ZARZĄDZENIE NR 150/18
PREZYDENTA MIASTA SZCZECIN
z dnia 6 kwietnia 2018 r.

w sprawie określenia zasad bezpieczeństwa informacji oraz wytycznych dla Polityki Bezpieczeństwa Informacji Urzędu Miasta Szczecin.

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 roku o samorządzie gminnym (Dz. U. z 2017 r. poz. 1875 i 2232 oraz z 2018 r. poz.130), art. 3 ust. 1, art. 7 pkt 4, art. 26 ust. 1, art. 36, art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922 oraz z 2018 r. poz. 138), art. 1 oraz art. 13 ust. 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2017 r. poz. 570), **zarządzam**, co następuje:

§ 1. 1. Urząd Miasta Szczecin - zwany dalej Urzędem deklaruje, że System Zarządzania Bezpieczeństwem Informacji - zwany dalej SZBI, w tym Polityka Bezpieczeństwa Informacji - zwana dalej - PBI, został opracowany na podstawie 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 (Dz.U z 2017 r. poz. 2247) – zwanego dalej KRI, w świetle wytycznych standaryzujących obszary zabezpieczeń według Polskiej Normy PN-ISO/IEC 27001, oraz PN-ISO/IEC 27002 – w odniesieniu do ustanawiania zabezpieczeń, PN-ISO/IEC 27005:10 – w odniesieniu do zarządzania ryzykiem w bezpieczeństwie informacji, PN-ISO/IEC 24762 – w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.

2. Wynikające z SZBI zawarte w PBI zasady ochrony oraz środki zabezpieczenia danych - w tym danych osobowych - są zgodne z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r., poz. 922 oraz z 2018 r. poz.138) - zwaną dalej ustawą oraz rozporządzeniem z dnia 29 kwietnia 2004 r. Ministra Spraw Wewnętrznych i Administracji 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. Nr 100, poz. 1024) - zwanym dalej rozporządzeniem.

3. PBI służy do regulacji spraw dotyczących ochrony danych w szczególności danych osobowych zawartych w systemie informatycznym Urzędu, a także zasad użytkowania programów komputerowych i baz danych (Pkt 4.*).

4. Nadrzędnym celem PBI jest:

1) zapewnienie właściwej ochrony zasobów w Urzędzie Miasta Szczecin;

2) określenie wymagań SZBI;

3) właściwy dobór zabezpieczeń (środków bezpieczeństwa) oparty na rezultatach i wnioskach wynikających z procesów szacowania i postępowania z ryzykiem, wymagań prawnych, wymagań nadzoru, zobowiązań kontraktowych oraz pozostałych wymagań dotyczących bezpieczeństwa informacji.

5. Zakres obowiązywania PBI:

1) dokument dotyczy wszystkich jednostek organizacyjnych Urzędu Miasta Szczecin, wszystkich pracowników w rozumieniu ustawy Kodeks Pracy, a także innych osób mających dostęp do informacji chronionych w Urzędzie (w tym pracowników firm zewnętrznych realizujących prace na rzecz Urzędu Miasta Szczecin);

2) dokument ma zastosowanie do wszystkich informacji chronionych niezależnie od formy, w jakiej są przechowywane (papierowej, elektronicznej, video lub innej);

3) z dokumentem PBI są zobowiązani zapoznać się wszyscy pracownicy Urzędu posiadający dostęp do danych osobowych i informacji chronionych ustawowo.

6. SZBI w Urzędzie to system zapewniający poufność, dostępność i integralność informacji z uwzględnieniem dodatkowo takich atrybutów, jak: autentyczność, rozliczalność, niezaprzeczalność i niezawodność oraz ciągłość działania.

7. Prezydent Miasta, Zastępcy Prezydenta Miasta, Sekretarz Miasta, Skarbnik Miasta, dyrektorzy i kierownicy jednostek organizacyjnych Urzędu oraz podmioty zewnętrzne - Miejska Jednostka Obsługi Gospodarczej Miasta Szczecin – zwana dalej MJOG, dostawcy oprogramowania i usług teleinformatycznych, z którymi Urząd zawarł umowy, są proporcjonalnie zaangażowani w działaniach wspierania przestrzegania procedur zmierzających do zapewnienia bezpieczeństwa informacyjnego, na założonym poziomie (Pkt 5.3*).

8. Wdrożony SZBI, którego elementem jest niniejsza PBI, podlega ciągłemu doskonaleniu, zgodnie z wymaganiami normy PN-ISO/IEC 27001:2014-12

9. Celem wdrożonego w Urzędzie Miasta Szczecin SZBI jest osiągnięcie właściwego poziomu organizacyjnego i technicznego, który:

1) maksymalnie ograniczy występowanie zagrożeń dla bezpieczeństwa informacji, które wynikają z celowej bądź przypadkowej działalności człowieka oraz ich ewentualnego wykorzystania na szkodę Urzędu Miasta Szczecin;

2) zapewni zachowanie poufności informacji chronionych, integralności i dostępności informacji chronionych (niepublicznych) oraz jawnych (publicznych);

3) zapewni poprawne i bezpieczne funkcjonowanie wszystkich systemów informatycznych przetwarzających informacje;

4) zapewni gotowość do podjęcia działań w sytuacjach kryzysowych dla bezpieczeństwa działania Urzędu Miasta Szczecin, jego interesów, posiadanych i powierzonych jemu informacji oraz będzie gwarantem właściwej ochrony informacji oraz ciągłości procesu ich przetwarzania.

10. Programy komputerowe użytkowane w Urzędzie zgodnie z ustawą z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2017 r. poz. 880 i 1089 oraz z 2018 r. poz. 650) są przedmiotem prawa autorskiego i podlegają ochronie. Urząd obejmuje ochroną wszystkie formy wdrażania programu komputerowego, eksploatacji oraz dokumentację projektową, techniczną i użytkową (A.18.1.2*).

