Maja 15
ąbkowice Śląskie

OR.0050.363.2015.AJ

ZARZĄDZENIE NR 363 /XII /OR-2015
Burmistrza Ząbkowic Śląskich
z dnia 29 grudnia 2015 r.

w sprawie ustalenia Polityki bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych oraz ustalenia Instrukcji określającej sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Ząbkowicach Śląskich

Na podstawie art. 31, 33 ust. 3 i 5 ustawy z dnia 8 marca 1990 roku o samorządzie gminnym (t.j. Dz.U. z 2015 poz. 1515 ze zm.) w związku z art. 36 ust. 1 i 2 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (t.j.Dz. U z 2015 r. poz. 2135 z późn. zm.) oraz w związku z 3 ust. 3, § 4 i § 5 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych , jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100 poz. 1024) **zarządzam co następuje** :

§ 1. Ustalam „Politykę bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Miejskim w Ząbkowicach Śląskich zwaną dalej „Polityką bezpieczeństwa", która stanowi załącznik nr 1 do niniejszego zarządzenia.

§ 2. Ustalam „Instrukcję określającą sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Ząbkowicach Śląskich" zwaną dalej „Instrukcją", która stanowi załącznik nr 2 do niniejszego zarządzenia.

§ 3. Zobowiązuję pracowników Urzędu Miejskiego w Ząbkowicach Śląskich do stosowania zasad określonych w „Polityce bezpieczeństwa".

§ 4. Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ
Marcin Orzeszek

Uzasadnienie

Zgodnie z art. 31, 33 ust. 3 i 5 ustawy z dnia 8 marca 1990 roku o samorządzie gminnym (t.j. Dz.U. z 2015 poz. 1515 ze zm.) Burmistrz jest kierownikiem urzędu, kieruje bieżącymi sprawami gminy oraz reprezentuje ją na zewnątrz. Zadania wykonuje przy pomocy urzędu gminy.
Zgodnie z art. 36 ust. 1 i 2 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (t.j. Dz. U z 2015 r. poz. 2135 z późn. zm.) Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Biorąc powyższe pod uwagę wprowadzenie niniejszego zarządzenia uważam za zasadne.

Sporządził: .....
Andrzej Janke
Podinspektor ds. informatycznych

Ząbkowice Śląskie, dnia ....grudnia 2015 r.

Podpis i Pieczątka Radcy Prawnego.

Rozdzielnik dla odbiorców:

1) Wewnętrzny::

a) BIP
b) Rejestr Zarządzeń Monika Krakowska
c) Folder „Zarządzanie" Monika Krakowska

2) A/a

Złącznik nr 1 do Zarządzenia
nr 43 Burmistrza Ząbkowic Śl.
z dnia 29. grudnia 2015

POLITYKA BEZPIECZEŃSTWA
w Urzędzie Miejskim w Ząbkowicach Śląskich

I. Postanowienia ogólne.

II. Cele i zakres polityki bezpieczeństwa.

III. Obowiązki i zakresy odpowiedzialności zarządzania bezpieczeństwem.

IV. Gromadzenie i przetwarzanie danych osobowych

V. Rejestracja i przetwarzanie zbiorów danych osobowych

VI. Środki ochrony

VII. Postanowienia końcowe.

I
Postanowienia ogólne.

§ 1.

Polityka Bezpieczeństwa Urzędu Miejskiego w Ząbkowicach Śląskich, zwana dalej Polityką, została opracowana zgodnie § 3, § 4 i § 5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r., Nr 100 poz. 1024).

Polityka określa zasady i procedury obowiązujące przy przetwarzaniu i wykorzystywaniu danych we wszystkich zbiorach danych osobowych administrowanych przez Urząd Miejski w Ząbkowicach Śląskich.

Polityka bezpieczeństwa zawiera:

- Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe (załącznik nr 1 do niniejszej polityki bezpieczeństwa),
- Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych (załącznik nr 2 do niniejszej polityki bezpieczeństwa),
- Opis struktury zbiorów danych oraz sposób przepływu danych pomiędzy poszczególnymi systemami (załącznik nr 3 do niniejszej polityki).

§ 2.

Skróty i określenia użyte w Polityce oznaczają:

1. Ustawa - ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182 z późń. zm.)
2. Urząd - Urząd Miejski w Ząbkowicach Śląskich
3. Administrator Danych Osobowych (ADO) - Burmistrz Ząbkowic Śląskich, zwany dalej Administratorem.
4. Administrator Bezpieczeństwa Informacji (ABI) - osoba wyznaczona przez Administratora (ADO), w rozumieniu art. 36a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz.U. z 2014 r., poz. 1182 z późn. zm.)
5. Administratorzy Systemów Informatycznych (ASI) - pracownicy wyznaczeni przez Administratora Danych Osobowych odpowiedzialni za wdrożenie i stosowanie zasad bezpieczeństwa systemów informatycznych, zobowiązani do stosowania technicznych i organizacyjnych środków ochrony przewidzianych w systemach informatycznych.

6. Administratorzy Kopii Bezpieczeństwa (AKB) - ASI.
7. Kierownik Wydziału, zwany dalej przełożonym - osoba odpowiedzialna za przestrzeganie zasad przetwarzania i ochrony danych przez podległych mu pracowników.
8. Użytkownik systemu - osoba posiadająca upoważnienie do wprowadzania i przetwarzania danych w systemie informatycznym w zakresie wskazanym w upoważnieniu.
9. Identyfikator użytkownika - ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych w systemie informatycznym.
10. Hasło - ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.
11. Dane osobowe - zbiór informacji pozwalających na identyfikację konkretnej osoby
12. Dane sensytywne - dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, a także informacje o innych orzeczeniach wydanych w postępowaniu sądowym lub administracyjnym.
13. Zbiór danych - zestaw danych o charakterze osobowym, dostępny wg określonych kryteriów
14. Przetwarzanie danych osobowych - wykonywanie wszelkich czynności na danych osobowych (zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, usuwanie), bez względu na formę w jakiej wykonywane są te czynności
15. Rejestr udostępnionych danych osobowych, zwany dalej Rejestrem - rejestr, w którym odnotowywane są informacje o odbiorcach danych z systemu/aplikacji, prowadzony dla danego systemu/aplikacji.

II
Cele i zakres polityki bezpieczeństwa.

§ 3.

1. W polityce określone są podstawowe zasady bezpieczeństwa i zarządzania bezpieczeństwem systemów.
2. Polityka dotyczy wszystkich danych osobowych, przetwarzanych w Urzędzie Miejskim w Ząbkowicach Śląskich niezależnie od formy ich przetwarzania (zbiory ewidencyjne, systemy informatyczne) oraz od tego czy dane są lub mogą być przetwarzane w zbiorach danych.

§ 4.

1. Celem Polityki jest określenie działań i zapewnienie wysokiego poziomu bezpieczeństwa danych przetwarzanych w Urzędzie Miejskim w Ząbkowicach Śląskich.
2. Bezpieczeństwo danych osobowych polega na zapewnieniu ich poufności, integralności i rozliczalności.

- poufność - zapewnienie, że informacja nie jest udostępniana lub ujawniana nieupoważnionym osobom.
- integralność - zapewnienie, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
- rozliczalność - zapewnienie, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

Za podmiot nieupoważniony uważa się podmiot, który nie otrzymał zgody Administratora na udostępnienie mu danych osobowych oraz osobę nie posiadającą upoważnienia do przetwarzania danych osobowych, nadanego przez Administratora w trybie art. 37 ustawy.

§ 5.

1. Zakres polityki bezpieczeństwa obejmuje dane osobowe przetwarzane w Urzędzie w formie tradycyjnej oraz elektronicznej.
2. zasady i procedury określone w niniejsze Polityce stosuje się do wszystkich pracowników Urzędu, a także innych osób, które mają dostęp do danych osobowych, które są przetwarzane w Urzędzie (zatrudnionych na podstawie umów zlecenia, o dzieło, praktykantów, stażystów, serwisantów).

III
Obowiązki i zakresy odpowiedzialności zarządzania bezpieczeństwem.

§ 6.

1. Zarządzanie bezpieczeństwem systemów realizowane jest przy współdziałaniu użytkowników systemu z ABI i ASI.
2. Dostęp do danych osobowych oraz ich przetwarzania mają wyłącznie osoby wpisane do ewidencji prowadzonej przez ABI (załącznik nr 4 do niniejszej Polityki)
3. Osoby przetwarzające dane osobowe zobowiązane są do przetwarzania danych osobowych zgodnie z obowiązującymi przepisami oraz przechowywania ich nie dłużej niż jest to niezbędne dla osiągnięcia celu przetwarzania.;
4. Osoby przetwarzające dane osobowe zobowiązane są do postępowania zgodnie z ustaloną przez Administratora Polityką Bezpieczeństwa oraz z „Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych";
5. W przypadku naruszenia przepisów lub zasad postępowania użytkownik podlega odpowiedzialności służbowej i karnej.

