ZARZĄDZENIE NR 120/ 16 /12

PREZYDENTA MIASTA TYCHY

z dnia 25 kwietnia 2012 r.

w sprawie zasad postępowania przy przetwarzaniu danych osobowych w Urzędzie Miasta Tychy

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2001 r. Nr 142, poz. 1591 z późn. zm.), art. 36 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.) oraz 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)

zarządza się, co następuje:

§ 1

1. Przetwarzanie danych osobowych służy realizacji zadań wynikających z bieżącej pracy i działalności Urzędu.
2. Dokumentacja przetwarzania danych prowadzona jest w formie papierowej.
3. Dokumentacja jest wdrażana do stosowania na podstawie zarządzenia, wprowadzanie zmian w dokumentacji następuje w tej samej formie.

§ 2

1. Administratorem danych w Urzędzie Miasta Tychy w rozumieniu ustawy jest Prezydent Miasta Tychy.
2. Obowiązki wynikające z ustawy Prezydent Miasta Tychy powierza:
   1) Pani Ewie TURLEWICZ Sekretarzowi Miasta – Administratorowi Bezpieczeństwa Informacji w zakresie nadzoru nad przestrzeganiem zasad ochrony dotyczących:
      a) stosowanych środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych stosownie do zagrożeń oraz kategorii danych objętych ochroną,
      b) zabezpieczenia danych przed ich udostępnianiem osobom nieupoważnionym, zabraniem przez osobę nieupoważnioną, przetwarzaniem ich z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;
   2) Panu Sebastianowi WIKA Naczelnikowi Wydziału Informatyki – Administratorowi Systemów Informatycznych (ASI_GWI) w zakresie:
      a) tworzenia warunków technicznych i organizacyjnych, zapewniających ochronę przetwarzanych danych osobowych,
      b) prowadzenia i przechowywania dokumentacji przetwarzania danych;
      c) prowadzenia ewidencji baz danych w systemach informatycznych, w których przetwarzane są dane osobowe w Urzędzie Miasta Tychy
      d) prowadzenia ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych w systemach informatycznych i ich identyfikatorów,
      e) prowadzenie ewidencji miejsc [przetwarzania danych osobowych i sposobu ich zabezpieczania,
   3) Pani Alicji KULKA Naczelnikowi Wydziału Geodezji – Administratorowi Systemów Informatycznych SIT i SOWA (ASI_GWG) w zakresie:
      a) tworzenia warunków technicznych i organizacyjnych, zapewniających ochronę przetwarzanych danych osobowych,
      b) prowadzenia i przechowywania dokumentacji przetwarzania danych;
   4) Pani Sylwii UCHNAST – GARA Pełnomocnikowi ds. Jakości – Głównemu Specjaliście w Wydziale Organizacyjnym, Kadr i Szkolenia w zakresie opracowywania dokumentacji oraz dokonywania zmian w dokumentacji na podstawie złożonych wniosków, przedstawianie dokumentacji (zmian) Administratorowi Danych do zatwierdzenia.
   5) kierownikom jednostek organizacyjnych Urzędu, w których następuje przetwarzanie danych osobowych w zakresie tworzenia warunków organizacyjnych i przestrzegania zasad ochrony danych osobowych, o których mowa w rozporządzeniu i Polityce Bezpieczeństwa w zakresie

przetwarzania danych osobowych w Urzędzie;

§ 3

1. Zgodnie z wymogami § 3 ust. 1 rozporządzenia wprowadza się do stosowania Politykę Bezpieczeństwa w zakresie przetwarzania danych osobowych w Urzędzie Miasta Tychy, stanowiącą załącznik do niniejszego zarządzenia.
2. Zgodnie w wymogami § 3 ust. 1 rozporządzenia wprowadza się do stosowania Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, stanowiącą załącznik do Polityki Bezpieczeństwa w zakresie przetwarzania danych osobowych w Urzędzie Miasta Tychy.

§ 4

Kierowników jednostek organizacyjnych zobowiązuje się do zaznajomienia podległych im osób z treścią zarządzenia.

§ 5

Osoby nieprzestrzegające przepisów podlegają sankcjom przewidzianym w rozdziale 8 ustawy o ochronie danych osobowych.

§ 6

Nadzór nad wykonaniem Zarządzenia powierza się Sekretarzowi Miasta.

§ 7

Traci moc Zarządzenie Nr 0152/122/09 Prezydenta Miasta Tychy z dnia 27 lutego 2009 r. w sprawie określenia zasad postępowania przy przetwarzaniu danych osobowych w Urzędzie Miasta Tychy.

§ 8

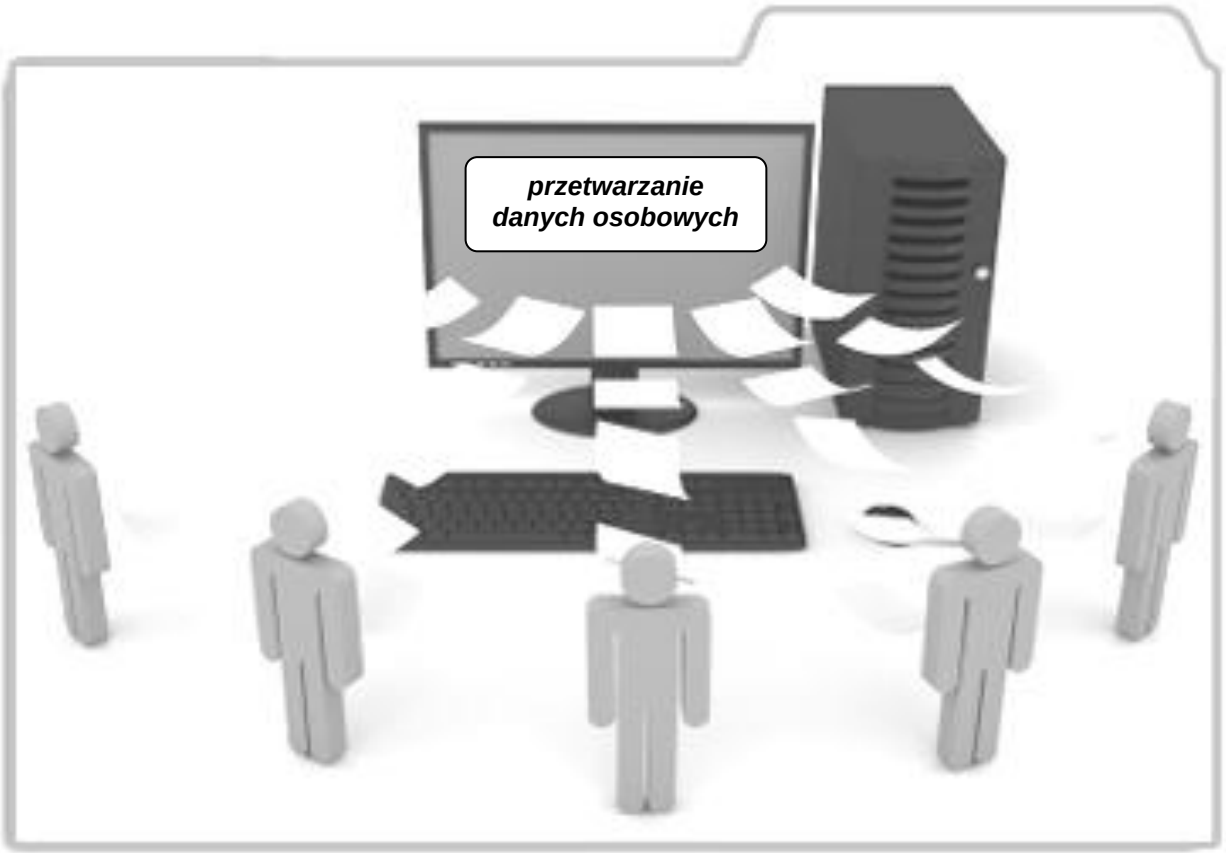
Zarządzenie wchodzi w życie z dniem podpisania.

http://bip.umtychy.pl/index.php?action=PobierzPlik&id=37637

Załącznik do Zarządzenia Nr 120/ 16 /12
Prezydenta Miasta Tychy z dnia 25 kwietnia 2012 r.

URZĄD MIASTA TYCHY

POLITYKA
BEZPIECZEŃSTWA



Kwiecień 2012 rok

Data wygenerowania dokumentu: 2024-11-21 16:00:36

http://bip.umtychy.pl/index.php?action=PobierzPlik&id=37637

Spis treści

Data wygenerowania dokumentu: 2024-11-21 16:00:36

http://bip.umtychy.pl/index.php?action=PobierzPlik&id=37637

§ 1

PODSTAWA PRAWNA

„Polityka Bezpieczeństwa" stanowi wykonanie obowiązku, o którym mowa w § 4 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).

§ 2

WSTĘP

1. Kierownictwo Urzędu świadome wagi problemów związanych z ochroną prawa do prywatności, w tym w szczególności prawa osób fizycznych powierzających swoje dane osobowe do właściwej i skutecznej ochrony tych danych deklaruje zamiar:
   1) podejmowania wszystkich działań niezbędnych dla ochrony praw i usprawiedliwionych interesów jednostki związanych z bezpieczeństwem danych osobowych;
   2) stałego podnoszenia świadomości oraz kwalifikacji osób przetwarzających dane osobowe w Urzędzie w zakresie problematyki bezpieczeństwa tych danych;
   3) traktowania obowiązków osób zatrudnionych przy przetwarzaniu danych osobowych jako należących do kategorii podstawowych obowiązków pracowniczych oraz stanowczego egzekwowania ich wykonania przez zatrudnione osoby;
   4) podejmowania w niezbędnym zakresie współpracy z instytucjami powołanymi do ochrony danych osobowych.
2. Kierownictwo Urzędu świadome jest zagrożeń związanych z przetwarzaniem przez Urząd danych osobowych na dużą skalę – w tym, w szczególności, z zagrożeń wynikających z dynamicznego rozwoju metod i technik przetwarzania tych danych w systemach informatycznych oraz sieciach telekomunikacyjnych. Jednocześnie zamierza doskonalić i rozwijać nowoczesne metody przetwarzania danych.
3. Kierownictwo Urzędu deklaruje, że będzie stale doskonaliło i rozwijało organizacyjne, techniczne oraz informatyczne środki ochrony danych osobowych przetwarzanych zarówno metodami tradycyjnymi jak i elektronicznymi tak, aby skutecznie zapobiegać zagrożeniom związanym z:
   1) infekcjami wirusów i koni trojańskich, które instalując się na komputerze mogą przyczynić się do nieautoryzowanego przejęcia zasobów komputera lokalnego lub danych przetwarzanych sieciowo;
   2) spamem, wprowadzającym nieład informacyjny mogącym stanowić potencjalne zagrożenie dla informatycznych zasobów Urzędu;
   3) dostępem do stron internetowych, które zaopatrzone są w skrypty pozwalające wykradać zasoby komputera;
   4) użytkowaniem oprogramowania do wymiany plików, mogącym służyć do łatwego skopiowania pliku poza Urzędem;
   5) możliwością niekontrolowanego kopiowania danych na zewnętrzne, przenośne nośniki;
   6) możliwością podsłuchiwania sieci, dzięki któremu można zdobyć hasła i skopiować objęte ochroną dane;
   7) lekceważeniem zasad ochrony danych polegającym na pozostawianiu pomieszczenia lub stanowiska pracy bez ich zabezpieczenia;
   8) brakiem świadomości niebezpieczeństwa dopuszczania osób postronnych do swojego stanowiska pracy;
   9) atakami z sieci mającymi na celu opóźnienie lub uniemożliwienie dostępu do danych;
   10) działaniami mającymi na celu zaburzenie integralności danych, w celu uniemożliwienia ich przetwarzania lub osiągnięcia korzyści;
   11) kradzieżą sprzętu lub nośników z danymi;
   12) przekazywaniem sprzętu z danymi do serwisu;
   13) innymi zagrożeniami mogącym wystąpić w przyszłości w związku z rozwojem technik i metod przetwarzania danych.
4. Dane osobowe w Urzędzie Miasta Tychy przetwarzane są z poszanowaniem obowiązujących w tym zakresie przepisów prawa, a w szczególności:
   1) przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz.926 z późn. zm.) oraz przepisów wykonawczych z nią związanych;

Data wygenerowania dokumentu: 2024-11-21 16:00:36

http://bip.umtychy.pl/index.php?action=PobierzPlik&id=37637

2) przepisów art.22^1 § 1 - 5 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 1998 r. Nr 21, poz.94 z późn. zm.) i przepisów wykonawczych z nią związanych;
3) oraz innych przepisów ustaw i rozporządzeń normujących przetwarzanie danych osobowych określonych kategorii.

