

**ZARZĄDZENIE NR 211/2016
PREZYDENTA MIASTA SUWAŁK**

z dnia *30. września* 2016 r.

w sprawie ustanowienia Systemu Zarządzania Bezpieczeństwem Informacji oraz Polityki Bezpieczeństwa Informacji Urzędu Miejskiego w Suwałkach.

Na podstawie art. 30 ust.1 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz.U. z 2016 r. poz. 446,) w związku 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 (t.j. Dz. U. z 2016 r. poz. 113) zarządzam, co następuje:

§ 1. Ustanawiam System Zarządzania Bezpieczeństwem Informacji oraz Politykę Bezpieczeństwa Informacji Urzędu Miejskiego w Suwałkach w brzmieniu określonym w załączniku nr 1 do zarządzenia.

§ 2. Wykonanie zarządzenia powierzam Sekretarzowi Urzędu, Naczelnikom Wydziałów, Kierownikom równorzędnych komórek organizacyjnych Urzędu Miejskiego w Suwałkach.

§ 3. Zarządzenie wchodzi w życie z dniem podpisania.

PREZYDENT
Czesław Rezkiewicz

*Załącznik do Zarządzenia Nr 211/2016
z dnia 30 czerwca 2016*

System Zarządzania Bezpieczeństwem Informacji

Urzędu Miejskiego w Suwałkach

Deklaracja

1. Kierownictwo Urzędu zapewnia zaangażowanie w odniesieniu do Systemu Zarządzania Bezpieczeństwem Informacji poprzez:
 - 1) zapewnienie, że Polityka Bezpieczeństwa Informacji oraz cele bezpieczeństwa informacji są ustanowione i zgodne z potrzebami właściwego funkcjonowania Urzędu;
 - 2) zapewnienie dostępności zasobów potrzebnych w Systemie Zarządzania Bezpieczeństwem Informacji;
 - 3) zapewnienie, że System Zarządzania Bezpieczeństwem Informacji osiągnie zamierzony wynik;
 - 4) kierowanie i wspieranie osób przyczyniających się do osiągnięcia skuteczności Systemu Zarządzania Bezpieczeństwem Informacji;
 - 5) promowanie ciągłego doskonalenia;
 - 6) podnoszenia świadomości pracowników Urzędu o zagrożeniach związanych z bezpieczeństwem informacji.
2. W celu ochrony informacji, minimalizacji ryzyka i przeciwdziałaniu zagrożeniom ustanawia się **Politykę Bezpieczeństwa Informacji**.
3. Zasady, działania, kompetencje i zakresy odpowiedzialności opisane w dokumentach Polityki Bezpieczeństwa Informacji obowiązują **wszystkich pracowników Urzędu Miejskiego w Suwałkach**.
4. Zobowiązuję się do spełnienia wymagań dotyczących bezpieczeństwa informacji, podejmowania wszelkich niezbędnych działań zmierzających do ciągłego doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji.

Prezydent Miasta Suwałk
Czesław Renkiewicz

Polityka Bezpieczeństwa Informacji

Urzędu Miejskiego w Suwałkach

§1.

Cel Polityki

1. Polityka Bezpieczeństwa Informacji, zwana dalej PBI ma na celu zapewnienie bezpieczeństwa informacji przetwarzanej w Urzędzie i umożliwienie działania zgodne z wymaganiami prawa, normami nadzorczymi.
2. Niniejszy dokument wyraża również zaangażowanie kierownictwa Urzędu w zakresie utrzymania odpowiedniego poziomu bezpieczeństwa informacji oraz określa podstawowe cele i strategię w tym obszarze.
3. Kierownictwo Urzędu aktywnie wspiera zapewnienie bezpieczeństwa informacji w całej organizacji wskazując kierunki działania oraz przyjmując odpowiedzialność w zakresie bezpieczeństwa informacji.

§ 2.

Zakres PBI

1. Niniejsza PBI określa podstawowe zasady, normy i wymagania zgodności w zakresie bezpieczeństwa informacji przetwarzanej w urzędzie. Dotyczy wszystkich pracowników Urzędu, a także innych osób mających dostęp do chronionych informacji (np. pracowników firm zewnętrznych realizujących prace w urzędzie).
2. Dokument ma zastosowanie do wszystkich informacji chronionych niezależnie od formy, w jakiej są przechowywane (papierowej, elektronicznej i innej) z wyjątkiem informacji niejawnych. Obszar ochrony informacji niejawnych posiada własne regulacje prawne i stosowne mechanizmy ochronne oraz struktury organizacyjne dedykowane do ochrony informacji niejawnych wytwarzanych, przetwarzanych oraz przechowywanych w wydzielonych systemach teleinformatycznych.
3. Niniejszy dokument został opracowany w oparciu o najlepsze praktyki z obszaru bezpieczeństwa informacji oraz z wymaganiami normy PN-ISO/IEC 27001:2014-12.
4. Niniejsza PBI jest częścią Systemu Zarządzania Bezpieczeństwem Informacji 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 (t.j. Dz. U. z 2016 r. poz. 113).

