ZARZĄDZENIE NR 685/2017
PREZYDENTA MIASTA WAŁBRZYCH

z dnia 23 października 2017 r.

w sprawie wprowadzenia dokumentacji przetwarzania danych osobowych w Urzędzie Miejskim w Wałbrzychu

Na podstawie art. 36 ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tj. Dz. U. z 2016r. poz. 922), Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. 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 2004r. Nr 100, poz. 1024) zarządza się co następuje:

§ 1. Wprowadza się:

1) Politykę Bezpieczeństwa przetwarzania danych osobowych Urzędu Miejskiego stanowiącą załącznik nr 1 do zarządzenia.
2) Instrukcję Zarządzania Systemem Informatycznym Urzędu Miejskiego w Wałbrzychu stanowiącą załącznik nr 2 do zarządzenia.

§ 2. Wykonanie zarządzenia i prowadzenie bieżącej kontroli jego wykonywania powierzam Kierownikowi Biura Informatyki Urzędu Miejskiego w Wałbrzychu.

§ 3. Traci moc zarządzenie nr 769/2016 Prezydenta Miasta Wałbrzycha z dnia 19.10.2016r. w sprawie wprowadzenia dokumentacji przetwarzania danych osobowych w Urzędzie Miejskim w Wałbrzychu.

§ 4. Zarządzenie wchodzi w życie z dniem podpisania i podlega ogłoszeniu w Biuletynie Informacji Publicznej Urzędu Miejskiego w Wałbrzychu.

TYTUŁ:	**Polityka Bezpieczeństwa**		
OPRACOWAŁ:	Piotr Müller Imię i nazwisko	Podpis	19-10-2017 Data
SPRAWDZIŁ:	Joanna Stypułkowska Imię i nazwisko	Podpis	19-10-2017 Data
ZATWIERDZIŁ:	Piotr Müller Imię i nazwisko	Podpis	19-10-2017 Data
OBOWIĄZUJE OD DNIA:	***23-10-2017***		

Metryka zmian z edycji I do edycji J		
Punkt	**Było**	**Jest**
3	x	j. Budynek Dmowskiego 2 – adres Dmowskiego 2;
6.2 p.5	Wdrożono system kopii zapasowych z wykorzystaniem nośników zewnętrznych.	Wdrożono system kopii zapasowych będący kompletnym wewnętrznie redundantnym systemem zarządzania kopią zapasową o wysokiej niezawodności i dostępności.
6.2 p.6	Nośniki zawierające kopie zapasowe przechowywane są w szafie pancernej, w innym pomieszczeniu niż serwerownia – miejsce składowania danych.	System kopii zapasowych działa niezależnie od systemu składowania danych. W innym pomieszczeniu, innego budynku.
6.2	X	1. Kluczowe składniki systemy informatycznego takie jak: a. routery (UTM) styku LAN – WAN, b. macierze dyskowe, c. serwery, d. przełączniki dystrybucyjne sieci Lan i Sun muszą winny być wdrażane w systemie redundancji wewnętrznej lub zewnętrznej (high availability), to jest posiadać zwielokrotnione podzespoły lub instancje tak, by awaria pojedynczego elementu nie powodowała przerw w pracy systemu informatycznego.
6.	Połączono punkty **6.3 Środki ochrony w ramach oprogramowania systemu** i **6.5 Środki ochrony w ramach systemu informatycznego.** Pozostałe akapity zostały przenumerowane.	
6.5 (pop. 6.6)	x	16. W kontaktach z kontrahentami przy których dochodzi do przetwarzania danych osobowych wymagane wydanie upoważnienia do przetwarzania danych osobowych w formie upoważnienia imiennego, klauzuli na umowie lub osobnej umowy o przetwarzanie danych osobowych.

SPIS TREŚCI

1 POSTANOWIENIA OGÓLNE

1.1 DEFINICJE

Ilekroć w niniejszym dokumencie jest mowa o :

1. **Urzędzie** – należy przez to rozumieć Urząd Miejski w Wałbrzychu;
2. **Administratorze Danych Osobowych (dalej Administratorze danych)** – należy przez to rozumieć Prezydenta Miasta Wałbrzycha, który poprzez wyznaczone osoby sprawuje ogólną kontrolę i nadzór nad przestrzeganiem postanowień Polityki Bezpieczeństwa;
3. **Pełnomocnik Bezpieczeństwa Informacji** – należy przez to rozumieć pracownika wyznaczonego przez Administratora danych by w jego imieniu nadzorował przestrzeganie zasad ochrony określonych w niniejszym dokumencie oraz wymagań w zakresie ochrony wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych,
4. **Kierowniku Biura Informatyki** – należy przez to rozumieć pracownika Urzędu odpowiedzialnego za funkcjonowanie systemu informatycznego Urzędu oraz stosowanie technicznych i organizacyjnych środków ochrony,
5. **Administratorze systemu** – należy przez to rozumieć pracownika Biura Informatyki, który posiada uprawnienia do administrowania określonymi zasobami informatycznymi Urzędu. Czasowo, za zgodą Pełnomocnika Bezpieczeństwa Informacji (z up. Administratora danych) oraz Kierownika Biura Informatyki Administratorem Systemu pracującym może zostać inny pracownik urzędu lub przedstawiciel firmy współpracującej.
6. **Użytkowniku systemu** – należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym Urzędu. Użytkownikiem może być pracownik Urzędu, osoba wykonująca pracę na podstawie umowy zlecenie lub innej umowy cywilnoprawnej, osoba odbywająca, praktykę, staż w Urzędzie lub wolontariusz,
7. **Sieci lokalnej** - należy przez to rozumieć połączenie systemów informatycznych Urzędu wyłącznie dla własnych jej potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnej,
8. **Sieci rozległej** - należy przez to rozumieć publiczną sieć telekomunikacyjną w rozumieniu ustawy z dnia z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dziennik Ustaw z 2004 r. Nr 171 poz. 1800 ze zmianami) i niebędącą siecią lokalną.
9. **Ustawie** – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz. U. z 2016r. poz. 922 z późn. zm.),
10. **Rozporządzeniu** – 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),

1.2 CEL

Wdrożenie polityki bezpieczeństwa w Urzędzie ma na celu zabezpieczenie przetwarzanych przez niego danych osobowych, w tym danych przetwarzanych w systemie informatycznym Urzędu i poza nim, poprzez wykonanie obowiązków wynikających z ustawy i rozporządzenia.

W związku z tym, że w zbiorach danych Urzędu przetwarzane są między innymi dane wrażliwe, a system informatyczny administratora danych posiada szerokopasmowe połączenie z internetem, niniejsza polityka bezpieczeństwa służy zapewnieniu wysokiego poziomu bezpieczeństwa danych w rozumieniu § 6

rozporządzenia. Niniejszy dokument opisuje niezbędny do uzyskania tego bezpieczeństwa zbiór procedur i zasad dotyczących przetwarzania danych osobowych oraz ich zabezpieczenia.

1.3 ZAKRES STOSOWANIA

1. Niniejsza polityka bezpieczeństwa dotyczy zarówno danych osobowych przetwarzanych w sposób tradycyjny w księgach, wykazach i innych zbiorach ewidencyjnych, jak i w systemach informatycznych.
2. Procedury i zasady określone w niniejszym dokumencie stosuje się do wszystkich osób upoważnionych do przetwarzania danych osobowych, zarówno zatrudnionych, jak i innych, np. wolontariuszy, praktykantów, stażystów.

2 ADMINISTRATOR DANYCH I ADMINISTRATOR BEZPIECZEŃSTWA INFORMACJI

2.1 WYZNACZENIE ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI

Administrator danych nie powołuje Administratora Bezpieczeństwa Informacji.