5. Dane osobowe w Urzędzie Miasta Tychy przetwarzane są w celu realizacji statutowych celów.
6. Polityka bezpieczeństwa w zakresie ochrony danych osobowych w Urzędzie Miasta Tychy odnosi się do danych osobowych przetwarzanych w zbiorach danych:
   1) tradycyjnych, w szczególności w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych;
   2) w systemach informatycznych, także w przypadku przetwarzania danych poza zbiorem danych osobowych.
7. Kierownictwo Urzędu realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia, aby dane te były:
   1) przetwarzane zgodnie z prawem;
   2) zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami;
   3) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane;
   4) przechowywane w postaci umożliwiającej identyfikacje osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.
8. Pod szczególną ochroną pozostają wrażliwe dane osobowe wymienione w art. 27 ust.1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Przetwarzanie danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym dopuszczalne jest tylko w związku z realizacją celów statutowych i w granicach wynikających z przepisów art. 27 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.
9. Kierownictwo Urzędu realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych stosuje odpowiednie środki informatyczne, techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednio do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności:
   1) zabezpiecza dane przed ich udostępnieniem osobom nieupoważnionym;
   2) zabraniem przez osobę nieuprawnioną;
   3) przetwarzaniem z naruszeniem ustawy;
   4) zmianą, utratą, uszkodzeniem lub zniszczeniem.
10. Kierownictwo Urzędu realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych dąży do systematycznego unowocześniania stosowanych na jego terenie informatycznych, technicznych i organizacyjnych środków ochrony tych danych. W szczególności zapewnia aktualizacje informatycznych środków ochrony danych osobowych pozwalającą na zabezpieczenie przed wirusami, nieuprawnionym dostępem oraz innymi zagrożeniami danych, płynącymi z funkcjonowania systemu informatycznego oraz sieci telekomunikacyjnych.

§ 3

ZAKRES STOSOWANIA

Polityka dotyczy przetwarzania danych osobowych w Urzędzie Miasta Tychy i zawiera następujące dokumenty dotyczące rozpoznania procesów na danych osobowych oraz określające wprowadzone zabezpieczenia techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych:

1) wykaz pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe – obszar przetwarzania danych osobowych;
2) wykaz zbiorów danych osobowych i programów zastosowanych do przetwarzania danych;
3) opis struktury zbiorów, zawartości poszczególnych pól informacyjnych i powiązania pomiędzy nimi;
4) sposób przepływu danych pomiędzy poszczególnymi systemami;
5) środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Data wygenerowania dokumentu: 2024-11-21 16:00:36

http://bip.umtychy.pl/index.php?action=PobierzPlik&id=37637

§ 4

OBSZAR PRZETWARZANIA DANYCH OSOBOWYCH

1. Obszarem przetwarzania danych osobowych w Urzędzie Miasta Tychy są:
   1) pomieszczenia w budynku głównym Urzędu Miasta Tychy przy Al. Niepodległości 49;
   2) biura Wydziału Komunikacji i Miejskiego Zarządu Ulic i Mostów w budynku przy ul. Budowlanych 59;
   3) biura Straży Miejskiej w budynku przy ul. Budowlanych 67;
   4) biuro Pracowni Planowania Przestrzennego i Architektury w budynku przy ul. Piłsudskiego 12;
   5) biura Miejskiego Rzecznika Konsumentów, archiwum Zakładu Lecznictwa Ambulatoryjnego, biura Doradców Prezydenta oraz Powiatowego Inspektoratu Nadzoru Budowlanego w budynku przy ul. Grota Roweckiego 42;
   6) pomieszczenia Inkubatora Społecznej Przedsiębiorczości w budynku przy ul. Barona 30;
   7) pomieszczenia w budynku Teleinformatycznego Centrum Bezpieczeństwa – Centrum Zarządzania Kryzysowego przy al. Niepodległości 230;
   8) dyżurka Straży Miejskiej na dworcu PKP przy ul. Asnyka 1.
2. Przebywanie na obszarach przetwarzania danych osobowych odbywa się za zgodą Administratora Danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.
3. Osoby pracujące w obszarach przetwarzania danych zobowiązane są do stosowania „zasady czystego biurka” oraz „zasady czystego ekranu”.
4. W obszarach przetwarzania danych jest ścisły obowiązek zamykania wszelkich mebli, w których przechowywane są dane osobowe.

§ 5

WYKAZ ZBIORÓW DANYCH OSOBOWYCH I PROGRAMÓW ZASTOSOWANYCH DO PRZETWARZANIA DANYCH

1. Wykaz zbiorów danych przetwarzanych w Urzędzie Miasta Tychy i programów zastosowanych do przetwarzania danych prowadzi ASI.
2. Wykaz przetwarzanych zbiorów danych zawiera następujące informacje:
   1) liczba porządkowa;
   2) nazwa zbioru danych;
   3) lokalizacja zbioru (oznaczenie miejsca – określenie serwera);
   4) nazwy programów używanych do przetwarzania zbioru;
   5) lokalizacja programów;
   6) opis struktur, w których przechowywane są dane osobowe;
   7) symbol jednostki organizacyjnej wykorzystującej zbiór danych;
   8) typ zbioru;
   9) nr księgi rejestrowej;
   10) uwagi.

§ 6

OPIS STRUKTURY ZBIORÓW, ZAWARTOŚCI POSZCZEGÓLNYCH PÓL INFORMACYJNYCH I POWIĄZANIA POMIĘDZY NIMI

Opis struktury zbiorów, zawartości poszczególnych pól informacyjnych i powiązania pomiędzy nimi prowadzony jest przez ASI.

§ 7

SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY POSZCZEGÓLNYMI SYSTEMAMI

1. W ramach procesów przetwarzania danych dochodzi do przepływu danych pomiędzy różnymi systemami informatycznymi. Szczegółowy opis przepływu danych pomiędzy systemami prowadzi ASI.
2. Opis przepływu, o którym mowa w ust.1 aktualizuje ASI każdorazowo na pisemny wniosek kierownika jednostki organizacyjnej Urzędu odpowiedzialnego za dane przetwarzane w systemie

Data wygenerowania dokumentu: 2024-11-21 16:00:36

http://bip.umtychy.pl/index.php?action=PobierzPlik&id=37637

informatycznym (system docelowy), do którego powinny trafić dane z innego systemu informatycznego (system źródłowy).

3. W przypadku konieczności cyklicznego przepływu danych ze zbioru przetwarzanego w Urzędzie do zbioru przetwarzanego poza siecią lokalną Urzędu, wniosek przygotowany przez kierownika jednostki organizacyjnej Urzędu merytorycznie odpowiedzialnego za zbiór musi uzyskać akceptację ASI.
4. We wniosku, o którym mowa w ust.3 należy wskazać:
   1) nazwy systemów, pomiędzy którymi planowany jest przepływ danych;
   2) cel przepływu danych – zadanie ustawowe, do realizacji którego niezbędne są te dane;
   3) zakres przesyłanych danych;
   4) ogólne informacje na temat sposobu przesyłania danych;
   5) częstotliwość przepływu danych;
   6) jednostkę organizacyjną Urzędu odpowiedzialną za realizację przepływu danych.

§ 8

OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH NIEZBĘDNYCH DO ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH

1. Do elementów zabezpieczenia danych osobowych w Urzędzie Miasta Tychy zalicza się:
   1) stosowane metody ochrony pomieszczeń, w których przetwarzane są dane osobowe – zabezpieczenia fizyczne;
   2) zabezpieczenie wszystkich procesów przetwarzania danych (w szczególności dokumentów papierowych i informatycznych);
   3) nadzór Administratora Bezpieczeństwa Informacji nad wprowadzonymi zasadami i procedurami zabezpieczenia danych – zabezpieczenia organizacyjne;
   4) kompleksowe i całościowe traktowanie zabezpieczenia danych przez wszystkie podmioty i osoby biorące udział w przetwarzaniu danych osobowych.
2. W Urzędzie Miasta Tychy rozróżnia się następujące kategorie środków zabezpieczeń danych osobowych:
   1) zabezpieczenia fizyczne;
      a) wszystkie pomieszczenia są zamykane,
      b) obiekt jest strzeżony,
      c) alarmy antywłamaniowe jako dodatkowe zabezpieczenie,
      d) wyznaczone pomieszczenia dodatkowo są plombowane,
      e) wyznaczone pomieszczenia zabezpieczone są czujnikami ruchu oraz temperatury,
      f) system monitoringu wizyjnego,
      g) systemy podtrzymywania napięcia – zasilacze awaryjne, agregat prądotwórczy.
   2) zabezpieczenia procesów przetwarzania danych w dokumentacji papierowej;
      a) dokumenty papierowe przechowywane są w zamykanych szafach,
      b) stosowane są niszczarki dokumentów,
      c) zamontowane są czujniki przeciwpożarowe,
      d) we wszystkich pomieszczeniach Urzędu zamontowany został system DSO (dźwiękowy system ostrzegania),
   3) zabezpieczenia organizacyjne;
      a) został wyznaczony Administrator Bezpieczeństwa Informacji,
      b) dane osobowe są przetwarzane przez osoby posiadające upoważnienie,
      c) prowadzi się ewidencję osób upoważnionych do przetwarzania danych osobowych,
      d) pracownicy zobowiązani są do realizacji ustawy w zakresie ochrony danych osobowych w ramach wykonywanych obowiązków,
      e) przeprowadzane są okresowe szkolenia z zakresu ochrony danych osobowych.
3. W ramach zabezpieczenia danych osobowych ochronie podlegają:
   1) sprzęt komputerowy – serwery, komputery osobiste, drukarki i inne urządzenia zewnętrzne;
   2) infrastruktura sieciowa – urządzenia aktywne i pasywne, okablowanie;
   3) oprogramowanie, programy użytkowe, systemy operacyjne, narzędzia wspomagające i programy komunikacyjne;
   4) dane zapisane na dyskach oraz dane podlegające przetwarzaniu w systemie;
   5) identyfikatory w systemach informatycznych wraz z hasłami dostępu;
   6) pliki dziennych operacji systemowych i baz danych, kopie zapasowe i archiwa;
   7) dokumentacja – zawierająca dane systemu, opisująca jego zastosowanie, przetwarzane informacje, itp.;

Data wygenerowania dokumentu: 2024-11-21 16:00:36

http://bip.umtychy.pl/index.php?action=PobierzPlik&id=37637

8) wydruki;
9) związana z przetwarzaniem danych dokumentacja papierowa.