§ 3.

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. (t.j. Dz. U. z 2016 r., poz. 922).
2. Ustawą o ochronie informacji niejawnych z dnia 5 sierpnia 2010 r. (Dz. U. z 2010 r. Nr 182 poz. 1228 z późn. zm.).
3. Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (t.j. Dz. U. z 2015 r. poz. 2058 z późn. zm.).
4. Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym (t.j. Dz. U. z 2013 r. poz. 262 z późn. zm.).
5. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (j.t. Dz. U. z 2014 r., poz. 1114 z późn. zm.).
6. Ustawa z dnia 26 czerwca 1974 r. - Kodeks pracy (t.j. Dz. U. z 2014 r. poz. 1502 z późn. zm.).
7. 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).
8. 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).
9. 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 (t.j. Dz. U. z 2016 r. poz. 113).
10. Rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 1 grudnia 1998 r. w sprawie bezpieczeństwa i higieny pracy na stanowiskach wyposażonych w monitory ekranowe (Dz. U. z 1998 r., Nr 148, poz. 973).

§ 4 .

Struktura i zakres regulacji wewnętrznych w zakresie bezpieczeństwa informacji

Za dokumenty związane z niniejszą PBI będą uznawane wszystkie dokumenty niższych poziomów takie jak polityki, procedury, instrukcje, zasady i regulaminy wymienione w Załączniku nr 1 do PBI, a także dokumentacja Systemu Zarządzana Bezpieczeństwem Informacji powstała w wyniku stosowania regulacji wymienionych w Załączniku nr 1.

§ 5.

Przeglądy PBI

1. Niniejsza PBI podlega przeglądom zarządczym i weryfikacji zgodnie z odpowiednimi regulacjami wewnętrznymi dotyczącymi przeglądów zarządczych w Urzędzie.
2. Przeglądy powinny być dokonywane co najmniej raz do roku lub też w trakcie roku w przypadku wystąpienia znaczących zmian, powinny obejmować weryfikację zasad i ewentualne dostosowanie PBI do zmieniającego się profilu ryzyka Urzędu, zmian środowiska organizacyjnego, warunków biznesowych, środowiska technicznego, a także w zakresie zachowania zgodności z przepisami prawa i normami nadzorczymi.
3. Wszelkie zmiany w niniejszej PBI przyjmowane są zarządzeniami Prezydenta Miasta.

§ 6.

Terminologia

1. Ogólne definicje związane z bezpieczeństwem informacji:
 - 1) **bezpieczeństwo informacji** – zachowanie poufności, integralności i dostępności informacji; w ramach bezpieczeństwa informacji mogą być uwzględniane również inne właściwości, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność;
 - 2) **dostępność danych** – właściwość informacji polegająca na tym, że jest ona dostępna i może być wykorzystywana na żądanie uprawnionej jednostki;
 - 3) **incydent naruszenia bezpieczeństwa środowiska teleinformatycznego** – pojedyncze niepożądane lub niespodziewane zdarzenie bezpieczeństwa środowiska teleinformatycznego (tj. wystąpienie stanu komponentu środowiska teleinformatycznego wskazującego na potencjalne naruszenie jego bezpieczeństwa, błąd mechanizmu kontrolnego lub uprzednio nieznaną sytuację, która może być istotna z perspektywy bezpieczeństwa) lub seria takich zdarzeń, w przypadku których występuje

znaczne prawdopodobieństwo zakłócenia działalności lub naruszenia bezpieczeństwa informacji;

- 4) **integralność danych** – właściwość danych stanowiąca o ich dokładności i kompletności;
- 5) **informacja** – treści wszelkiego rodzaju przechowywane na dowolnym nośniku informacji. Informacja może być wyrażona za pomocą mowy, pisma, obrazu, rysunku, znaku, kodu, dźwięku lub w jakikolwiek inny sposób;
- 6) **kluczowe procesy** – wskazane przez Urząd procesy w obrębie jego działalności, które warunkują realizację zadań Urzędu;
- 7) **krytyczne procesy** – wskazane przez Urząd procesy w obrębie jego działalności, w przypadku których szybkie odzyskanie sprawności działania może mieć istotne znaczenie z punktu widzenia ciągłości działania;
- 8) **podatność** – słabość zasobu lub mechanizmu kontrolnego, która może być wykorzystana przez zagrożenie;
- 9) **postępowanie z ryzykiem** – metody obejmujące akceptację ryzyka, ograniczanie, transfer lub unikanie ryzyka;
- 10) **poufność danych** – właściwość danych polegająca na tym, że pozostają one niedostępne lub niejawne dla nieuprawnionych osób, procesów lub innych podmiotów;
- 11) **profil ryzyka** – skala i struktura ekspozycji na ryzyko;
- 12) **rozliczalność danych** - zachowanie dowodów o podjętych czynnościach względem przetwarzanej informacji;
- 13) **zagrożenie** – potencjalna przyczyna niepożądanego incydentu, który może spowodować szkodę dla systemu lub organizacji.