§ 7.

Zakres odpowiedzialności i zadania Administratora Danych Osobowych:

1. Administrator odpowiedzialny jest za zgodność Polityki z obowiązującymi przepisami dotyczącymi zasad przetwarzania danych osobowych, tj.:

- ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. z 2014 r., poz. 1182 z późn. zm.);
- rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r., Nr 100, poz. 1024);

2. Administrator realizuje zadania w zakresie ochrony danych osobowych, a w szczególności:
    - nadaje upoważnienia do przetwarzania danych osobowych osobom w indywidualnie określonym zakresie i prowadzi ewidencję wydanych upoważnień
    - zgłasza zbiory danych osobowych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (tzw. dane sensytywne, wskazane w art. 27 ust. 1 Ustawy.)
    - wyznacza ABI i określa jego zakres czynności.
    - zaleca by ABI we współpracy z Kierownikiem Wydziału Organizacyjnego zapewnili odpowiednie stanowiska pracy dla użytkowników, umożliwiające bezpieczne przetwarzanie danych.
    - podejmuje wszelkie działania (na wniosek ABI) w celu usunięcia zagrożenia lub minimalizacji jego skutków w przypadku stwierdzenia lub podejrzenia naruszenia zasad przetwarzania i ochrony danych osobowych.
    - udostępnia dane osobowe ze zbioru na żądanie podmiotów uprawnionych zgodnie z obowiązującymi przepisami prawa.

§ 8.

Obowiązki i zadania Administratora Bezpieczeństwa Informacji:

1. Do obowiązków ABI należy kontrola i nadzór przestrzegania zasad bezpieczeństwa i ochrony danych osobowych określonych w dokumentacji, o której mowa w § 6 ust. 4.
2. Zadania ABI:

- prowadzi i aktualizuje dokumentację dotyczącą przetwarzania i ochrony danych osobowych
- nadzoruje i kontroluje przestrzeganie zasad określonych w Polityce Bezpieczeństwa i Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych
- prowadzi szkolenia dla osób dopuszczonych do przetwarzania danych lub przebywania w obszarze przetwarzania danych w zakresie zasad przetwarzania i ochrony tych danych.
- nadzoruje prawidłowość udostępniania danych osobowych
- prowadzi nadzór nad zamieszczaniem odpowiednich zapisów dotyczących ochrony danych osobowych w: umowach z użytkownikami upoważnionymi do przetwarzania danych osobowych, firmami którym powierzono przetwarzanie danych osobowych lub konserwację urządzeń służących do przetwarzania tych danych.
- nadzoruje wdrożenie technicznych i organizacyjnych środków mających na celu zapewnienie bezpieczeństwa danych.
- nadzoruje obieg i przechowywanie dokumentów zawierających dane osobowe w zakresie bezpieczeństwa tych danych.
- podejmuje lub wnioskuje o podjęcie odpowiednich działań w przypadku naruszenia lub podejrzenia naruszenia bezpieczeństwa systemu informatycznego oraz prowadzi dokumentacje w tym zakresie (załącznik nr 5 do niniejszej Polityki).
- Prowadzi w formie papierowej i elektronicznej ewidencje i wykazy tworzone w procesie przetwarzania i ochrony danych osobowych.

§ 9.

ASI realizuje zdania w zakresie zarządzania i nadzoru nad systemem informatycznym. Do jego zadań należy:

- administrowanie systemami, w których są przetwarzane dane osobowe, posługując się przy tym hasłem dostępu z poziomu administratora.
- przyznawanie użytkownikom indywidualnych identyfikatorów oraz haseł do systemu informatycznego, oraz dokonuje modyfikacji uprawnień, które wynikają z nadanego użytkownikowi upoważnienia do przetwarzania danych.

- w porozumieniu z Kierownikiem Wydziału Organizacyjnego usuwa konta użytkowników zgodnie z zasadami określonymi w „Instrukcji zarządzania systemem informatycznym w Urzędzie".
- zmienia okresowo hasła dostępu użytkowników do systemu informatycznego, w przypadku gdy system nie wymusza okresowej zmiany haseł użytkowników.
- instaluje, aktualizuje, konfiguruje oprogramowania systemowe, aplikacje oraz urządzenia, o ile czynności tych nie musi dokonać przedstawiciel dostawcy systemu na podstawie zawartej z nim umowy.
- instaluje i aktualizuje oprogramowanie antywirusowe.
- tworzy, rejestruje, przechowuje oraz archiwizuje kopie zapasowe baz danych osobowych.
- osobiście wykonuje lub sprawuje nadzór nad wykonywaniem napraw, konserwacji oraz likwidacji urządzeń komputerowych, na których mogą być dane osobowe.
- przekazuje do ABI opisy struktur zbiorów danych, schematy przepływu danych między systemami i wszelkie zmiany w tym zakresie.
- reaguje w przypadku naruszenia lub podejrzenia naruszenia bezpieczeństwa danych przetwarzanych w systemie. Natychmiast informuje Administratora o tych zdarzeniach.

§ 10.

1. Wydział Organizacyjny Urzędu zapewnia wszelkie czynności techniczne związane ze skuteczną ochroną przetwarzanych danych osobowych.
2. Wydział Organizacyjny przy współudziale ABI zapewnia techniczne zabezpieczenia i wyposażenie obszarów przetwarzania danych ze szczególnym uwzględnieniem:
    - wyposażenia pomieszczeń w odpowiednio zabezpieczone okna, zamknięcia, zabezpieczenia alarmowe.
    - gromadzenia danych sensytywnych, nośników wymiennych i nośników na których gromadzone są kopie zapasowe, w odpowiednio zabezpieczonych szafach.
    - odpowiedniego zabezpieczenia i wyposażenia serwerowi.
3. Do zadań Wydziału Organizacyjnego Urzędu należy:
    - wyznaczanie ASI w Urzędzie oraz określenie jego zadań.
    - dostosowanie systemów informatycznych do wymogów prawa określonych w Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29

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

- planowanie i wdrażanie rozwiązań systemowych oraz technicznych elementów bezpieczeństwa przetwarzania danych osobowych . Czynności tych dokonuje się w porozumieniu z Kierownikami Wydziałów oraz ABI/ ASI.
- zapewnienie sprzętu i oprogramowania zgodnego z normami przewidzianymi dla prawidłowego zabezpieczenia przetwarzanych w systemach danych.
- nadzór nad technicznym zabezpieczeniem i odpowiednim wyposażeniem pomieszczeń, w których znajdują się serwery.

4. Kierownik Wydziału Organizacyjnego realizuje następujące zadania z zakresu ochrony danych osobowych:
   - Prowadzi ewidencję upoważnień do przetwarzania danych osobowych.
   - Przechowuje upoważnienia do przetwarzania danych osobowych w aktach osobowych pracowników.
   - Informuje ABI o nadaniu, modyfikacji lub odwołaniu przez Administratora upoważnienia do przetwarzania danych osobowych.
   - ma obowiązek przekazywać informacje dotyczące osób, które biorą udział w przetwarzaniu i ochronie danych osobowych w Urzędzie:
     a) zmiany w nawiązaniu i rozwiązaniu stosunku pracy,
     b) zmiany miejsc świadczenia pracy
     c) oddelegowanie lub przeniesienie pracownika do innego Wydziału,
     d) przebywanie na urlopie macierzyńskim, wychowawczym, bezpłatnym (powyżej 1 miesiąca),
     e) przebywanie na zwolnieniu lekarskim (powyżej 1 miesiąca),
     f) zmiany Burmistrza, Zastępców Burmistrza, Kierowników Wydziałów Urzędu.
   - Nadzoruje wykonywanie i przechowywanie kopii bezpieczeństwa zbiorów danych.
   - Nadzoruje czynności wykonywane przez ASI.

§ 11.

1. Kierownicy Wydziałów Urzędu oraz samodzielne stanowiska odpowiedzialni są za przestrzeganie przepisów dotyczących przetwarzania danych osobowych przez

podległych im pracowników, w zakresie nadanych im przez Administratora upoważnień do przetwarzania danych

2. Do zadań Kierowników Wydziałów i pracowników na samodzielnych stanowiskach należy:
    - Decydowanie o udostępnianiu danych osobowych
    - Zachowanie szczególnej staranności przy przetwarzaniu danych osobowych (zgodnie z art. 26 Ustawy)
    - Zapewnienie kontroli wprowadzania i przekazywania danych osobowych (zgodnie z art. 38 Ustawy)
    - Odpowiednie zabezpieczanie danych osobowych zgodnie z przepisami dokumentacji przetwarzania i ochrony danych osobowych
    - Udzielanie informacji, uzupełnianie, aktualizacja lub prostowanie danych osobowych (art. 32 ust. 1 pkt. 6 Ustawy)
    - Zawieranie umów dotyczących udostępniania i przetwarzania danych osobom i podmiotom zewnętrznym.
    - Rozpatrywanie skarg i wniosków dotyczących przetwarzania i ochrony danych osobowych (w porozumieniu w ABI)
    - Przeprowadzanie okresowej oceny analizy ryzyka dla poszczególnych systemów (na żądanie Administratora)
    - Przedstawianie Administratorowi propozycji w zakresie zastosowania środków technicznych mających na celu zapewnienie skuteczności ochrony przetwarzania danych.