5. Administratorzy Systemów Informatycznych będą okresowo dokonywać inwentaryzacji systemów informatycznych i zbiorów danych w celu zapewnienia aktualności opisowi zawartemu w § 4 – 7 Polityki Bezpieczeństwa.
6. W systemach informatycznych obowiązują zabezpieczenia na poziomie:
   1) podstawowym;
   2) podwyższonym;
   3) wysokim.
7. Najważniejszymi zastosowanymi środkami zabezpieczenia danych w systemach informatycznych Urzędu Miasta Tychy są:
   1) serwery zlokalizowane w wydzielonym, klimatyzowanym pomieszczeniu niedostępnym dla osób postronnych. Pomieszczenie serwerowni zabezpieczone jest przed nieautoryzowanym wejściem osób nieupoważnionych;
   2) wydzielona sieć energetyczna, która wykorzystywana jest do podłączania urządzeń informatycznych (komputery, monitory, switche, itp.). Gniazda elektryczne tej sieci zabezpieczone są przed wpięciem innego urządzenia specjalną wkładką. Tak dedykowana sieć energetyczna zaopatrzona jest w urządzenia zasilania awaryjnego między innymi UPS podtrzymujący zasilanie całej sieci na czas potrzebny do bezpiecznego wyłączenia serwerów oraz agregat prądotwórczy, który automatycznie podtrzymuje napięcie w przypadku dłuższej przerwy w dostawie prądu;
   3) stacje robocze, na których zainstalowano oprogramowanie antywirusowe;
   4) stacje robocze są zabezpieczone przed nieautoryzowanym uruchomieniem indywidualnymi identyfikatorami i hasłami dostępowymi. W systemie operacyjnym zastosowano mechanizm wymuszający zmianę haseł, co 30 dni;
   5) dostęp do każdego systemu informatycznego, w którym przetwarzane są dane osobowe poprzedzony jest koniecznością autoryzacji poprzez wpisanie identyfikatora i hasła dostępu do systemu informatycznego. Poprzez hierarchizację uprawnień w systemie użytkownik otrzymuje dostęp tylko do funkcji programu, które są niezbędne do wykonywania jego obowiązków służbowych;
   6) okresowo sporządzane kopie bezpieczeństwa przechowywane w ognioodpornym sejfie znajdującym się w Wydziale Informatyki, a także w sejfie zlokalizowanym w Wydziale Komunikacji (ul. Budowlanych 59);
   7) w trakcie pracy na stacjach roboczych w przypadku dłuższej nieobecności stosuje się wygaszacze ekranu chronione hasłem lub mechanizm automatycznego blokowania komputera.
8. Dokumentem, który normuje procedury zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych jest instrukcja (Załącznik), która określa w szczególności:
   1) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności;
   2) stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;
   3) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;
   4) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;
   5) sposób, miejsce i okres przechowywania;
      a) elektronicznych nośników informacji zawierających dane osobowe,
      b) kopii zapasowych,
   6) sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego;
   7) sposób realizacji wymogów odnotowywania przez system informatyczny informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia;
   8) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych;
   9) zasady postępowania w sytuacji naruszenia ochrony danych osobowych;
   10) odpowiedzialność użytkownika.

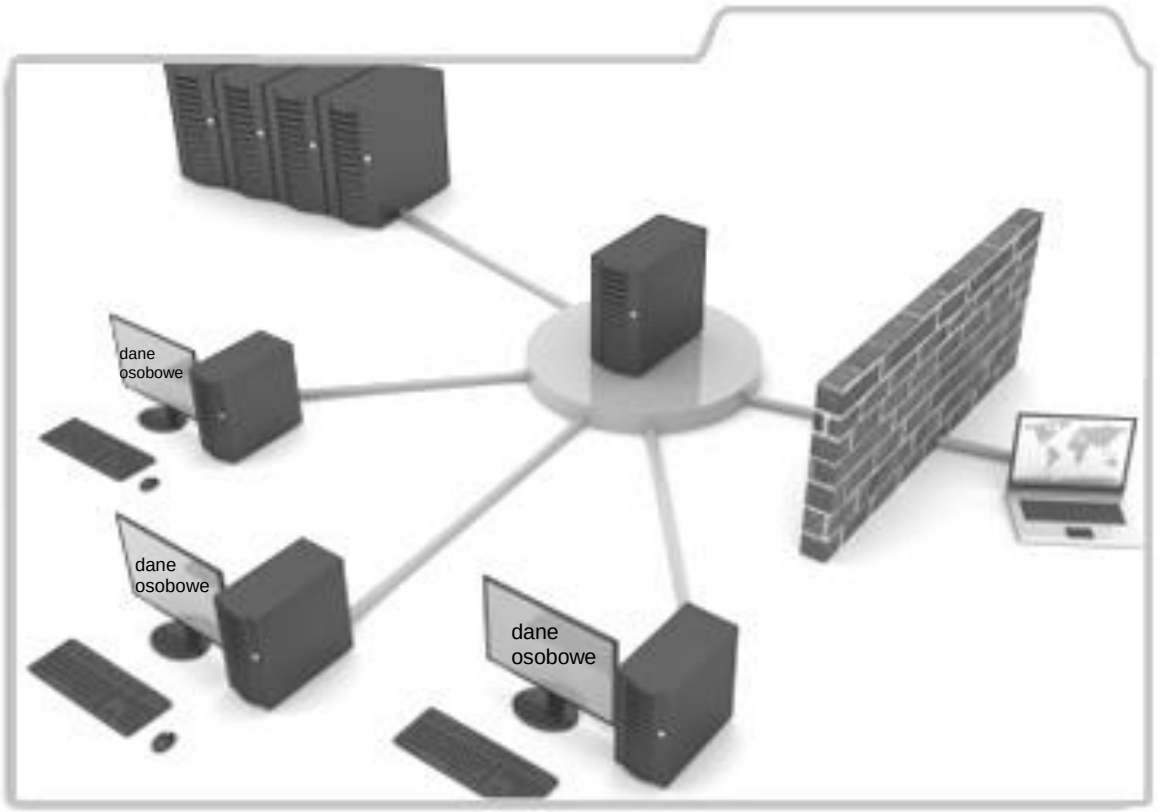
Data wygenerowania dokumentu: 2024-11-21 16:00:36

http://bip.umtychy.pl/index.php?action=PobierzPlik&id=37637

URZĄD MIASTA TYCHY

INSTRUKCJA

ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI, SŁUŻĄCYMI DO PRZETWARZANIA DANYCH OSOBOWYCH



Kwiecień 2012 rok

Data wygenerowania dokumentu: 2024-11-21 16:00:36

http://bip.umtychy.pl/index.php?action=PobierzPlik&id=37637

Zawartość Instrukcji

Załączniki do Instrukcji

Nr 1 Zasady użytkowania sprzętu komputerowego obowiązujące w Urzędzie Miasta Tychy.

Nr 2 Regulamin korzystania z sieci lokalnej i Internetu obowiązujący w Urzędzie Miasta Tychy.

Nr 3 Zasady tworzenia haseł obowiązujące w Urzędzie Miasta Tychy.

Nr 4 Wniosek o nadanie uprawnień do pracy w sieci lokalnej i systemach informatycznych użytkowanych w Urzędzie Miasta Tychy

Data wygenerowania dokumentu: 2024-11-21 16:00:36

http://bip.umtychy.pl/index.php?action=PobierzPlik&id=37637

Rozdział 1
Postanowienia ogólne – podstawa prawna, zakres instrukcji, definicje pojęć użytych w instrukcji

§ 1

„Instrukcja określająca sposób zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych", zwana dalej „Instrukcją", stanowi wykonanie obowiązku, o którym mowa w § 3 ust. 1 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).

§ 2

1. Instrukcja określa zasady zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Miasta Tychy, a w szczególności:
   1) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz osoby odpowiedzialne za te czynności;
   2) metody i środki uwierzytelnienia w systemie oraz procedury związane z ich zarządzaniem i użytkowaniem;
   3) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;
   4) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;
   5) sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych;
   6) środki ochrony systemu przed złośliwym oprogramowaniem, w tym wirusami komputerowymi,
   7) zasady i sposób odnotowywania w systemie informacji: komu, kiedy i w jakim zakresie dane osobowe ze zbioru zostały udostępnione;
   8) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych.
2. Celem utworzenia instrukcji jest podniesienie poziomu bezpieczeństwa systemów informatycznych, w których są prowadzone i przetwarzane dane oraz określenie odpowiedzialności użytkowników za prawidłowe działanie tych systemów i bezpieczeństwo przetwarzania w nim danych osobowych.

§ 3

Przez użyte w instrukcji określenia rozumie się:

1) **Administrator Bezpieczeństwa Informacji** (ABI) – Sekretarz Miasta, wyznaczony przez Prezydenta do nadzorowania przestrzegania zasad ochrony przy przetwarzaniu danych osobowych w Urzędzie Miasta Tychy,
2) **Administrator Danych Osobowych** (AD) – Prezydenta Miasta Tychy
3) **administrator systemu** – pracownik Wydziału Informatyki odpowiedzialny za administrację, konfigurację i konserwację systemu informatycznego. Osoba ta, po akceptacji ASI, nadaje użytkownikowi systemu uprawnienia niezbędne do pracy w systemie informatycznym,
4) **Administrator Systemu Informatycznego** (ASI) – Naczelnik Wydziału Informatyki (ASI_GWI) lub Naczelnik Wydziału Geodezji (ASI_GWG) odpowiedzialny za funkcjonowanie systemów oraz stosowanie technicznych i organizacyjnych środków ochrony przewidzianych w tych systemach,
5) **hasło** – ciągu znaków literowych, cyfrowych lub innych specjalnych, znanym jedynie osobie uprawnionej do pracy w systemie informatycznym, służącym do weryfikacji tożsamości w procesie uwierzytelnienia.
6) **identyfikator użytkownika** – ciąg znaków literowych, cyfrowych lub innych specjalnych, jednoznacznie identyfikującym osobę upoważnioną do przetwarzania danych w systemie informatycznym,
7) **jednostka organizacyjna** – każde samodzielne, wyodrębnione w strukturze Urzędu Miasta ogniwo organizacyjne, np.: wydział, urząd, samodzielne stanowisko itp.,
8) **nośnik informatyczny** – przedmiot fizyczny lub urządzenie umożliwiające zapisywanie i przenoszenie danych (np. dyskietka, twardy dysk, płyta CD, pamięć masowa flash).
9) **osoba trzecia** – każdą osoba nieupoważniona i przez to nieuprawniona do dostępu do danych osobowych zbiorów będących w posiadaniu AD. Osobą trzecią jest również osoba posiadająca upoważnienie wydane przez ABI i podejmująca czynności w zakresie przekraczającym ramy tego upoważnienia,

Data wygenerowania dokumentu: 2024-11-21 16:00:36

http://bip.umtychy.pl/index.php?action=PobierzPlik&id=37637

10) **serwis Wydziału Informatyki** – pracownicy Wydziału Informatyki przyjmujących i realizujących zgłoszone problemy dotyczące użytkowania sprzętu komputerowego i oprogramowania,
11) **sieć lokalna** – połączenie systemów informatycznych Urzędu wyłącznie dla własnych jego potrzeb przy wykorzystaniu urządzeń i sieci wewnętrznej Urzędu,
12) **sprzęt komputerowy** – komputer oraz urządzenia peryferyjne (monitor, drukarka, skaner itp.) wymagające do swojego działania połączenia z komputerem,
13) **Urząd** – Urząd Miasta Tychy,
14) **użytkownik systemu** – osoba upoważniona i uprawniona do przetwarzania danych osobowych w systemie. Użytkownikiem może być wyłącznie osoba posiadająca upoważnienie do przetwarzania danych osobowych nadane przez Administratora Bezpieczeństwa Informacji,

Rozdział 2
Procedury nadawania i zmiany uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz osoby odpowiedzialne za te czynności

§ 4

1. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych zapoznaje się z niniejszą Instrukcją oraz z jej załącznikami.
2. Stosowany w Urzędzie Miasta Tychy schemat uprawnień dostępu do sieci lokalnej i systemów informatycznych zakłada, iż użytkownicy uzyskują uprawnienia na z góry zdefiniowanym poziomie w zależności od zakresu obowiązków i powierzonych zadań do wykonania na danym stanowisku.
3. Niezbędne dla uzyskania uprawnień do systemu informatycznego w którym przetwarzane są dane osobowe jest posiadanie ważnego upoważnienia do przetwarzania danych osobowych.

§ 5

Procedura nadawania upoważnień do przetwarzania danych osobowych.