2. Systemy przetwarzania informacji:

- 1) **PBI** – Polityka Bezpieczeństwa Informacji;
- 2) **SZBI**- System Zarządzania Bezpieczeństwem Informacji;
- 3) **infrastruktura teleinformatyczna** – zespół urządzeń, oprogramowania i łączy transmisyjnych obejmujący w szczególności platformy sprzętowe (w tym: serwery, macierze, stacje robocze), sieć teleinformatyczną (w tym: routery, przełączniki, zapory sieciowe oraz inne urządzenia sieciowe), oprogramowanie systemowe (w tym systemy operacyjne i systemy zarządzania bazami danych) oraz inne elementy umożliwiające bezawaryjną i bezpieczną pracę ww. zasobów (w tym zasilacze UPS, generatory

prądotwórcze, urządzenia klimatyzacyjne), także te wykorzystywane w ośrodkach zapasowych Urzędu;

- 4) **przetwarzanie danych** - jakiejkolwiek operacje wykonywane na danych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie;
- 5) **system informatyczny** – aplikacja komputerowa lub zbiór powiązanych aplikacji komputerowych, którego celem jest przetwarzanie danych;
- 6) **nośnik informacji** – medium magnetyczne, optyczne lub papierowe, na którym zapisuje się i przechowuje informacje.

3. Terminy dotyczące ról w zakresie zapewniania bezpieczeństwa informacji:

- 1) **Administrator Danych** – Prezydent Miasta Suwałk;
- 2) **Administrator Bezpieczeństwa Informacji (ABI)** – osoba powołana przez Administratora Danych Osobowych, nadzorująca przestrzeganie zasad ochrony danych obejmujących środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną;
- 3) **Główny Administrator Bezpieczeństwa Informacji (GABI)**- osoba odpowiedzialna za nadzór nad bezpieczeństwem informacji w Urzędzie, opracowanie, wdrożenie i kontrolowanie PBI;
- 4) **Administrator Systemu Informatycznego (ASI)** – osoba lub osoby odpowiedzialne za prawidłowy stan i działanie środowiska teleinformatycznego od strony technicznej. W Urzędzie rolę ASI pełnią pracownicy Wydziału Informatyki;
- 5) **Urząd** – Urząd Miejski w Suwałkach.

4. Klasyfikacja informacji (zasobów) ze względu na ich znaczenie dla Urzędu:

- 1) **informacje wrażliwe** – informacje przetwarzane w Urzędzie, chronione prawnie lub chronione z powodu uznania za podlegające ochronie, np. w związku z istotną wagą informacji dla prawidłowej realizacji procesów kluczowych. Informacje wrażliwe mają jasno określone reguły dostępu i odpowiednio do wymagań podlegają ochronie w zakresie poufności, integralności i dostępności;
- 2) **informacje niewrażliwe** – informacje nie należące do informacji wrażliwych, podlegają ochronie w zakresie integralności i dostępności w stopniu wynikającym z potrzeby ochrony interesów Urzędu;
- 3) **informacje publiczne**- informacje publicznie dostępne;

- 4) **informacje niejawne** – informacje, które wymagają ochrony przed nieuprawnionym ujawnieniem, niezależnie od formy i sposobu jej wyrażenia, także w trakcie jej opracowania - posiadają własne regulacje prawne i stosowne mechanizmy ochronne.

§ 7.