§ 12.

Użytkownicy systemu zobowiązani są do:

- ścisłego przestrzegania zakresu nadanego upoważnienia;
- przetwarzania i ochrony danych osobowych zgodnie z przepisami;
- zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia;
- zgłaszania ASI incydentów związanych z naruszeniem bezpieczeństwa danych oraz niewłaściwym funkcjonowaniem systemu, a także informowania ABI o przypadkach naruszenia zasad ochrony danych.

IV
Gromadzenie i przetwarzanie danych osobowych

§ 13.

1. Dane osobowe przetwarzane w Urzędzie Miejskim w Ząbkowicach Śląskich w celu realizacji zadań określonych przepisami prawa gromadzone są bezpośrednio od osób, których dotyczą lub z innych źródeł (w granicach dozwolonych przepisami prawa).
2. Zgromadzone dane mogą być wykorzystywane wyłącznie do celów, do jakich były (są lub będą) przetwarzane. Po ich wykorzystaniu powinny być przechowywane w sposób uniemożliwiające identyfikację osób, których one dotyczą.
3. Użytkownicy systemu i ich przełożenie mają obowiązek zapewnienia odpowiedniej ochrony przetwarzanych danych.
4. Przesyłanie danych osobowych za pomocą urządzeń telekomunikacyjnych wymaga wykorzystania odpowiednich urządzeń, które zapewnią poufność i integralność ich przekazu.
5. Drukowanie i kopiowanie danych osobowych jest zabronione, chyba że wynika to z nałożonych na użytkownika obowiązków i wynika z przepisów prawa.

§ 14

1. Dane osobowe mogą być przetwarzane wyłącznie przez osoby spełniające wymagania określone w art. 37 ustawy,
2. W Urzędzie funkcjonuje procedura nadawania (zmiany i wycofywania) upoważnień do przetwarzania danych osobowych. Przebiega ona w trzech etapach:
    - Przełożony składa wniosek o nadanie (zmianę lub wycofanie) upoważnienia do przetwarzania danych osobowych (załącznik nr 6 do niniejszej Polityki).
    - Osoba ubiegająca się o nadanie upoważnienia podpisuje oświadczenie o zachowaniu w tajemnicy zasad przetwarzania danych osobowych oraz sposobów ich zabezpieczania. Tajemnica obowiązuje również po ustaniu stosunku pracy (załącznik nr 7 do niniejszej Polityki).
    - Administrator nadaje upoważnienie do przetwarzania danych osobowych (załącznik nr 8 do niniejszej Polityki)

3. Kopie upoważnień i dokumentów wymienionych w ust. 2 przechowywane są w Wydziale Organizacyjnym Urzędu.
4. Przełożony zobowiązany jest do realizacji procedur określonych w ust. 2.
5. ABI kontroluje realizację obowiązku wymienionego w ust. 1.

§ 15

1. W obszarach przetwarzania danych osobowych przebywanie osób nieuprawnionych jest ograniczone i może odbywać się wyłącznie w obecności użytkowników i za zgodą przełożonych.
2. Administrator ma obowiązek zapewnić ochronę obszarów Urzędu, w których przetwarzane są dane osobowe.
3. Obszarami podlegającymi szczególnej ochronie są: serwerowania oraz pomieszczenia, w których przetwarzane są dane sensytywne.

V
Rejestracja i przetwarzanie zbiorów danych osobowych

§ 16

1. Kierownicy Wydziałów Urzędu, w których przetwarzane są dane osobowe, mają obowiązek dokonać zgłoszenia ABI informacji na temat:
    - planowanego założenia nowego zbioru danych osobowych, który wymaga rejestracji
    - zmian wnoszonych do zbiorów, które są już zarejestrowane.
2. Użytkownicy, którzy w związku z realizacją swoich zadań służbowych tworzą zbiory lub wnioskują o ich zmianę (wycofanie), informują o tym swoich bezpośrednich przełożonych

§ 17

Użytkownicy, którzy przetwarzają dane osobowe mają obowiązek zgłoszenia ABI aktualnych wykazów zbiorów danych osobowych (które przetwarzają na swoim stanowisku pracy), przy jednoczesnym powiadomieniu o tym fakcie bezpośredniego przełożonego.

§ 18

1. ABI prowadzi rejestr zbiorów danych.

2. Dane osobowe mogą być przetwarzane w zbiorze od momentu zgłoszenia go do ABI, chyba, że zbiór zawiera dane sensytywne. W takim wypadku dane można przetwarzać po potwierdzeniu przez GIODO jego zarejestrowania.

VI
Środki ochrony.

§ 19

1. Administrator zapewnia zastosowanie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.
2. Środki techniczne:
    a) pomieszczenia, w których przetwarzane są dane osobowe wyposażone są w system alarmowy, przeciwwłamaniowy,
    b) dostęp do pomieszczeń, w których przetwarzane są dane osobowe objęte są systemem kontroli dostępu,
    c) zbiory danych osobowych w formie papierowej przechowywane są w szafach zamykanych na klucz, w pomieszczeniach zamykanych na klucz,
    d) kopie zapasowe zbioru danych przechowywane są w szafie zamykanej na klucz, w pomieszczeniach zamykanych na klucz,
    e) pomieszczenia, w których przetwarzane i gromadzone są zbiory danych osobowych zabezpieczone są przed skutkami pożaru za pomocą wolnostojącej gaśnicy,
    f) dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.
3. Środki organizacyjne:
    a) do przetwarzania danych osobowych dopuszczone są wyłącznie osoby posiadające upoważnienie nadane przez ADO,
    b) prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych,
    c) wyznaczono Administratora Bezpieczeństwa Informacji,
    d) osoby zatrudnione przy przetwarzaniu danych osobowych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych,
    e) przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego

f) osoby zatrudnione przy przetwarzaniu danych osobowych zobowiązane zostały do zachowania ich w tajemnicy,

g) monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym,

h) kopie zapasowe zbioru danych osobowych przechowywane są innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco.

4. Kierownicy Wydziałów Urzędu analizują na bieżąco możliwość wystąpienia ryzyka dla poszczególnych systemów, a w przypadku wystąpienia ryzyka przedstawiają Administratorowi propozycje zastosowania środków ochrony (technicznych i organizacyjnych) dla zapewnienia przetwarzanym danym właściwej ochrony.
5. Analiza ryzyka polega na:
   a. identyfikacji występujących zagrożeń dla systemów, zbiorów i baz danych;
   b. ocenie dotychczas stosowanej ochrony obszarów przetwarzania danych osobowych;
   c. określeniu wielkości ryzyka, tj. prawdopodobieństwa, że określone zagrożenie wykorzysta podatność (słabość) zasobu;
   d. identyfikacji obszarów wymagających szczególnych zabezpieczeń.
6. Zastosowane środki ochrony (techniczne i organizacyjne) powinny być adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych osobowych.

§ 20

1. Uwzględniając kategorie przetwarzanych danych oraz zagrożenia zidentyfikowane w wyniku przeprowadzonej analizy ryzyka dla poszczególnych systemów, stosuje się następujące poziomy bezpieczeństwa:
   a. podstawowy;
   b. podwyższony;
   c. wysoki.
2. Określenia poziomu bezpieczeństwa systemu informatycznego dokonuje ABI na wniosek Kierowników Wydziałów.
3. Poziomy bezpieczeństwa odnotowuje się w dokumentacji prowadzonej przez ABI.

§ 21

Systemy informatyczne, którym przypisano poziomy bezpieczeństwa wymienione w § 20 muszą spełniać wymagania wymienione w załączniku do rozporządzenia 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).

VII
Postanowienia końcowe.

§ 22

W sprawach nieuregulowanych w niniejszej polityce stosuje się:

1. Ustawę z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity Dz. U. z 2014 roku, poz. 1182 z późń. zm.),
2. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r., Nr 100, poz. 1024),
3. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych z dnia 11 grudnia 2008 roku, (Dz.U. z 29 grudnia 2008 r., Nr 229 poz. 1536 z późń. zm.).

Sporicka

Załącznik nr 1
do Polityki Bezpieczeństwa
w Urzędzie Miejskim w Ząbkowicach Śl.

WYKAZ BUDYNKÓW, POMIESZCZEŃ LUB CZĘŚCI POMIESZCZEŃ, TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE.