11. System Zarządzania Bezpieczeństwem Informacji nie obejmuje w szczególności:

1) przetwarzania przez Urząd informacji poza systemami teleinformatycznymi, za wyjątkiem prowadzenia dokumentacji systemów teleinformatycznych oraz dokumentacji związanej z administracją i eksploatacją systemów teleinformatycznych;

2) bezpieczeństwa informacji w ramach procesów zarządzania personelem w zakresie innym niż eksploatacja systemów teleinformatycznych.

3) przetwarzania informacji niejawnych w rozumieniu ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U z 2018 r. poz. 412 i 650).

4) aktywów służących do przetwarzania informacji niejawnych, w szczególności systemów teleinformatycznych, sprzętu oraz pomieszczeń, w których przetwarzane są informacje niejawne.

§ 2. Wprowadza się słownik pojęć mających zastosowanie w zarządzeniu, gdzie użyte pojęcia informatyczne mają następujące znaczenie:

1) Active Directory (AcDi) - usługa katalogowa, która przechowuje informacje dotyczące obiektów w sieci i udostępnia je użytkownikom i administratorom sieci. Active Directory

jest implementacją protokołu LDAP w postaci hierarchicznej bazy danych dla systemów MS Windows. Podstawowym pojęciem w AcDi jest Domena, która zawiera zazwyczaj wszystkie informacje dotyczące danej organizacji;

2) Administrator Danych Osobowych – zwany dalej AD, w rozumieniu art. 7 pkt 4) ustawy Prezydent Miasta Szczecin;

3) Administrator Bezpieczeństwa Informacji zwany dalej ABI – rozumie się przez to osobę, którą AD na postawie art. 36a ust. 1 ustawy powołał do pełnienia obowiązków administratora bezpieczeństwa informacji, odpowiedzialny jest za zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez: sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych, nadzorowanie opracowania i aktualizowania dokumentacji, o której mowa w art. 36 ust. 2 ustawy, oraz przestrzegania zasad w niej określonych, zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz prowadzenie rejestru zbiorów danych przetwarzanych przez AD, z wyjątkiem zbiorów, o których mowa w art. 43 ust. 1 ustawy, zawierającego nazwę zbioru oraz informacje, o których mowa w art. 41 ust. 1 pkt 2-4a i 7 ustawy;

4) Administrator Systemu Informatycznego zwany dalej ASI – rozumie się przez to osobę wyznaczoną przez Dyrektora Wydziału Informatyki do pełnienia takiej funkcji, odpowiedzialny za bezpieczeństwo i funkcjonowanie systemów informatycznych oraz stosowanie technicznych i organizacyjnych środków ochrony w tym systemie;

5) Administrator Systemu Użytkowego zwany dalej ASU – rozumie się przez to osobę wyznaczoną przez Dyrektora Wydziału Informatyki do pełnienia takiej funkcji, odpowiedzialny za funkcjonowanie systemów użytkowych, nadawanie, odbieranie uprawnień do poszczególnych modułów lub funkcji systemu użytkowego;

6) Aktywa – wszystko co ma wartość dla Urzędu Miasta Szczecin - zasoby: osobowe, majątkowe, rzeczowe i inne;

7) Dane osobowe - rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne;

8) Dane wrażliwe - rozumie się przez to wszelkie informacje ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, o stanie zdrowia, kodzie genetycznym, nałogach, życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym;

9) Dostępność - właściwość bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu;

10) Elektroniczne nośniki informacji (ENI) - zewnętrzne nośniki danych, w szczególności płyty CD, DVD, Pendrive, pamięci typu FLASH, które muszą zostać zgłoszone i zarejestrowane przez ASI;

11) Firewall - mechanizm separujący komputer lub lokalną sieć komputerów podłączonych do sieci publicznej i zabezpieczający przed różnego rodzaju zagrożeniami. Firewall może mieć postać specjalizowanego urządzenia sieciowego lub programu komputerowego LAN lub sieć LAN - Sieć komputerowa o zasięgu lokalnym, zbudowana z kabli miedzianych, światłowodowych, i innych mediów oraz urządzeń aktywnych, której administratorem i właścicielem jest w tym przypadku Urząd Miasta Szczecin;

12) Hasło - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi;

13) Identyfikator – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący użytkownika upoważnionego do przetwarzania danych osobowych w systemie informatycznym;

14) Incydent związany z bezpieczeństwem informacji - jest to pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań zagrażających bezpieczeństwu informacji;

15) Internet - ogólnoświatowy system połączeń między komputerami, określany również jako sieć sieci. To przestrzeń adresów komputerowych przydzielonych komputerom połączonych za pomocą urządzeń sieciowych, takich jak karty sieciowe , modemy i koncentratory , komunikujących się za pomocą odpowiedniego protokołu z wykorzystaniem infrastruktury telekomunikacyjnej ;

16) Intranet – sieć komputerowa usług typowo internetowych ograniczająca się do komputerów w Urzędzie umożliwiająca korzystanie przez użytkowników usług takich, jak przeglądanie wewnętrznych stron WWW czy poczty elektroniczn ej;

17) Integralność danych – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

18) Jednostka - jednostka organizacyjna Urzędu (wydział, biuro, komórka samodzielna, np. ABI, BHP);

19) Kierownik - kierownik jednostki organizacyjnej Urzędu, w szczególności Dyrektor Wydziału lub Biura, Kierownik Biura, Koordynator;

20) LAN (od ang. local area network) - lokalna sieć komputerowa – sieć komputerowa łącząca komputery na określonym obszarze np. Urzędzie;

21) Osoba upoważniona do przetwarzania danych osobowych – rozumie się przez to osobę, która upoważniona została do przetwarzania danych osobowych poprzez upoważnienie na piśmie przez AD lub upoważnioną osobę;

22) Podatności (vulnerability) - jest to pewnego rodzaju słabość. Odnosi się do braku odporności (systemu lub jednostki) na skutki wrogiego środowiska lub działań celowych. Zjawisko podatności wykorzystywane jest przez zagrożenia i prowadzi do strat;

23) Podmiot zewnętrzny: inna organizacja, instytucja, inny urząd;

24) Poufność danych – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;

25) Przetwarzający – rozumie się przez to podmiot, któremu zostało powierzone przetwarzanie danych osobowych na podstawie umowy zawartej zgodnie z art. 31 ustawy;