2.2 ZADANIA ADMINISTRATORA DANYCH

Administrator danych za pomocą Pełnomocnika Bezpieczeństwa Informacji realizuje zadania w zakresie nadzoru nad przestrzeganiem zasad ochrony danych osobowych, w tym zwłaszcza:

1. Sprawuje nadzór nad wdrożeniem stosownych środków fizycznych, a także organizacyjnych i technicznych – w celu zapewnienia bezpieczeństwa danych;
2. Sprawuje nadzór nad funkcjonowaniem systemu zabezpieczeń, w tym także nad prowadzeniem ewidencji z zakresu ochrony danych osobowych;
3. Koordynuje wewnętrzne audyty przestrzegania przepisów o ochronie danych osobowych;
4. Nadzoruje udostępnianie danych osobowych odbiorcom danych i innym podmiotom;
5. Przygotowuje wnioski zgłoszeń rejestracyjnych i aktualizacyjnych zbiorów danych oraz prowadzi inną korespondencję z Generalnym Inspektorem Danych Osobowych;
6. Zatwierdza wzory dokumentów (odpowiednie klauzule w dokumentach) dotyczących ochrony danych osobowych; przygotowywane przez komórki organizacyjne Urzędu.
7. Nadzoruje prowadzenie ewidencji i innej dokumentacji z zakresu ochrony danych osobowych;
8. Prowadzi oraz aktualizuje dokumentację opisującą sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych;
9. Podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia systemu informatycznego;
10. Zatwierdza materiały szkoleniowe z zakresu ochrony danych osobowych i nadzoruje szkolenia osób upoważnianych do przetwarzania danych osobowych;

2.3 PEŁNOMOCNIK BEZPIECZEŃSTWA INFORMACJI

1. Administrator danych wyznacza na Pełnomocnika Bezpieczeństwa Informacji Sekretarza Miasta
2. Pełnomocnik Bezpieczeństwa Informacji z upoważnienia Administratora danych w jego imieniu wykonuje zadania z p. 2.2 oraz:
    a. w porozumieniu z Administratorem Danych na czas nieobecności (urlop, choroba) wyznacza swojego zastępcę,
    b. z upoważnienia Administratora Danych podpisuje zgłoszone do GIODO zbiory danych osobowych.

3. Pełnomocnik Bezpieczeństwa Informacji wykonuje powierzone zadania osobiście lub poprzez wyznaczonych przez siebie pracowników.

3 OBSZAR PRZETWARZANIA DANYCH OSOBOWYCH.

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;

1. Obszarem, w którym przetwarzane są dane osobowe są niżej wymienione budynki:
   a. Budynek Ratusz – adres: pl. Magistrackim 1;
   b. Budynek Matejki 1 – adres: ul. Matejki 1;
   c. Budynek Matejki 2 – adres: ul. Matejki 2;
   d. Budynek Matejki 3 – adres: ul. Matejki 3;
   e. Budynek Kopernika – adres: ul. Kopernika 2;
   f. Budynek Sienkiewicza – adres: ul. Sienkiewicza 6-8;
   g. Budynek Sienkiewicza 9 – adres: ul. Sienkiewicza 9;
   h. Budynek Słowackiego – adres: ul. Słowackiego 23A;
   i. Budynek Rynek 23 – adres: Rynek 23;
   j. Budynek Dmowskiego 2 – adres Dmowskiego 2;
2. Obszar, w którym przetwarzane są dane osobowe należy zamykać na czas nieobecności w nim osób zatrudnionych przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do niego osób trzecich.
3. Szczególnym obszarem, w którym przetwarzane są dane o wysokim priorytecie i przebywać w nim mogą jedynie osoby zatrudnione ze specjalnym upoważnieniem są pomieszczenia:
   a. Pokój 24 parteru budynku Kopernika oznaczony jako Serwerownia Główna;
   b. Pokój 116 pierwszego piętra budynku Kopernika oznaczony jako pomieszczenie szaf krosowniczych;
   c. Pokój 21 parteru budynku Kopernika oznaczony jako pomieszczenie UPS;
   d. Pokój nr 4 pomieszczeń przyziemia budynku Ratusza będący pomieszczeniem urządzenia UPS Ratusza;
   e. Wewnętrzny pokój w pokoju 28 w budynku Ratusza oznaczony jako Serwerownia;
   f. Pomieszczenie szafy krosowniczej dostępne z sali operacyjnej budynku Sienkiewicza;
   g. Wewnętrzny pokój w pokoju 15 w budynku Matejki 3 oznaczony jako pomieszczenie szafy informatycznej;
   h. Pokój nr 9 na Sienkiewicza 9 oznaczony jako Serwerownia Biura Komunikacji;
   i. Pokój w budynku Rynek 23 będący krosownią parteru budynku;
   j. Pokój w budynku Rynek 23 będący krosownią główną budynku;

4 WYKAZ ZBIORÓW DANYCH OSOBOWYCH PRZETWARZANYCH W SYSTEMIE INFORMATYCZNYM

W skład zbioru wchodzą :

- dokumentacja papierowa (korespondencja, wnioski, deklaracje itd.),
- urządzenia i oprogramowanie komputerowe służące do przetwarzania informacji oraz procedury przetwarzania danych w tym systemie, w tym procedury awaryjne,
- wydruki komputerowe.

Wykaz zbiorów danych osobowych przetwarzanych w systemie informatycznym prowadzi Kierownik Biura Informatyki według wzoru określonego w załączniku nr 1.1 do niniejszego opracowania.

5 STRUKTURY ZBIORÓW DANYCH OSOBOWYCH ORAZ SPOSÓB PRZEPŁYWU DANYCH

Opisy struktur zbiorów danych osobowych oraz powiązań miedzy zbiorami jak również sposób przepływu danych pomiędzy poszczególnymi systemami prowadzi Kierownik Biura Informatyki według wzoru określonego w załączniku nr 1.1 do niniejszego opracowania.

6 ŚRODKI TECHNICZNE I ORGANIZACYJNE NIEZBĘDNE DO ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH.

6.1 ŚRODKI OCHRONY FIZYCZNEJ

1. Budynki Urzędu, w których zlokalizowany jest obszar przetwarzania danych osobowych jest zamykany po zakończeniu pracy. Budynki, które nie są dozorowane w sposób stały zostały wyposażone w system alarmowy z monitoringiem.
2. Urządzania służące do przetwarzania danych osobowych znajdują się w pomieszczeniach zabezpieczonych.
3. Serwerownie stanowią dodatkowo zamykane i klimatyzowane pomieszczenia do których dostęp jest monitorowany i rejestrowany.
4. Komputery serwery służące do przechowywania danych są zamknięte w szafach informatycznych, do których klucze są w posiadaniu Biura Informatyki. Szafy są wentylowane automatycznymi wentylatorami z termostatem.
5. Przebywanie osób nieuprawnionych w pomieszczeniach tworzących obszar przetwarzania danych osobowych dopuszczalne jest tylko w obecności osoby zatrudnionej przy przetwarzaniu danych lub w obecności Administratora Danych lub innej osoby upoważnionej.
6. Pomieszczenia, o których mowa powyżej powinny być zamykane na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich.
7. W przypadku przebywania osób postronnych w pomieszczeniach, o których mowa wyżej, monitory stanowisk dostępu do danych osobowych powinny być ustawione w taki sposób aby uniemożliwiać im wgląd w dane.
8. Do przebywania w pomieszczeniach serwerowni i Serwerowni Głównej uprawnieni są Administrator Danych, Pełnomocnik Bezpieczeństwa Informacji oraz pracownicy Biura Informatyki.
9. Przebywanie w pomieszczeniach serwerowni i Serwerowni Głównej osób nieuprawnionych (konserwator, osoba sprzątająca) dopuszczalne jest tylko w obecności jednej z osób upoważnionych, o których mowa w pkt. 8, a w przypadku ich nieobecności – w obecności osoby pisemnie upoważnionej przez Administratora Danych. Rejestr wejść jest prowadzony w Biurze Informatyki.

6.2 ŚRODKI SPRZĘTOWE, INFORMATYCZNE I TELEKOMUNIKACYJNE

2. System informatyczny oraz systemy przetwarzające dane zabezpieczone są przed nieupoważnionym dostępem osób trzecich systemem uwierzytelniania i autoryzacji użytkowników.
3. Urządzenia wchodzące w skład systemu informatycznego podłączone są do odrębnego obwodu elektrycznego, systemy składowania danych zabezpieczone na wypadek zaniku napięcia albo awarii w sieci zasilającej urządzeniami podtrzymującymi napięcie (UPS).
4. Siec lokalna podłączona do Internetu za pomocą zestawu „Zapór Ogniowych” (Firewall) tworzących strefę zdemilitaryzowaną (ang. demilitarized zone – DMZ).