1. Urząd Miejski w Ząbkowicach Śląskich - Ząbkowice Śląskie, ul. 1 Maja 15.

2. Urząd Stanu Cywilnego w Ząbkowicach Śląskich, Ząbkowice Śląskie, Rynek 56.

Załącznik nr 2
do Polityki Bezpieczeństwa
w Urzędzie Miejskim w Ząbkowicach Śl.

WYKAZ ZBIORÓW DANYCH OSOBOWYCH WRAZ ZE WSKAZANIEM PROGRAMÓW ZASTOSOWANYCH DO PRZETWARZANIA TYCH DANYCH .

l.p	Nazwa Wydziału	Nazwa zbioru danych	Programy zastosowane do przetwarzania danych / forma rejestru	Lokalizacja zbioru
1.	EKS	Ewidencja osób uzależnionych	Rejestr papierowy	UM, ul. 1 Maja 15
2.	EKD	Ewidencja osób uzależnionych	Pakiet OFFICE	UM, ul. 1 Maja 15
3.	EKS	Obowiązek szkolny	Rejestr papierowy	UM, ul. 1 Maja 15
4.	EKS	Obowiązek szkolny	Pakiet OFFICE	UM, ul. 1 Maja 15
5.	EKS	Oświadczenia majątkowe (EKS)	Rejestr papierowy	UM, ul. 1 Maja 15
6.	EKS	Oświadczenia majątkowe (EKS)	Pakiet OFFICE	UM, ul. 1 Maja 15
7.	EKS	Pomoc materialna dla uczniów	Rejestr papierowy	UM, ul. 1 Maja 15
8.	EKS	Pomoc materialna dla uczniów	Pakiet OFFICE	UM, ul. 1 Maja 15
9.	FP	Ewidencja tytułów wykonawczych	Rejestr papierowy	UM, ul. 1 Maja 15
10.	FP	Ewidencja tytułów wykonawczych	FK2000	UM, ul. 1 Maja 15
11.	FP	Płace	Rejestr papierowy	UM, ul. 1 Maja 15
12.	FP	Płace	Płatnik	UM, ul. 1 Maja 15
13.	FP	Płace	PUMA dla potrzeb Urzędów Miast i Gmin	UM, ul. 1 Maja 15
14.	FP	Płace	FK2000	UM, ul. 1 Maja 15
15.	FP	Rejestr decyzji o zwrocie opłaty skarbowej	Rejestr papierowy	UM, ul. 1 Maja 15
16.	FP	Rejestr decyzji o zwrocie opłaty skarbowej	FK2000	UM, ul. 1 Maja 15
17.	FP	Rejestr druków ścisłego zarachowania	Rejestr papierowy	UM, ul. 1 Maja 15
18.	FP	Rejestr druków ścisłego zarachowania	FK2000	UM, ul. 1 Maja 15
19.	FP	Rejestr wezwań i upomnień	Rejestr papierowy	UM, ul. 1 Maja 15
20.	FP	Rejestr wezwań i	FK2000	UM, ul. 1 Maja 15

		upomnień		
21.	FP	Rejestr wymiarowy oraz przypisów i odpisów	Rejestr papierowy	UM, ul. 1 Maja 15
22.	FP	Rejestr wymiarowy oraz przypisów i odpisów	FK2000	UM, ul. 1 Maja 15
23.	FP	Rejestr wymiarowy oraz przypisów i odpisów opłaty za gospodarowanie odpadami komunalnymi	Rejestr papierowy	UM, ul. 1 Maja 15
24.	FP	Rejestr wymiarowy oraz przypisów i odpisów opłaty za gospodarowanie odpadami komunalnymi	FK2000	UM, ul. 1 Maja 15
25.	FP	Rejestr zaświadczeń	Rejestr papierowy	UM, ul. 1 Maja 15
26.	FP	Rejestr zaświadczeń	FK2000	UM, ul. 1 Maja 15
27.	FP	Rejestr zaświadczeń o niezaleganiu	Rejestr papierowy	UM, ul. 1 Maja 15
28.	FP	Rejestr zaświadczeń o niezaleganiu	FK2000	UM, ul. 1 Maja 15
29.	FP	Rejestr zwrotu podatku akcyzowego	Rejestr papierowy	UM, ul. 1 Maja 15
30.	FP	Rejestr zwrotu podatku akcyzowego	FK2000	UM, ul. 1 Maja 15
31.	GN	Dodatki mieszkaniowe	Rejestr papierowy	UM, ul. 1 Maja 15
32.	GN	Dodatki mieszkaniowe	PUMA dla potrzeb Urzędów Miast i Gmin	UM, ul. 1 Maja 15
33.	GN	Ewidencja gruntów mienia gminnego	Rejestr papierowy	UM, ul. 1 Maja 15
34.	GN	Ewidencja gruntów mienia gminnego	EGB-2005	UM, ul. 1 Maja 15
35.	GN	Wieczyste użytkowanie	Rejestr papierowy	UM, ul. 1 Maja 15
36.	GN	Wieczyste użytkowanie	FK2000	UM, ul. 1 Maja 15
37.	IGP	Decyzje	Rejestr papierowy	UM, ul. 1 Maja 15

		środowiskowe		
38.	IGP	Decyzje środowiskowe	Pakiet OFFICE	UM, ul. 1 Maja 15
39.	IGP	Rejestr decyzji	Rejestr papierowy	UM, ul. 1 Maja 15
40.	IGP	Rejestr decyzji	Pakiet OFFICE	UM, ul. 1 Maja 15
41.	IGP	Rejestr decyzji i zaświadczeń	Rejestr papierowy	UM, ul. 1 Maja 15
42.	IGP	Rejestr decyzji i zaświadczeń	Pakiet OFFICE	UM, ul. 1 Maja 15
43.	OR	ABI	Rejestr papierowy	UM, ul. 1 Maja 15
44.	OR	ABI	ABI	UM, ul. 1 Maja 15
45.	OR	Kadry	Rejestr papierowy	UM, ul. 1 Maja 15
46.	OR	Kadry	Pakiet OFFICE	UM, ul. 1 Maja 15
47.	OR	Kadry	PUMA dla potrzeb Urzędów Miast i Gmin	UM, ul. 1 Maja 15
48.	OR	Oświadczenia majątkowe (radni)	Rejestr papierowy	UM, ul. 1 Maja 15
49.	OR	Oświadczenia majątkowe (radni)	Pakiet OFFICE	UM, ul. 1 Maja 15
50.	OR	Oświadczenia majątkowe pracowników	Rejestr papierowy	UM, ul. 1 Maja 15
51.	OR	Oświadczenia majątkowe pracowników	Pakiet OFFICE	UM, ul. 1 Maja 15
52.	OR	Rejestr kandydatów na ławników	Rejestr papierowy	UM, ul. 1 Maja 15
53.	RP	Działalność gospodarcza	Rejestr papierowy	UM, ul. 1 Maja 15
54.	RP	Działalność gospodarcza	Ewidencja Działalności gospodarczej „PUMA"	UM, ul. 1 Maja 15
55.	RP	Oświadczenia majątkowe spółek gminnych	Rejestr papierowy	UM, ul. 1 Maja 15
56.	RP	Oświadczenia majątkowe spółek gminnych	Ewidencja Działalności gospodarczej „PUMA"	UM, ul. 1 Maja 15
57.	RP	Oświadczenia majątkowe spółek gminnych	Pakiet OFFICE	UM, ul. 1 Maja 15
58.	SM	Straż Miejska	Rejestr papierowy	UM, ul. 1 Maja 15
59.	SM	Straż Miejska	Pakiet OFFICE	UM, ul. 1 Maja 15
60.	USC	Dowody osobiste	Rejestr papierowy	UM, ul. 1 Maja 15
61.	USC	Dowody osobiste	Źródło	UM, ul. 1 Maja 15
62.	USC	Ewidencja ludności	Rejestr papierowy	UM, ul. 1 Maja 15
63.	USC	Ewidencja ludności	PUMA dla potrzeb Urzędów Miast i Gmin	UM, ul. 1 Maja 15

64.	USC	Ewidencja ludności	Źródło	UM, ul. 1 Maja 15
65.	USC	Urząd Stanu Cywilnego	Rejestr papierowy	USC, Rynek 56
66.	USC	Urząd Stanu Cywilnego	PB USC Technika Gliwice	USC, Rynek 56
67.	USC	Urząd Stanu Cywilnego	Źródło	USC, Rynek 56
68.	ZP	Zamówienia publiczne	Rejestr papierowy	UM, ul. 1 Maja 15
69.	ZP	Zamówienia publiczne	Pakiet OFFICE	UM, ul. 1 Maja 15

Załącznik nr 3
do Polityki Bezpieczeństwa
w Urzędzie Miejskim w Ząbkowicach Śl.

OPIS STRUKTURY ZBIORÓW DANYCH ORAZ SPOSÓB PRZEPŁYWU TYCH DANYCH POMIĘDZY POSZCZEGÓLNYMI SYSTEMAMI.