1) kierownik jednostki organizacyjnej przekazuje do Wydziału Organizacyjnego, Kadr i Szkolenia „wniosek o nadanie upoważnienia do przetwarzania danych osobowych” (Załącznik Nr 4) zawierający imię i nazwisko pracownika (stażysty lub praktykanta) ze wskazaniem czy będzie on przetwarzać dane osobowe w systemie informatycznym,
2) Wydział Organizacyjny, Kadr i Szkolenia przygotowane upoważnienie przekazuje do podpisu ABI,
3) ewidencję osób upoważnionych do przetwarzania danych osobowych prowadzi Wydział Organizacyjny, Kadr i Szkolenia,
4) upoważnienia tracą ważność z dniem ustania stosunku pracy, ukończenia stażu lub praktyki.

§ 6

1. Procedura nadawania uprawnień do sieci lokalnej i systemu informatycznego nadzorowanego przez kierownika jednostki organizacyjnej:
   1) przełożony użytkownika systemu (kierownik jednostki) występuje w formie elektronicznej lub pisemnej do Wydziału Informatyki z wnioskiem o nadanie uprawnień, w którym zamieszczone są następujące informacje;
      a) imię i nazwisko użytkownika systemu,
      b) nazwa udostępnianej użytkownikowi usługi lub systemu informatycznego,
      c) zakres dostępu,
      d) inne dyspozycje dla serwisu Wydziału Informatyki.
   2) ASI weryfikuje wniosek pod względem możliwości nadania uprawnienia w systemie,
   3) po pozytywnej weryfikacji ASI wydaje dyspozycję przyznania dostępu i nadania uprawnień w systemach informatycznych, bądź w przypadku systemów przestrzennych przekazuje wniosek do ASI_GWG.
2. Procedura nadawania uprawnień do systemu informatycznego, nad którym nadzór pełni inna jednostka organizacyjna:
   1) przełożony użytkownika systemu występuje w formie pisemnej do Wydziału Informatyki z wnioskiem o nadanie uprawnień do pracy w sieci lokalnej i systemach informatycznych (Załącznik Nr 5);
   2) przełożony użytkownika systemu uzyskuje zgodę kierownika jednostki organizacyjnej pełniącego nadzór nad systemem informatycznym którego dotyczy wniosek o nadanie uprawnień;
   3) ASI weryfikuje wniosek pod względem możliwości nadania uprawnienia w systemie;
   4) po pozytywnej weryfikacji ASI przyznaje dostęp i nadaje uprawnienia w w systemach informatycznych, bądź w przypadku systemów przestrzennych przekazuje wniosek do ASI_GWG.

Data wygenerowania dokumentu: 2024-11-21 16:00:36

http://bip.umtychy.pl/index.php?action=PobierzPlik&id=37637

3. W przypadku, gdy nadanie wymaganych uprawnień grozi naruszeniem standardów bezpieczeństwa bądź warunków licencjonowania systemów informatycznych, ASI informuje o tym fakcie przełożonego użytkownika i wstrzymuje proces nadawania uprawnień.

§ 7

Pracownik Wydziału Informatyki lub Wydziału Geodezji na podstawie otrzymanego od ASI zadania:
1) rejestruje użytkownika w systemie i nadaje mu lub modyfikuje wymagane uprawnienia,
2) instaluje na stacji roboczej użytkownika systemu niezbędne składniki oraz informuje użytkownika o fakcie nadania/modyfikacji uprawnień. W przypadku nadania bądź odebrania uprawnień rejestruje nadane uprawnienie w ewidencji uprawnień.

§ 8

1. Użytkownik systemu, po otrzymaniu informacji o nadaniu uprawnień:
   1) loguje się do systemu informatycznego w celu sprawdzenia poprawności konta i uprawnień;
   2) przy pierwszym logowaniu się do systemu informatycznego, użytkownik musi zmienić nadane mu hasło.
2. Powyższy schemat nadania uprawnień dostępu do usług sieciowych i systemów informatycznych należy stosować również w przypadku wymaganej zmiany w istniejących uprawnieniach użytkownika systemu.
3. Powyższe zasady nadawania uprawnień dostępu do usług sieciowych i systemów informatycznych eksploatowanych w Urzędzie Miasta Tychy obowiązują wszystkich pracowników.
4. Ewidencję osób uprawnionych do pracy w systemie informatycznym prowadzą Wydział Informatyki i Wydział Geodezji.

§ 9

1. Ewidencja osób upoważnionych do przetwarzania danych osobowych oraz ewidencja uprawnionych do pracy w systemie informatycznym prowadzona jest w jednym wspólnym systemie.
2. W przypadku utraty ważności upoważnienia, ASI blokuje uprawnienia w systemie informatycznym.

Rozdział 3
Stosowane metody i środki uwierzytelnienia w systemie oraz procedury związane z ich zarządzaniem i użytkowaniem

§ 10

Naczelną zasadą bezpieczeństwa systemów informatycznych i sieci lokalnej jest ochrona informacji przed nieuprawnionym dostępem, ujawnieniem, przypadkowym lub nieautoryzowanym zniszczeniem lub modyfikacją danych. Stosowanie zasad uwierzytelniania użytkowników systemów i sieci ma bezpośredni wpływ na zachowanie poufności, rozliczalności oraz integralności danych.

§ 11

1. W systemie informatycznym użytkowanym na stacji roboczej pracującej poza siecią lokalną stosuje się uwierzytelnianie dwustopniowe na poziomie:
   1) dostępu do stacji roboczej;
   2) dostępu do systemu informatycznego lub usługi na stacji roboczej.
2. W przypadku stacji roboczych włączonych do sieci lokalnej, uwierzytelnianie zachodzi na dwóch poziomach:
   1) dostępu do sieci lokalnej;
   2) dostępu do systemu informatycznego lub usługi na serwerze.
3. Do uwierzytelnienia użytkownika systemu na wszystkich poziomach stosuje się identyfikatory, hasła lub karty mikroprocesorowe.
   1) stosowanie unikalnych identyfikatorów użytkownika zapewnia bezpieczeństwo i realizuje zasady rozliczalności w systemach informatycznych i sieci lokalnej;
   2) zasada ta ma na celu przypisanie w sposób jednoznaczny wszelkich działań w systemie konkretnemu użytkownikowi systemu. Nie dopuszcza się, aby użytkownik systemu korzystał z kont ogólnych typu gość, a także z konta innego użytkownika systemu,
4. W Urzędzie Miasta Tychy stosuje się poziom bezpieczeństwa przetwarzania danych zależny od klasyfikacji danych w systemie informatycznym. W związku z powyższym, obowiązujące są trzy poziomy bezpieczeństwa:
   1) poziom podstawowy – dla systemów informatycznych, w których nie są przetwarzane dane osobowe wrażliwe, czyli takie, które nie ujawniają pochodzenia rasowego lub etnicznego,

Data wygenerowania dokumentu: 2024-11-21 16:00:36

http://bip.umtychy.pl/index.php?action=PobierzPlik&id=37637

poglądów politycznych, przekonań religijnych lub filozoficznych, przynależności wyznaniowej, partyjnej lub związkowej, jak również informacji o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz informacji dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także informacji o innych orzeczeniach wydanych w postępowaniu sądowym lub administracyjnym, oraz żadne urządzenie systemu informatycznego służące do przetwarzania danych osobowych nie jest połączone z siecią publiczną. W takim przypadku hasło musi się składać z co najmniej 6-ciu znaków;
2) poziom podwyższony – dla systemów informatycznych, w których są przetwarzane dane osobowe wrażliwe oraz żadne urządzenie systemu informatycznego służące do przetwarzania danych osobowych nie jest połączone z siecią publiczną. W tym przypadku hasło musi składać się z co najmniej 8 znaków, i musi zawierać małe i wielkie litery oraz cyfry lub znaki specjalne;
3) poziom wysoki – dla systemów informatycznych, w których są przetwarzane dane osobowe wrażliwe oraz co najmniej jedno urządzenie systemu informatycznego służące do przetwarzania danych osobowych jest połączone z siecią publiczną. W tym przypadku muszą być stosowane środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelniania.

§ 12

1. W przypadku weryfikacji tożsamości użytkownika przy użyciu karty mikroprocesorowej użytkownik jest zobowiązany do:
   1) umieszczenia karty mikroprocesorowej w czytniku kart;
   2) wpisania indywidualnego kodu PIN.
2. Hasło dostępu do systemu informatycznego i sieci lokalnej musi składać się z minimum 8 znaków oraz zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.
3. W Urzędzie Miasta Tychy hasła są konstruowane zgodnie z zasadami opisanymi w Załączniku Nr 3 do niniejszej Instrukcji. Zobowiązuje się wszystkich użytkowników do przestrzegania opisanych tam wytycznych.
4. Zabrania się ujawniania haseł jakimkolwiek osobom trzecim, lub takiego z nimi postępowania, które umożliwia lub ułatwia dostęp do haseł osobom trzecim. Punkt ten obowiązuje również w odniesieniu do haseł, których ważność wygasła.
5. System automatycznie powinien wymuszać zmianę hasła nie rzadziej, niż jeden raz w miesiącu. Hasło musi być zmienione przez użytkownika niezwłocznie w przypadku podejrzenia lub stwierdzenia jego ujawnienia.
6. W przypadku gdy system nie posiada funkcji automatycznego wymuszenia zmiany hasła, bądź nie ma wbudowanych mechanizmów kontroli dostępu, wówczas należy niezwłocznie rozbudować taki system o te mechanizmy, a do czasu wdrożenia takich mechanizmów należy zaimplementować ograniczenia dostępu na poziomie systemu operacyjnego bądź sieci lokalnej, lub wprowadzić odrębne ograniczenia proceduralne. Sytuacja taka nie zwalnia użytkownika od obowiązku cyklicznej zmiany hasła dostępu.
7. Dopuszcza się wykorzystanie aplikacji dedykowanych bądź innych metod bezpiecznego zapamiętywania haseł po uprzedniej ich akceptacji przez ASI.

§ 13

1. Procedura zarządzania środkami uwierzytelniania:
   1) administrator nadaje identyfikator i hasło dostępu do systemu informatycznego lub sieci lokalnej dla nowego użytkownika albo zmienia hasło użytkownikowi, który nie ma możliwości uwierzytelnienia;
   2) po nadaniu hasła przez administratora użytkownik systemu informatycznego lub sieci lokalnej niezwłocznie ustala swoje, znane tylko jemu hasło. System automatycznie wymusza na użytkowniku zmianę nadanego przez administratora hasła przy pierwszym logowaniu;
   3) użytkownik systemu w dowolnym momencie może zmienić swoje hasło dostępu do systemu informatycznego lub sieci lokalnej;
   4) obowiązuje bezwzględny zakaz notowania w jakiejkolwiek formie obecnych oraz wygasłych haseł dostępu;
   5) hasła użytkowników systemów informatycznych i sieci lokalnej nie są przechowywane. W przypadku zagubienia hasła użytkownik zwraca się do administratora o nadanie nowego hasła;
   6) hasła użytkowników posiadających uprawnienia administratorów przechowywane są w sejfie Wydziału Informatyki w zamkniętej kopercie. O awaryjnym ich użyciu decyduje każdorazowo

Data wygenerowania dokumentu: 2024-11-21 16:00:36

http://bip.umtychy.pl/index.php?action=PobierzPlik&id=37637

ASI. Po awaryjnym użyciu hasła, musi ono zostać jak najszybciej zmienione przez właściwego administratora.

2. Szczegółowe zasady związane z zarządzaniem uprawnieniami do systemów informatycznych i sieci lokalnej Urzędu Miasta Tychy opisane są w załączniku 2 do niniejszej Instrukcji.
3. Podstawą czasowego lub stałego zablokowania konta użytkownika sieci i jego uprawnień dodatkowych jest informacja przekazana do Wydziału Informatyki przez pracownika Wydziału Organizacyjnego, Kadr i Szkolenia dotycząca jego zwolnienia lub nieobecności dłuższej niż 30 dni.