5. Na wszystkich serwerach oraz wszystkich stacjach roboczych zainstalowano oprogramowanie antywirusowe. Poczta elektroniczna wpływająca do Urzędu skanowana jest programem antywirusowym zarówno przed wysłaniem jak i podczas odbierania wiadomości.
6. Wdrożono system kopii zapasowych będący kompletnym wewnętrznie redundantnym systemem zarządzania kopią zapasową o wysokiej niezawodności i dostępności.
7. System kopii zapasowych działa niezależnie od systemu składowania danych. W innym pomieszczeniu, innego budynku.
8. Kluczowe składniki systemu informatycznego tj. serwery, macierze dyskowe, brzegowe urządzenia sieciowe, stacje robocze, nośniki danych oraz strategiczne urządzenie wspomagające (urządzenia UPS, streamery, NAS itp.) posiadają określony cykl życia (ang. live time). Po upłynięciu tego okresu winny być wymienione na nowe. Zestawienie sprzętu wraz z określonym cyklem życia stanowi załącznik nr 3 do Polityki Bezpieczeństwa (ozn. 1.3).
9. Kluczowe składniki systemy informatycznego takie jak:
    a. routery (UTM) styku LAN – WAN,
    b. macierze dyskowe,
    c. serwery,
    d. przełączniki dystrybucyjne sieci Lan i Sun

   muszą winny być wdrażane w systemie redundancji wewnętrznej lub zewnętrznej (high availability), to jest posiadać zwielokrotnione podzespoły lub instancje tak, by awaria pojedynczego elementu nie powodowała przerw w pracy systemu informatycznego.

6.3 ŚRODKI OCHRONY W RAMACH OPROGRAMOWANIA SYSTEMU

1. Dostęp fizyczny do baz danych osobowych zastrzeżony jest wyłącznie Administratora Systemu.
2. Konfiguracja systemu umożliwia użytkownikom końcowym dostęp do danych osobowych jedynie za pośrednictwem aplikacji.
3. System informatyczny pozwala zdefiniować odpowiednie prawa dostępu do zasobów informatycznych systemu.
4. W sieciowym systemie operacyjnym zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do systemu.
5. Wszystkie komputery Urzędu są skonfigurowane w sposób uniemożliwiający logowanie lokalne. Jedynym możliwym uruchomieniem systemu jest logowanie do domeny Active Directrory o nazwie um.local za pomocą ważnego identyfikatora i hasła dostępu.
6. Zastosowano automatyczny i zabezpieczony hasłem wygaszacz ekranu w przypadku dłuższej nieaktywności użytkownika.
7. Każdy użytkownik systemu może i powinien na czas przerwy w pracy w systemie informatycznym zablokować komputer za pomocą klawiatury, kombinacją klawiszy [windows] + L.

6.4 ŚRODKI OCHRONY W RAMACH NARZĘDZI BAZ DANYCH I INNYCH NARZĘDZI PROGRAMOWYCH

1. Aplikacje służące do przetwarzania danych osobowych muszą posiadać mechanizmy jednoznacznego uwierzytelniania użytkownika i autoryzacji poziomu uprawnień za pomocą 1 z 2 metod:
    a. Uwierzytelnienie i autoryzacja za pomocą domeny MS Active Directory protokołem Kerberos, ADSI, LDAP ;
    b. Dodatkowego loginu i hasła dostępu na poziomie aplikacji przetwarzającej dane.
2. Dla każdego użytkownika systemu informatycznego jest ustalony odrębny identyfikator.
3. Zdefiniowano użytkowników i ich prawa dostępu do danych osobowych na poziomie systemu informatycznego (unikalny identyfikator i hasło w domenie MS Active Driectory).

4. Systemy informatyczne, które udostępniają dane osobowe muszą spełniać warunki opisane z art. 32 i 33 ustawy i § 7 rozporządzenia. Wymagane w przywołanych przepisach obowiązki sprowadzają się m.in. do zapewnienia i udostępniania – na żądanie osoby, której dane są przetwarzane – informacji o:
    a. Dacie, od kiedy przetwarza się w zbiorze jej dane osobowe, oraz treści tych danych;
    b. Źródle, z którego pochodzą dane jej dotyczące, chyba że administrator jest obowiązany do zachowania w tym zakresie tajemnicy państwowej, służbowej lub zawodowej;
    c. Sposobie i zakresie udostępniania jej danych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym dane te są udostępniane;
    d. Sposobie, w jaki zebrano dane;

6.5 ŚRODKI ORGANIZACYJNE

1. Administrator danych przyznaje uprawnienia dostępu do przetwarzania danych osobowych w formie pisemnego upoważnienia.
2. Osoby upoważnione do przetwarzania danych osobowych są przed dopuszczeniem ich do pracy z tymi danymi szkolone w zakresie obowiązujących przepisów o ochronie danych osobowych, procedur przetwarzania danych oraz informowane o podstawowych zagrożeniach związanych z przetwarzaniem danych w systemie informatycznym.
3. Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych.
4. Osobę, która utraciła uprawnienia dostępu do danych osobowych, należy niezwłocznie wyrejestrować i unieważnić jej hasło oraz podjąć inne niezbędne czynności uniemożliwiające jej dalszy dostęp do danych.
5. Czynności wymienione w pkt. 4 wykonuje Administrator Systemu samodzielnie lub na polecenie Administratora danych lub osoby upoważnionej.
6. Nie wolno wykorzystywać identyfikatora osoby, która utraciła uprawnienia do dostępu do danych. Identyfikator osoby winien być unikalny.
7. Wprowadzono Instrukcje Zarządzania Systemem Informatycznym.
8. Wprowadzono zasadę czystego biurka i czystego ekranu.
9. Zdefiniowano procedury postępowania w sytuacji naruszenia ochrony danych osobowych.
10. Wprowadzono obowiązek rejestracji wszystkich przypadków awarii systemu, działań konserwacyjnych w systemie oraz naprawy systemu.
11. Określono sposób postępowania z nośnikami informacji.
12. Podczas wymiany informacji z osobą której tożsamości nie można zweryfikować (np. rozmowa telefoniczna, nie podpisany podpisem elektronicznym e-mail) urzędnik może przekazać informacje dotyczące pracy Urzędu nie zakazane prawem, a będące w jego posiadaniu lub objęte zakresem jego kompetencji lub uprawnień.
    Szczególnie powinny to być informacje zależne od potrzeb i oczekiwań klientów a dotyczące:
    a. organizacji pracy Urzędu,
    b. obowiązującego prawa zewnętrznego i miejscowego w tym treści tego prawa oraz
    c. zmianach tego prawa,
    d. naborze kandydatów do służby urzędniczej,
    e. obowiązujących procedur,
    f. prowadzonych rejestrach, ewidencjach i archiwach oraz o sposobach i zasadach udostępniania danych w nich zawartych,
    g. rodzajów usług publicznych,
    h. treści aktów administracyjnych i ich rozstrzygnięć nie rozstrzygnięć dotyczących spraw indywidualnych bo nie wiemy z kim rozmawiamy ,
    i. stanowiska w prawach publicznych zajęte przez organy władzy stanowiącej i wykonawczej,
    j. kompetencji kierownictwa Urzędu i urzędników,

k. inne informacje, będące powszechnie znanymi, które mogą przyczynić się do nawiązania kontaktu z klientem i są potrzebne lub oczekiwane przez klienta.

13. Podczas wymiany informacji z osobą której tożsamości nie można zweryfikować (np. rozmowa telefoniczna, niepodpisany podpisem elektronicznym e-mail) urzędnik nie może przekazać informacji dotyczących:
    a. danych osobowych stron postępowania administracyjnego,
    b. przebiegu indywidualnego postępowania administracyjnego,
    c. tajemnicy handlowej i skarbowej,
    d. informacji niejawnych,
14. Każdy dokument papierowy przeznaczony do wyrzucenia powinien być uprzednio zniszczony w sposób uniemożliwiający jego odczytanie (np. przy pomocy niszczarki do dokumentów).
15. W umowach zawieranych z kontrahentami zewnętrznymi należy umieszczać klauzulę o zachowaniu poufności. W uzasadnionych przypadkach w powyższych umowach należy określić sankcję za złamanie takiej klauzuli.
16. W kontaktach z kontrahentami przy których dochodzi do przetwarzania danych osobowych wymagane wydanie upoważnienia do przetwarzania danych osobowych w formie upoważnienia imiennego, klauzuli na umowie lub osobnej umowy o przetwarzanie danych osobowych.

6.6 ODPOWIEDZIALNOŚĆ OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Niezastosowanie się do prowadzonej przez administratora danych polityki bezpieczeństwa przetwarzania danych osobowych, której założenia określa niniejszy dokument, i naruszenie procedur ochrony danych przez pracowników upoważnionych do przetwarzania danych osobowych będzie potraktowane jako ciężkie naruszenie obowiązków pracowniczych.

Niezależnie od powyższego, osoby popełniające przestępstwo mogą być pociągnięte do odpowiedzialności karnej zwłaszcza na podstawie art. 51-52 ustawy oraz art. 266 Kodeksu karnego.

