Załącznik nr 2 do Zarządzenia nr 26/2009

INSTRUKCJA ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI

W ZAKRESIE WYMOGÓW BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH

w

Urzędzie Miasta i Gminy

w Ostrzeszowie

Ostrzeszów 2009

SPIS TREŚCI

I. POSTANOWIENIA OGÓLNE

§1.

1. Instrukcja określa procedury zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych, zwanych dalej danymi, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji w Urzędzie Miasta i Gminy w Ostrzeszowie zwanym dalej Urzędem.
2. Instrukcja pozwala stosować ujednolicone zasady ochrony danych w systemach i sieciach informatycznych Urzędu.
3. Celem utworzenia instrukcji jest podniesienie poziomu bezpieczeństwa systemów informatycznych, w których są gromadzone i przetwarzane dane oraz określenie odpowiedzialności pracowników Urzędu za prawidłowe działanie tych systemów i bezpieczeństwo przetwarzanych w nim danych.

§2.

Instrukcja w szczególności zawiera:

1. określenie procedury przydziału haseł dla użytkowników i częstotliwość ich zmiany, ze wskazaniem osoby odpowiedzialnej za te czynności,
2. określenie procedury rejestrowania i wyrejestrowywania użytkowników oraz wskazanie osoby odpowiedzialnej za te czynności,
3. procedury rozpoczęcia i zakończenia pracy w systemach informatycznych,
4. opis metod oraz procedurę i harmonogram tworzenia kopii bezpieczeństwa,
5. opis metod i harmonogram sprawdzania obecności wirusów komputerowych oraz metody ich usuwania,
6. procedurę i okres przechowywania elektronicznych nośników informacji i wydruków,
7. procedurę i harmonogram dokonywania przeglądów i konserwacji systemów oraz zbiorów danych osobowych,
8. zasady wyposażania i eksploatacji stacji roboczych,
9. zasady wymiany informacji w sieciach komputerowych.

§3.

Określenia użyte w instrukcji oznaczają:

1. Ustawa – Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2002r. Nr 101 poz. 926, ze zm.),
2. Rozporządzenie – Rozporządzenie 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. 2004r. Nr 100 poz. 1024),

3. Urząd – Urząd Miasta i Gminy w Ostrzeszowie,
4. Komórka organizacyjna – odpowiednio komórki organizacyjne,
5. Naruszenie bezpieczeństwa systemu informatycznego – jakiekolwiek naruszenie poufności, integralności, dostępności do systemu informatycznego spowodowane przez ludzi, jak też powstałe na skutek oddziaływania sił przyrody, katastrof, itp.,
6. Administrator Danych – Burmistrz Miasta i Gminy Ostrzeszów,
7. ABI - Administrator Bezpieczeństwa Informacji,
8. Administrator systemu – osoba zarządzająca bieżącą pracą systemu informatycznego i zbiorami danych w Urzędzie Miasta i Gminy w Ostrzeszowie.
9. Systemy informatyczne Urzędu zwane dalej systemami – zespoły współpracujących ze sobą urządzeń, programów, procedur gromadzenia i przetwarzania informacji, narzędzi programowych zastosowanych do przetwarzania danych wraz ze zgromadzonymi danymi oraz osobami upoważnionymi do pracy na tych systemach (w tym obsługa techniczna urządzeń),
10. Przetwarzanie danych – jakiekolwiek operacje wykonywane na danych, takie jak utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, przekazywanie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,
11. Obszar przetwarzania danych – obiekty, pomieszczenia jednostek i komórek organizacyjnych Urzędu, w których odbywa się gromadzenie i przetwarzanie danych w układach elektronicznych na nośnikach magnetycznych, optycznych (również w postaci papierowej np. kartoteki czy inne zbiory informacji), urządzenia, elementy techniczne, z których charakteru pracy wynika wydawanie informacji na zewnątrz tzn. monitory, drukarki itp.,
12. Zabezpieczenie danych w systemie Urzędu – wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym pozyskiwaniem, gromadzeniem i przetwarzaniem,
13. Użytkownik systemu zwany dalej użytkownikiem:
    1) osoba zatrudniona przy przetwarzaniu danych w Urzędzie, która posiada upoważnienie do obsługi systemu oraz urządzeń wchodzących w jego skład, a także osoba przetwarzająca dane w toku wykonywania umowy cywilnoprawnej zawartej ze Urzędem (np. umowy zlecenia, umowy o dzieło, itp.),
    2) pracownik innego podmiotu, który świadczy usługi związane z pracą w systemie Urzędu, na podstawie odrębnych umów z tym podmiotem (np. serwis, zlecenie przetwarzania danych, itp.),
14. Gromadzenie danych – zbieranie na nośnikach elektronicznych oraz wydrukach danych.