26) Przetwarzanie danych - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;

27) Publiczna sieć telekomunikacyjna – rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 29 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 217 r. poz. 1907 i 2201oraz z 2018 r. poz. 106, 138, 650);

28) Raport – rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;

29) Rozliczalność – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;

30) Rozporządzenie – rozumie się przez to 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. Nr 100, poz. 1024);

31) Ryzyko - należy rozumieć wszystko co może zagrażać realizacji celów działania Urzędu,
a działania z nim związane to:

a) akceptowanie ryzyka – decyzja, aby zaakceptować ryzyko,

b) analiza ryzyka – systematyczne wykorzystanie informacji do zidentyfikowania źródeł i oszacowania ryzyka,

c) ocena ryzyka – proces porównywania oszacowanego ryzyka z określonymi kryteriami w celu określenia znaczenia ryzyka,

d) szacowanie ryzyka – całościowy proces analizy i oceny ryzyka,

e) zarządzanie ryzykiem – skoordynowane działania kierowania i zarządzania organizacją
z uwzględnieniem ryzyka,

f) postępowanie z ryzykiem – proces wyboru i wdrażania środków modyfikujących ryzyko;

32) Serwisant – rozumie się przez to pracownika Referatu Wsparcia Użytkowników WInf, firmę lub pracownika firmy zajmującej się instalacją, naprawą, konserwacją sprzętu komputerowego lub systemu/programu komputerowego;

33) Sieć lokalna VPN - (ang. Virtual Private Network, Wirtualna Sieć Prywatna)- połączenie jednostek komputerowych pracujących w Urzędzie w celu wymiany danych (informacji) dla własnych potrzeb, przy wykorzystaniu urządzeń telekomunikacyjnych, realizowane przez sieć prywatną lub sieć publiczną, taką jak internet. Jest to połączenie, ustanowione logicznie (wirtualnie) pomiędzy dwoma (lub wieloma) węzłami sieci komputerowej, umożliwiające bezpieczną łączność pomiędzy uczestnikami tej sieci;

34) Słowniki systemowe - Składniki programu (systemu) jak obiekty i procedury służące do gromadzenia stale powtarzających się informacji np. słowniki kodów pocztowych, nazw ulic, miejscowości, organizacji, imion oraz ich udostępniania;

35) System informatyczny – rozumie się przez to sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów procedur przetwarzania informacji i narzędzi programowych; w systemie tym pracuje co najmniej jeden komputer centralny i system ten tworzy sieć teleinformatyczną AD;

36) System pocztowy - Oprogramowanie zgodne ze standardami poczty elektronicznej w Internecie służące do wymiany informacji oraz zarządzania kalendarzami współdzielonymi;

37) System zarządzania bezpieczeństwem informacji (SZBI) - jest to część całościowego systemu zarządzania, oparta na podejściu wynikającym z ryzyka, odnosząca się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji. SZBI zawiera strukturę organizacyjną, polityki, planowane działania, zakresy odpowiedzialności, zasady, procedury, procesy i zasoby;

38) System ZSIFK - oprogramowanie, system informatyczny klasy ERP (ang. Enterprise Resource Planning - Planowanie Zasobów Organizacji) zakupiony przez Urząd w roku 2008 r. i rozwijany do chwili obecnej. Wielomodułowa konstrukcja systemu obejmuje

głównie sfery finansową, podatkową, zarządzania nieruchomościami oraz zarządzania personelem;

39) Teletransmisja – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;

40) Umowa – rozumie się przez to umowę zawartą na piśmie przez AD z podmiotem zewnętrzym, któremu zostało powierzone przetwarzanie danych zgodnie z art. 31 ustawy;

41) Urząd - rozumie się przez to Urząd Miasta Szczecin;

41) Usługa - czynności niematerialne (np. porada techniczna, audyt, szkolenie) lub materialne (produkcja, dostarczanie, wykonawstwo);

42) Ustawa – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U z 2016 r. poz. 922, zm. z 2018 r. poz.138) – zwana dalej ustawą;

43) Uwierzytelnianie – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;

44) Użytkownik – rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych, zarówno w systemach tradycyjnych jak i w systemie informatycznym (między innymi: pracownik, osoba wykonująca pracę na podstawie umowy cywilno-prawnej, osoba odbywająca staż pracy, praktykant), której nadano identyfikator i hasło oraz przyznano uprawnienia;

45) WInf – Wydział Informatyki Urzędu Miasta Szczecin;

46) Właściciel zasobu – jednostka lub podmiot zewnętrzny odpowiedzialny za dostarczanie określonej usługi lub danych w ramach uzgodnionego poziomu jej świadczenia;

47) Zdarzenie związane z bezpieczeństwem informacji – jest określonym stanem systemu, usługi lub sieci, który wskazuje na możliwe naruszenie polityki bezpieczeństwa informacji, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem;

48) Zgoda osoby, której dane dotyczą - rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści oraz może być odwołana w każdym czasie.

§ 3. Postanowienia ogólne PBI.

1. Celem działań w zakresie zapewnienia bezpieczeństwa informacji i jej ochrony w Urzędzie jest zapewnienie właściwej organizacji pracy, kompetencji pracowników, infrastruktury oraz wybór i zastosowanie odpowiednich zabezpieczeń, które zagwarantują spełnienie wymagań prawnych i zachowanie wizerunku solidnej, rzetelnej i zaufanej instytucji przy akceptowalnym poziomie ryzyka.

2. PBI oparta jest na przepisach prawa i nie narusza procedur realizowanych w Urzędzie wynikających z ustaw, regulacji wewnętrznych, czy zawartych umów. PBI jest zbiorem spójnych, precyzyjnych i zgodnych z obowiązującym prawem i innymi uregulowaniami Urzędu dokumentów, określających metody, zasady postępowania i ochrony oraz zapewnienia bezpieczeństwa informacji w Urzędzie. PBI jednoznacznie wskazuje wyłączenia z zakresu jej stosowania.

3. Zapewnienie bezpieczeństwa informacji dotyczy każdej jej formy (tradycyjnej i cyfrowej),
w szczególności w zakresie: ochrony danych osobowych, ochrony informacji niejawnych oraz ochrony własności intelektualnej.