7 POSTANOWIENIA KOŃCOWE.

Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest przed dopuszczeniem do przetwarzania danych zapoznać się:

1. Z niniejszym dokumentem;
2. Ustawą,
3. Rozporządzeniem,
4. Zarządzeniem nr ____/2017 Prezydenta Miasta Wałbrzycha w sprawie wprowadzenia dokumentacji przetwarzania danych osobowych w Urzędzie Miejskim w Wałbrzychu, oraz złożyć stosowne oświadczenie, potwierdzające znajomość treści ww. dokumentów.

TYTUŁ:	**Instrukcja Zarządzania Systemem Informatycznym Urzędu Miejskiego w Wałbrzychu.**		
OPRACOWAŁ:	Piotr Müller Imię i nazwisko	Podpis	19-10-2017 Data
SPRAWDZIŁ:	Joanna Stypułkowska Imię i nazwisko	Podpis	19-10-2017 Data
ZATWIERDZIŁ:	Piotr Müller Imię i nazwisko	Podpis	19-10-2017 Data
OBOWIĄZUJE OD DNIA:	***23-10-2017***		

Metryka zmian z edycji I do edycji J		
Punkt	Było	Jest
4.3.1	System informatyczny Urzędu działa w oparciu o sieć komputerową Ethernet w 6 budynkach należących do Urzędu.	System informatyczny Urzędu działa w oparciu o sieć komputerową Ethernet w 10 lokalizacjach należących do Urzędu.
4.3.2 p.1	W sieci informatycznej urzędu wypromowano domenę Active Directory o nazwie um.local.	W sieci informatycznej urzędu wypromowano domenę Active Directory (AD) o nazwie um.local.
4.3.2 p.2	Z serwerów urzędowych pracujących pod kontrolą systemu Windows 2003 wyodrębniono 4 kontrolery domeny Active Directory wszystkie zlokalizowane w serwerowni głównej w budynku przy ul. Kopernika 2	Z serwerów urzędowych pracujących w domenie AD o funkcjonalności na poziomie Windows Server 2003 wyodrębniono 4 kontrolery domeny. Wszystkie zlokalizowane w serwerowni głównej w budynku przy ul. Kopernika 2
4.3.2 p.4	Stacje robocze pracujące w sieci informatycznej Urzędu muszą poprawnie zalogować się do domeny Active Directory. W związku z tym ustala się jako minimalny system Windows XP Professional, a zalecany system to Windows 7, 8 lub 10 w wersji Professional.	Stacje robocze pracujące w sieci informatycznej Urzędu muszą poprawnie zalogować się do domeny Active Directory.
4.3.2 p.5	Dodano punkt i od punktu 6 wszystkie dotychczasowe punkty zostały przenumerowane o 1 w górę	Ze względów bezpieczeństwa i dostępności aktualizacji zabezpieczeń minimalnym systemem operacyjnym dopuszczalnym do zalogowania się w sieci informatycznej urzędu to system MS Windows 7, 8, 8.1 lub 10 w wersjach Professional.
4.3.2 p.6 (pop. 5)	Niedopuszczalne jest stosowanie systemów nie posiadających odpowiedniego systemu zabezpieczeń (np. Windows 98, Windows 95) oraz systemów nie posiadających systemu logowania do domeny Windows (np. Windows XP Home Edition, Windows Vista Home Basic, Windows 7 Home itp.).	Niedopuszczalne jest stosowanie systemów nie posiadających odpowiedniego systemu zabezpieczeń (np. Windows 98, Windows 95, Windows XP i Vista) oraz systemów nie posiadających systemu logowania do domeny Windows (np. wersje Windows Home).

SPIS TREŚCI

1 CEL

Celem instrukcji jest określenie sposobu zarządzania systemem informatycznym Urzędu Miejskiego w Wałbrzychu.

2 ZASADY OGÓLNE

Zawarte w instrukcji procedury i wytyczne są przekazywane osobom odpowiedzialnym za ich realizację stosownie do przyznanych uprawnień i zakresu obowiązków.

3 DEFINICJE

Ilekroć w niniejszym dokumencie jest mowa o :

1. **Urzędzie** – należy przez to rozumieć Urząd Miejski w Wałbrzychu
2. **Administratorze Danych** – należy przez to rozumieć Prezydenta Miasta Wałbrzycha, który poprzez wyznaczone osoby sprawuje ogólną kontrolę i nadzór nad przestrzeganiem postanowień Instrukcji Zarządzenia Systemem Informatycznym
3. **Pełnomocnik Bezpieczeństwa Informacji** – należy przez to rozumieć pracownika wyznaczonego przez Administratora Danych by w jego imieniu nadzorował przestrzeganie zasad ochrony określonych w niniejszym dokumencie oraz wymagań w zakresie ochrony wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych,,
4. **Kierowniku Biura Informatyki** – należy przez to rozumieć pracownika Urzędu odpowiedzialnego za funkcjonowanie systemu informatycznego Urzędu oraz stosowanie technicznych i organizacyjnych środków ochrony,
5. **Administrator systemu** – należy przez to rozumieć pracownika Biura Informatyki, który posiada uprawnienia do administrowani określonymi zasobami informatycznymi Urzędu. Czasowo, za zgodą Administratora Bezpieczeństwa Informacji oraz Kierownika Biura informatyki Administratorem Systemu może zostać inny pracownik urzędu lub przedstawiciela firmy współpracującej.
6. **Użytkowniku systemu** – należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym Urzędu. Użytkownikiem może być pracownik Urzędu, osoba wykonująca pracę na podstawie umowy zlecenie lub innej umowy cywilnoprawnej, osoba odbywająca staż w Urzędzie lub wolontariusz,
7. **Sieci lokalnej** - należy przez to rozumieć połączenie systemów informatycznych Urzędu wyłącznie dla własnych jej potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnej,
8. **Sieci rozległej** - należy przez to rozumieć publiczną sieć telekomunikacyjną w rozumieniu ustawy z dnia z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dziennik Ustaw z 2004 r. Nr 171 poz. 1800 ze zmianami) i niebędącą siecią lokalną.
9. **Zasobie wspólnym** – należy rozumieć wydzieloną przestrzeń dysków serwerów z przeznaczeniem na służbowe dane i dokumenty elektroniczne. Zasoby te budowane są hierarchicznie zgodnie ze schematem organizacyjnym urzędu.
10. **Uwierzytelnianie** – należy przez to rozumieć proces rozpoznawania użytkownika w systemie komputerowym. W systemach komputerowych urzędu funkcjonują trzy sposoby uwierzytelniania.
    - Login użytkownika,
    - Karta mikroprocesorowa

- Osobno zdefiniowane metody biometryczne.

11. **Autoryzacji** – jest to proces identyfikacji uprawnień do systemu. Autoryzacja odbywa się za pomocą hasła użytkownika lub pinu karty mikroprocesorowej. Zasady uprawnień do systemów określa poszczególna polityka uprawnień w każdym systemie.
12. **Portalu Miejskim** – należy rozumieć zespół stron www w zarządzie Urzędu stanowiącym logicznie powiązany serwis informacyjny publikujący treści z zakresu działania Urzędu i Miasta Wałbrzycha.

4 SYSTEM INFORMATYCZNY

4.1 WYMAGANIA TECHNICZNE

1. Wszystkie środki sprzętowe i programowe, również nowo kupowane, służące do przetwarzania informacji elektronicznej podlegają autoryzacji przez Kierownika Biura Informatyki.
2. Wszystkie zasoby systemu informatycznego Urzędu podlegają ewidencjonowaniu w elektronicznej Ewidencji Sprzętu Komputerowego.
3. Każdorazowe zmiany w konfiguracji zarówno sprzętowej jak i programowej podlegają ewidencjonowaniu w ww. Ewidencji.
4. Każdy z wdrażanych systemów informatycznych podlega audytowi Biura Informatyki i jego działanie oraz bezpieczeństwo przechowywania danych jest odbierane przez Kierownika Biura Informatyki.
5. W uzasadnionych przypadkach zastępowany system (tradycyjny lub informatyczny) prowadzony jest równolegle z nowo wdrażanym systemem informatycznym, a dane wejściowe i wyniki wyjściowe polegają weryfikacji.
6. Każdy system informatyczny musi mieć przynajmniej dwa poziomy autoryzacji. Użytkownika i Administracyjny. W trybie użytkownika nie może być dostępna kontrola pracy innych użytkowników, jak i zarządzanie ich uprawnieniami do systemu.
7. System informatyczny nie dopuszcza logowania anonimowego. Dane przechowywane w systemie informatycznym nie są dostępne dla klientów urzędu. Dane publikowane, dostępne dla klientów urzędu publikowane są w Biuletynie Informacji Publicznej i stronach internetowych Urzędu Miasta.
8. Każdy serwer Urzędu musi być zasilany za pośrednictwem urządzenia do awaryjnego zasilania (UPS). Urządzenie to w razie awarii zasilania ma bezpieczne i automatyczne zakończyć pracę serwera oraz powiadomić o tym fakcie administratora za pomocą poczty elektronicznej i lub wiadomości SMS.
9. Każdy komputer użytkownika musi być zasilany z wydzielonej linii energetycznej poprzez elektryczną listwę z zabezpieczeniem przeciwprzepięciowym.
10. Tam gdzie to możliwe, komputery użytkowników, zwłaszcza komputery przetwarzające dane osobowe i systemów merytorycznych przechowujących zasoby w bazach danych zgromadzonych na serwerach urzędu powinny być zasilane za pomocą zasilaczy awaryjnych (UPS). Urządzenia UPS powinny umożliwić bezpieczne zakończenie pracy w systemie w przypadku braku zasilania. Jeżeli urządzenie UPS to umożliwia, zamknięcie sytemu powinno odbywać się automatycznie.
11. Sprzęt informatyczny podlega konserwacji wg instrukcji stanowiącej procedurę „Konserwacja urządzeń informatycznych” w „Zestawieniu procedur pomocniczych” będącym Załącznikiem nr 2.1 do niniejszej instrukcji.
12. Nie rzadziej niż raz na 12 miesięcy Biuro Informatyki sporządza raport z wykorzystania posiadanych zasobów oraz plan ich wykorzystania na następne 12 miesięcy.