Do przetwarzania danych osobowych w systemie informatycznym urzędu stosuje się aplikacje :

Bestia@ - firmy Sputnik Software ,
Płatnik - firmy Asseco Poland SA ,
Puma - firmy Zeto Olsztyn ,
eCorpoNet - System Bankowości Korporacyjnej
PBUSC - Technika IT Gliwice
FK2000 - firmy Infospółka

Źródłowy system informatyczny	Docelowy system informatyczny (lokalny/zewn.)	Kierunek przepływu Danych osobowych	Sposób transmisji
Bestia	Bestia (lokalny)	< = >	eksport / import pliku
Źródło	Główny Urząd Statystyczny (zewnętrzny)	= >	transmisja bezpośrednio z programu
Źródło	Puma (wewnętrzny)	= >	import pliku
PBUSC	Źródło (zewnętrzny)	< = >	eksport / import pliku
FK2000	eCorpoNet (wewnętrzny)	< = >	eksport /import pliku
FK2000	Płatnik (wewnętrzny)	< = >	eksport / import pliku
Płatnik	Zus (zewnętrzny)	< = >	eksport / import pliku
Puma	eCorpoNet (zewnętrzny)	= >	eksport / import pliku

Pozostałe programy działają niezależnie w oparciu o własne bazy danych.

Załącznik nr 4
do Polityki Bezpieczeństwa
w Urzędzie Miejskim w Ząbkowicach Śl.

EWIDENCJA OSÓB POSIADAJĄCYCH UPRAWNIENIA W ZAKRESIE DOSTĘPU DO DANYCH OSOBOWYCH I ICH PRZETWARZANIA.

l.p.	Imię i nazwisko użytkownika	Data nadania uprawnień	Data ustania uprawnień	zakres uprawnień	Nazwa wydziału	Identyfikator użytkownika	Data rejestracji w systemie	Data wyrejestrowania z systemu

Załącznik nr 5
do Polityki Bezpieczeństwa
w Urzędzie Miejskim w Ząbkowicach Śl.

ZGŁOSZENIE NARUSZENIA BEZPIECZEŃSTWA SYSTEMU INFORMATYCZNEGO

DATA:	
GODZINA:	
OSOBA POWIADAMIAJĄCA O ZAISTNIAŁYM ZDARZENIU: **imię i nazwisko,** **wydział,** **stanowisko,** **podpis**	
LOKALIZACJA ZDARZENIA: **nr pokoju,** **nazwa pomieszczenia**	
RODZAJ NARUSZENIA BEZPIECZEŃSTWA ORAZ OKOLICZNOŚCI TOWARZYSZĄCE:	
PRZYCZYNY WYSTĄPIENIA ZDARZENIA:	
PODJĘTE DZIAŁANIA:	

POSTEPOWANIE WYJAŚNIAJĄCE:	
DATA I GODZINA PRZYJĘCIA ZGŁOSZENIA:	
PODPIS ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI:	

Załącznik nr 6
do Polityki Bezpieczeństwa
w Urzędzie Miejskim w Ząbkowicach Śl.

..... Ząbkowice Śląskie, dnia .....
pieczęć komórki organizacyjnej

WNIOSEK

Zgodnie z art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r., poz. 1182 z późń. zm.)

wnioskuję o nadanie / zmianę / pozbawienie*

Pani/Panu .....*

upoważnienia do przetwarzania danych osobowych w Urzędzie Miejskim w Ząbkowicach Śląskich w związku z: podjęciem pracy, zmianą stanowiska, zwolnieniem z pracy, zmianą uprawnień lub inne (podać jakie)*
.....

Upoważnienie wydaje się na czas nieokreślony/ określony – od kiedy*
.....

1. Zakres przetwarzania danych osobowych .....
.....
2. Uprawnienia: użytkownika/ użytkownika uprzywilejowanego/ ASI* w związku z zajmowanym stanowiskiem (wskazać jakie) .....
.....
3. Sposób przetwarzania danych osobowych: wersja papierowa / elektroniczna*
4. Obszar przetwarzania danych (siedziba – adres, piętro, nr pokoju) .....
.....
5. Uprawnienia obejmują przetwarzanie danych sensytywnych: tak/nie*
6. Osoba została zapoznana z przepisami ustawy o ochronie danych osobowych: tak/nie*

.....
(podpis przełożonego)

*właściwe zaznaczyć

Załącznik nr 7
do Polityki Bezpieczeństwa
w Urzędzie Miejskim w Ząbkowicach Śl.

Ząbkowice Śląskie, dnia .....

.....
(imię i nazwisko)

.....
(stanowisko, wydział)

OŚWIADCZENIE

Ja niżej podpisana/y oświadczam, że podczas wykonywania obowiązków służbowych przetwarzam oraz mam dostęp do danych osobowych i w związku z tym zapoznałam/em się z niżej wymienionymi przepisami dotyczącymi przetwarzania i ochrony danych osobowych i zobowiązuje się do ich przestrzegania:

1. Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 roku (Dz. U z 2014 r., poz. 1182 z późń. zm.)
2. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r., w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne, służące do przetwarzania danych osobowych (Dz. U. z 2004r., Nr 100, poz. 1024)
3. Polityka bezpieczeństwa w Urzędzie Miejskim w Ząbkowicach Śląskich
4. Instrukcja zarządzania systemami informatycznymi w Urzędzie Miejskim w Ząbkowicach Śląskich.

Ponadto oświadczam, że:

1. zapewnię ochronę danym osobowych przetwarzanym w Urzędzie Miejskim w Ząbkowicach Śląskich tzn. zabezpieczę je przed dostępem osób nieupoważnionych, zabraniem, uszkodzeniem oraz nieuzasadnioną modyfikacją lub zniszczeniem;
2. zachowam w tajemnicy w czasie odbywania pracy/stażu/praktyki/innej umowy, jak również po ustaniu stosunku pracy, wszelkie informacje dotyczące przetwarzania i sposobów zabezpieczania danych osobowych w Urzędzie Miejskim w Ząbkowicach Śląskich;
3. zgłoszę stwierdzenie faktu lub próby naruszenia ochrony lub bezpieczeństwa systemu informatycznego, w którym przetwarzane są dane osobowe bezpośredniemu przełożonemu lub Administratorowi Bezpieczeństwa Informacji Urzędu Miejskiego w Ząbkowicach Śląskich.

.....
(podpis pracownika)

Załącznik nr 8
do Polityki Bezpieczeństwa
w Urzędzie Miejskim w Ząbkowicach Śl.

Ząbkowice Śląskie, dnia .....

UPOWAŻNIENIE

do przetwarzania danych osobowych w Urzędzie Miejskim w Ząbkowicach Śląskich

Zgodnie z art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r., poz. 1182 z późń. zm.) upoważniam/zmieniam upoważnienie/wycofuję upoważnienie dla Pani/Pana

.....
(imię i nazwisko osoby upoważnionej)

.....
(wydział)

.....
(stanowisko)

do przetwarzania danych osobowych w zakresie:
.....
.....

z uprawnieniami: użytkownika/użytkownika uprzywilejowanego/ASI*

Sposób przetwarzania danych: wersja papierowa/wersja elektroniczna*

Upoważnienie wydaje się na czas nieokreślony/określony* .....

.....
(podpis)

*właściwe zaznaczyć

Złącznik nr 2 do Zarządzenia
nr 362 Burmistrza Ząbkowic Śl.
z dnia 19 grudnia 2015

INSTRUKCJA ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI

w Urzędzie Miejskim w Ząbkowicach Śląskich

I. Postanowienia ogólne.

II. Procedury nadawania, zmiany uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym.

III. Metody i środki uwierzytelniania w systemie informatycznym.

IV. Procedury rozpoczęcia, zawieszenia, zakończenia pracy przez użytkowników w systemie informatycznym.

V. Procedury tworzenia kopii zapasowych.

VI. Przechowywanie nośników z danymi oraz kopii zapasowych.

VII. Środki ochrony systemów informatycznych.

VIII. Monitorowanie dostępu do danych.

IX. Procedury przeglądów i konserwacji systemów oraz zbiorów danych osobowych.

X. Postanowienia końcowe.

Załączniki do Instrukcji:

1. Wniosek przełożonego o nadanie uprawnień dla użytkownika w systemie informatycznym.
2. Rejestr kopii zapasowych.

I
Postanowienia ogólne.

§ 1.