4. Przetwarzanie informacji oznacza jakiekolwiek działanie polegające na zastosowaniu szeregu metod i procedur transformacji informacji (w tym odczytywanie, zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, usuwanie, przesyłanie) zgodnie z określonymi potrzebami.

5. Pracownicy Urzędu oraz pracownicy podmiotów zewnętrznych, realizujący zadania na rzecz Urzędu są zobowiązani postępować zgodnie z regułami PBI.

6. Cele wyznaczone przez PBI powinny być osiągane poprzez działania gwarantujące:

1) zachowanie poufności, dostępność i integralność informacji;

2) przypisanie kompetencji i odpowiedzialności w zakresie bezpieczeństwa informacji;

3) zapewnienie szkoleń oraz utrzymanie odpowiedniego poziomu kompetencji i świadomości pracowników Urzędu;

4) zarządzanie poziomem bezpieczeństwa przetwarzanych informacji;

5) analizę i minimalizację zagrożeń oraz właściwe reakcje w sytuacjach zagrożeń;

6) zarządzanie podatnościami, zapewnienie poprawnego i bezpiecznego funkcjonowanie systemów przetwarzania informacji;

7) zarządzanie ciągłością działania;

8) zarządzanie incydentami bezpieczeństwa;

9) zapewnienie monitorowania, podejmowanie działań zapobiegawczych i usprawniania skuteczności przyjętych zasad;

10) zapewnienia zgodności, jako unikania przekroczeń jakichkolwiek przepisów prawa, przyjętych zobowiązań czy posiadanych regulacji wewnętrznych ze szczególnym uwzględnieniem:

a) ochrony własności intelektualnej,

b) ochrony danych osobowych i prywatności osób fizycznych,

c) regulacji dotyczących zabezpieczeń kryptograficznych,

d) zgodności z politykami bezpieczeństwa, standardami ISO i PN oraz zabezpieczenia audytu systemów informatycznych.

§ 4. Organizacja bezpieczeństwa informacji. AD wydaje i akceptuje uregulowania dotyczące zapewnienia bezpieczeństwa informacji. Podejmuje określone prawem działania zmierzające do minimalizowania ryzyka zagrożeń bezpieczeństwa informacji, zmniejszania ich skutków oraz zapobiegania im w przyszłości. PBI stanowi wytyczne do podejmowania działań i tworzenia dokumentów o charakterze instrukcji, zasad postępowania zawierających specyficzne wymagania dla konkretnych grup informacji oraz do sformułowania pryncypiów dotyczących SZBI. PBI określa warunki, jakie muszą spełniać informacyjne, informatyczne i pozainformatyczne systemy do przetwarzania informacji, przypisuje odpowiedzialność za bezpieczeństwo informacji, reguluje relacje z otoczeniem oraz metody nadzoru i doskonalenia. Zasoby, tj. informacja oraz aktywa (składniki majątku) powiązane ze środkami przetwarzania informacji podlegają klasyfikacji ze względu na potrzeby, priorytety, wymagania prawne, co wyraża się w ich wartości, krytyczności dla organizacji. Klasyfikacja informacji służy do określenia odpowiedniego poziomu ochrony oraz uzasadnia stosowane środki zapewniające jej ochronę. Wprowadza się obowiązek definiowania właściciela dla każdego zasobu, który odpowiada za przeprowadzenie analizy ryzyka tego zasobu. W wyniku analizy właściciel zasobu wdraża odpowiednie zasady korzystania z zasobu, środki bezpieczeństwa i ponosi odpowiedzialność w czasie całego okresu eksploatacji zasobu. Odpowiedzialnymi za realizację procesów analizy ryzyk są kierownicy. Potrzeby ochrony informacji i obowiązek, zachowania poufności ze stronami trzecimi należy regulować zapisami lub umowami o zachowaniu poufności lub powierzeniu przetwarzania danych osobowych. Umowy te muszą regulować zakres podejmowanych działań i konsekwencje naruszenia jej warunków.

§ 5. Organizacja bezpieczeństwa przetwarzania danych osobowych.

1. AD w Urzędzie, jest Prezydent Miasta Szczecin.

2. AD powołuje ABI zapewniającego przestrzeganie przepisów o ochronie danych osobowych.

3. W zakresie środowiska teleinformatycznego ABI współpracuje z ASI oraz ASU.

4. W celu określenia zasad przetwarzania danych osobowych oraz korzystania z Internetu
w sieci teleinformatycznej Urzędu, wraz z zapewnieniem identyfikacji użytkowników, określeniem obowiązków zabezpieczania posiadanych zasobów teleinformatycznych wprowadza się:

1) Politykę Bezpieczeństwa Przetwarzania Danych Osobowych w Urzędzie Miasta Szczecin, określoną w **Załączniku Nr 1** do Zarządzenia;

2) Instrukcję Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych określoną w **Załączniku Nr 2** do Zarządzenia;

5. Prezydent Miasta Szczecin wyznacza obszary przetwarzania danych osobowych w Urzędzie określone w **Załączniku Nr 3** do Zarządzenia.

§ 6. Analiza ryzyka dla pełnego zakresu zagadnień bezpieczeństwa informacji.

1. Wszystkie zasoby (informacje i aktywa) w Urzędzie podlegają analizie ryzyka z określeniem prawdopodobieństwa ich wystąpienia, potencjalnego wpływu każdego ryzyka i wynikowy poziom ryzyka w odniesieniu do procesów w organizacji z uwzględnieniem warunków prawno-organizacyjnych.

2. W ramach PBI definiuje się metodę szacowania ryzyka oraz opracowuje się kryteria akceptacji ryzyka w odniesieniu do informacji oraz zapewnia się zgodność z mechanizmami zarządzania ryzykiem w Urzędzie.

3. W ramach wykonywanej analizy ryzyka szczegółowej ocenie podlegają:

1) skutki ekonomiczne lub finansowe dla Urzędu;

2) skutki na poziomach społecznym i gospodarczym dla miasta Szczecina i regionu;

3) skutki wizerunkowe, opinie czy pozycje w rankingach turystycznych, kulturalnych i innych podobnych dotyczących rankingów miast.