4.2 ZGŁASZANIE AWARII:

1. Wszelkie nieprawidłowości w działaniu systemu informatycznego użytkownicy mają obowiązek zgłaszać do Biura Informatyki za pomocą specjalnej aplikacji QDesk, do której skrót znajduje na pulpicie każdego użytkownika.
2. W przypadkach kiedy nie można uruchomić komputera, zgłoszenie awarii może nastąpić z dowolnego sąsiedniego, sprawnego komputera.
3. Jeżeli nie można zrealizować zgłoszenia systemem QDesk za pomocą powyższych punktów dopuszczalne jest zgłoszenie telefoniczne lub inne skuteczne.
4. Zgłoszenie awarii zrealizowane poza systemem QDesk musi zostać do tego systemu niezwłocznie wprowadzone przez przyjmującego zgłoszenie.

4.3 OPIS SYSTEMU INFORMATYCZNEGO URZĘDU.

4.3.1 STRUKTURA FIZYCZNA.

System informatyczny Urzędu działa w oparciu o sieć komputerową Ethernet w 7 budynkach należących do Urzędu. Opis sieci informatycznej zawarty jest w opracowaniu będącym załącznikiem nr 2.2 do niniejszej instrukcji.

4.3.2 STRUKTURA LOGICZNA

Logiczna struktura sieci informatycznej Urzędu oparta jest na domenowej, hierarchicznej usłudze katalogowej Active Directory opracowanej przez firmę Microsoft. Składa się z warstwy fizycznej i logicznej.

Na warstwę fizyczną składają się Lokalizacje (Site), Kontrolery Domeny Actitve Directory oraz komputery do domeny Active Directory podłączone.

1. W sieci informatycznej urzędu wypromowano domenę Active Directory (AD) o nazwie um.local.
2. Z serwerów urzędowych pracujących w domenie AD o funkcjonalności na poziomie Windows Server 2003 wyodrębniono 4 kontrolery domeny. Wszystkie zlokalizowane w serwerowni głównej w budynku przy ul. Kopernika 2:
   a) Serwer o adresie domenowym atena.um.local.
   b) Serwer o adresie domenowym zeus.um.local,
   c) Serwer o adresie domenowym atlas.um.local,
3. Serwery zostały opisane i skatalogowane w elektronicznym opracowaniu pomocniczym typu „Wiki" dostępnym pod adresem: http://wiki.um.local/index.php/Serwery
4. Stacje robocze pracujące w sieci informatycznej Urzędu muszą poprawnie zalogować się do domeny Active Directory.
5. Ze względów bezpieczeństwa i dostępności aktualizacji zabezpieczeń minimalnym systemem operacyjnym dopuszczalnym do zalogowania się w sieci informatycznej urzędu to system MS Windows 7, 8, 8.1 lub 10 w wersjach Professional.
6. Niedopuszczalne jest stosowanie systemów nie posiadających odpowiedniego systemu zabezpieczeń (np. Windows 98, Windows 95, Windows XP i Vista) oraz systemów nie posiadających systemu logowania do domeny Windows (np. wersje Windows Home).
7. Każdy użytkownik, aby pracować w systemie informatycznym Urzędu, musi posiadać indywidualne konto.
8. Konta użytkowników w Active Directory stosują system zabezpieczeń i uprawnień nazywanych Polityką Zasad Grup (GPO), która jest określona jako podstawowa w domenie um.local.
9. Główny kontroler domeny jest serwerem czasu rzeczywistego, aktualizującym czas nie rzadziej niż raz na dobę z 3 serwerów czasu sieciowego o wartości STRATUM nie większej niż 2.

10. Wszystkie stacje robocze synchronizują swoje wewnętrzne zegary czasu rzeczywistego z kontrolerem domeny, do którego zostały zalogowane. Użytkownik zalogowany do domeny nie ma uprawnień do zmiany czasu.
11. Dane osobowe przechowywanie na dyskach lokalnych komputerów Urzędu podlegają szyfrowaniu. Certyfikat szyfrujący musi być na osobnym, zabezpieczonym przed dostępem fizycznym jak i zdalnym serwerze.
12. W Urzędzie przechowywane są 3 podstawowe grupy certyfikatów:
    a) Certyfikaty identyfikacji komputerów przechowywane na serwerze, głównym kontrolerze domeny i replikowane na pozostałem kontrolery domeny,
    b) Certyfikaty identyfikacji komputerów zdalnego dostępu VPN. Centrum Certyfikacji znajduje się na serwerze o nazwie ZEUS. Ze względów bezpieczeństwa musi to być inny serwer niż udostępniający połączenie VPN,
    c) Certyfikaty – klucze szyfrujące – danych osobowych, które z przyczyn technicznych znajdują się na dyskach lokalnych. Certyfikaty te, zależnie od lokacji komputera, znajdują się na najbliższym serwerze będącym kontrolerem domeny.

5 STOSOWANE METODY I ŚRODKI UWIERZYTELNIANIA, AUTORYZACJI I KONTROLI UŻYTKOWNIKÓW SYSTEMU.

5.1 UWAGI OGÓLNE

1. W systemach komputerowych wspomagających czynności merytoryczne, a w szczególności przetwarzających dane osobowe, użytkownicy podlegają uwierzytelnieniu za pomocą identyfikatora użytkownika i autoryzacji z pomocą hasła.
2. Przy opuszczeniu stanowiska pracy na odległość uniemożliwiającą jego obserwację należy zablokować system kombinacją klawiszy [Windows] + [L].
3. Osoba udostępniająca stanowisko komputerowe innemu upoważnionemu pracownikowi zobowiązana jest wylogować się z systemu.
4. Przed wyłączeniem komputera należy bezwzględnie:
    a) zakończyć pracę uruchomionych programów,
    b) wykonać zamknięcie systemu połączone z wylogowaniem.
5. Niedopuszczalne jest wyłączenie komputera bez zamknięcia wszystkich użytkowanych programów i wylogowania się z systemu,
6. Niedopuszczalne są praktyki blokowania automatycznego włączania zabezpieczonego hasłem wygaszacza ekranu na czas nieobecności pracownika,
7. Biuro Spraw Pracowniczych najpóźniej do godziny 9:00 dnia następnego po nastąpieniu zdarzenia zawiadamia Biuro Informatyki o wszelkich zmianach dotyczących statusu zatrudnienia pracowników, a zwłaszcza o terminie rozwiązania umowy o pracę.

5.2 ZASADY NADAWANIA IDENTYFIKATORA

1. Identyfikator użytkownika jest unikalny w obrębie systemu, w którym jest stosowany.
2. Identyfikator konstruowany jest z pierwszej litery imienia oraz nazwiska użytkownika.
3. W przypadku dublowania się identyfikatora, identyfikator składa się z dwóch pierwszych liter imienia i nazwiska. Jeżeli nadal identyfikator by się dublował należy użyć trzech pierwszych liter imienia itd. Po wyczerpaniu algorytmu do imienia dodaje się kolejną cyfrę arabską.
4. Identyfikator użytkownika nie powinien być zmieniany bez wyraźnej przyczyny, a po wyrejestrowaniu użytkownika z systemu informatycznego nie może być przydzielony innej osobie.