Rozdział 4
Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu

§ 14

1. Przed przystąpieniem do pracy w systemie informatycznym użytkownik zobowiązany jest sprawdzić urządzenie komputerowe i stanowisko pracy ze zwróceniem uwagi, czy nie zaszły okoliczności wskazujące na naruszenie ochrony danych osobowych. W przypadku naruszenia ochrony danych osobowych użytkownik niezwłocznie powiadamia ABI za pośrednictwem ASI.
2. Użytkownik rozpoczyna pracę w systemie informatycznym od następujących czynności:
   1) uruchomienie komputera wchodzącego w skład systemu informatycznego, podłączonego fizycznie do sieci lokalnej;
   2) uwierzytelnienie się („zalogowanie") za pomocą własnego identyfikatora użytkownika i hasła. 5-krotne wprowadzenie błędnego hasła powoduje czasowe zablokowanie identyfikatora i hasło dostępu. W celu wcześniejszego odblokowania identyfikatora, użytkownik winien skontaktować się z administratorem;
   3) uruchomienie wybranego systemu informatycznego bądź aplikacji i uzyskanie dostępu do tej aplikacji poprzez podanie identyfikatora użytkownika i hasła, lub weryfikacji tożsamości przy użyciu karty mikroprocesorowej.
3. Po zalogowaniu się w systemie użytkownik ma obowiązek ocenić pracę systemu i stan zbioru danych a w przypadku jakichkolwiek wątpliwości zgłosić ten fakt przełożonego oraz ASI.
4. Użytkownicy zobowiązani są do natychmiastowego stosowania się do komunikatów pojawiających się na monitorach.
5. W trakcie pracy użytkownik powinien stosować przedsięwzięcia zapewniające bezpieczeństwo przetwarzania danych osobowych w systemie, a w szczególności:
   1) ustawić ekrany monitorów w sposób uniemożliwiający podgląd osobom nieupoważnionym,
   2) dopilnować aby w pomieszczeniach, stanowiących obszar przetwarzania danych nie przebywały jakiekolwiek osoby trzecie, a jeśli przebywają to tylko za zgodą przełożonych i w obecności osób uprawnionych.
6. W przypadku konieczności zawieszenia pracy i opuszczenia stanowiska komputerowego, należy dopilnować, aby na ekranie nie były wyświetlane informacje lub dane, poprzez zablokowanie komputera. Dopuszczalne jest zaktywowanie wygaszacza ekranu zabezpieczonego hasłem, którego wpisanie daje możliwość wznowienia pracy na stacji roboczej. W przypadku dłuższego opuszczenia stanowiska pracy, użytkownik zobowiązany jest do zamknięcie aplikacji i wylogowania się z systemu informatycznego.
7. Zakończenie pracy użytkownika w systemie następuje po wylogowaniu się z systemu oraz wyłączeniu wszystkich urządzeń. Po zakończeniu pracy użytkownik zabezpiecza swoje stanowisko pracy, a w szczególności nośniki informatyczne, dokumenty i wydruki zawierające dane osobowe, przed dostępem osób nieupoważnionych.
8. W przypadku wystąpienia nieprawidłowości w mechanizmie uwierzytelnienia w systemie użytkownik niezwłocznie powiadamia o nich administratora.

§ 15

1. Praca użytkownika w systemie komputerowym po godzinach pracy Urzędu wymaga zgody przełożonego i powinna być wcześniej uzgodniona z ASI.
2. Użytkownik w pełnym zakresie odpowiada za powierzony mu sprzęt komputerowy i wykonywane czynności aż do momentu rozliczenia ze sprzętu komputerowego.

Data wygenerowania dokumentu: 2024-11-21 16:00:36

http://bip.umtychy.pl/index.php?action=PobierzPlik&id=37637

Rozdział 5
Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

§ 16

1. W celu zoptymalizowania procesu tworzenia kopii zapasowych oraz zapewnienia optymalnego poziomu ochrony danych gromadzonych w systemach informatycznych w Urzędzie Miasta Tychy przyjęto zasadę przetwarzania informacji zawartych w bazach danych w oparciu o architekturę klient – serwer. Wynika stąd praktyka przetwarzania danych w bazach danych na dedykowanych dla systemów informatycznych serwerach.
2. Jeśli stosowane dotychczas rozwiązania nie są zgodne z architekturą klient – serwer, to należy zapewnić możliwość przechowywania gromadzonych za ich pomocą danych na serwerze plików znajdującym się w sieci lokalnej (macierzy dyskowej).
3. Wszelkie informacje (w tym dane osobowe) przetwarzane przy pomocy uruchamianych na poszczególnych stanowiskach aplikacjach bazodanowych są zapisywane bezpośrednio na serwerach. Zabronione jest zapisywanie i przechowywanie informacji zawierających dane osobowe na dyskach lokalnych stacji roboczych.
4. Tworzenie kopii bezpieczeństwa baz danych i zawartości serwerów oraz ich bezpieczne przechowywanie nadzoruje ASI lub osoba upoważniona do zastępstwa.
5. Za dane przechowywane na dyskach lokalnych komputerów działających w sieci lokalnej odpowiadają użytkownicy stacji roboczych.
6. W szczególnych przypadkach, za zgodą ASI, aplikacje oraz dane, w tym dane osobowe, mogą być przechowywane lokalnie na stanowiskach komputerowych niepodłączonych do sieci lokalnej Urzędu. W takich przypadkach obowiązek wykonania kopii bezpieczeństwa bazy danych i aplikacji oraz ich bezpiecznego przechowywania zgodnie z zasadami opisanymi w niniejszej Instrukcji, spoczywa bezpośrednio na użytkowniku danej aplikacji.
7. Kopiowanie baz danych na nośniki informacji przez osoby nieupoważnione, robienie wydruków oraz wykorzystywanie danych w celach innych niż wynikających z nałożonych na użytkowników obowiązków służbowych jest zabronione.

§ 17

1. Za tworzenie kopii bezpieczeństwa baz danych i zawartości serwera oraz okresową weryfikację ich poprawności odpowiada administrator systemu informatycznego.
2. Kopie zapasowe baz danych oraz aplikacji bazodanowych zlokalizowanych na serwerach wykonywane są:
   1) w cyklu dobowym (w godzinach nocnych);
   2) w cyklu tygodniowym;
   3) w cyklu rocznym.
3. Zasady tworzenia kopii zapasowych opisuje odrębna procedura tworzenia kopii zapasowych, za której opracowanie odpowiedzialny jest ASI.
4. Zasady przechowywania i weryfikacji kopii zapasowych.
   1) kopie zapasowe baz danych oraz aplikacji bazodanowych są przechowywane w ogniotrwałym sejfie zlokalizowanym w wyznaczonym pomieszczeniu Wydziału Informatyki oraz w kasetce metalowej w Wydziału Komunikacji;
   2) dostęp do sejfu mają tylko upoważnieni pracownicy, tj. ASI_GWI oraz administratorzy systemów informatycznych;
   3) okresowe sprawdzenie poprawności utworzenia kopii zapasowej wykonuje się nie rzadziej niż raz na miesiąc.
5. Sporządzający kopie zapasowe zobowiązani są do okresowego ich sprawdzania pod kątem dalszej przydatności. O usunięciu danych nieprzydatnych decyduje ASI.

Rozdział 6
Sposób, miejsce i okres przechowywania nośników danych oraz zasady ich przekazywania

§ 18

1. Elektroniczne nośniki informacji zawierające dane osobowe:
   1) wymienne elektroniczne nośniki danych powinny być oznaczone i używane zgodnie z Instrukcją kancelaryjną;
   2) wymienne elektroniczne nośniki informacji są przechowywane w pokojach budynków stanowiących obszar przetwarzania danych osobowych, określony w Wykazie przetwarzanych zbiorów danych osobowych w Urzędzie Miasta Tychy;

Data wygenerowania dokumentu: 2024-11-21 16:00:36

http://bip.umtychy.pl/index.php?action=PobierzPlik&id=37637

3) po zakończeniu pracy przez użytkowników systemu, wymienne elektroniczne nośniki informacji są przechowywane w zamykanych na klucze szafach biurowych lub kasetkach;
4) dane osobowe w postaci elektronicznej należy usunąć z nośnika informacji w sposób uniemożliwiający ich ponowne odtworzenie, po utracie ich przydatności dla użytkownika;
5) jeżeli z przyczyn technicznych danych nie można usunąć z nośnika w sposób trwały, należy nośnik zniszczyć fizycznie w sposób uniemożliwiający odczyt danych;
6) użytkownik komputera przenośnego obowiązany jest do zachowania szczególnej ostrożności podczas jego transportu i przechowywania poza obszarem Urzędu, w celu zapobieżenia dostępowi do danych na nim zgromadzonych osobom niepowołanym.

2. Zasady przekazywania nośników danych:
1) elektroniczne nośniki informacji zawierające dane osobowe można przekazywać tylko podmiotom lub osobom uprawnionym na podstawie przepisów prawa, za zgodą osoby do tego upoważnionej przez AD;
2) dane osobowe na każdym nośniku zewnętrznym powinny być zabezpieczone przed odczytem (minimum hasłem);
3) dane osobowe przenoszone za pomocą zewnętrznych nośników informacji powinny być z nich trwale usunięte po poprawnym ich przeniesieniu na docelowy sprzęt komputerowy i do docelowej bazy danych;
4) przekazanie i niszczenie elektronicznych nośników informacji zawierających dane osobowe, odbywa się na podstawie protokołu podpisanego przez osoby upoważnione.

3. Zasady postępowania z wydrukami:
1) wydruki i dokumenty papierowe zawierające dane osobowe przechowywane są wyłącznie w zamykanych na klucz szafach;
2) osoba zatrudniona przy przetwarzaniu danych osobowych sporządzająca wydruk zawierający dane osobowe ma obowiązek na bieżąco sprawdzać przydatność wydruku w wykonywanej pracy, a w przypadku jego nieprzydatności – niezwłocznie wydruk zniszczyć.

4. Dane wejściowe do systemu. Dane osobowe zapisane w formie papierowej innej niż wydruki z systemów (pisma, ankiety itp.) są przechowywane na podobnych zasadach jak wydruki.

Rozdział 7
Sposób zabezpieczenia systemu informatycznego przed złośliwym oprogramowaniem, w tym wirusami komputerowymi

§ 19

1. Ochrona antywirusowa:
1) za ochronę antywirusową odpowiada ASI;
2) czynności związane z ochroną antywirusową systemu informatycznego wykonują pracownicy Wydziału Informatyki, wykorzystując w trakcie pracy systemu informatycznego moduł programu antywirusowego w aktualnej wersji, sprawdzający na bieżąco zasoby systemu informatycznego. Moduł programu antywirusowego działający „w tle” należy zainstalować na każdym komputerze działającym w sieci lokalnej Urzędu;
3) ochroną antywirusową objęto następujące punkty infrastruktury Urzędu;
a. punkt styku sieci rozległej z siecią lokalną,
b. stacje robocze użytkowników,
c. serwer pocztowy urzędu,
4) program antywirusowy zainstalowany na stacjach roboczych jest zasilany automatycznie nowymi definicjami wirusów nie rzadziej niż raz na tydzień;
5) użytkownik systemu na stanowisku komputerowym, używający w trakcie wykonywanej pracy informatycznych nośników danych (płytka CD, dyskietka, pendrive i inne) jest odpowiedzialny za sprawdzenie tych nośników pod kątem możliwości występowania wirusów;
6) użytkownik ma obowiązek zgłosić pracownikom wydziału informatyki każdy fakt, który może świadczyć o obecności w systemie szkodliwego oprogramowania;
7) należy zachować szczególną ostrożność na stacjach roboczych, z których możliwe jest korzystanie z sieci Internet. Aby ograniczyć ryzyko przedostania się szkodliwego oprogramowania do systemów informatycznych nie należy: instalować dodatkowych programów narzędziowych i dodatków do przeglądarek internetowych, unikać otwierania stron o nieznanym pochodzeniu i podejrzanej treści, otwierać załączników pocztowych od nieznanych adresatów;
8) oprogramowanie należy skonfigurować w sposób wymuszający automatyczne usuwanie wirusów, zaś w przypadku gdy ich usunięcie jest niemożliwe – obejmowanie ich kwarantanną. Wskazane jest okresowe skanowanie wszystkich dysków lokalnych, a także sporządzanie

Data wygenerowania dokumentu: 2024-11-21 16:00:36

http://bip.umtychy.pl/index.php?action=PobierzPlik&id=37637

raportów oraz powiadamianie osoby odpowiedzialnej o wykrytych wirusach, robakach czy innym szkodliwym oprogramowaniu.