4. W zakresie przyjętej metodyki szacowania ryzyk dla zasobów Urzędu i postępowania z tymi ryzykami przyjmuje się powtarzalne kryteria szacowania ryzyk i określenia procedur, Rekomendowane jest zastosowanie normy PN-ISO/IEC 27005:2014-01 dla przeprowadzenia analizy ryzyka.

§ 7. Bezpieczeństwo osobowe w zakresie przetwarzania informacji.

1. Przekazanie lub wymiana informacji z pracownikami podmiotów zewnętrznych następuje po ustaleniu podstaw i zgodności przepisów dotyczących wskazanego zakresu wymiany informacji. Zasady, warunki w zakresie bezpieczeństwa informacji następują na podstawie umowy formalnoprawnej.

2. Pracownicy Urzędu zobowiązani są do świadomego i odpowiedzialnego przestrzegania bezpieczeństwa informacji i podlegają obowiązkowym szkoleniom z zakresu ochrony informacji w szczególności:

1) przed zatrudnieniem;

2) podczas zatrudnienia;

3) w trakcie zmiany zatrudnienia.

3. Wymagania z zakresu bezpieczeństwa informacji zawarte są w warunkach zatrudnienia, opisach stanowisk pracy oraz umowach z wykonawcami, gdzie stanowią one integralną część zobowiązań pracowników Urzędu oraz pracowników podmiotów zewnętrznych. Wymagania te powinny odzwierciedlać:

1) zapisy polityki bezpieczeństwa informacji;

2) wymagania zachowania poufności;

3) prawa i obowiązki w odniesieniu do praw autorskich;

4) odpowiedzialność za działania lub brak działań w zakresie przetwarzania danych osobowych;

5) konsekwencje nieprzestrzegania procedur bezpieczeństwa.

4. Wszystkie mechanizmy identyfikacji i autoryzacji uprawniające pracownika do dostępu do zasobów, kończącego zatrudnienie lub zmieniającego stanowisko pracy, winny być odebrane, anulowane czy wyłączone. Pracownik kończący zatrudnienie w Urzędzie lub zmieniający stanowisko pracy jest zobowiązany do przekazania wszystkich posiadanych zasobów informacyjnych użytkownikowi wskazanemu przez jego kierownika, z zachowaniem wszystkich aspektów bezpieczeństwa informacji. Kierownik pracownika przeprowadza analizę oraz rozpatruje czynniki ryzyka odejścia pracownika lub zmiany stanowiska pracy.

§ 8. Bezpieczeństwo fizyczne, środowiskowe i sprzętu.

1. W ramach ochrony informacji i aktywów zapewnia się ochronę przed nieautoryzowanym dostępem fizycznym, uszkodzeniami lub zakłóceniami w siedzibie Urzędu poprzez umieszczanie w obszarach chronionych fizycznie krytycznych środków przetwarzania informacji i zapewnienie dostępu do pomieszczeń objętych ochroną tylko autoryzowanemu personelowi.

2. W ramach ochrony fizycznej, która dotyczy bezpieczeństwa fizycznego i środowiskowego należy uwzględnić zagrożenia zewnętrzne i środowiskowe (pożar, zalanie, wybuch, itd.).

3. Zapewnienie ochrony fizycznej przed nieuprawnionym dostępem, uszkodzeniem lub zakłóceniem obejmuje:

1) ochronę przed nieuprawnionym dostępem;

2) zapewnienie ochrony dla przetwarzania informacji krytycznych;

3) zapewnienie ochrony dla eksploatowanego sprzętu teleinformatycznego z uwzględnieniem instalacji wspomagających;

4) zapewnienie ochrony sprzętu używanego poza siedzibą Urzędu.

4. Obszary dostępne dla osób nieupoważnionych (np. obszary dostaw, przewóz korespondencji, przewóz dokumentacji pracowników przy ich przeprowadzaniu) są nadzorowane i o ile to możliwe odizolowane od środków przetwarzania informacji.

5. Ochronie podlega sprzęt (łącznie ze sprzętem wykorzystywanym poza siedzibą Urzędu oraz wynoszonym mieniem) ze szczególnym uwzględnieniem warunków zabezpieczenia przed utratą, uszkodzeniem, kradzieżą.

6. Zbywanie, likwidacja lub zmiana użytkownika składnika sprzętu informatycznego (system informatyczny lub nośniki) wymaga skutecznego usunięcia informacji ze szczególnym uwzględnieniem zawartości dysków twardych komputerów, gdzie, jako zalecenie podstawowe należy przyjąć skuteczne niszczenie takich nośników.

7. Do ochrony sprzętu stosuje się środki i systemy wspomagające zabezpieczające przed awariami lub zakłóceniami infrastruktury innego rodzaju: zasilanie awaryjne, klimatyzacja.

8. Zapewnienie prawidłowej i bezpiecznej eksploatacji posiadanych środków przetwarzania informacji następuje poprzez:

1) określenie procedur w zakresie przetwarzania i administrowania;

2) przypisanie odpowiedzialności w zakresie przetwarzania i administrowania;

3) rozdzielenie odpowiedzialności;

4) nadzór nad pracownikami podmiotów zewnętrznych biorącymi udział w przetwarzaniu i administrowaniu;

5) prognozowanie zasobów i wydajności zasobów;

6) zapewnienie integralności i dostępności informacji Urzędu;

7) zapewnienie bezpieczeństwa informacji wymienianej z innymi podmiotami;

8) monitorowanie i wykrywanie działań nieautoryzowanych;

9) monitorowanie i rejestrowanie zdarzeń związanych z bezpieczeństwem informacji z zachowaniem warunku, o nie przekraczaniu uprawnień;

10) zarządzanie incydentami związanymi z bezpieczeństwem informacji, w tym gromadzenie materiałów dowodowych;

11) skuteczną likwidację lub usuniecie informacji ze szczególnym uwzględnieniem dysków twardych komputerów przed zbyciem, likwidacją lub zmianą właściciela środków przetwarzania informacji.