1. Instrukcja zarządzania systemami informatycznymi, zwana dalej instrukcją, reguluje zasady i procesy zarządzania i administrowania Systemami Informatycznymi w Urzędzie Miejskim w Ząbkowicach Śląskich, w celu bezpiecznego ich przetwarzania.
2. Instrukcja opracowana została zgodnie z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz.U. z 2014 r., poz. 1182 z późn. zm.) oraz z Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r., Nr 100 poz. 1024).
3. Instrukcja obejmuje swoim zakresem wszystkie osoby biorące udział w procesie przetwarzania danych osobowych w systemach informatycznych:

- Administratora Bezpieczeństwa informacji w Urzędzie (ABI),
- Administratorów Systemów Informatycznych w Urzędzie (ASI),
- Kierowników Wydziałów Urzędu Miejskiego w Ząbkowicach Śląskich (bezpośredni przełożeni osób przetwarzających dane osobowe),
- Inne osoby, wskazane przez Administratora Danych Osobowych (podmioty zewnętrzne współpracujące z Urzędem Miejskim w Ząbkowicach Śląskich, biorące udział w przetwarzaniu danych osobowych).

§ 2.

Skróty i określenia użyte w Instrukcji oznaczają:

1. Urząd - Urząd Miejski w Ząbkowicach Śląskich,
2. Administrator Danych Osobowych (ADO) - Burmistrz Ząbkowic Śląskich, zwany dalej Administratorem,
3. Administrator Bezpieczeństwa Informacji (ABI) - osoba wyznaczona przez Administratora (ADO), w rozumieniu art. 36a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz.U. z 2014 r., poz. 1182 z późn. zm.),

4. Administratorzy Systemów Informatycznych (ASI) - pracownicy wyznaczeni przez Administratora Danych Osobowych odpowiedzialni za wdrożenie i stosowanie zasad bezpieczeństwa systemów informatycznych, zobowiązani do stosowania technicznych i organizacyjnych środków ochrony przewidzianych w systemach informatycznych.
5. Administratorzy Kopii Bezpieczeństwa (AKB) - ASI.
6. Kierownik Wydziału, zwany dalej przełożonym - osoba odpowiedzialna za przestrzeganie zasad przetwarzania i ochrony danych przez podległych mu pracowników.
7. Użytkownik systemu - osoba posiadająca upoważnienie do wprowadzania i przetwarzania danych w systemie informatycznym w zakresie wskazanym w upoważnieniu.
8. Hasło - ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.
9. Identyfikator użytkownika - ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych w systemie informatycznym.
10. Dane osobowe - zbiór informacji pozwalających na identyfikację konkretnej osoby
11. Dane sensytywne - dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, a także informacje o innych orzeczeniach wydanych w postępowaniu sądowym lub administracyjnym.
12. Sieć LAN - sieć lokalna, służąca do połączenia systemów informatycznych przy wykorzystaniu specjalistycznych urządzeń i sieci telekomunikacyjnych.
13. Rejestr udostępnionych danych osobowych, zwany dalej rejestrem, prowadzony dla danego systemu, w którym odnotowywane są informacje o odbiorcach z systemu danych.

II
Procedury nadawania, zmiany uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym.

§ 3.

1. Każdy pracownik Urzędu, przed przystąpieniem do pracy zobowiązany jest do zapoznania się z niniejszą Instrukcją oraz:
   - Ustawą dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz.U. z 2014 r., poz. 1182 z późn. zm.),
   - Polityką bezpieczeństwa w Urzędzie Miejskim w Ząbkowicach Śląskich,

2. Przetwarzać dane osobowe może jedynie użytkownik systemu upoważniony przez ADO. Użytkownik systemu może wykonywać tylko te czynności, do których został upoważniony.

3. Podstawą nadania, zmiany lub cofnięcia uprawnień, jest wniosek Kierownika Wydziału (załącznik nr 1 do niniejszej Instrukcji).

§ 4.

1. W Urzędzie funkcjonuje schemat nadawania, zmiany i cofnięcia uprawnień dostępu do sieci LAN. Zakłada on, że użytkownicy systemu mają dostęp do sieci LAN na określonym poziomie użytkownika, w zależności od indywidualnego zakresu obowiązków, a także powierzonych zadań na danym stanowisku.

2. Zadania Kierownika Wydziału:

   - Wnioskuje o nadanie, zmianę lub cofnięcie uprawnień dla pracownika do przetwarzania danych w systemie, w sieci LAN, w związku z wykonywaniem przez niego obowiązków służbowych,

   - Zgłasza ASI potrzebę nadania uprawnień dla konkretnego pracownika w systemie informatycznym na określonym poziomie.

3. Zadania ASI:

   - Rejestruje, zmienia lub usuwa użytkownika w systemie i nadaje mu określone uprawnienia,

   - Informuje Kierownika Wydziału oraz ABI o nadaniu, zmianie, cofnięciu uprawnień. W przypadku nadania uprawnień dodatkowo o założonym koncie wnioskowanym dla użytkownika oraz o nadanych uprawnieniach.

   - Jeżeli nadanie pracownikowi wymaganych uprawnień miałoby naruszyć bezpieczeństwo systemów działających w sieci, ASI ma obowiązek poinformować o tym Kierownika Wydziału oraz ABI i jednocześnie wstrzymuje proces nadania uprawnień. Kierownik Wydziału może ponownie zawnioskować o nadanie pracownikowi uprawnień , które nie będą stanowiły zagrożenia bezpieczeństwa systemu. Wniosek ten musi zostać zaakceptowany przez ABI.

4. Użytkownik systemu, po uzyskaniu informacji od ASI o założonym koncie z uprawnieniami zobowiązany jest do:

   - Zalogowania się do systemu, w celu sprawdzenia poprawności działania konta i nadanych mu uprawnień,

- Zmiany nadanego mu przez ASI hasła (obowiązek ten musi być wykonany przy pierwszym logowaniu)

§ 5.

Wyżej wymienione zasady obowiązują wszystkich pracowników Urzędu Miejskiego w Ząbkowicach Śląskich i odnoszą się do wszystkich systemów eksploatowanych w sieci LAN.

§ 6.

1. Zasady korzystania z sieci LAN przez pracowników Urzędu Miejskiego:
a) Każdy pracownik posiada konto użytkownika uprawniające go do pracy na jednym z serwerów w sieci LAN Urzędu Miejskiego w Ząbkowicach Śląskich.
b) Konta na serwerze przydziale są każdemu pracownikowi zgodnie z procedurą określoną w § 4 pkt. 2 niniejszej Instrukcji.
c) ASI określa warunki techniczne korzystania z kont oraz ograniczenia rozmiaru zużywanej przestrzeni dyskowej.
d) Pracownicy Urzędu korzystają z poczty poprzez wskazanego przez ASI klienta serwera pocztowego lub dowolną przeglądarkę internetową.
2. Każdy użytkownik systemu Urzędu powinien postępować zgodnie z powierzonymi mu obowiązkami, a w szczególności:
a) używać poczty elektronicznej tylko do celów służbowych,
b) korzystać z Internetu tylko do celów służbowych,
c) korzystać z systemów/aplikacji Urzędu tylko do celów służbowych.
3. Zabrania się:
a) wysyłania masowej poczty kierowanej do losowych odbiorców (spam),
b) udostępniania treści chronionych prawem autorskim (filmy, utwory muzyczne),
c) udostępniania treści zakazanych,
d) nieuzasadnionego wynoszenia danych zawartych na nośnikach zewnętrznych poza Urząd,
e) podejmowania prób wykorzystania obcego konta, uruchamiania aplikacji deszyfrujących hasła, prowadzenia działań mających na celu podsłuchiwanie lub przechwytywanie informacji przepływającej w sieci,
f) uruchamiania aplikacji, które mogą zakłócić i destabilizować pracę systemu lub sieci komputerowej, bądź naruszyć prywatność zasobów systemowych.
4. W przypadku naruszenia zasad określonych w pkt. 2 i 3 ASI blokuje dostęp do konta użytkownika, powiadamiając jednocześnie o tym fakcie ABI i przełożonego pracownika.
5. W przypadku zaistnienia potrzeby podłączenia komputera prywatnego pracownika do sieci LAN Urzędu, wymagana jest akceptacja ASI.
6. W przypadku stwierdzenia, że komputer podłączony do sieci LAN zakłóca pracę sieci lub wskazuje na używanie tego komputera jako niezarejestrowanego serwera danych, ASI blokuje dostęp do tego komputera do czasu wyjaśnienia sprawy. O tym fakcie powiadamia ABI i przełożonego pracownika.

§ 7.

1. Zasady użytkowania sprzętu komputerowego przez pracowników Urzędu Miejskiego:

a) użytkownik korzysta ze sprzętu komputerowego i sieci LAN wyłącznie w zakresie powierzonych mu zadań,
b) informacje zapisane na nośnikach informatycznych są własnością pracodawcy - Urzędu Miejskiego w Ząbkowicach Śląskich,
c) o przekazaniu sprzętu komputerowego pracownikowi decyduje przełożony pracownika lub ASI,
d) użytkownik jest materialnie odpowiedzialny za sprzęt komputerowy, który otrzymał do wykonywania obowiązków służbowych.