§ 20

1. Ochrona przed nieautoryzowanym dostępem do sieci lokalnej:
   1) ASI jest odpowiedzialny za monitorowanie sieci lokalnej w celu wykrycia prób nieautoryzowanego dostępu, skanowania sieci itp.;
   2) ASI jest odpowiedzialny za zapewnienie bezpieczeństwa wymiany danych na styku;
      a) sieci lokalnej i sieci rozległej,
      b) stanowiska komputerowego użytkownika systemu i pozostałych urządzeń wchodzących w skład sieci lokalnej.
   3) ASI jest zobowiązany do utrzymywania stałej aktywności zainstalowanego specjalistycznego oprogramowania monitorującego wymianę danych oraz do jego aktualizacji.
2. Ochrona przed awarią zasilania:
   1) system, w którym przetwarzane są dane osobowe powinien posiadać mechanizmy pozwalające zabezpieczyć je przed ich utratą lub nieautoryzowaną zmianą spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej;
   2) dane osobowe przetwarzane w systemie chroni się stosując filtry zabezpieczające przed skutkami spadku napięcia oraz urządzenia podtrzymujące zasilanie do momentu poprawnego zapisania danych i wylogowania się użytkownika z systemu;
   3) dane osobowe przetwarzane z wykorzystaniem serwera w wewnętrznych sieciach teleinformatycznych zabezpiecza się przed zanikiem napięcia wykorzystując centralny UPS i generator prądu;
   4) stacje robocze oraz inne urządzenia pracujące w sieci lokalnej należy zasilać z gniazdek wydzielonej sieci elektrycznej, które w Urzędzie Miasta Tychy oznaczone są kolorem czerwonym. Zabrania się wykorzystywania opisanych gniazdek do zasilania urządzeń innego zastosowania.

Rozdział 8
Zasady i sposób odnotowywania w systemie informacji, komu, kiedy i w jakim zakresie dane osobowe ze zbioru zostały udostępnione

§ 21

1. W systemach informatycznych odnotowywane są informacje o odbiorcach.
2. Odbiorcą danych jest każdy, komu udostępnia się dane osobowe, z wyłączeniem:
   1) osoby, której dane dotyczą;
   2) osoby użytkownika systemu lub innej osoby upoważnionej do przetwarzania danych osobowych w Urzędzie;
   3) podmiotu, któremu powierzono przetwarzanie danych;
   4) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.
3. Odnotowanie obejmuje informacje o:
   1) nazwie jednostki organizacyjnej lub imieniu i nazwisku osoby, której udostępniono dane;
   2) zakresie udostępnianych danych;
   3) dacie udostępnienia,
4. Obowiązek odnotowania ww. informacji spoczywa na użytkowniku systemu, w tym celu wypełnia on odpowiednie pole w bazie danych osobowych, arkuszu kalkulacyjnym lub tabele w edytorze tekstu.
5. Odnotowanie informacji powinno nastąpić niezwłocznie po udostępnieniu danych.
6. Udostępnienie danych osobowych może nastąpić wyłącznie na pisemną prośbę odbiorcy danych.
7. Nadzór nad prawidłowością odnotowywania w systemie ww. informacji sprawuje kierownik jednostki organizacyjnej, który merytorycznie odpowiada za funkcjonowanie danego systemu informatycznego.

Rozdział 9
Procedury wykonywania przeglądów i konserwacji sprzętu, systemów oraz nośników informacji służących do przetwarzania danych osobowych

§ 22

1. Dla zachowania ciągłości pracy i bezpieczeństwa danych przeprowadza się przegląd i konserwację infrastruktury sprzętowej, na której eksploatowane są systemy informatyczne.

Data wygenerowania dokumentu: 2024-11-21 16:00:36

http://bip.umtychy.pl/index.php?action=PobierzPlik&id=37637

2. Przeglądy i konserwacja urządzeń wchodzących w skład infrastruktury sprzętowej:
   1) przeglądy i konserwacja urządzeń wchodzących w sieci lokalnej powinny być wykonywane w terminach określonych przez producenta sprzętu;
   2) jeśli producent nie przewidział dla danego urządzenia potrzeby dokonywania przeglądów eksploatacyjnych, lub też nie określił ich częstotliwości, to o dokonaniu przeglądu oraz sposobie jego przeprowadzenia decyduje ASI;
   3) przegląd i konserwacja urządzeń może być wykonana na żądanie ABI, a w przypadku stacji roboczych – na prośbę użytkownika systemu lub jego przełożonego;
   4) nieprawidłowości ujawnione w trakcie przeglądów bądź konserwacji, powinny być niezwłocznie usunięte, a ich przyczyny przeanalizowane.

§ 23

1. Celem przeglądu i konserwacji systemów informatycznych jest zapewnienie bezawaryjnej pracy Urzędu i przeciwdziałanie utracie danych osobowych przetwarzanych przez użytkowników systemu.
2. Przegląd i konserwacja systemów informatycznych wykonywane są w przypadku:
   1) zmiany wersji oprogramowania systemu informatycznego;
   2) zmiany wersji oprogramowania lub wymiany elementów składowych systemu;
   3) zmiany systemu operacyjnego platformy sprzętowej, na której eksploatowany jest system informatyczny;
   4) zgłoszenia przez użytkowników systemu nieprawidłowości w ich działaniu;
   5) po awarii systemu informatycznego lub serwera, na którym umieszczone były zbiory danych przetwarzanych przez system.
3. Przeglądu i konserwacji systemów informatycznych dokonuje administrator systemu lub pracownicy firm zewnętrznych na podstawie aktualnych umów nadzoru autorskiego.
4. W przypadku zlecenia wykonywania czynności, o których mowa wyżej, podmiotowi zewnętrznemu, wszelkie prace powinny odbywać się pod nadzorem administratora systemu.
5. Przed wykonaniem przeglądu i konserwacji administrator systemu sporządza odpowiednie kopie bezpieczeństwa.
6. Przed wdrożeniem wymaganych przez użytkownika zmian w systemie informatycznym, należy dokonać sprawdzenia poprawności działania zmodyfikowanego systemu w warunkach testowych na testowej bazie danych.
7. Po dokonaniu zmian w systemie informatycznym sprawdzenie jego funkcjonowania powinno obejmować:
   1) poprawność logowania się do systemu, w zależności od posiadanych uprawnień;
   2) poprawność działania wszystkich elementów oraz funkcjonalności aplikacji.
8. Bieżące przeglądanie danych osobowych wykonują osoby zatrudnione przy ich przetwarzaniu.

§ 24

1. Zasady postępowania z nośnikami informacji:
   1) za konserwację nośników, na których przechowywane są kopie bezpieczeństwa baz danych i zawartości serwerów, odpowiada ASI i administratorzy systemów informatycznych,
   2) za konserwację nośników zawierających dane użytkowników stacji roboczych odpowiadają użytkownicy,
   3) urządzenia, dyski lub inne informatyczne nośniki informacji, przeznaczone do napraw w firmach zewnętrznych pozbawia się wcześniej zapisu danych,
   4) w przypadku, gdy zapis danych nie może zostać usunięty, dopuszczalne jest przeprowadzenie naprawy nośnika informacji pod nadzorem ASI, bądź, w przypadku konieczności naprawy urządzenia w specjalistycznym laboratorium, przekazanie nośnika firmie zewnętrznej po podpisaniu stosownych dokumentów zawierających klauzulę poufności,
   5) Urządzenia, dyski lub inne informatyczne nośniki informacji posiadające zapis danych osobowych, które przeznaczone są do likwidacji, pozbawia się zapisu lub uszkadza mechanicznie w sposób uniemożliwiający ich odczytanie.

Rozdział 10
Zasady postępowania w sytuacji naruszenia ochrony danych osobowych

§ 25

1. W przypadku naruszenia danych osobowych w systemach informatycznych użytkownik bezzwłocznie zgłasza o tym przełożonemu, ABI lub ASI.

Data wygenerowania dokumentu: 2024-11-21 16:00:36

http://bip.umtychy.pl/index.php?action=PobierzPlik&id=37637

2. ABI przy pomocy ASI oraz przełożonego użytkownika niezwłocznie dokonuje czynności mających na celu sprawdzenie zasadności podejrzenia i dokumentuje wykonane czynności w notatce służbowej, która zawiera: datę, opis stanu faktycznego, stopień naruszenia danych (ewentualne uszkodzenie sprzętu, itp.) i (w miarę możliwości) sposób usunięcia naruszenia. Notatkę tę podpisuje użytkownik, przełożony użytkownika, ABI oraz ASI.
3. ABI powiadamia Administratora Danych i ewentualnie inne organy o fakcie naruszenia danych osobowych i, o ile jest to możliwe, podejmuje kroki przeciwdziałające rozpowszechnieniu chronionych danych. Podejmuje także działania mające na celu zapobieganie podobnym naruszeniom w przyszłości.
4. W przypadku gdy dane zostały zniszczone (uszkodzone) ASI podejmuje następujące czynności: dokonuje uzupełnienia, uaktualnienia lub odtworzenia danych osobowych z nośników archiwalnych i w zależności od konkretnego przypadku dokonuje innych czynności niezbędnych do zabezpieczenia systemu tj. zmienia identyfikator użytkownika i hasło.
5. W sytuacji permanentnego naruszania ochrony danych osobowych, gdy pomimo działań ABI podjętych wskutek naruszenia ochrony informacji, stan się nie poprawia i następują ponownie przypadki naruszenia tej ochrony, ABI powiadamia Administratora Danych i Generalnego Inspektora Ochrony Danych Osobowych, ewentualnie inne organy, a ASI zabezpiecza kopie archiwalne danych oraz wyrejestrowuje wszystkich użytkowników.
6. W przypadku stwierdzenia naruszenia danych osobowych w pozostałych zbiorach np. skorowidzach, wykazach mogą wskazywać między innymi uszkodzenia dokumentów, ślady włamania itp. użytkownik bezzwłocznie zgłasza ten fakt przełożonemu oraz ABI, który: powiadamia Administratora Danych, ewentualnie inne organy, dokonuje oględzin i zabezpieczenia miejsca zdarzenia, spisuje notatkę służbową, podejmuje działania niezbędne do odtworzenia treści danych i podejmuje działania mające na celu zapobieganie podobnym naruszeniom w przyszłości.

Rozdział 11
Postanowienia końcowe

§ 26

1. W sprawach nie uregulowanych niniejszą Instrukcją zastosowanie znajdują:
   1) Norma PN-I-13335-1 „Technika informatyczna. Wytyczne do zarządzania bezpieczeństwem systemów informatycznych”;
   2) Norma PN-ISO/IEC-17799 „Technika informatyczna. Praktyczne zasady zarządzania bezpieczeństwem informacji,
   3) Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.);
   4) 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),
2. Każdy użytkownik systemu przetwarzający dane osobowe zobowiązany jest stosować przepisy niniejszej Instrukcji na swoim stanowisku pracy.
3. Naruszenie postanowień niniejszej Instrukcji może zostać potraktowane jako naruszenie obowiązków i powodować określoną przepisami odpowiedzialność użytkownika systemu.

Data wygenerowania dokumentu: 2024-11-21 16:00:36

http://bip.umtychy.pl/index.php?action=PobierzPlik&id=37637

Załącznik nr 1 do Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Miasta Tychy

Zasady użytkowania sprzętu komputerowego obowiązujące w Urzędzie Miasta Tychy

Niniejsze zasady określają prawa i obowiązki użytkowników sprzętu komputerowego, którymi są pracownicy, stażyści, praktykanci oraz inne osoby wykorzystujące sprzęt komputerowy należący do Urzędu Miasta Tychy.