§4.

1. Ochrona zasobów danych Urzędu jako całości, przed ich nieuprawnionym użyciem lub zniszczeniem, jest jednym z podstawowych obowiązków każdego pracownika Urzędu.
2. Obowiązkiem każdego pracownika Urzędu jest zachowanie tajemnicy służbowej, w tym ochrony danych osobowych gromadzonych i przetwarzanych przez Urząd. Obowiązek ten istnieje również po ustaniu zatrudnienia.
3. Osoby zatrudnione przy przetwarzaniu danych (także poza systemami) są zobowiązane do szczególnej dbałości o zachowanie poufności, integralności i dostępności do danych gromadzonych w kartotekach, skorowidzach itp. oraz infrastruktury sprzętowo – programowej systemu.

§5.

1. Za bezpieczeństwo danych osobowych Urzędu, odpowiadają:
   1) Administrator danych osobowych – Burmistrz Miasta i Gminy Ostrzeszów,
   2) Administrator Bezpieczeństwa Informacji Urzędu.

§6.

Obowiązki wynikające z ustawy o ochronie danych osobowych Burmistrz Miasta i Gminy Ostrzeszów powierza lokalnym administratorom - naczelnikom wydziałów - w zakresie podległych im pracowników.

§7.

1. Obszary przetwarzania danych w obiektach i pomieszczeniach Urzędu nie mogą być dostępne dla osób nieuprawnionych.
2. Dopuszczalne odstępstwo stanowią pomieszczenia, w których przyjmowani są interesanci. Jeżeli pomieszczenia te wyposażone są jednocześnie w urządzenia z dostępem do systemów bazodanowych albo tradycyjne kartoteki, należy w nich stosować szczególne środki ostrożności, w tym:
   1) interesanci powinni wchodzić pojedynczo i pozostawać w pomieszczeniu tylko w obecności użytkownika systemu,
   2) kartoteki tradycyjne należy zabezpieczyć przed dostępem osób nieuprawnionych,
   3) nie należy pozostawiać dokumentów papierowych i nośników elektronicznych w miejscach umożliwiających ich wykorzystanie, przez osoby nieuprawnione,
   4) monitory powinny być usytuowane tak, aby ekrany były niewidoczne dla osób nieuprawnionych,
   5) drukarki i urządzenia peryferyjne powinny być usytuowane tak, aby znajdowały się z dala od przestrzeni, po której poruszają się osoby nieuprawnione,

6) naczelnik komórki organizacyjnej określi szczegółowe zasady ogłoszenia alarmu i wezwania pomocy przez pracownika w przypadku bezpośredniego zagrożenia jego życia lub zdrowia, albo ujawnienia próby pozyskania danych osobowych.

§8.

Systemy informatyczne w Urzędzie powinny być tak zaprojektowane, aby wymuszać autoryzację osoby przystępującej do pracy na zbiorach danych osobowych.

§9.

Odpowiedzialność za ochronę danych zawartych na komputerach przenośnych i innych przenośnych urządzeniach umożliwiających gromadzenie danych, spoczywa wyłącznie na dysponentach tych urządzeń; minimalnym wymaganym zabezpieczeniem każdego komputera PC w Urzędzie jak również komputera przenośnego jest ograniczenie dostępu do tego komputera hasłem (hasło na BIOS, Windows, wygaszasz ekranu).

§10.

1. Dane wyeksportowane z systemu do komputera mogą znajdować się na tym komputerze tylko przez niezbędny do ich wykorzystania czas.
2. Po wykorzystaniu danych określonych w ust. 1 należy je niezwłocznie usunąć.
3. Danych określonych w ust. 1 nie można udostępniać osobom nieuprawnionym.

§11.

1. Wszelkie informacje zawierające dane, udostępniane podmiotom zewnętrznym Urzędu, mogą zostać przekazane tylko za pośrednictwem kancelarii ogólnej Urzędu, w której odnotowywany jest zakres podmiotowy i przedmiotowy udostępnienia.
2. W uzasadnionych przypadkach dane mogą być przesyłane drogą elektroniczną w formie zaszyfrowanej.

§12.