2. Kierownik Wydziału Organizacyjnego wraz z informatykiem Urzędu prowadzi sprawy z zakresu użytkowania sprzętu i oprogramowania komputerowego:
a) nadzoruje wykonywanie umów, dotyczących zakupu/serwisu sprzętu i oprogramowania,
b) prowadzi ewidencję sprzętu i oprogramowania,
c) zabezpiecza sprawne działanie sprzętu i oprogramowania,
d) zapewnia standardy sprzętu i oprogramowania spełniające wymagania Urzędu Miejskiego.
3. Każdy użytkownik posiada indywidualny identyfikator i hasło, które zabezpieczają dostęp do komputera, sieci LAN, baz danych i skrzynki pocztowej.
4. Zabrania się:
a) podłączania przez użytkowników własnych urządzeń do sprzętu komputerowego lub sieci LAN,
b) podłączania innych urządzeń niż informatyczne do wydzielonej sieci energetycznej do zasilania komputerów,
c) instalowania oprogramowania na sprzęcie komputerowym,
d) przemieszczania sprzętu komputerowego do innych lokalizacji lub zmiany użytkownika bez zgody ASI
e) samowolnego odłączania lub przyłączania sprzętu komputerowego do sieci LAN,
f) udostępniania swojego identyfikatora i hasła do pracy innym osobom,
g) pozyskiwania informacji z komputerów innych użytkowników bez ich wiedzy,
h) wykonywania czynności, które mogą spowodować zakłócenia lub awarię sieci LAN,
i) wynoszenia poza miejsce pracy nośników informacji oraz przesyłanie danych poczta elektroniczną na zewnątrz.

§ 8.

Zasady udzielania pomocy użytkownikom sprzętu komputerowego w Urzędzie Miejskim:
1. Pracownik zgłasza telefonicznie lub osobiście informatykowi problem z użytkowaniem sprzętu lub oprogramowania komputerowego,
2. informatyk dokonuje oceny problemu, a także podejmuje działania mające na celu usunięcie zaistniałego problemu,
3. w przypadku braku możliwości usunięcia problemu ze sprzętem komputerowym lub oprogramowaniem, informatyk zgłasza awarię do serwisu zewnętrznego w celu dokonania naprawy serwisowej,
4. w przypadku konieczności oddania sprzętu komputerowego do zewnętrznego serwisu, informatyk wymontowuje i zabezpiecza dysk twardy i inne nośniki danych zainstalowane na sprzęcie.

III
Metody i środki uwierzytelniania w systemie informatycznym.

§ 9.

1. Naczelną zasadą bezpieczeństwa systemu informatycznego jest ochrona informacji przed dostępem osób nieuprawnionych, ujawnianiem, przypadkowym zniszczeniem lub modyfikacja danych.
2. Stosowanie zasad uwierzytelniania użytkowników ma podstawowy wpływ na zachowanie poufności, rozliczalności i integralności danych.
3. W systemie informatycznym w Urzędzie stosowane jest uwierzytelnianie użytkownika przy pomocy: identyfikatorów i haseł.
4. Stosowanie identyfikatorów ma na celu zapewnienie bezpieczeństwa i realizuje zasadę rozliczalności w systemach i sieciach Urzędu. Wszelkie działania w systemach przypisane są konkretnemu użytkownikowi.
5. Identyfikator składa się z 6 znaków (trzy pierwsze odpowiadają literom nazwiska, a trzy kolejne literom imienia). W identyfikatorze pomija się polskie znaki diakrytyczne.
6. Identyfikator użytkownika systemu, który utracił uprawnienia do dostępu do danych osobowych należy wyrejestrować z systemu informatycznego i unieważnić hasło.
7. Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu z systemu nie może być przydzielony innej osobie.
8. Stosowanie haseł ma na celu ograniczenie dostępu do informacji jedynie dla kręgu użytkowników uprawnionych.
9. Hasło należy zmienić na indywidualne (przy pierwszym logowaniu do systemu informatycznego). System powinien automatycznie wymuszać zmianę hasła.
10. Hasło musi zawierać co najmniej 8 znaków i jednocześnie: duże i małe litery, cyfry i znaki specjalne.
11. Każdy użytkownik systemu utrzymuje hasło w tajemnicy (również po upływie jego ważności). Ma to na celu realizacje zasady poufności. Hasło powinno być wprowadzane w taki sposób, aby uniemożliwić innym osobom jego poznanie.
12. Hasło jest wpisywane i przechowywane w systemie informatycznym w postaci zaszyfrowanej.

13. Hasło użytkownika musi być zmieniane nie rzadziej niż raz na 30 dni. W przypadku, gdy hasło nie jest używane przez użytkownika przez okres dłuższy niż 30 dni, musi być zmienione podczas najbliższego ponownego logowania.

14. Hasło użytkownika, który utracił uprawnienia dostępu do danych osobowych unieważnia się bezzwłocznie, a także podejmuje się wszelkie działania, mające na celu zapobieżenie dalszemu dostępowi tej osoby do danych.

15. Użytkownik systemu ponosi odpowiedzialność za czynności wykonywane w systemie przy użyciu identyfikatora i hasła. Zobowiązany jest również do utrzymania haseł dostępu w tajemnicy, nawet po ustaniu ich ważności.

16. ASI jest odpowiedzialny za prawidłowe funkcjonowanie mechanizmów zawartych w § 9 niniejszej Instrukcji.

§ 10.

Procedura zarządzania środkami uwierzytelniania:

1. ASI nadaje nowemu użytkownikowi systemu hasło dostępu do systemu lub sieci LAN (podobnie jest w sytuacji, gdy użytkownik systemu zapomniał ostatnio używanego hasła),

2. Użytkownik systemu, przy pierwszym zalogowaniu zmienia hasło nadane przez ASI na swoje indywidualne hasło (znane tylko jemu). System automatycznie wymusza zmianę hasła nadanego przez ASI przy pierwszym logowaniu do systemu,

3. Użytkownik w każdym momencie może zmienić sobie hasło dostępu do systemu,

4. Obowiązuje bezwzględny zakaz notowania (w jakiejkolwiek formie) haseł aktualnych oraz wygasłych,

IV
Procedury rozpoczęcia, zawieszenia, zakończenia pracy przez użytkowników w systemie informatycznym.

§ 11.

1. Procedura rozpoczęcia pracy:

   - rozpoczynając pracę użytkownik systemu po uruchomieniu komputera loguje się podając identyfikator i hasło.

   - użytkownik systemu rozpoczynając pracę uruchamia system/aplikację. Loguje się podając identyfikator i hasło.

2. Procedura zawieszenia pracy:

- przy każdorazowym opuszczeniu stanowiska komputerowego należy dopilnować, aby na ekranie monitora nie były wyświetlane informacje lub dane, poprzez zabezpieczenie komputera lub wylogowanie się z systemu.

3. Procedura zakończenia pracy w systemie:

   - użytkownik zamyka system/aplikację i sprawdza czy nie zostały pozostawione bez nadzoru nośniki informacji.

   - użytkownik zamyka system operacyjny komputera i czeka na jego wyłączenie.

4. Użytkownik w pełnym zakresie odpowiada za sprzęt komputerowy i wykonywanie czynności, aż do momentu rozliczenia ze sprzętu komputerowego.

V
Procedury tworzenia kopii zapasowych.

§ 12.

1. W Urzędzie praktykowane jest przetwarzanie danych w bazach danych na dedykowanych dla systemu informatycznego serwerach.

2. Kopie zapasowe baz danych zlokalizowanych na serwerach wykonywane są:

   - w cyklu dobowym (w godzinach nocnych) - za pomocą programów archiwizujących tworzone są pełne kopie baz danych,

   - w cyklu tygodniowym - tworzony jest „ręczny" pełny backup baz danych systemu wraz z kopią systemu operacyjnego serwera.

3. W przypadku braku technicznych możliwości wykonania kopii zgodnie z planem, należy je wykonać w najbliższym możliwym terminie.

4. Kopiami zapasowymi zabezpieczane są dane i programy służące do ich przetwarzania.

5. ASI jest odpowiedzialny za przygotowywanie kopii bezpieczeństwa i prowadzi rejestr kopii zapasowych (załącznik nr 2 do niniejszej Instrukcji).

6. Każdy użytkownik systemu we własnym zakresie tworzy kopie zapasowe wytworzonych przez siebie dokumentów i danych.

VI
Przechowywanie nośników z danymi oraz kopii zapasowych.

§ 13.

1. Elektroniczne nośniki informacji:

- Dane w postaci elektronicznej przetwarzane w systemach zapisywane są na nośnikach zewnętrznych (dyski HDD)
- Nośniki przechowywane są w pokojach stanowiących obszar przetwarzania danych osobowych określony w Polityce Bezpieczeństwa.
- Po zakończeniu pracy przez użytkowników systemu nośniki przechowywane są w meblach biurowych (zamykanych szafach).
- w/w nośniki powinny być oznaczone w sposób, który umożliwi ich identyfikację.