Zadania i odpowiedzialność

1. Ochrona zasobów informacyjnych Urzędu wymaga wspólnego działania i zaangażowania wszystkich pracowników. Zarówno kierownictwo jak i wszyscy użytkownicy są obowiązani do przestrzegania PBI, a zwłaszcza zasad zawartych w politykach, procedurach, instrukcjach i innych dokumentach związanych z PBI.
2. Zadaniem pracowników (użytkowników informacji) jest:
 - 1) przestrzegania zasad PBI;
 - 2) przestrzeganie zasad zawartych w obowiązujących regulacjach wewnętrznych, na które wskazuje niniejsza PBI, odpowiednio do zakresu swoich zadań i obowiązków;
 - 3) w każdym przypadku bezpieczne i rozważne postępowanie z informacją, systemami, dokumentami i nośnikami informacji, w tym bezwzględne zachowanie tajemnicy;
 - 4) zgłaszania incydentów związanych z bezpieczeństwem informacji;
 - 5) potwierdzenie zapoznania się z treścią PBI oraz innych regulacji dotyczących bezpieczeństwa informacji w postaci odpowiedniego oświadczenia, którego wzór stanowi Załącznik nr 2 do PBI.
3. Osoby kierujące komórkami organizacyjnymi Urzędu realizują następujące zadania:
 - 1) nadzór nad przestrzeganiem PBI w pracy kierowanej komórki;
 - 2) promowanie i wymaganie postaw zgodnych z zasadami przyjętymi w Urzędzie, w tym reakcja na nieprawidłowości, w tym incydenty związane z bezpieczeństwem informacji.
4. W przypadku osób, z którymi Urząd zawiera umowy cywilno-prawne na dostęp do informacji, systemów, dokumentów i nośników informacji należy w zawieranej umowie wprowadzić klauzulę dotyczącą obowiązku przestrzegania postanowień PBI. Obowiązuje ona wszystkich dostawców usług i oprogramowania, jednostki zewnętrzne i ich pracowników, o ile w trakcie realizacji umowy otrzymają dostęp do zasobów informatycznych Urzędu. Dostęp do zasobów jest ograniczony do okresu zdefiniowanego w umowie.

§ 8.

Role

1. W Urzędzie Miejskim w Suwałkach wyróżnione zostały role:

- 1) Administrator Danych (**AD**);
- 2) Główny Administrator Bezpieczeństwa Informacji (**GABI**);
- 3) Administrator Bezpieczeństwa Informacji (**ABI**);
- 4) Administrator systemu Informatycznego (**ASI**);
- 5) Audytor Wewnętrzny (**AW**).

2. Administrator Danych (**AD**) - Prezydent Miasta Suwałk, odpowiedzialny jest za:

- 1) stawianie celów PBI zgodnych z potrzebami Urzędu;
- 2) ustanowienie i realizację PBI adekwatnie do postawionych celów;
- 3) wspieranie inicjatyw i rozwoju SZBI;
- 4) wyznaczanie właściwych zakresów obowiązków związanych z realizacją PBI i zapewnienie ich realizacji przez wyznaczone osoby.

3. Główny Administrator Bezpieczeństwa Informacji (**GABI**) - Naczelnik Wydziału Informatyki, odpowiedzialny jest za:

- 1) nadzór nad bezpieczeństwem informacji oraz systemów informatycznych;
- 2) stały nadzór nad realizacją PBI, w tym kontrolowanie prawidłowego wykorzystywania wdrożonych do stosowania procedur;
- 3) identyfikację grup informacji podlegających ochronie;
- 4) przygotowanie i aktualizację dokumentu głównego PBI;
- 5) nadzór pod względem bezpieczeństwa nad pracą wszystkich ASI;
- 6) przechowywanie, aktualizację i przeglądy dokumentacji, ocenę ryzyka i definicję poziomu bezpieczeństwa w szczególności: analizę ryzyka, rejestry aktywów i karty systemów;
- 7) zapewnienie zgodności SZBI z wymaganiami oraz przedstawianie kierownictwu wyników działania SZBI.

4. Administrator Systemów Informatycznych (**ASI**) – pracownik Wydziału Informatyki, odpowiedzialny jest za:

- 1) efektywne działanie środowiska teleinformatycznego Urzędu;
- 2) dbanie o poprawne i efektywne działanie administrowanych systemów, a także administrowanie elementami infrastruktury teleinformatycznej;

- 3) uczestniczenie w identyfikacji i ocenie ryzyka operacyjnego związanego ze środowiskiem teleinformatycznym (tzw. ryzyko bezpieczeństwa informacji);
- 4) dokonanie klasyfikacji systemów, na podstawie kryteriów zawartych w regulacjach wewnętrznych Urzędu;
- 5) analizę ryzyka, ewentualną analizę dotyczącą możliwości wymiany komponentów pozbawionych wsparcia producenta;
- 6) wdrożenie odpowiednich zabezpieczeń technologicznych;
- 7) prowadzenie dokumentacji systemów i infrastruktury teleinformatycznej;
- 8) świadczenie serwisu i pomocy technicznej pracownikom Urzędu w zakresie eksploatacji systemów informatycznych, zgłaszanie zleceń firmom zewnętrznym oraz nadzór wykonywanych napraw;
- 9) wykonywanie lub nadzór procedur archiwizowania danych (sporządzania kopii awaryjnych);
- 10) reagowanie na incydenty naruszenia bezpieczeństwa informacji w zakresie wynikającym ze szczegółowych zadań;
- 11) wprowadzanie praw dostępu użytkowników do informacji i danych w systemach, zgodnie z wnioskiem o dostęp;
- 12) testowanie nowych wersji oprogramowania w środowisku testowym oraz środowisku roboczym;
- 13) monitorowanie wykorzystanie kluczowych aktywów, włączając w to procesory, pamięć główną, pamięć dyskową, drukarki i inne urządzenia wyjściowe oraz systemy komunikacyjne;
- 14) prowadzenie dokumentacji systemów i komponentów systemów zgodnie z regulacjami wewnętrznymi Urzędu;
- 15) odtworzenie danych przechowywanych na nośnikach elektronicznych lub odtworzenie innych zasobów krytycznych (komponentów infrastruktury teleinformatycznej);
- 16) nadzór zewnętrznych dostawców usług w zakresie jakości i przestrzegania standardów bezpieczeństwa w zakresie czynności technicznych realizowanych w związku z wykonaniem umów.