5. Z przyczyn technicznych nie należy stosować identyfikatorów zawierających znaki diakrytyczne charakterystyczne dla języka polskiego (ę, ą, ż itp.).

5.3 ZASADY ZARZĄDZANIA HASŁAMI.

1. Nowe konto jest zakładane przez Administratora systemu zgodnie z procedurą *„Wdrożenie nowego stanowiska komputerowego”* zapisaną w załączniku 2.1 do niniejszej instrukcji.
2. W systemach umożliwiających samodzielną zmianę haseł przez użytkowników hasło powinno być zmienione przy pierwszym logowaniu do systemu.
3. Hasło użytkownika jest poufne, jest własnością użytkownika i zna je tylko dany użytkownik. Zabronione jest przekazywanie hasła innym lub w jakikolwiek sposób narażanie na poznanie hasła przez osoby postronne.
4. Za zachowanie poufności swoich haseł odpowiedzialni są użytkownicy.
5. Hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności.
6. Wszystkie hasła są tajne. Nie mogą pojawiać się w formie elektronicznej otwartym tekstem bez bezpiecznego szyfrowania, a w oknach edycyjnych bez zaciemnienia. W formie papierowej może występować tylko w uzasadnionych i opisanych odrębnymi procedurami przypadkach.
7. Dla haseł grupowych, użytkownik nie ma prawa do udostępnienia haseł danej grupy osobom spoza grupy, dla której zostały one utworzone.
8. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie.
9. W sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, pracownik zobowiązany jest do natychmiastowej zmiany hasła.
10. Przy wyborze hasła obowiązują zasady:
    a) minimalna długość hasła – 8 znaków,
    b) zakazuje się stosować:
        - haseł, które użytkownik stosował uprzednio w okresie minionego roku,
        - swojej nazwy użytkownika w jakiejkolwiek formie (pisanej dużymi literami, w odwrotnym porządku, dublując każdą literę, itp.),
        - swojego imienia, drugiego imienia, nazwiska, przezwiska, pseudonimu w jakiejkolwiek formie,
        - imion (w szczególności imion osób z najbliższej rodziny jak i zwierząt domowych),
        - ogólnie dostępnych informacji o użytkowniku takich jak: numer telefonu, numer rejestracji samochodu, jego marka, numer dowodu osobistego, nazwa ulicy na której mieszka lub pracuje, itp.
        - występujących pojedynczo wyrazów słownikowych,
        - przewidywalnych sekwencji znaków z klawiatury np.: „ QWERTY”, „12345678”, itp.
    c) należy stosować :
        - hasła zawierające kombinacje dużych i małych liter i cyfr,
        - hasła zawierające znaki specjalne zawarte w tabeli:

Znak	Opis
!	wykrzyknik
"	cudzysłów
#	kratka (hash)
$	dolar

Znak	Opis
%	procent
&	and
'	apostrof
(	nawias otwierający
)	nawias zamykający
*	gwiazdka
+	plus
,	przecinek
-	myślnik
.	kropka
/	ukośnik
:	dwukropek
;	średnik
<	znak mniejszości
>	znak większości
@	małpa
=	znak równości
[	nawias kwadratowy otwierający
\	odwrotny ukośnik
]	nawias kwadratowy zamykający
^	daszek
_	podkreślenie
{	nawias klamrowy otwierający
|	pałka pionowa
}	nawias klamrowy zamykający

- hasła, które można zapamiętać bez zapisywania,
- hasła łatwe i szybkie do wprowadzenia, po to by trudniej było podejrzeć je osobom trzecim,

11. Zmiany hasła nie wolno zlecać innym osobom.
12. Hasło użytkownika o prawach administratora powinno znajdować się w zalakowanej kopercie w zamykanej na klucz szafie metalowej, do której dostęp mają:
    a) Administrator Danych lub osoba przez niego wyznaczona,
    b) Pełnomocnik Bezpieczeństwa Informacji,
    c) Kierownik Biura Informatyki.
13. W przypadku systemów uwierzytelnianych za pomocą kart kryptograficznych piny do kart nie mogą być nigdzie zapisywane, a w szczególności nie na kartach lubi ich bezpośrednim pobliżu.
14. Karty z kodami PUK pozwalającymi na zmianę kodu PIN kart kryptograficznych winny być przechowywane oddzielnie od odpowiadających im kart kryptograficznych.

5.4 ZASADY WYREJESTROWANIA UŻYTKOWNIKA Z SYSTEMU INFORMATYCZNEGO

1. Wyrejestrowania użytkownika z systemu informatycznego dokonuje administrator systemu na wniosek kierownika Biura Spraw Pracowniczych lub po zgłoszeniu się użytkownika z kartą obiegową z podanym terminem zakończenia pracy w Urzędzie.
2. Wyrejestrowanie, o którym mowa w ust. 1, może mieć charakter czasowy, trwały lub automatyczny.
3. Wyrejestrowanie następuje poprzez:
    a) zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe),
    b) Trwałe zablokowanie danych użytkownika w bazie użytkowników systemu (wyrejestrowanie trwałe),
    c) upłynięcie terminu ważności konta w domenie Active Directory w przypadku zatrudnienia na czas określony.
4. Czasowe wyrejestrowanie użytkownika z systemu informatycznego musi nastąpić w razie:
    a) nieobecności użytkownika w pracy trwającej dłużej niż 21 dni kalendarzowych,
    b) zawieszenia w pełnieniu obowiązków służbowych,
    c) wypowiedzenie umowy o pracy,
    d) wszczęcie postępowania dyscyplinarnego względem osoby upoważnionej do przetwarzania danych osobowych,
    e) incydentu bezpieczeństwa z udziałem konta nieobecnego w danej chwili użytkownika systemu informatycznego
5. Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy lub innego stosunku prawnego, w ramach którego zatrudniony był użytkownik.

5.5 ZASADY ZARZĄDZANIA UPRAWNIENIAMI.

1. Nowy użytkownik systemu może dostać uprawnienia do systemu komputerowego po:
    a) otrzymaniu upoważnienia do przetwarzania danych osobowych,
    b) zapoznaniu się z niniejszą Instrukcją Zarządzania Systemem Informatycznym Urzędu Miejskiego w Wałbrzychu i potwierdzeniu na piśmie faktu zapoznania się z ww. dokumentami oraz złożyć stosowne oświadczenie, potwierdzające znajomość jego treści.
2. Użytkownik systemu nie może uruchamiać innego oprogramowania niż zainstalowane przez Biuro Informatyki i do którego ma przyznane kartą uprawnień uprawnienia. W szczególności nie może samodzielnie instalować oprogramowania i w jakikolwiek sposób obchodzić zabezpieczenia uniemożliwiające instalację lub uruchomienie innego oprogramowania.

3. Administrator systemu ma dostęp do całości systemu informatycznego w tym uprawnienia do nadawania i odbierania uprawnień, zakładania kont użytkowników, zakładania i zmiany haseł.
4. Użytkownik systemu może mieć dostęp tylko do tych zasobów sieci informatycznej Urzędu do której posiada, przyznane mu przez Administratora uprawnienia.
5. Zmiany uprawnień dokonuje się każdorazowo na wniosek przełożonego Użytkownika poprzez złożenie Karty Uprawnień. Kartę Uprawnień można złożyć wyłącznie za pomocą Elektronicznego Systemu Obiegu Dokumentów IntraDOK używając kategorii komórkowej „Karta uprawnień jednostkowych".
6. Osoby trzecie wykonujące zadania w sieci Urzędu muszą każdorazowo uzyskać pozwolenie Administratora Danych lub osób przez niego upoważnionych. W przypadku pracy na – czasowo nadanych – uprawnieniach administracyjnych, praca taka musi przebiegać pod nadzorem przynajmniej jednego administratora systemu.
7. Każde oprogramowanie konieczne do uruchomienia lub instalacji przez osoby trzecie musi być sprawdzone przez Administratora Systemu i zatwierdzone przez Kierownika Biura Informatyki.

5.6 MONITORING I KONTROLA DZIAŁAŃ UŻYTKOWNIKA SYSTEMU.

Do monitorowania działań użytkowników w systemie służy oprogramowanie LOG System. Agent Systemu LOG musi być zainstalowany na każdym komputerze i automatycznie uruchamiany na każdym z profili użytkownika. Agent jest zabezpieczony przed wyłączeniem go przez użytkownika.

