyjątków , sporządza sprawozdanie podsumowujące wyniki oceny ryzyka oraz rekomenduje decyzje dotyczące rozwoju SZBI.

11. Zasady współpracy z osobami trzecimi i stronami zewnętrznymi

W Urzędzie Miejskim w Czarnej Białostockiej bezpieczeństwo fizyczne zapewnia się poprzez wyodrębnienie obszarów , które są niedostępne dla klientów i pracowników podmiotów zewnętrznych z uwagi na przetwarzane informacje bądź funkcje techniczne . Są

one chronione systemem kontroli dostępu i systemem alarmowym. W przypadku konieczności ich udostępnienia w celu wykonywania prac zleconych na terenie Urzędu, w umowach stosować klauzule dotyczące zachowania poufności a przetwarzane tam informacje zabezpieczyć przed nieuprawnionym dostępem. W sytuacji gdy niezbędne jest udostępnienie danych osobowych podmiotowi zewnętrznemu konieczne jest zawieranie umów powierzenia. Celem takiego postępowania jest zapewnienie bezpieczeństwa informacji przed dostępem osób niepowołanych, uszkodzeniem lub innymi zakłóceniami w obiektach Urzędu Miejskiego. Z uwagi na obsługę większości interesantów w Kancelarii , Kasie , Referacie Spraw Obywatelskich i Urzędu Stanu Cywilnego na parterze budynku, nie mają oni uzasadnionej potrzeby poruszania się po innych obszarach. Ciągi komunikacyjne pozostają pod stałym nadzorem zainstalowanego systemu monitoringu wizyjnego.

12. Utrzymanie odpowiedniego poziomu bezpieczeństwa informacji.

1. Niezbędną praktyką po wdrożeniu mechanizmów ochrony informacji jest monitorowanie zagrożeń i zabezpieczeń, systematyczna weryfikacja i aktualizacja dokumentów Polityki Bezpieczeństwa Informacji i stosowanych zabezpieczeń. Nakłady ponoszone na zabezpieczenia muszą być poprzedzone analizą ryzyka i kosztów, adekwatnie do potencjalnych strat spowodowanych naruszeniem bezpieczeństwa. Zadaniem Polityki Bezpieczeństwa Informacji jest zmniejszenie ryzyka płynącego z zagrożeń do akceptowalnego poziomu, to znaczy:
    - zapobieganie przypadkom naruszenia bezpieczeństwa zasobów informacyjnych Urzędu,
    - zminimalizowanie możliwości takiego naruszenia bezpieczeństwa
    - umożliwienie wczesnego jego wykrycia,
    - zminimalizowanie strat związanych z takim naruszeniem oraz sprawne usunięcie jego skutków.
    - zminimalizowanie strat związanych z takim naruszeniem oraz sprawne usunięcie jego skutków.
    - zminimalizowanie strat związanych z takim naruszeniem oraz sprawne usunięcie jego skutków.

2. System Zarządzania Bezpieczeństwem Informacji wprowadzony w Urzędzie uwzględnia procesy utrzymania odpowiedniego poziomu bezpieczeństwa w tym:

    1) Zarządzanie ryzykiem.
    2) Zarządzania dostępem do zasobów.
    3) Monitorowania poziomu bezpieczeństwa
    4) Zarządzania incydentem
    5) Nadzoru nad dokumentacją Systemu Zarządzania Bezpieczeństwem Informacji

3. Dla utrzymania odpowiedniego poziomu bezpieczeństwa informacji istotne jest:
    - systematyczne szkolenie oraz podnoszenie kwalifikacji zawodowych pracowników (w szczególności dotyczy to informatyków).
    - Prowadzenie przez Administratora systemu informatycznego szkoleń

wewnętrznych doskonalących praktyczne umiejętności z zakresu bezpieczeństwa informacji (ochrona antywirusowa, szyfrowanie informacji)

- okresowe wykonywanie przeglądów Polityki Bezpieczeństwa Informacji
- przeprowadzanie audytów bezpieczeństwa informacji.

13. Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji

1. Dokumentacja Systemu Zarządzania Bezpieczeństwem informacji składa się z czterech głównych elementów. Są nimi:

1) Polityka Bezpieczeństwa Informacji w Urzędzie Miejskim w Czarnej Białostockiej;
2) Deklaracja Stosowania - dokument zawierający wzorcowy wykaz celów stosowania zabezpieczeń i zabezpieczenia, zgodnie z ISO/IEC 27001:2014.
3) Procedury i instrukcje bezpieczeństwa, które szczegółowo określają zasady postępowania;
4) Raporty z analizy ryzyka i plany postępowania ryzykiem.

Uzupełnieniem dokumentacji SZBI są wprowadzone zarządzeniami Burmistrza i wdrożone w Urzędzie: : Polityka Bezpieczeństwa Przetwarzania Danych Osobowych, Instrukcja Zarządzania Systemem Informatycznym Służącym Do Przetwarzania Danych Osobowych Urzędu, Regulamin funkcjonowania monitoringu wizyjnego w budynku Urzędu Miejskiego w Czarnej Białostockiej, Instrukcja w sprawie określenia procedury postępowania z kluczami oraz zabezpieczenia pomieszczeń w Urzędzie Miejskim w Czarnej Białostockiej, Regulamin określający zasady i procedury korzystania z oprogramowania, sprzętu komputerowego i sieci komputerowej oraz poczty elektronicznej w Urzędzie Miejskim w Czarnej Białostockiej, Procedura nadawania uprawnień do potwierdzania, przedłużania ważności i unieważniania profili zaufanych ePUAP w Urzędzie Miejskim w Czarnej Białostockiej, Regulamin Kontroli Zarządczej.

2. Procedury, instrukcje i polityki regulują szczegółowe zasady korzystania z zasobów informacyjnych, a także użytkowania systemów informatycznych. Są to następujące dokumenty:

1) Polityka Kontroli Dostępu do Informacji - załącznik nr 1 -zawiera zasady kontroli dostępu do informacji w Urzędzie, a w szczególności zapewniania dostępu uprawnionymi użytkownikom i zapobiegania nieuprawnionemu dostępowi, zarządzania uprawnieniami i przywilejami, loginami i hasłami, kontroli dostępu do sieci, w tym zdalnego dostępu spoza Urzędu oraz postępowania ze sprzętem przenośnym;

2) Polityka Tworzenia Kopii Zapasowych - załącznik nr 2 - Określa zasady tworzenia, przechowywania i testowania kopii zapasowych danych;

3) Procedura zarządzania ryzykiem w bezpieczeństwie informacji –załącznik nr 3 – określa metodykę i zasady zarządzania ryzykiem w Urzędzie;

4) Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji - załącznik nr 4- określa zasady postępowania z incydentami bezpieczeństwa informacji, zgłaszania zdarzeń, zgłaszania słabości systemu bezpieczeństwa, odpowiedniego reagowania na incydenty, analizy przyczyn, podejmowania działań naprawczych, wyciągania wniosków z incydentów i gromadzenia materiału dowodowego;
5) Ewidencja i klasyfikacja systemów informatycznych - załącznik nr 5 - Określa zasady ewidencjonowania i klasyfikowania systemów informatycznych;
6) Instrukcja w zakresie profilaktyki antywirusowej - załącznik nr 6 -określa zasady ochrony przed wirusami i innym złośliwym kodem;
7) Procedura postępowania z nośnikami wymiennymi – załącznik nr 7
8) Procedura świadczenia usług przez firmy zewnętrzne – załącznik nr 8
9) Polityka czystego biurka i ekranu- załącznik nr 9
10) Plan ciągłości działania - załącznik nr 10

14. Dobór zabezpieczeń

Urząd dobiera cele stosowania zabezpieczeń i zabezpieczenia odpowiednio do wymagań prawnych i wyników analizy ryzyka dla bezpieczeństwa informacji. Zabezpieczenia fizyczne, techniczne i organizacyjne powinny uzupełniać się wzajemnie zapewniając wspólnie wymagany poziom bezpieczeństwa informacji. W doborze celów stosowania zabezpieczeń i zabezpieczeń należy kierować się zaleceniami Polskiej Normy PN-ISO/IEC 17799.