5. Administrator Bezpieczeństwa Informacji (**ABI**) - osoba powołana przez Administratora Danych Osobowych, odpowiedzialny jest za:

- 1) głównym zadaniem ABI jest zapewnianie przestrzegania przepisów o ochronie danych osobowych (zgodnie z art. 36a ust. 2 pkt 1 u.o.d.o.);

- 2) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych;
 - 3) nadzorowanie opracowania i aktualizowania dokumentacji opisującej sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną oraz przestrzegania zasad w niej określonych;
 - 4) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych;
 - 5) dodatkowym zadaniem ABI jest prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych (zgodnie z art. 36a ust. 2 pkt 2 u.o.d.o.), zawierającego nazwę zbioru oraz informacje, o których mowa w art. 41 ust. 1 pkt 2–4a i 7 u.o.d.o.;
6. Audytor Wewnętrzny (AW) – pracownik Wydziału Audytu, odpowiada za coroczne przeprowadzanie audytu 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 (tj. Dz. U. z 2016 r., poz. 113).

§ 9.

Zakres ochrony informacji

1. Urząd chroni informacje podlegające ochronie z mocy prawa, a także istotne z uwagi na prawidłowość realizacji kluczowych procesów.
2. W sytuacjach kryzysowych, ujawnienie informacji wrażliwych pod względem poufności uznawane jest jako zagrożenie mniejsze od zniszczenia informacji.
3. Użytkownicy Urzędu zobowiązani są do używania zasobów informacyjnych wyłącznie do celów służbowych. Wszyscy użytkownicy zasobów informacyjnych podlegają kontroli dostępu do tych zasobów.
4. Każdy pracownik posiada uprawnienia dostępu na poziomie i zakresie niezbędnym do wykonywania obowiązków służbowych.
5. Użytkownicy Urzędu posiadają wiedzę o zasobach Urzędu ograniczoną do informacji wymaganych do realizacji powierzonych zadań.
6. Ochrona zasobów musi opierać się na co najmniej dwóch mechanizmach zabezpieczeń.

7. Użytkownicy są odpowiedzialni za powierzone im zasoby i ponoszą odpowiedzialność za zaniedbanie swoich obowiązków w zakresie bezpieczeństwa informacji.
8. Użytkownicy stosują zasadę „czystego biurka”. Podczas pracy na biurku znajdują się dokumenty papierowe i nośniki informacji niezbędne do wykonywania powierzonych zadań. Po skończonej pracy należy uprzątnąć biurko z dokumentów i nośników informacji.
9. Naruszenie ww. zasad jest naruszeniem obowiązków pracowniczych i może pociągnąć za sobą odpowiedzialność karną, wynikającą z przepisów:
 - 1) ustawy o ochronie danych osobowych;
 - 2) kodeksu karnego dot. przestępstw przeciwko ochronie informacji;
 - 3) przepisów chroniących tajemnicę skarbową.

§ 10.

Klasyfikacja informacji

1. Kryteriami klasyfikacji informacji jest wymagany poziom: poufności, integralności, dostępności, rozliczalności.
2. W przypadku konieczności stosowania wielu kryteriów rozstrzygające jest kryterium przyjmujące najwyższym poziom.
3. Ocenę wrażliwości aktywów prowadzi się w Urzędzie przez identyfikowanie konsekwencji biznesowych, w szczególności przez analizę
 - 1) poufności informacji;
 - 2) integralności informacji;
 - 3) dostępności informacji (potrzeby dostępności);
 - 4) wymiernych kosztów odtworzenia:
 - a) aktywów,
 - b) informacji i danych,
 - c) odtworzenia działalności operacyjnej,
 - d) niewymiernych kosztów odtworzenia informacji w kontekście:
 - dobrego imienia Urzędu,
 - konsekwencji karnych, cywilnoprawnych lub służbowych.
4. W celu identyfikacji poziomu istotności informacji i wymaganego poziomu ochrony informacja klasyfikowana jest wg następujących kategorii:

- 1) informacje wrażliwe – informacje chronione prawnie (kryterium poufności) lub chronione z powodu uznania za podlegające ochronie, np. w związku z istotną wagą informacji dla prawidłowej realizacji procesów krytycznych (kryterium integralności, dostępności), dane osobowe;
- 2) informacje niewrażliwe – informacje nie należące do informacji wrażliwych (kryterium integralności, dostępności);
- 3) informacje publiczne - informacje publicznie dostępne (kryterium integralności, dostępności);
- 4) informacje niejawne - informacje, do których stosuje się przepisy o ochronie informacji niejawnych.