W zakres kontroli mogą wchodzić następujące rodzaje aktywności użytkowników:

1. Rzeczywisty czas aktywności czyli dokładny czas pracy użytkownika na komputerze z godziną rozpoczęcia i zakończenia pracy oraz przerwami.
2. Monitorowanie procesów w tym rejestracja jakie procesy zostały na danym komputerze uruchomione, całkowity czas działania danego procesu oraz czas pracy użytkownika w danym procesie.
3. Rzeczywiste użytkowanie programów – dokładne informacje o wykorzystywanych programach (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona) oraz plikach jakie były używane w ramach użytkowania danego programu. Monitoring zapisuje również informacje dot. czasu konwersacji przez komunikatory, grania, zakupów online itp.
4. Zdalny podgląd pulpitu użytkownika (z możliwością przejęcia zdalnej kontroli nad komputerem – sygnalizowane stosownym komunikatem) oraz możliwość wprowadzenia wykonywania automatycznie cyklicznych zrzutów z ekranu.
5. Lista odwiedzanych stron wraz z adresami stron, z nagłówkami, liczbą i czasem wizyt.
6. Monitorowanie transferu sieciowego użytkowników
   a) ruch sieciowy lokalny,
   b) transfer internetowy wygenerowany przez danego użytkownika,
   c) zapis informacji o plikach pobieranych z Internetu.
7. Monitorowanie wydruków w tym informacje o dacie wydruku, wykorzystanej drukarce, użytkowniku oraz stacji roboczej, drukowanym dokumencie (nazwa dokumentu, ilość wydrukowanych stron, kolor, duplex, format, itp.).
8. Monitoring wiadomości e-mailowych wraz z wykonaniem pełnej kopii zapasowej wiadomości.
9. Możliwość zezwolenia lub zablokowania całego ruchu WWW dla danego użytkownika z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danej.
10. Szczegóły dotyczące użytkowanego sprzętu: zapis szczegółowej konfiguracji sprzętowej oraz softwarowej komputera wraz z rejestracją i automatycznym powiadamianiem administratora o wszelkich zmianach.

6 SYSTEM TWORZENIA KOPII BEZPIECZEŃSTWA.

System przygotowywania kopi bezpieczeństwa został opisany w procedurze „Tworzenie, dystrybucja i przechowywanie kopii bezpieczeństwa" opisanej w „Zestawieniu procedur pomocniczych" stanowiącym załącznik nr 2.1 do niniejszej instrukcji.

7 ŚRODKI OCHRONY SYSTEMU PRZED WIRUSAMI I INNYM ZŁOŚLIWYM OPROGRAMOWANIEM.

1. Na każdym stanowisku komputerowym musi być zainstalowane oprogramowanie antywirusowe pracujące i wychwytujące wirusy jak i inne złośliwe oprogramowanie.
2. Każdy odbierana wiadomości przychodząca drogą elektroniczną musi być sprawdzony pod względem występowania ww. oprogramowania. Zarówno treść jak i załączniki włączając te spakowane popularnymi algorytmami (zip, rar).
3. Definicje wzorców wirusów aktualizowane są przy każdym starcie systemu nie rzadziej niż raz na 3 dni. Aktualizacja odbywa się automatycznie z określonego serwera Urzędu.
4. Komputery przenośne, przebywające często poza siecią Urzędu, mają zdefiniowany inny, globalny serwer aktualizacji. Sprawdzenie aktualności i ewentualna aktualizacja sygnatur musi się odbywać przy każdym podłączeniu komputera do sieci internet.
5. Aktualność sygnatur programów antywirusowych na serwerze Urzędu sprawdzana jest min 3 razy dziennie.
6. Każdy nośnik wymienny (dyskietka, pamięć Flash) po podłączeniu powinna być sprawdzona na obecność występowania ww. oprogramowania. Niedopuszczalne jest użytkowanie nośnika bez sprawdzenia jeżeli był poprzednio użyty w innym systemie, zarówno komputerowym jak i innym.
7. Zabrania się pobierania z Internetu plików niewiadomego pochodzenia. Każdy plik pobrany z Internetu musi być sprawdzony programem antywirusowym. Sprawdzenia dokonuje użytkownik, który pobrał plik. Za sprawdzenie odpowiada Użytkownik. Kontrola antywirusowa przeprowadzana jest na komputerach, co do których istnieje podejrzenie, że nieprawidłowości w działaniu mogą być przyczyną ww. oprogramowania.
8. W przypadku wykrycia wirusów komputerowych sprawdzane jest:
   a) stanowisko komputerowe na którym wirusa wykryto,
   b) wszystkie nośniki wymienne i zapisywalne posiadane przez użytkowników pracującym na ww. stanowisku komputerowym,
   c) komputery wszystkich osób logujących się na danej stacji,
   d) zasoby i użytkownicy wspólnych grup uprawnień dzielących zasoby,

8 DOKUMENTY ELEKTRONICZNE.

8.1 ZASADY PRZECHOWYWANIA DOKUMENTÓW ELEKTRONICZNYCH.

1. Podczas logowania tworzony jest na pulpicie dynamicznie skrót do zasobu wspólnego właściwego dla komórki organizacyjnej użytkownika.
2. Wszystkie dokumenty elektroniczne danej komórki należy przechowywać na zasobach wspólnych lub w programie ESOD Intradok.
3. Przydział uprawnień do czynności wykonywanych na zasobach wspólnych dokonuje się za pomocą kart uprawnień.

8.2 ZASADA „CZYSTEGO EKRANU”

1. Dokumenty elektroniczne powinny być przechowywane w sposób zapewniający im bezpieczeństwo.
2. Dokumenty zawierające dane poufne lub osobowe winny być wyświetlane na monitorze w sposób uniemożliwiający ich odczyt przez osoby nieuprawnione.
3. Po zakończeniu pracy na pulpicie oraz w folderach umieszczonych na nim nie wolno przechowywać żadnych dokumentów lub bezpośrednich skrótów do nich.
4. Dokumenty wolno przechowywać na pulpicie tylko podczas bezpośredniej edycji. Po zakończeniu pracy winny zostać przeniesione na zasób wspólny, a z pulpitu usunięte.

9 NOŚNIKI MOBILNE.

9.1 RODZAJE NOŚNIKÓW MOBILNYCH.

Do nośników mobilnych zalicza się: Dyskietki, Płyty CD, DVD i Bluray, Taśmy streamerów, masowe urządzenia magazynujące podłączane pod port USB, FireWire lub inny port wymiany danych komputera, pamięć wewnętrzna komputerów przenośnych i innych urządzeń taką pamięć posiadających takie jak odtwarzacze mp3 i mp4, palmtopy, telefony komórkowe, smartfony, nawigacje satelitarne i podobne.

9.2 ZASADY UŻYTKOWANIA NOŚNIKÓW MOBILNYCH

1. Uprawnienia do użytkowania nośników mobilnych nadawane są i odbierane za pomocą karty uprawnień jednostkowych.
2. Nośniki USB są imiennie rejestrowane w systemie DRP i tylko zarejestrowane nośniki mogą być skutecznie użytkowane w Systemie Informatycznym.
3. Rejestr użytkowników posiadających uprawnienia do składowania danych na nośnikach mobilnych oraz ich ewentualnego wynoszenia poza teren urzędu prowadzi Biuro Informatyki.
4. Nośniki mobilne muszą być w sposób trwały oznaczone:
   a) środki trwałe posiadające wbudowane nośniki mobilne powinny być oznaczone etykietą wg. oznaczeń środków trwałych Urzędu.,
   b) inne nośniki powinny być oznaczone bądź pieczątką Urzędu (dyskietki, taśmy streamerów) bądź niezmywalnym markerem,
   c) minimalne oznaczenie to napis „UM w Wałbrzychu”,
   d) jeżeli ilość miejsca jest niewystarczająca (napędy typu pendrive) minimalne oznaczenie to napis „UMW”.
5. Nie wolno dokonywać zapisu i odczytu nośników danych innych niż oznaczone z wyjątkiem nośników obrotu danymi podlegających regulacjom za pomocą odrębnych umów.
6. Dane osobowe i dane uznawane za wrażliwe powinny być przechowywane na nośnikach mobilnych w sposób bezpieczny. Chronione programem pozwalającym na szyfrowanie oparte na algorytmach AES (symetryczny) lub RSA (niesymetryczny) i kluczem minimum 128 bitowym. Można posłużyć się innym nieskompromitowanym algorytmem lecz należy wówczas zwiększyć bezpieczeństwo szyfrowania do 256 bitowego klucza.
7. Nośniki wykorzystywane do przenoszenia danych poufnych i osobowych przed ponownym wykorzystaniem winny być czyszczone oprogramowaniem nadpisującym wolną przestrzeń np. Eraser.
8. Niepotrzebne lub uszkodzone mobilne nośniki danych oddawane są do Biura Informatyki gdzie podlegają zniszczeniu w niszczarce płyt w przypadku nośników optycznych i dyskietek lub poprzez fizyczne zniszczenie w przypadku innego nośnika.