9. Do zapewnienia ciągłej dostępności i integralności sprzętu zaleca się jego okresową konserwację.

§ 9. Zarządzanie systemami i sieciami.

1. Środki w zakresie rozwiązań teleinformatycznych stosowane na terenie i na rzecz Urzędu podlegają analizie i są adekwatne do wymagań ochrony przetwarzanej informacji wynikającej z przeprowadzanej w Urzędzie analizy ryzyka.

2. Zapewnienie prawidłowej i bezpiecznej eksploatacji teleinformatycznych środków przetwarzania informacji oparte jest na udokumentowanych procedurach. Zmiany środowiskach przetwarzania informacji wymagają dokumentowania i kontroli.

3. Środowisko przetwarzania informacji podlega zarządzaniu i obejmuje:

1) zbiory i pliki z danymi, licencje i dokumentacje systemów;

2) sprzęt komputerowy, jak serwery, komputery PC, komputery przenośne, macierze dyskowe, przełączniki, routery, etc.;

3) usługi obliczeniowe, przesyłania i przechowywania danych, udostępniania Internetu i poczty elektronicznej;

4) inne usługi infrastruktury jak zasilanie i klimatyzacja;

5) kwalifikacje zawodowe informatyczne pracowników i ich doświadczenie;

6) wartości niematerialne, takie jak marka posiadanych systemów.

4. Dla obszaru systemów teleinformatycznych i zarządzanych sieci komputerowych wprowadza się następujące wymagania:

1) rozdzielanie obowiązków i odpowiedzialności za środki przetwarzania informacji (systemy), aby uniknąć nieuprawnionej lub nieumyślnej modyfikacji lub niewłaściwego użycia aktywu;

2) oddzielenie aktywów przeznaczonych do działań rozwojowych, testowych i eksploatacyjnych;

3) właściwego zdefiniowania poziomów dostępności usług oraz zapewnienia monitorowania dostarczanych usług. W przypadku świadczenia tych usług przez podmiot zewnętrzny wymagane jest definiowanie usług oraz poziom dostaw w umowach serwisowych,

4) poddawanie nowych usług procesom planowania i przeprowadzania odbiorów poprzedzonych testami i szkoleniami dla użytkowników;

5) wycofywanie z eksploatacji nieużywanych usług i infrastruktury i ich likwidowanie po usunięciu informacji;

6) zapewnienie wykonywania kopii bezpieczeństwa zasobów informacyjnych;

7) sieci teleinformatyczne wymagają zarządzania i nadzoru;

8) właściwe wdrażanie procedur obsługi nośników wymiennych oraz ich zastosowania przy wymianie informacji;

9) monitorowanie właściwego zabezpieczenia systemów informatycznych i sieci komputerowych oraz rejestrowanie zdarzeń, błędów oraz informacji w systemie informatycznym.

§ 10. Kontrola dostępu.

1. Procedury kontroli dostępu do informacji i środków przetwarzania informacji są ustanowione, udokumentowane i monitorowane w zgodzie z potrzebami Urzędu i wymaganiami bezpieczeństwa określonymi w PBI.

2. W szczególności dostęp do wszelkich systemów informatycznych wymaga uregulowania w zakresie rejestrowania użytkowników, obowiązku stosowania haseł dostępu, zarządzania uprawnieniami i hasłami, izolowania systemów wrażliwych. Wymagane jest wykonywanie regularnych przeglądów praw dostępu. Uregulowania te powinny obejmować wszystkich użytkowników, ASI i ASU.

3. Użytkownicy, ASI i ASU są odpowiedzialni za ochronę haseł do systemów, prawidłową eksploatację systemów informatycznych i użytkowany sprzęt zgodnie z uregulowaniami poszczególnych systemów.

4. Usługi sieciowe są chronione przed nieautoryzowanym dostępem poprzez określenie zasad korzystania z tych usług, zasad konfiguracji i kontroli zdarzeń w sieci, tj. identyfikację urządzeń, kontrolę połączeń i ruchu w sieciach Urzędu.

5. Przetwarzanie na urządzeniach mobilnych i praca na odległość są uregulowane poprzez określenie zasad korzystania z tych usług oraz wdrożenie odpowiednich zabezpieczeń.

§ 11. Pozyskiwanie, rozwój i utrzymanie systemów informacyjnych.

1. Procesy projektowania systemów teleinformatycznych uwzględniają aspekty bezpieczeństwa informacji oraz koszty wdrożenia i utrzymania odpowiedniego stopnia zabezpieczeń, utraty lub ograniczenia dostępności do zasobu informacyjnego. Procesy te zakresem obejmują aplikacje, rozwiązania projektowe i pliki systemowe.

2. Metody potwierdzania poprawności danych wejściowych, podlegają kontroli przetwarzania i integralności informacji oraz potwierdzania poprawności danych wyjściowych. W uzasadnionych sytuacjach wdraża się zabezpieczenia kryptograficzne.

3. Procedury i metody wprowadzania zmian w aplikacjach oraz nadzór i monitoring prac rozwojowych zapewniają bezpieczeństwo na wszystkich etapach rozwoju i pozyskania.

4. Procesy utrzymania i rozwoju systemów teleinformatycznych zapewniają administrowanie poprawkami do systemów operacyjnych i narzędziowych, z uwzględnieniem szczególnej roli poprawek dla bezpieczeństwa systemów,

§ 12. Zarządzanie incydentami i naruszeniami związanymi z bezpieczeństwem informacji.

1. Ustanawia się procedury postępowania z incydentami, zasady ich identyfikacji, zasady zgłaszania zdarzeń, zasady monitorowania incydentów i obowiązki związane z zabezpieczaniem materiału dowodowego.

2. Użytkownicy zobowiązani są do zgłaszania kierownikowi naruszeń związanych z incydentami i zagrożeniami naruszenia bezpieczeństwa informacji w sytuacjach:

1) utraty lub nieuprawnionego ujawnienia informacji;

2) podejrzenia lub diagnozy słabości systemu przetwarzania informacji;

3) podejrzenia lub stwierdzenia nieprawidłowości zabezpieczeń informacji.