§ 11.

Podstawowe zasady zapewnienia bezpieczeństwa informacji

1. Poprzez zapewnienie bezpieczeństwa informacji należy rozumieć działania oparte na systematycznym zarządzaniu ryzykiem, obejmujące wybór, wdrożenie i utrzymanie zabezpieczeń składających się z technicznych i organizacyjnych środków ochrony danych i infrastruktury teleinformatycznej.
2. W celu zapewnienia bezpieczeństwa zasobów Urzędu stosuje się następujące ogólne zasady:
 - 1) zasada przywilejów koniecznych - każdy pracownik posiada prawa dostępu do zasobów Urzędu ograniczone wyłącznie do tych, które są konieczne do wykonywania powierzonych mu obowiązków;
 - 2) zasada wiedzy koniecznej - użytkownicy posiadają wiedzę o zasobach Urzędu ograniczoną wyłącznie do zagadnień, które są konieczne do realizacji powierzonych im zadań;
 - 3) zasada asekuracji zabezpieczeń - ochrona zasobów winna opierać się na co najmniej dwóch mechanizmach zabezpieczenia;
 - 4) zasada rozliczalności - Urząd dąży do zapewnienia jednoznacznej odpowiedzialności pracowników za powierzone im zasoby;
 - 5) wszyscy użytkownicy zasobów informacyjnych ponoszą odpowiedzialność za zaniedbanie swoich obowiązków w zakresie bezpieczeństwa informacji;
 - 6) zasada czystego biurka - należy unikać pozostawiania dokumentów na biurku bez opieki. Po zakończeniu pracy należy uprzątnąć biurko z dokumentów papierowych oraz informatycznych nośników informacji. Zaleca się przechowywanie pod

zamknięciem (najlepszym rozwiązaniem jest sejf, szafa lub inna forma zabezpieczenia) dokumentów i nośników zawierających wrażliwe lub krytyczne informacje służbowe;

- 7) zasada czystego ekranu - zamykanie sesji lub blokowanie komputera i terminala pozostawionego bez opieki lub czasowo nieużywanego (za pomocą mechanizmu blokowania ekranu i klawiatury kontrolowanego hasłem, tokenem lub innego podobnego mechanizmu). Po zakończonym dniu pracy komputer powinien zostać wyłączony.

3. W szczególności zapewnienie bezpieczeństwa obejmuje obszary :

- 1) bezpieczeństwa organizacyjnego,
- 2) bezpieczeństwa fizycznego i środowiskowego,
- 3) bezpieczeństwa systemów i infrastruktury teleinformatycznej,
- 4) zarządzanie ciągłością działania,
- 5) reagowania na incydenty bezpieczeństwa informacji,
- 6) zarządzanie jakością danych.

§ 12.

Zarządzanie ryzykiem

1. Częścią SZBI jest Analiza Ryzyka, która obejmuje:

- 1) zasoby systemu teleinformatycznego;
- 2) zagrożenia dla systemu teleinformatycznego;
- 3) skalę skutków;
- 4) skalę podatności;
- 5) skalę ryzyka;
- 6) ryzyko akceptowalne;
- 7) zabezpieczenia wdrożone w systemie teleinformatycznym;
- 8) macierz ryzyka po wdrożeniu niezbędnych zabezpieczeń.

2. Systematyczne zarządzanie ryzykiem, obejmujące wybór, wdrożenie i utrzymanie zabezpieczeń składających się z technicznych i organizacyjnych środków ochrony danych i infrastruktury teleinformatycznej.

§ 13.

Bezpieczeństwo organizacyjne

1. W Urzędzie dokonuje się wewnętrznego podziału użytkowników ze względu na ich role i poziomy uprawnień.
2. Urząd podejmuje systematyczne działania związane z edukacją i szkoleniem pracowników w zakresie zagrożeń i istniejących regulacji wewnętrznych odpowiednio do ich obowiązków.
3. Urząd zapewnia odpowiednią ciągłość działania poprzez Politykę zapewnienia ciągłości bezpieczeństwa informacji.

§ 14.