Dokumentem nadrzędnym w stosunku do niniejszego dokumentu jest Instrukcja Zarządzania Systemami Informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Miasta Tychy

1. Użytkownikowi systemu przysługuje prawo do korzystania:
   1) ze sprzętu komputerowego, sieci lokalnej i Internetu wyłącznie w zakresie powierzonych mu zadań,
   2) z oprogramowania komputerowego zgodnie z umowami i ustawą z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2006 r., Nr 90, poz. 631 z późn. zm.).
2. Informacje przetwarzane przez użytkownika sprzętu komputerowego zapisane na nośnikach informatycznych należą do Urzędu Miasta Tychy.
4. Użytkownik jest materialnie odpowiedzialny za sprzęt komputerowy, który otrzymał do wykonywania obowiązków służbowych.
5. Wydział Informatyki prowadzi sprawy w zakresie użytkowania sprzętu komputerowego i oprogramowania, a w szczególności:
   1) zabezpiecza sprawne działanie sprzętu komputerowego i oprogramowania,
   2) prowadzi ewidencję sprzętu komputerowego i oprogramowania,
   3) sprawuje nadzór nad wykonaniem umów dotyczących zakupu i serwisu sprzętu komputerowego i oprogramowania,
   4) zapewnia standardy sprzętu komputerowego i oprogramowania spełniające wymagania Urzędu Miasta Tychy.
6. Sprzęt komputerowy zostaje przydzielony użytkownikowi na podstawie wniosku przełożonego użytkownika przekazanego do Wydziału Informatyki wraz z kartą obiegową przyjęcia do pracy bądź w innym terminie w przypadku zmiany zakresu obowiązków użytkownika.
7. W przypadku przejścia użytkownika do innej jednostki organizacyjnej Urzędu Miasta Tychy, sprzęt komputerowy pozostaje w dotychczasowej jednostce organizacyjnej.
8. Na przeniesienie sprzętu komputerowego wraz z użytkownikiem do nowej jednostki organizacyjnej musi wyrazić zgodę dotychczasowy przełożony użytkownika.
9. Nowy przełożony użytkownika jest zobowiązany do przekazania informacji do Wydziału Informatyki o przeniesieniu pracownika do nowej jednostki organizacyjnej.
10. Przełożony użytkownika zobowiązany jest do:
    1) zlecenia serwisowi Wydziału Informatyki zmiany lokalizacji sprzętu komputerowego,
    2) informowania serwisowi Wydziału Informatyki o przekazaniu sprzętu innemu użytkownikowi,
    3) informowania ASI o wszelkich zmianach związanych z użytkownikiem, które mają wpływ na jego pracę w sieci lokalnej Urzędu Miasta Tychy, np. zmiana uprawnień, nazwiska, dłuższe urlopy lub zwolnienia zdrowotne.
11. Każdy użytkownik systemu posiada identyfikator i hasło lub kartę inteligentną, które zabezpieczają dostęp do komputera, sieci lokalnej, baz danych i skrzynki pocztowej użytkownika.
12. Użytkownik zobowiązany jest do przestrzegania zasad tworzenia haseł obowiązujących w Urzędzie Miasta Tychy.
13. Zabronione jest:
    1) podłączanie przez użytkownika własnych urządzeń do sprzętu komputerowego lub sieci lokalnej,

Data wygenerowania dokumentu: 2024-11-21 16:00:36

http://bip.umtychy.pl/index.php?action=PobierzPlik&id=37637

2) podłączania do wydzielonej sieci energetycznej innych urządzeń niż informatyczne,
3) samodzielnego instalowania oprogramowania na sprzęcie komputerowym,
4) przemieszczenia sprzętu komputerowego do innej lokalizacji (pokoju) lub zmiany użytkownika bez uzgodnienia z serwisem Wydziału Informatyki,
5) fizyczne ingerowanie w konfigurację sprzętową urządzeń,
6) samowolne odłączanie od sieci lub włącznie do sieci lokalnej sprzętu komputerowego,
7) udostępnianie swojego identyfikatora i hasła do pracy innym osobom,
8) pozyskiwanie informacji z komputerów innych użytkowników bez ich wiedzy,
9) wykonywanie czynności, które mogą spowodować zakłócenia lub awarię sieci lokalnej,
10) tworzenie przez użytkowników na dysku lokalnym bądź nośnikach informatycznych kopii baz danych systemów informatycznych bez uzgodnienia z ASI,
11) wynoszenie poza miejsce pracy nośników informatycznych zawierających dane wrażliwe oraz ich przesyłanie pocztą elektroniczną na zewnątrz,
12) pozostawianie włączonego sprzętu komputerowego poza godzinami pracy Urzędu bez wyraźnej potrzeby ustalonej z ASI.

14. Instalacja oprogramowania na sprzęcie komputerowym przez przedstawicieli firm zewnętrznych świadczących usługi serwisu i nadzoru autorskiego dla Urzędu Miasta Tychy wymaga obecności pracowników Wydziału Informatyki.
15. Użytkownik jest zobowiązany do gospodarnego użytkowania powierzonymi zasobami, w szczególności do oszczędnego korzystania z urządzeń drukujących.
16. Na stanowiskach pracy, na których używany jest sprzęt komputerowy obowiązują szczegółowe zasady jego użytkowania:
    1) zakaz spożywania posiłków przy sprzęcie komputerowym,
    2) zapewnienie warunków umożliwiających swobodne działanie układu chłodzenia użytkowanego sprzętu komputerowego,
    3) utrzymanie czystości przy stanowiskach komputerowych,
    4) zapewnienie odpowiedniego miejsca na lokalizację sprzętu komputerowego,
    5) odpowiednie meble umożliwiające bezpieczne podłączenie sprzętu komputerowego,
    6) ustawienie z dala od źródeł wilgoci, grzejników lub innych substancji mogących zakłócić prawidłowe działanie sprzętu komputerowego.
17. Jeżeli w jakiejkolwiek fazie pracy użytkownik sprzętu komputerowego podejmie podejrzenie o ingerencji osób trzecich (nieprawidłowe działanie sieci, podejrzany wygląd sprzętu) jest zobowiązany zgłosić ten fakt przełożonemu oraz ASI.
18. Przekazanie przenośnego sprzętu komputerowego (laptop, tablet, rzutnik multimedialny itp.) do stałego użytkowania odbywa się na podstawie Umowy o powierzeniu mienia pracownikowi zawieranej pomiędzy pracodawcą a użytkownikiem.
19. Użytkownik przenośnego sprzętu komputerowego zobowiązany jest do:
    1) zapoznania się instrukcji obsługi urządzenia,
    2) stosowania się do zasad opisanych w Umowie o powierzeniu mienia pracownikowi,
    3) prawidłowego zabezpieczenia przenośnego sprzętu komputerowego przed warunkami atmosferycznymi i kradzieżą,
    4) zachowania szczególnej ostrożności podczas jego użytkowania poza obszarem Urzędu Miasta Tychy w celu zapobieżenia dostępowi osobom niepowołanym do danych na nim zgromadzonych.
20. Serwis Wydziału Informatyki ma prawo odmówić wykonania zlecenia, które narusza zasady określone w powyższym dokumencie lub są niezgodne z normami bezpieczeństwa i higieny pracy.

Data wygenerowania dokumentu: 2024-11-21 16:00:36

http://bip.umtychy.pl/index.php?action=PobierzPlik&id=37637

Załącznik nr 2 do Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Miasta Tychy

Regulamin korzystania z sieci lokalnej i Internetu obowiązujący w Urzędzie Miasta Tychy

Regulamin ustala zasady korzystania z sieci lokalnej Urzędu Miasta Tychy oraz Internetu przez użytkowników sieci, którymi są pracownicy, stażyści, praktykanci oraz inne osoby wykorzystujące sprzęt komputerowy podłączony do infrastruktury sieciowej Urzędu Miasta Tychy.

Dokumentem nadrzędnym w stosunku do niniejszego regulaminu jest Instrukcja Zarządzania Systemami Informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Miasta Tychy.

1. Sieć lokalną Urzędu Miasta Tychy tworzą:
   1) sieci lokalne poszczególnych jednostek organizacyjnych Urzędu Miasta Tychy oraz łącza między nimi,
   2) serwery AD (domenowe), serwery baz danych, usług sieciowych, macierze dyskowe oraz inne urządzenia sieciowe.
2. Użytkownikiem sieci jest każda osoba korzystająca ze sprzętu komputerowego podłączonego do sieci lokalnej Urzędu Miasta Tychy.
3. Konto użytkownika sieci to zarejestrowane uprawnienie do pracy na jednym z serwerów w sieci lokalnej Urzędu Miasta Tychy.
4. Konta na serwerze są przydzielane wszystkim osobom zatrudnionym w Urzędzie Miasta Tychy zgodnie z ustaloną procedurą:
   1) Wydział Organizacyjny, Kadr i Szkolenia przekazuje dane dotyczące zawarcia i rozwiązania umowy o pracę z osobami zatrudnianymi w Urzędzie Miasta Tychy do Wydziału Informatyki.
   2) konto użytkownika sieci tworzone jest przez pracownika Wydziału Informatyki na podstawie karty obiegowej przyjęcia do pracy. Konto użytkownika sieci bez dodatkowych uprawnień umożliwia korzystanie ze sprzętu komputerowego przyłączonego do sieci lokalnej bez możliwości przeglądania dokumentów jednostki organizacyjnej oraz dostęp do serwisów internetowych Urzędu Miasta Tychy na poziomie czytelnika,
   3) w przypadku potrzeby dostępu do pozostałych serwerów, usług, zasobów sieciowych lub Internetu przełożony użytkownika sieci zgłasza do ASI potrzebę zwiększenia uprawnień przypisanych do konta użytkownika sieci,
   4) w przypadku gdy uprawnienia dotyczą systemów informatycznych, w których przetwarzane są dane osobowe, należy stosować zasady opisane w rozdziale 2 Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Miasta Tychy,
   5) użytkownik sieci może mieć tylko jedno konto w sieci lokalnej. Uprawnienia użytkowników ewidencjonowane są przez ASI w rejestrze uprawnień,
5. ASI określa warunki techniczne korzystania z kont oraz ograniczenia rozmiaru zużywanej przestrzeni dyskowej.
6. W przypadku uzyskania uprawnienia do korzystania z poczty elektronicznej użytkownik sieci korzysta z niej poprzez wskazanego przez ASI klienta serwera pocztowego lub dowolną przeglądarkę internetową.
7. Ze względów technicznych pojemność indywidualnych skrzynek pocztowych jest ograniczona. Po przekroczeniu maksymalnej wielkości skrzynki zostanie zablokowana możliwość wysyłania i odbierania wiadomości do momentu jej oczyszczenia. W uzasadnionych przypadkach, na wniosek przełożonego użytkownika, ASI może zwiększyć wielkość skrzynki.
8. W przypadku przechowywania poczty elektronicznej na stacjach roboczych odpowiedzialność za ewentualną utratę danych leży po stronie użytkownika sieci.
9. W przypadku pracownika, z którym został rozwiązany stosunek pracy:

Data wygenerowania dokumentu: 2024-11-21 16:00:36

http://bip.umtychy.pl/index.php?action=PobierzPlik&id=37637

1) przełożony użytkownika sieci jest zobowiązany do przejęcia i zabezpieczenia dokumentów oraz innych ważnych danych od zwalnianego użytkownika,
2) ASI na podstawie karty obiegowej zwolnienia wydaje dyspozycje o zablokowaniu konta użytkownika sieci oraz uprawnień w systemach informatycznych,
3) pracownicy Wydziału Informatyki realizują zadanie i nanoszą zmiany w rejestrze uprawnień,
4) w przypadku dokumentów pozostawionych na kontach osób, z którymi został rozwiązany stosunek pracy, zostaną one skasowane po upływie 6 miesięcy od momentu zablokowania konta.