15. Sankcje za naruszenie zasad bezpieczeństwa informacji.

Nieprzestrzeganie zasad zawartych w dokumentach Polityki Bezpieczeństwa Informacji Urzędu, jest naruszeniem obowiązków pracowniczych wynikających w szczególności z ustaw o służbie cywilnej, o pracownikach urzędów państwowych 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 karnej wynikającej z przepisów:

- ustawy o ochronie danych osobowych
- kodeksu karnego dot. przestępstw przeciwko ochronie informacji
- przepisów chroniących tajemnice zawodowe.

16. Zasady rozpowszechniania dokumentu oraz tryb wprowadzania zmian.

Do zapoznania się z Polityką Bezpieczeństwa Informacji Urzędu i dokumentami związanymi zobligowana jest kadra kierownicza oraz wszyscy pracownicy. Niniejszy dokument winien

być udostępniony również uprawnionym podmiotom zewnętrznym w celu zapoznania się i postępowania w zgodzie z postanowieniami niniejszego dokumentu.

Komórka odpowiedzialna za sprawy kadrowe przekazuje, do zapoznania się, nowo zatrudnionym pracownikom oraz stażystom i praktykantom Politykę Bezpieczeństwa Informacji 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/w dokumentach.

Dokumentacja PBI powinna być przeglądana i weryfikowana:

- 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 dotyczących bezpieczeństwa informacji
- w przypadku poważnych modyfikacji infrastruktury teleinformatycznej
- w przypadku zawarcia umów, z których wynikają zobowiązania związane z bezpieczeństwem informacji
- w przypadku istotnych zmian organizacyjnych w Urzędzie,
- okresowo, nie rzadziej niż raz w roku

Zmiany w dokumentach wprowadza Zespół ds. monitorowania bezpieczeństwa informacji na podstawie okresowych przeglądów. Zmieniony dokument zatwierdza Burmistrz Czarnej Białostockiej i wprowadza w drodze zarządzenia.

17.Przepisy prawne i polskie normy.

W Urzędzie informacje podlegają ochronie zgodnie z następującymi wymogami prawa:

1. Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz. U. z 2016 r., poz.922),
2. Ustawą o ochronie informacji niejawnych z dnia 5 sierpnia 2010 r. (Dz. U. z 2016 r., poz..1167, z 2017 r poz. 935),
3. Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (j.t. Dz. U. z 2016 r., poz. 1764),
4. Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym (j.t. Dz. U. z 2013 r., poz. 262),
5. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (tekst jednolity Dz. U. z 2017 r., poz. 570),
6. Ustawa z dnia 21 listopada 2008r o służbie cywilnej (tekst jednolity Dz.U. z 2016 r., poz.1345),
7. Ustawa z dnia 21 listopada 2008 r. o pracownikach samorządowych (Dz.U. z 2016 r., poz. 902),
8. Ustawa z dnia 26 czerwca 1974 r. - Kodeks pracy (. Dz. U. z 2016 r., poz.1666),
9. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia

2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r., Nr 100, poz. 1024).

10. Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. z 2011 r., Nr 159, poz. 948)
11. Rozporządzenie Rady Ministrów z dnia 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 (tekst jednolity Dz. U. z 2016 r., poz. 113)

Podstawą normalizacyjną dokumentu Polityki Bezpieczeństwa Informacji są niżej wymienione polskie normy:

PN ISO/IEC 27001:2007 Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji-Wymagania.

PN ISO/IEC 27005 Technika informatyczna - Techniki bezpieczeństwa - Zarządzanie ryzykiem w bezpieczeństwie informacji.

PN-ISO/IEC 17799:2007 Technika informatyczna - Techniki bezpieczeństwa - Praktyczne zasady zarządzania bezpieczeństwem informacji