Bezpieczeństwo fizyczne i środowiskowe

1. Stosowane w Urzędzie mechanizmy bezpieczeństwa adekwatne są do potrzeb i skali działalności Urzędu, w taki sposób aby pozwalało to na bieżące funkcjonowanie kluczowych procesów oraz ich odtworzenie w przypadku wystąpienia sytuacji awaryjnej.
2. Wrażliwe środki przetwarzania informacji są umieszczane w obszarach bezpiecznych, chronionych fizyczną granicą przez odpowiednie bariery bezpieczeństwa oraz zabezpieczenia wejścia. Zapewnia się, aby były one chronione fizycznie przed nieuprawnionym dostępem fizycznym, uszkodzeniami lub zakłóceniami pracy.
3. Stosowana jest ochrona sprzętu (łącznie ze sprzętem wykorzystywanym poza siedzibą Urzędu) niezbędna do redukcji ryzyka nieautoryzowanego dostępu do informacji i ochrony przed utratą lub uszkodzeniem. Ochrona obejmuje również odpowiednią lokalizację (miejsce instalacji), konserwację, zbywanie lub przekazanie sprzętu podmiotom zewnętrznym w sposób zapewniający bezpieczeństwo informacji.
4. Chroni się przed zagrożeniami instalacje wspomagające, takie jak zasilanie lub okablowanie sieciowe.

§ 15.

Bezpieczeństwo systemów i infrastruktury teleinformatycznej

1. Stosowana jest zasada, że wszystkie komponenty środowiska teleinformatycznego (systemy, komponenty infrastruktury teleinformatycznej) powinny być zinwentaryzowane i udokumentowane oraz mają wyznaczonego właściciela odpowiedzialnego za właściwą ochronę i utrzymanie zabezpieczeń danego komponentu.

2. Stosowane są następujące mechanizmy bezpieczeństwa:
 - 1) rozdzielanie obowiązków zapobiegające celowej lub nieumyślnej modyfikacji lub niewłaściwego użycia systemów;
 - 2) regulacje wewnętrzne w zakresie eksploatacji komponentów;
 - 3) zarządzanie zmianami w środowisku teleinformatycznym;
 - 4) świadczenie pomocy technicznej użytkownikom systemów;
 - 5) ochrona przed złośliwym oprogramowaniem;
 - 6) stosowanie zabezpieczeń kryptograficznych;
 - 7) stosowanie regularnego dokonywania i testowania kopii zapasowych;
 - 8) zapewnianie bezpieczeństwa sieci teleinformatycznych;
 - 9) zapewnianie bezpieczeństwa nośników informacji;
 - 10) zapewnianie bezpieczeństwa wymiany informacji;
 - 11) kontrola dostępu i nadawanie uprawnień;
 - 12) zarządzanie oprogramowaniem użytkownika końcowego.
3. Sposób inwentaryzacji, dokumentowania komponentów infrastruktury środowiska teleinformatycznego, a także realizacji mechanizmów bezpieczeństwa uregulowany jest w pozostałych politykach SZBI.

§ 16.

Zarządzanie ciągłością działania

1. W celu zapewnienia bezpieczeństwa informacji Urząd stosuje Politykę zapewnienia ciągłości bezpieczeństwa informacji tak, aby zminimalizować wpływ utraty i odtwarzania aktywów wynikającego z katastrof naturalnych, wypadków, awarii urządzeń oraz celowego działania.
2. Odpowiedni poziom ciągłości działania w zakresie środowiska teleinformatycznego uzyskiwany jest poprzez stosowanie kombinacji zabezpieczeń prewencyjnych i środków służących do odtwarzania komponentów środowiska teleinformatycznego.

§ 17.

Reagowanie na incydenty bezpieczeństwa informacji

1. Urząd wdraża i stosuje regulacje wewnętrzne dotyczące zgłaszania i reagowania na zidentyfikowane incydenty bezpieczeństwa informacji, w tym incydenty naruszenia bezpieczeństwa środowiska teleinformatycznego.

2. Obowiązkiem wszystkich pracowników jest stosowanie zasad w zakresie zgłaszania incydentów.
3. Podmioty trzecie, podczas przetwarzania informacji Urzędu, są zobowiązane stosownymi zapisami w umowach do informowania Urzędu o incydentach bezpieczeństwa informacji po swojej stronie, niezwłocznie po ich wykryciu.
4. Informacje dotyczące stwierdzonych incydentów wraz z opisem ich przyczyny i podjętymi działaniami korygującymi są rejestrowane w celu dalszej analizy.
5. Urząd podejmuje działania zmierzające do ustalenia przyczyn i usunięcia skutków incydentów bezpieczeństwa.
6. Informacje dotyczące incydentów są uwzględniane w procesie analizy ryzyka.

§ 18.