10. Każdy użytkownik sieci lokalnej Urzędu Miasta Tychy powinien postępować zgodnie z powierzonymi mu obowiązkami, a w szczególności wykorzystywać pocztę elektroniczną, dostęp do Internetu oraz uprawnienia do systemów informatycznych i aplikacji tylko do celów służbowych.
11. Zabronione jest:
    1) wysyłanie masowej poczty kierowanej do losowych odbiorców (spam),
    2) udostępnianie treści chronionych prawem autorskim (filmy, czy utwory muzyczne),
    3) udostępnianie treści zakazanych (np. pornografia),
    4) nieuzasadnione wynoszenie danych zawartych na nośnikach informatycznych bądź przesyłania danych pocztą elektroniczną poza obręb sieci lokalnej,
    5) samowolne włącznie do sieci lokalnej prywatnego sprzętu komputerowego lub innych urządzeń sieciowych.
12. Pracodawca zastrzega sobie prawo do monitorowania ruchu w sieci lokalnej Urzędu Miasta Tychy, w zakresie określonym w powyższych ust. 1 i 2.
13. Jeżeli zaistnieje potrzeba podłączenia do sieci lokalnej prywatnego sprzętu komputerowego, wymaga to każdorazowo:
    1) akceptacji przełożonego użytkownika,
    2) akceptacji ASI po wcześniejszym jego sprawdzeniu pod względem złośliwego oprogramowania.
14. Zabrania się podejmowania prób wykorzystania obcego konta, uruchamiania aplikacji deszyfrujących hasła, prowadzenia działań mających na celu podsłuchiwanie lub przechwytywanie informacji przepływającej w sieci.
15. Zabrania się uruchamiania aplikacji, które mogą zakłócić i destabilizować pracę systemu lub sieci lokalnej, bądź naruszyć prywatność zasobów systemowych.
16. W przypadku naruszenia zasad opisanych niniejszym regulaminie ASI blokuje dostęp do konta użytkownika. O tym fakcie powiadamiany jest ABI oraz przełożony użytkownika sieci.
17. W przypadku stwierdzenia, że komputer dołączony do sieci lokalnych generuje strumień danych zakłócający pracę sieci lub wskazujący na używanie tego komputera jako niezarejestrowanego serwera danych, ASI ma prawo zablokować dostęp do tego komputera do czasu wyjaśnienia sprawy. O tym fakcie powiadamiany jest ABI oraz przełożony użytkownika sieci.

Data wygenerowania dokumentu: 2024-11-21 16:00:36

http://bip.umtychy.pl/index.php?action=PobierzPlik&id=37637

Załącznik nr 3 do Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Miasta Tychy

Zasady tworzenia haseł obowiązujące w Urzędzie Miasta Tychy

1. W Urzędzie Miasta Tychy uwierzytelnianie (weryfikacja tożsamości) w systemach operacyjnych komputerów oraz systemach informatycznych polega na podaniu osobistego identyfikatora użytkownika oraz hasła. Niektóre systemy wykorzystują do uwierzytelnienia karty kryptograficzne chronione kodem PIN.
2. Hasła użytkowane w sieci lokalnej i systemach informatycznych Urzędu Miasta Tychy tworzy się zgodnie z treścią Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku do Ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych określającym minimalne normy, które musi spełniać hasło użyte do uwierzytelnienia.
3. Procedura przyznawania konta użytkownika uprawniającego do korzystania z sieci lokalnej (konto użytkownika sieci) a także konta dostępowego w systemach informatycznych opisane są w rozdziale 2 Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Miasta Tychy, oraz z § 3 Regulaminu korzystania z sieci lokalnej i Internetu obowiązujący w Urzędzie Miasta Tychy.
4. Administrator sieci lokalnej Urzędu Miasta Tychy tworzy identyfikator użytkownika i hasło konta użytkownika sieci niezbędnego do rozpoczęcia pracy na sprzęcie komputerowym przyłączonym do sieci lokalnej i przekazuje te dane bezpośrednio użytkownikowi. Podczas pierwszego logowania użytkownik jest zobowiązany zmienić hasło.
5. Hasło musi się składać **z co najmniej 8 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.**
6. Użytkownik jest zobowiązany do zmiany hasła konta użytkownika sieci oraz konta dostępowego do każdego systemu informatycznego przetwarzającego dane osobowe **nie rzadziej niż co 30 dni.**
7. W przypadku braku hasła, jego zagubienia bądź ujawnienia osobie trzeciej, użytkownik zobowiązany jest do jego natychmiastowej zmiany.
8. W przypadku braku możliwości samodzielnej zmiany hasła użytkownik zwraca się osobiście do administratora sieci bądź właściwego systemu informatycznego z wnioskiem o jego zmianę. Administrator ma prawo do sprawdzenia tożsamości osób występujących o zmianę hasła.
9. W przypadku systemów informatycznych, które są obsługiwane przez jednostki działające poza siecią lokalną Urzędu Miasta Tychy (m.in. BIP), z wnioskiem o zmianę hasła występuje przełożony użytkownika.
10. W przypadku braku możliwości jednoznacznej weryfikacji tożsamości osoby wnioskującej o zmianę hasła administrator ma obowiązek odmówić dokonania jego zmiany.
11. Zabrania się:
    1) przekazywania haseł użytkowników innym osobom, w tym współpracownikom,
    2) zapisywania haseł użytkowników w formie jawnej,
    3) wykorzystywania haseł użytkowników, które nie spełniają minimalnych norm określonych w powyższym dokumencie,
    4) zmiany haseł użytkowników poprzez jego klonowanie – zmianę jednego znaku w haśle. Kolejne hasło użytkownika powinno w znaczny sposób różnić się od poprzedniego i co najmniej kilku wcześniejszych,
    5) używania tego samego hasła użytkownika w wielu różnych systemach,
    6) używanie hasła użytkownika w komputerze, co do którego istnieje podejrzenie, że może być nieodpowiednio zabezpieczony (m.in. poprzez brak systemu antywirusowego, wyświetlenie komunikatu o zawirusowaniu systemu, itp.).
12. Dopuszcza się wykorzystanie aplikacji dedykowanych bądź innych metod bezpiecznego zapamiętywania haseł użytkowników po uprzedniej ich akceptacji przez ASI.

Data wygenerowania dokumentu: 2024-11-21 16:00:36

http://bip.umtychy.pl/index.php?action=PobierzPlik&id=37637

13. W przypadku dłuższych nieobecności pracownika (urlop, choroba) należy wystąpić do administratora systemu o rozszerzenie uprawnień osobie zastępującej w sposób umożliwiający wykonanie wszystkich wymaganych operacji z poziomu konta osoby zastępującej.
14. Ze względów technicznych w haśle użytkownika nie powinny być używane spacje i polskie znaki diakrytyczne (ł, ą, ć, ź, ó, itp.).
15. Bardzo częstą próbą wyłudzenia hasła użytkownika są ataki polegające na podaniu się za administratora lub serwisanta danego systemu, z prośbą o podanie hasła w celu przeprowadzenia konkretnych prac w systemie. W przypadku podejrzenia próby wyłudzenia hasła w opisany powyżej sposób, użytkownik powinien pilnie zgłosić ten fakt ASI.
16. Charakterystyczną cechą dobrego hasła jest to, że będąc trudne do odgadnięcia przez osobę postronną, pozostają jednocześnie łatwe do zapamiętania. Podczas konstruowania haseł użytkownik powinien kierować się następującymi wskazówkami:
    1) hasło powstaje poprzez wstawienie jednego słowa w środek drugiego, np.: poliautoTyka2*,
    2) utworzenie hasła przez błędne napisanie słowa lub zamianę poszczególnych znaków, np.: 1Samohud&,
    3) hasło jako połączenie kilku wyrazów z liczbami i znakami specjalnymi, np.: 20majagramWszachy, 9razyJem2razy!,
    4) hasło tworzą pierwsze litery piosenek, wierszy, przysłów lub zdań, np.: LomTjjZ - Litwo Ojczyzno Moja...,
    5) dodatkową zaletą hasła jest łatwość wpisywania – na hasło może składać się ciąg znaków, który daje się szybko wpisać w sposób uniemożliwiający ich podejrzenie przez ramię.
17. Należy unikać wykorzystywania jako haseł:
    1) imion, nazwisk rodziny, dzieci, znajomych, współpracowników, zwierząt domowych;
    2) znanych postaci bajkowych, literackich, filmowych;
    3) popularnych nazw komputerowych;
    4) numerów rejestracyjnych samochodu, jego nazwy;
    5) dat urodzenia, dat historycznych;
    6) nazw użytkowników komputerów w żadnej postaci;
    7) słów dostępnych w słownikach (różnych języków);
    8) nazw ulic, parków, miast;
    9) wyrazów złożonych z sekwencji odczytywanej z klawiatury (np. qwerty);
    10) żadnych z powyższych pisanych wspak, lub z dołączoną pojedynczą cyfrą.

Data wygenerowania dokumentu: 2024-11-21 16:00:36

http://bip.umtychy.pl/index.php?action=PobierzPlik&id=37637

Załącznik nr 4 do Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Miasta Tychy

WNIOSEK O NADANIE UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

Proszę o nadanie upoważnienia do przetwarzania danych osobowych dla

Pana/i . . . . . .

Pracownika wydziału / stażysty / praktykanta*
Upoważniony/a będzie przetwarzać dane osobowe w systemie informatycznym*.
Upoważniony/a nie będzie przetwarzać danych osobowych w systemie informatycznym*.

data. . . . . .

……..……..
podpis kierownika jednostki

*- niepotrzebne skreślić

Data wygenerowania dokumentu: 2024-11-21 16:00:36

http://bip.umtychy.pl/index.php?action=PobierzPlik&id=37637

Załącznik nr 5 do Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Miasta Tychy

Wniosek o nadanie uprawnień do pracy w sieci lokalnej i systemach informatycznych użytkowanych w Urzędzie Miasta Tychy

Wydział Informatyki
w miejscu

W związku z zatrudnieniem / zmianą zakresu obowiązków …… (…….) [I]

proszę o utworzenie konta użytkownika sieciowego umożliwiającego pracę na sprzęcie komputerowym w sieci lokalnej Urzędu Miasta Tychy oraz wnioskuję o:

- ☐ utworzenie nowego stanowiska komputerowego [II] w pokoju nr .....,
- ☐ przygotowanie stanowiska komputerowego nr ..... do pracy,
- ☐ nadanie praw dostępu do sieciowych dokumentów wydziałowych,
- ☐ utworzenie imiennego konta poczty elektronicznej,
- ☐ przyznanie konta redaktora BIP (panel administracyjny),
- ☐ przyznanie dostępu do Internetu,
- ☐ inne

…...……..

Przyznanie uprawnień do następujących systemów informatycznych [III]:

☐ SODiS ☐ ZAMÓWIENIA PUBLICZNE ☐ DYSPONENT ☐ FAKTUROWANIE ☐ SIT [IV]

W przypadku systemów informatycznych, nad którym nadzór pełni inna jednostka organizacyjna, należy wypełnić poniższą tabelę:

DOTYCZY SYSTEMU: ……..……..……		
Posiada upoważnienie do przetwarzania danych osobowych:	☐ TAK	☐ NIE
Opis zakresu uprawnień użytkownika w systemie informatycznym i uzasadnienie:		
Opinia kierownika jednostki organizacyjnej pełniącej nadzór nad systemem informatycznym:	Podpis kierownika jedn. org. pełniącej nadzór nad systemem informatycznym:	

W przypadku zatrudnienia:

stażysty – proszę podać planowany termin zakończenia zatrudnienia: .....

pracownika „na zastępstwo” – proszę podać nazwisko osoby zastępowanej: .....

.....
data i podpis Naczelnika Wydziału

zaznaczyć właściwy □

I wpisać imię i nazwisko zatrudnianej osoby, skrót wydziału

II zaznaczyć tylko w przypadku braku sprzętu komputerowego na stanowisku

III w przypadku uprawnień do systemów informatycznych w których przetwarzane są dane osobowe konieczne jest posiadanie upoważnienia do przetwarzania danych osobowych

IV o przyznaniu uprawnień dostępu do SIT decyduje ASI_GWG

Data wygenerowania dokumentu: 2024-11-21 16:00:36