2. Przekazywanie i niszczenie elektronicznych nośników informacji:

- ADO upoważnia osobę, za zgodą której można przekazywać elektroniczne nośniki informacji tylko podmiotom lub osobom do tego uprawnionym na podstawie przepisów prawa.
- Dane osobowe znajdujące się na nośniku zewnętrznym muszą być zabezpieczone hasłem przed odczytem
- Dane osobowe przenoszone za nośniku zewnętrznym muszą być trwale usunięte po ich przeniesieniu do docelowej bazy danych na docelowy sprzęt komputerowy
- Przekazywanie i niszczenie elektronicznych nośników informacji zawierających dane osobowe dokonuje się komisyjnie, na podstawie protokołu przygotowanego przez ABI.

§ 14.

1. Kopie zapasowe:

- Kopie zapasowe wykonywane na nośnikach zewnętrznych nie powinny być przechowywane w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych eksploatowane na bieżąco.
- Kopie zapasowe należy przechowywać w miejscach zabezpieczonych przed ich nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem (tj. w zamykanej szafie na terenie Urzędu)
- Dostęp do kopii zapasowych mają tylko osoby upoważnione tj. ASI i ABI.
- Kopie zapasowe należy okresowo sprawdzać pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu
- Kopie zapasowe należy usuwać bezzwłocznie po ustaniu ich użyteczności.

§ 15.

1. Wydruki:

   - Wydruki zawierające dane osobowe należy przechowywać w pokojach stanowiących obszar przetwarzania danych osobowych określony w Polityce Bezpieczeństwa,
   - Wydruki zawierające dane osobowy niszczy się przez pocięcie w niszczarce.
   - Za bezpieczeństwo danych osobowych zapisanych w formie tradycyjnej odpowiedzialne są osoby je przetwarzające.

VII
Środki ochrony systemów informatycznych.

§ 16.

1. W celu zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych stosuje się środki ochrony przed tzw. „szkodliwym oprogramowaniem próbami dostępu przez osoby nieuprawnione.
2. Zasady ochrony systemów informatycznych:
   - Ochrona antywirusowa:
     a) ASI odpowiada za ochronę antywirusową,
     b) ASI wykonuje czynności związane z ochroną antywirusową, wykorzystując do tego moduły programu antywirusowego w aktualnej wersji. Program antywirusowy powinien na bieżąco sprawdzać zasoby systemu informatycznego,
     c) Oprogramowanie antywirusowe instalowane jest na serwerze, a także wszystkich stanowiskach komputerowych podłączonych do sieci,
     d) Aktualizacja oprogramowania antywirusowego odbywa się automatycznie dla wszystkich komputerów zainstalowanych w sieci, nie rzadziej niż raz w tygodniu,
     e) Aktualizacja oprogramowania antywirusowego (na komputerach niepodłączonych do sieci) wykonywana jest przez informatyka przy zastosowaniu nośników zewnętrznych, nie rzadziej niż raz w tygodniu,
     f) Każdy użytkownik systemu, przy imporcie danych do systemu informatycznego, zobowiązany jest do sprawdzenia tych danych pod kątem możliwości wystąpienia zagrożenia wirusowego i szkodliwego oprogramowania,
     g) Zabrania się pobierania z Internetu plików niewidomego pochodzenia,
     h) Użytkownik systemu, po każdym wykryciu wirusa, niezwłocznie informuje o tym fakcie informatyka, który analizuje problem i podejmuje działania naprawcze,
     i) W Urzędzie stosuje się urządzenia oddzielające sieć komputerową od bezpośredniego dostępu do Internetu, stanowiące blokadę przed nieuprawnionym dostępem z zewnątrz do systemu informatycznego,
     j) Niedopuszczalne jest używanie i wynoszenie urządzeń i nośników informacji wykorzystywanych do pracy w Urzędzie, poza obszar przetwarzania danych bez zgody ADO/ABI.

k) W razie konieczności podłączenia do systemu informatycznego zewnętrznego nośnika, nośnik ten musi być poddany weryfikacji przez ASI pod kątem szkodliwego oprogramowania lub wirusów.
l) Niedopuszczalne jest używanie do codziennej pracy nośników i urządzeń nie będących na wyposażeniu Urzędu.

- Ochrona przed awarią zasilania:
  a) System, w którym przetwarzane są dane osobowe powinien być zabezpieczony przed ich utratą na skutek awarii zasilania lub zakłóceniami w sieci zasilającej,
  b) W Urzędzie dane osobowe przetwarzane z wykorzystaniem serwera w wewnętrznych sieciach teleinformatycznych (w razie awarii zasilania) zabezpieczone są przy wykorzystaniu UPS-ów,
  c) Dodatkowo dla zachowania ciągłości pracy w razie braku zasilania Urząd posiada generator prądotwórczy.

VIII.
Monitorowanie dostępu do danych.

§ 17.

1. Każdy system, w którym przetwarzane są dane osobowe posiada rejestr. W rejestrze odnotowuje się informacje o odbiorcach danych, zakresie udostępnianych danych oraz dacie udostępnienia.

2. Obowiązek odnotowywania danych wymienionych w pkt. 1 spoczywa na użytkowniku systemu, który udostępnia dane. Odnotowanie powinno nastąpić niezwłocznie po udostępnieniu danych.

3. Odbiorca danych to każdy, komu udostępnia się dane: osoba, której dane dotyczą; podmiot, któremu powierzono przetwarzanie danych; organ państwowy lub organ samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

4. Udostępnianie danych osobowych następuje:

   - Na wniosek osób lub podmiotów uprawnionych do ich otrzymania z mocy przepisów prawa - w celu innym niż włączenie danych do zbioru

   - Na wniosek innych osób i podmiotów niż w/w , jeśli uzasadnią w sposób wiarygodny potrzebę posiadania tych danych (z wyjątkiem danych sensytywnych), a ich udostępnienie nie naruszy praw i wolności osób, których dane dotyczą

   - Na pisemny umotywowany wniosek, chyba że przepis innej ustawy stanowi inaczej. Wniosek taki musi zawierać: informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać zakres i przeznaczenie żądanych danych.

5. Udostępnione dane można wykorzystać wyłącznie zgodnie z ich przeznaczeniem.

6. Nadzór nad prawidłowością odnotowywania danych w rejestrze sprawuje ABI.

IX.
Procedury przeglądów i konserwacji systemów oraz zbiorów danych osobowych.

§ 18.

1. Dla zachowania ciągłości pracy oraz bezpieczeństwa danych przeprowadza się okresowe i bieżące przeglądy oraz konserwacje sprzętu komputerowego.
2. Przeglądy i konserwacje wykonuje w Urzędzie ASI w terminach określonych przez producenta sprzętu.
3. Przegląd programów i narzędzi programowych - konserwacja baz danych przeprowadzana jest zgodnie z zaleceniami twórców poszczególnych programów.

X.
Postanowienia końcowe.

§ 19.

W sprawach nieuregulowanych w niniejszej instrukcji stosuje się:

1. Ustawę z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity Dz. U. z 2014 roku, poz. 1182 z późń. zm.),
2. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r., Nr 100, poz. 1024),

Załącznik nr 1
do Instrukcji Zarządzania
Systemami Informatycznymi
w Urzędzie Miejskim w Ząbkowicach Śl.

WNIOSEK PRZEŁOZONEGO O NADANIE UPRAWNIEŃ DLA UŻYTKOWNIKA W SYSTEMIE INFORMATYCZNYM

☐ NADANIE UPRANIEŃ (NOWY UŻYTKOWNIK)	☐ MODYFIKACJA UPRAWNIEŃ	☐ ODEBRANIE UPRAWNIEŃ

DOTYCZY SYSTEMU: .....
(NAZWA APLIKACJI /BAZY DANYCH/, W KTÓREJ PRZETWARZANE SĄ DANE OSOBOWE)

IMIĘ I NAZWISKO UŻYTKOWNIKA:	**WYDZIAŁ:**	
POSIADA UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH:	☐ TAK	☐ NIE
OPIS ZAKRESU UPRAWNIEŃ UŻYTKOWNIKA W SYSTEMIE INFORMATYCZNYM I UZASADNIENIE:		
DATA ZGŁOSZENIA:	PRZEŁOŻONY UŻYTKOWNIKA:	
ASI:		

Załącznik nr 2
do Instrukcji Zarządzania
Systemami Informatycznymi
w Urzędzie Miejskim w Ząbkowicach Śl.

REJESTR KOPII ZAPASOWYCH:

L.p.	Imię i nazwisko osoby wykonującej kopię zapasową	Opis kopii zapasowej	Nazwa systemu / konta użytkownika	Rodzaj kopii (dobowa, tygodniowa)	Miejsce przechowywania kopii	Data i podpis	UWAGI