Publikowanie lub udostępnianie informacji niewrażliwych

1. Z uwagi na zagrożenie ryzykiem utraty reputacji, a także możliwość zwiększenia poziomu innych rodzajów ryzyka należy dochować jak największej ostrożności i staranności związanej z publikowaniem lub udostępnianiem informacji niewrażliwych podmiotom zewnętrznym – pomimo, że istnieje pewność, że informacja taka nie jest objęta ochroną prawa.
2. Szczególną uwagę należy zwrócić na informacje publikowane w sieci Internet, w tym w tzw. mediach społecznościowych, Biuletynie Informacji Publicznych, stronach internetowych Urzędu.
3. Publikowanie lub udostępnianie informacji niewrażliwych podmiotom zewnętrznym jest możliwe wyłącznie z zachowaniem zasad prawa, przepisów wewnętrznych i za każdym razem wymaga weryfikacji treści udostępnianej informacji pod kątem poprawności i zagrożenia dla reputacji Urzędu przez odpowiedniego dla sprawy pracownika.

§ 19.

Obowiązki pracowników

1. Użytkownicy przetwarzający informacje zobowiązani są do ścisłego przestrzegania przepisów prawa oraz przepisów wewnętrznych Urzędu oraz do nie rozpowszechniania wiadomości stanowiących tajemnicę urzędową lub objętych ochroną danych osobowych.

2. Użytkownicy, w szczególności zobowiązani są do przestrzegania Instrukcji pracy na stanowisku wyposażonym w monitor i drukarkę, Politykę w zakresie profilaktyki antywirusowej, a także do przestrzegania zakazu udostępniania hasła do swojego komputera, zakazu korzystania z nielegalnego oprogramowania oraz zakazu instalowania jakiegokolwiek oprogramowania bez zgody ASI.
3. Wszyscy użytkownicy są zobowiązani do przestrzegania zasad ochrony informacji prawnie chronionej np.: danych osobowych i informacji niejawnych.

§ 20.

Konsekwencje związane z naruszaniem postanowień PBI

Użytkownicy Urzędu mogą podlegać konsekwencjom dyscyplinarnym i prawnym za nieprzestrzeganie postanowień niniejszej Polityki, a także innych regulacji szczegółowo określających zasady zachowania bezpieczeństwa informacji, które wskazuje niniejsza PBI.

§ 21.

Dystrybucja Polityki

1. Z treścią niniejszego dokumentu, jak i innych regulacji związanych z PBI zapoznani są wszyscy użytkownicy Urzędu, odpowiednio do ich zakresów obowiązków.
2. Niniejszy dokument może być przedstawiany wszystkim innym podmiotom, w tym organom władzy i administracji publicznej, w celu prezentacji zasad ochrony informacji i środowiska teleinformatycznego obowiązujących w Urzędzie.

**Wykaz regulacji wewnętrznych i dokumentów stanowiących dokumenty powiązane z Polityką
Bezpieczeństwa Informacji.**

1. Polityka Bezpieczeństwa Urzędu Miejskiego w Suwałkach.
2. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w urzędzie Miejskim w Suwałkach.
3. Regulamin przestrzegania zasad i procedur korzystania z legalnego oprogramowania oraz ochrony własności intelektualnej w Urzędzie Miejskim w Suwałkach.
4. Analiza Ryzyka.
5. Polityka kontroli dostępu.
6. Polityka wykonywania kopii zapasowych.
7. Polityka w zakresie profilaktyki antywirusowej.
8. Instrukcja pracy na stanowisku wyposażonym w monitor i drukarkę.
9. Wykaz zabezpieczeń fizycznych i logicznych systemów.
10. Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji.
11. Polityka urządzeń mobilnych i telepracy.
12. Karty systemów i rejestr aktywów.
13. Polityka zabezpieczeń kryptograficznych.
14. Polityka postępowania z nośnikami.
15. Polityka przesyłania informacji.
16. Polityka zapewnienia ciągłości bezpieczeństwa informacji.
17. Polityka relacji z dostawcami.
18. Polityka zatrudnienia.
19. Polityka zatrudniania, zatrudnienia, zakończenia zatrudnienia.
20. Polityka sposobu połączenia infrastruktury Urzędu do SRP.

.....

....., data.....

Imię i nazwisko

Miejscowość

.....

komórka organizacyjna - stanowisko

OŚWIADCZENIE

Niniejszym oświadczam, iż znana mi jest treść dokumentu Polityka Bezpieczeństwa Informacji oraz innych powiązanych wymienionych w niej regulacji wewnętrznych przyjętych w Urzędzie Miejskim w Suwałkach.

Jednocześnie oświadczam, że będę się stosować do zawartych w wyżej wymienionych dokumentach zasad i procedur.

Jestem świadomy/a mojego wkładu w skuteczność Systemu Zarządzania Bezpieczeństwem Informacji.

.....

podpis