3. Kierownicy w sytuacjach związanych ze stwierdzeniem naruszeń, incydentów bezpieczeństwa czy sytuacji kryzysowych obowiązani są do wyjaśniania wszelkich aspektów utraty lub nieuprawnionego ujawnienia informacji, przedsięwzięcia środków zapobiegawczych oraz wdrożenia postępowania dyscyplinarnego.

4. W przypadku incydentu bezpieczeństwa związanego z zasobami teleinformatycznymi użytkownik jest zobowiązany zgłosić incydent ASI, który prowadzi rejestr zgłoszonych incydentów bezpieczeństwa.

5. Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych w Urzędzie stanowi **Załącznik nr 15** do Zarządzenia.

§ 13. Zarządzanie ciągłością działania.

1. Urząd posiada procedury zarządzania i nadzoru, które zapewnią ciągłość działania kluczowych funkcji, określonych, jako plany awaryjne zarówno w znaczeniu procesów biznesowych jak i organizacyjnych w przypadkach sytuacji kryzysowych, katastrof, awarii zabezpieczeń, utraty informacji i innych.

2. Realizacja procedury planu awaryjnego zapewnia ponowną dostępność informacji na odpowiednim, tj. akceptowalnym poziomie i w odpowiednim czasie, zwłaszcza z uwzględnieniem głównej misji usługowej Urzędu.

3. Plany awaryjne dla utrzymania działalności podlegają wdrożeniu wraz z ich okresowym testowaniem zgodnie z **Załącznikiem 21 i Załącznikiem 22** do Zarządzenia.

§ 14. Audyt i przegląd bezpieczeństwa informacji.

1. Audyty i przeglądy SZBI podlegają wdrożeniu, jako okresowe procedury komórek kontrolnych w Urzędzie.

2. Audyty i przeglądy mogą być realizowane przez podmiot zewnętrzny zgodnie z **Załącznikiem 23** do Zarządzenia.

3. Na podstawie audytu dokonuje się oceny, czy cele, zastosowane zabezpieczenia, procedury i procesy realizowane w Urzędzie są skuteczne i zgodne z wymaganiami PBI.

4. Na podstawie przeglądu dokonuje się oceny możliwości doskonalenia i potrzeb zmian w zarządzaniu bezpieczeństwem informacji.

5. Wyniki audytów i wnioski pokontrolne są przekazane AD oraz kierownikom w celu podjęcia i wdrożenia stosownych działań doskonalących.

§ 15. 1. W celu zapewnienia ochrony przetwarzanych informacji oraz zabezpieczenia prawidłowego przetwarzanie danych osobowych w Urzędzie wprowadza się:

1) Regulamin Korzystania z zasobów informatycznych Urzędu stanowiący Załącznik Nr 4 do Zarządzenia;

2) Zasady korzystania z Internetu oraz poczty elektronicznej Urzędu stanowiące Załącznik Nr 5 do Zarządzenia;

3) Kategorie uprawnień do systemów teleinformatycznych Urzędu stanowiące Załącznik Nr 6 do Zarządzenia;

4) Regulamin użytkowania urządzeń mobilnych w Urzędzie stanowiący Załącznik Nr 7 do Zarządzenia;

5) Klasyfikację incydentów bezpieczeństwa teleinformatycznego w Urzędzie stanowiącą Załącznik Nr 8 do Zarządzenia;

6) Klasyfikację incydentów i zdarzeń dotyczących bezpieczeństwa fizycznego w związku z bezpieczeństwem systemów i urządzeń teleinformatycznych w Urzędzie stanowiącą Załącznik Nr 9 do Zarządzenia;

7) Zasady stosowania pamięci komputerowych i pomocniczych w Urzędzie ze wskazaniem poziomu ich bezpieczeństwa stanowiące Załącznik Nr 10 do Zarządzenia;

8) Zgłoszenie użytkownika systemów informatycznych w Urzędzie stanowiące Załącznik Nr 11 do Zarządzenia;

9) Zgłoszenie podłączenia urządzenia do sieci LAN Urzędu stanowiące Załącznik Nr 12 do Zarządzenia;

10) Zasady wydawania upoważnień AD do przetwarzania danych osobowych oraz wniosek o wydanie/zmianę/odwołanie upoważnienia do przetwarzania danych osobowych stanowiące Załącznik Nr 13 do Zarządzenia;

11) Oświadczenie o zapoznaniu się z zarządzeniem stanowiące Załącznik Nr 14 do Zarządzenia;

12) Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych w Urzędzie stanowiąca Załącznik Nr 15 do Zarządzenia;

13) Procedura administrowania identyfikatorami i hasłami dostępu w Urzędzie stanowiąca Załącznik Nr 16 do Zarządzenia;

14) Procedura tworzenia i przechowywania kopii bezpieczeństwa i archiwum danych w Urzędzie stanowiąca Załącznik Nr 17 do Zarządzenia;

15) Procedura zarządzania ryzykiem z obszaru bezpieczeństwa informacji w Urzędzie stanowiąca Załącznik Nr 18 do Zarządzenia;

16) Arkusz identyfikacji, oceny oraz określenia metody przeciwdziałania ryzyku w obszarze bezpieczeństwa przetwarzanych informacji w Urzędzie stanowiący Załącznik Nr 19 do Zarządzenia;

17) Aktywa informacyjne Urzędu stanowiące Załącznik Nr 20 do Zarządzenia;

18) Strategia zapewnienia ciągłości działania przetwarzania informacji Urzędu stanowiąca Załącznik Nr 21 do Zarządzenia;

19) Bazowy plan ciągłości działania dokumentacji zarządzania ciągłością działania w Urzędzie Miasta Szczecin stanowiący Załącznik Nr 22 do Zarządzenia;

20) Wytyczne dotyczące audytu bezpieczeństwa informacji wykonywane przez podmiot zewnętrzny stanowiące Załącznik Nr 23 do Zarządzenia;

21) Procedura zarządzania uprawnieniami do zasobów/systemów informatycznych Urzędu stanowiąca Załącznik Nr 24 do Zarządzenia;

22) Zasady postępowania z informacjami skasyfikowanymi stanowiące Załącznik Nr 25 do Zarządzenia;

23) Procedura wymiany oraz udostępniania informacji z podmiotami zewnętrznymi stanowiąca Załącznik Nr 26 do Zarządzenia.