1. Zabrania się:
   1) zapisywania indywidualnych haseł dostępu,
   2) dokonywania samowolnych napraw sprzętu informatycznego oraz modyfikowania oprogramowania,

3) samodzielnego zakupu sprzętu komputerowego lub oprogramowania bez wiedzy i akceptacji Informatyka,
4) autoryzacji w systemie jako inny użytkownik,
5) samodzielnego wgrywania oprogramowania,
6) w celach innych niż służbowe, wynoszenia dokumentacji, w tym na nośnikach elektronicznych zawierającej dane, poza obszar jednostki organizacyjnej,
7) instalowania na komputerach urzędu prywatnych kont poczty elektronicznej,
8) wykorzystywania Internetu do celów innych niż służbowe oraz przeglądania stron o tematyce pornograficznej, nielegalnych stron z kodami aktywacyjnymi do programów lub programami łamiącymi zabezpieczenia programów przed nielegalnym kopiowaniem.
9) korzystania z czatów internetowych, ściągania plików muzycznych oraz filmów i innych.

2. Identyfikator i hasło osoby, która utraciła uprawnienia do korzystania z systemu należy bezzwłocznie unieważnić.
3. Identyfikator osoby, która utraciła uprawnienia i została wyrejestrowana z systemu nie może być przydzielony innej osobie.
4. Dostęp do poszczególnych elementów systemów bazodanowych powinien być realizowany tylko w zakresie określonym nadanymi uprawnieniami, po wydaniu upoważnienia użytkownikowi.

§13.

1. Osoby zatrudnione w Urzędzie potwierdzają własnoręcznym podpisem zapoznanie się z indywidualnym zakresem czynności osoby zatrudnionej przy przetwarzaniu danych (wzór w załączniku nr 5 do niniejszej Instrukcji).
2. Osoby zatrudnione w Urzędzie podlegają szkoleniu w zakresie ochrony danych, po którym otrzymują upoważnienie do obsługi systemów informatycznych w zakresie przetwarzania danych (wzór w załączniku nr 6 do niniejszej Instrukcji).
3. Upoważnienie do obsługi systemu w zakresie przetwarzania danych wydaje stanowisko ds. kadrowych, akceptuje Administrator Bezpieczeństwa Informacji oraz podpisuje Administrator Danych.
4. Indywidualny zakres czynności osoby zatrudnionej przy przetwarzaniu danych oraz Upoważnienie do obsługi systemów informatycznych w zakresie przetwarzania danych załącza się do akt personalnych pracownika.

§14.

1. Administrator Bezpieczeństwa Informacji prowadzi następujące ewidencje:

1) ewidencję baz danych w systemach informatycznych, w których przetwarzane są dane osobowe (wzór w załączniku nr 1 do niniejszej Instrukcji),
2) ewidencję osób upoważnionych do przetwarzania danych osobowych w systemach informatycznych (wzór w załączniku nr 2 do niniejszej Instrukcji),
3) ewidencję miejsc przetwarzania danych osobowych w systemach informatycznych i sposobu ich zabezpieczania (wzór w załączniku nr 3 do niniejszej Instrukcji),

2. Lokalni administratorzy danych zobowiązani są do przekazywania do administratora bezpieczeństwa informacji zaktualizowanych załączników nr 1, 2, 3, do dnia 15-go każdego miesiąca wg stanu na miesiąc poprzedni.
3. O zamiarze wypowiedzenia umowy o pracę, lub ustaniu stosunku pracy z osobą zatrudnioną w Urzędzie, właściwa ds. pracowniczych komórka organizacyjna Urzędu powiadamia Administratora Bezpieczeństwa Informacji.
4. Administrator Bezpieczeństwa Informacji niezwłocznie powiadamia o faktach wynikających z ust. 3, osobę odpowiedzialną za nadawanie haseł i kodów dostępu. Kody dostępu i hasła są likwidowane w ciągu 24 godzin od ustania uprawnień lub zatrudnienia.

II. Procedury rejestrowania i wyrejestrowywania użytkowników

§15.

1. Pracownika Urzędu korzystającego z systemu i jego oprogramowania rejestruje się jako użytkownika.
2. Niedopuszczalna jest praca w systemie na koncie innego użytkownika.

§16.