9. Użytkownik nośników mobilnych podlega wstępnemu i okresowemu szkoleniu z zasad bezpiecznego przechowywania danych, zasad ich udostępniania oraz bezpiecznej pracy na urządzeniach mobilnych zawierających nośniki danych.

10 POSŁUGIWANIA SIĘ POCZTĄ E-MAIL.

1. Serwer poczty elektronicznej funkcjonuje w wewnętrznej sieci Urzędu i zajmuje się dystrybucją wiadomości email zarówno w sieci wewnętrznej jak i na serwery zewnętrzne.
2. Wysyłanie poczty elektronicznej w Urzędzie działa w oparciu o protokół SMTP (ang. Simple Mail Transfer Protocol).
3. Pobierania wiadomości z serwera poczty elektronicznej wykonuje się w oparciu o protokół POP3 (Post Office Protocol version 3) lub IMAP (Internet Message Access Protocol).
4. Ustawienia serwera wymagają uwierzytelnienia wysyłania wiadomości tj. przed wysłaniem każdej wiadomości pocztowej program pocztowy musi podać dane uwierzytelniające - login i hasło.
5. Konta pocztowe poczty elektronicznej przydzielane są na podstawie modyfikacji uprawnień za pomocą karty uprawnień jednostkowych.
6. Konta poczty elektronicznej przydzielane każdorazowo są według następującego klucza pierwsza_litera_imienia.nazwisko@um.walbrzych.pl Jeżeli taka nazwa konta pocztowego jest już zajęta, używa się pierwszych dwóch liter imienia. Jeżeli nadal nazwa nie jest unikalna używa się trzech pierwszych liter imienia itd. Po wyczerpaniu algorytmu do imienia dodaje się kolejną cyfrę arabską.
7. Hasła do poczty elektronicznej generują i konfigurację programu pocztowego przeprowadzają pracownicy Biura Informatyki.
8. Ponieważ wiadomość pocztowa jest wysyłana i odbierana nieszyfrowanym połączeniem oraz otwartym tekstem nie wolno jej stosować do korespondencji zawierającej dane poufne oraz zawierającej dane osobowe bez odpowiednich procedur szyfrowania załączników.
9. Procedurę wysyłania danych poufnych oraz zawierających dane osobowe reguluję procedura „Udostępnianie i przekazywanie danych, w tym danych poufnych i osobowych” opisana w „Zestawieniu procedur pomocniczych” stanowiącym załącznik nr 2.1 do niniejszej instrukcji.
10. W przypadku wysyłania wiadomości wielu odbiorców, zwłaszcza na adresy prywatne lub instytucji innych iż administracja publiczna zabrania się podawania adresów w sposób jawny tj. w polu „DO” lub „DW”. Należy wówczas użyć pola ukrytego (UDW).

11 ZASADY I SPOSÓB ODNOTOWYWANIA W SYSTEMIE INFORMACJI O UDOSTĘPNIANIU DANYCH OSOBOWYCH.

1. Dane osobowe z eksploatowanych systemów mogą być udostępniane wyłącznie osobom upoważnionym.
2. Udostępnianie danych osobowych, w jakiejkolwiek postaci, jednostkom nieuprawnionym wymaga pisemnego upoważnienia Administratora Danych.
3. Udostępnienie danych osobowych osobom nie może być realizowane drogą telefoniczną.
4. Udostępnienie danych osobowych może nastąpić wyłącznie po zawarciu umowy,
5. Udostępnienia danych osobowych może być realizowane drogą elektroniczną za pomocą procedury „Udostępnianie i przekazywanie danych, w tym danych poufnych i osobowych” opisanej w „Zestawieniu procedur pomocniczych” stanowiącym załącznik nr 2.1 do niniejszej instrukcji
6. Kierownicy komórek organizacyjnych, prowadzą rejestry udostępnionych danych osobowych zawierające co najmniej: datę udostępnienia, podstawę, zakres udostępnionych informacji oraz osobę lub instytucje, której dane udostępniono.

12 PUBLIKACJA TREŚCI NA STRONACH PORTALU MIEJSKIEGO

1. Publikacja treści zajmują się uprawnione osoby będące Redaktorami Portalu.
2. Uprawnienia Redaktorów Portalu mogą dotyczyć całości lub wydzielonej części tematycznej stron www Urzędu.
3. Za publikowane treści odpowiada wyznaczony Redaktor Główny nadzorowany przez Kierownika Biura Informatyki.
4. Redaktor Główny portalu prowadzi listę osób i podmiotów – uzgodnionych dostawców treści – do Portalu Miejskiego.
5. Wszystkie dostarczone przez uzgodnionych dostawców treści publikacje muszą być wysłane do wiadomości do Rzecznika Prasowego Prezydenta Miasta.
6. Wszystkie publikowane treści dostarczone przez osoby lub podmioty spoza listy uzgodnionych dostawców treści wymagają akceptacji Rzecznika Prasowego Prezydenta Miasta.
7. Publikację nowych treści na Portalu Miejskim opisuje procedura: „Dostarczanie i publikacja nowych treści na stronach Portalu Miejskiego" opisanej w „Zestawieniu procedur pomocniczych" stanowiącym załącznik nr 2.1 do niniejszej instrukcji.
8. Poprawę lub zmianę istniejących treści na Portalu Miejskim opisuje procedura: „Poprawa lub zmiana treści opublikowanych na stronach Portalu Miejskiego" opisanej w „Zestawieniu procedur pomocniczych" stanowiącym załącznik nr 2.1 do niniejszej instrukcji.
9. Usunięcie opublikowanych treści z Portalu Miejskiego opisuje procedura: „Usunięcie opublikowanych treści ze stron Portalu Miejskiego" opisanej w „Zestawieniu procedur pomocniczych" stanowiącym załącznik nr 2.1 do niniejszej instrukcji.

13 ZASADY UŻYTKOWANIA KOMPUTERÓW PRZENOŚNYCH.

1. Osoba użytkująca przenośny komputer, służący do przetwarzania danych osobowych, obowiązana jest zachować szczególną ostrożność podczas transportu i przechowywania tego komputera poza obszarem, przeznaczonym do przetwarzania danych osobowych wskazanym w Polityce Bezpieczeństwa.
2. W celu zapobieżenia dostępowi do tych danych osobie niepowołanej, należy:
   a) Użytkować wyłącznie urządzenie zarejestrowane w domenie Acitve Directory um.local stosującej nieodwracalne szyfrowanie haseł i zasady GPO kontenera przeznaczonego dla komputerów przenośnych zwiększających liczbę logowań z bufora do 50.
   b) Dane osobowe i dane z baz danych programów merytorycznych użytkowanych w systemie informatycznym UM przetwarzać za pomocą zdalnego dostępu do bazy danych użytkując aplikacje trójwarstwowe (przeglądarkowe lub tzw. cienkiego klienta)
   c) W przypadku aplikacji dwu lub jednowarstwowych używać usług terminalowych (protokół RDP) realizowanych za pomocą serwera terminali Iris.
   d) Nie zezwalać na używanie komputera osobom nieupoważnionym do dostępu do danych osobowych.
   e) W przypadku konieczności przechowywania danych osobowych lub innych, poufnych na dysku lokalnym komputera przenośnego należy takie dane zaszyfrować.
   f) Wprowadzenie w BIOS/UEFI następujących ustawień:
      i) wejście i zmiana ustawień BIOS/UEFI wymaga podania hasła;
      ii) wyłączona jest możliwość uruchamiania systemu z sieci lub innych nośników niż dysk twardy komputera;
      iii) długość hasła BIOS/UEFI zgodne z polityką haseł z p. 5.3

14 SPOSÓB POSTĘPOWANIA W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH.

Sposób postępowania w sytuacji stwierdzenia naruszenia ochrony danych osobowych określa Instrukcja Postępowania w Sytuacji Naruszenia Ochrony Danych Osobowych Załącznik Nr 2.3 do niniejszej instrukcji.

15 POSTANOWIENIA KOŃCOWE

1. W sprawach nieuregulowanych niniejszą instrukcją należy stosować instrukcje obsługi i zalecenia producentów aktualnie wykorzystywanych urządzeń i programów.
2. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się przed dopuszczeniem do przetwarzania danych z niniejszą instrukcją oraz złożyć stosowne oświadczenie, potwierdzające znajomość jej treści.
3. Niezastosowanie się do procedur określonych w niniejszej instrukcji i załącznikach przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52 kodeksu pracy.