§ 16. Zarządzanie usługami, ich dostępność i koszty.

1. Celem procesu zarządzania usługami jest określenie zasad zarządzania wewnętrznymi usługami informatycznymi świadczonymi przez pracowników WInf oraz usługami świadczonymi przez podmioty zewnętrzne na rzecz Urzędu, na rzecz jednostek organizacyjnych Urzędu.

2. Usługi informatyczne są wdrażane w związku ze zdefiniowaną potrzebą Urzędu.

3. Potrzeby dotyczące usług informatycznych są identyfikowane:

1) w związku z analizą wykorzystania infrastruktury informatycznej przeprowadzaną przez WInf,

2) w związku ze zgłoszeniami użytkowników, w tym w ramach zarządzania zmianami,

3) w związku z planowanymi zmianami w sposobie funkcjonowania Urzędu, w tym wynikających z wymagań prawnych.

4. Przed wdrożeniem usługi informatycznej w Urzędzie, wymagane jest zdefiniowanie:

1) celu wdrażanej usługi;

2) użytkowników usługi, rozumianych jako jednostki, które będą korzystać z danej usługi;

3) wymagań w zakresie funkcjonalności usługi;

4) wymagań w zakresie dostępności usługi;

5) wymagań w zakresie wydajności usługi;

6) wpływu na zmianę funkcjonowania Urzędu.

5. Formalne warunki realizacji usługi uzgadniane są z kierownikami będących użytkownikami usługi.

6. Wymagania związane ze świadczeniem usługi zapewnia WInf poprzez:

1) ocenę, czy usługa może być świadczona przez WInf, lub czy konieczne jest zaangażowanie podmiotu zewnętrznego,

2) ocenę, czy wprowadzenie usługi nie wymaga zatrudnienia dodatkowego personelu,

3) określenie zmian w infrastrukturze informatycznej wymaganych w związku z realizacją usługi,

4) określenie udziału podmiotu zewnętrznego w związku z przygotowaniem Urzędu do świadczenia usługi.

7. WInf zapewnia oszacowanie wymaganych kosztów uruchomienia usługi oraz koszty utrzymania usługi.

8. W przypadku akceptacji Dyrektor WInf podejmuje działania celem wdrożenia usługi zgodnie z obowiązującymi w Urzędzie zasadami zarządzania zmianą.

9. Opis usługi uzgodniony z właściwymi kierownikami, będącymi użytkownikami zostaje zdefiniowany przez Dyrektora WInf jako umowa usługi informatycznej.

10. Wszystkie usługi opisane są w katalogu usług, który obejmuje:

1) usługi wdrożone,

2) usługi aktualnie wdrażane,

3) usługi wycofane.

11. Opis usługi w katalogu zawiera:

1) nazwę usługi,

2) specyfikację usługi,

3) warunki umowy usługi informatycznej,

4) sposób realizacji usługi,

5) wykaz pracowników WInf zaangażowanych w świadczenie usługi;

6) opis infrastruktury informatycznej wykorzystywanej do świadczenia usługi.

12. Dyrektor WInf lub osoba wyznaczona odpowiedzialny jest za prowadzenie aktualnego katalogu usług w Urzędzie.

13. Każdy użytkownik posiada dostęp do katalogu usług Urzędu wyłącznie w zakresie listy aktualnie wdrożonych usług wraz z ich specyfikacją oraz warunkami umowy usługi informatycznej.

14. Dyrektor WInf lub wyznaczony pracownik okresowo przeprowadza przegląd katalogu usług realizowanych w Urzędzie.

15. W przypadku wątpliwości czy dana usługa jest wykorzystywana, bądź użyteczna dla pracy Urzędu, Dyrektor WInf lub osoba wyznaczona przeprowadza uzgodnienia z kierownikami użytkującymi usługi.

16. O planowanym wycofaniu usługi Dyrektor WInf informuje wszystkich użytkowników usługi drogą elektroniczną.

17. W ramach monitorowania infrastruktury informatycznej i obsługi incydentów rejestruje się wszelkie zdarzenia mogące wpłynąć na niedostępność świadczonych usług.

18. WInf prowadzi rejestr przerw w świadczeniu usług, zawierający w szczególności przyczyny i czas niedostępności usług.

19. Dyrektor WInf przedkłada dwa razy w roku AD raport wskazujący:

1) spełnienie warunków umów usług informatycznych,

2) podjęte działania naprawcze,

3) koszty związane z realizacją usług w danym okresie czasu.

20. Monitorowanie usług świadczonych przez podmioty zewnętrzne na rzecz Urzędu jest prowadzone zgodnie z zapisami szczegółowymi umów.

21. Dyrektor WInf lub wyznaczony pracownik szacuje koszty związane ze świadczeniem usług na rzecz Urzędu. W szczególności dla każdej z usług określa:

1) niezbędne zaangażowanie pracowników WInf,

2) koszty związane z materiałami eksploatacyjnymi,

3) koszty związane z wprowadzaniem zmian w świadczeniu usługi.

22. Koszty usług świadczonych przez podmioty zewnętrzne wskazane są w stosownych umowach z tymi podmiotami.

23. Dyrektor WInf przedstawia AD raport zawierający:

1) zestawienie kosztów związanych ze świadczeniem usług w ujęciu miesięcznym lub kwartalnym.

2) listę jednostek będących użytkownikami poszczególnych usług.

24. Zapewnienie ciągłości świadczenia usług jest realizowane zgodnie z działaniami wynikającymi z Załącznika 21 i Załącznika 22 do Zarządzenia.

§ 17. Traci moc Zarządzenie Nr 49/10 Prezydenta Miasta Szczecin z dnia 5 lutego 2010 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji Urzędu Miasta Szczecin i Instrukcji zarządzania systemem informatycznym.

§ 18. Zarządzenie wchodzi w życie z dniem podpisania.

Prezydent Miasta

Piotr Krzystek