1. W celu zarejestrowania osoby jako użytkownika systemu, naczelnik komórki organizacyjnej Urzędu, w której zatrudniona jest osoba, kieruje wniosek do Informatyka Urzędu, w którym określa:
   1) konieczne uprawnienia (bądź zmianę, wycofanie uprawnień) ze szczególnym uwzględnieniem uprawnień do przetwarzania danych,
   2) informację o przeszkoleniu użytkownika w zakresie ochrony danych, potwierdzoną przez Administratora Bezpieczeństwa Informacji.
2. Założenie profilu, nadanie uprawnień, modyfikacja uprawnień użytkownika do systemu informatycznego następuje po przedłożeniu do Administratora Bezpieczeństwa Informacji wniosku (wzór w załączniku nr 11 do Instrukcji).

§17.

1. Nadawanie i rozszerzanie uprawnień użytkowników koordynuje Administrator Bezpieczeństwa Informacji, który zleca zarządzanie w tym zakresie administratorowi systemu bądź Lokalnemu Administratorowi Danych.
2. Administrator systemu w porozumieniu z Administratorem Bezpieczeństwa Informacji nadaje, nadzoruje i wycofuje uprawnienia.

§18.

Identyfikator użytkownika powinien spełniać następujące wymagania:

1. długość minimum trzy znaki,
2. musi być niepowtarzalny w skali systemu,
3. jednym identyfikatorem może posługiwać się tylko jeden użytkownik,
4. identyfikator jest natychmiast blokowany przez administratora systemu po rozwiązaniu z pracownikiem umowy o pracę, po uzyskaniu takiej informacji z kadr,
5. identyfikator pracownika, który rozwiązał umowę o pracę nie może zostać przydzielony innemu pracownikowi.

III. Budowa i procedura przydziału haseł dla administratorów systemów i użytkowników oraz częstotliwość ich zmiany

§19.

Określa się następujące zasady tworzenia haseł.

1. Hasło musi mieć nie mniej niż 8 znaków.
2. Hasło musi zawierać znaki z wszystkich trzech niżej wymienionych grup:
   1) małe i duże litery,
   2) cyfry,
   3) znaki specjalne.
3. W haśle nie wolno używać polskich znaków diakrytycznych lub innych znaków narodowych.
4. Hasło nie może mieć charakteru słownikowego.
5. Hasło jest obowiązkowe dla każdego użytkownika, posiadającego identyfikator w systemie.
6. Po założeniu hasła przez administratora użytkownik ma obowiązek zarejestrować się do systemu i zmienić hasło.

§20.

Określa się następujące zasady korzystania z haseł:

1. Nie wolno powtórnie używać hasła raz użytego.
2. Hasło znane jest tylko użytkownikowi.
3. Przy wpisywaniu hasła nie jest ono wyświetlane na ekranie.
4. Użytkownik odpowiada za systematyczną zmianę haseł.

§21.

Niedopuszczalne jest:

1. jakiekolwiek notowanie hasła,
2. podawanie swojego hasła innym użytkownikom bądź osobom nie uprawnionym do pracy w systemie lub nie posiadającym uprawnień do przetwarzania danych.

§22.

1. Hasła w systemach Urzędu zmienia się nie rzadziej niż raz w miesiącu.
2. Powyższe zalecenie jest obowiązujące w Urzędzie niezależnie od tego czy użytkownik przetwarza dane.

§23.

1. Administrator systemu tworzy i zmienia hasła zgodnie z zasadami określonymi w niniejszej

Instrukcji.

2. Hasła do serwerów, aktywnych urządzeń sieci i istotnych programów konfiguracyjnych, administrator systemów umieszcza w zapieczętowanych kopertach i składa w obecności Administratora Bezpieczeństwa Informacji w komórce Informatyki.
3. Otwarcie koperty określonej w ust. 2 może nastąpić w przypadku:
   1) kontroli przez Informatyka.
   2) zamiaru zniszczenia nieaktualnych haseł przez administratora systemu,
   3) zaistnienia konieczności zapoznania się z jej zawartością spowodowanej rezygnacją z pracy, pozbawieniem uprawnień lub śmiercią administratora systemu; uprawnienie w tym zakresie posiada Informatyk.
   4) innym określonym w „Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych w Urzędzie".

§24.

1. Hasło lokalnego administratora stacji roboczych pozostaje w wyłącznej dyspozycji komórki Informatyki.
2. Zabrania się nadawania użytkownikom stacji roboczych uprawnień administratora stacji roboczej.

§25.

Zobowiązuje się administratora systemów do uruchomienia na stacjach lokalnych (roboczych) procedury automatycznego wymuszania przez te systemy zmiany hasła.

IV. Procedura rozpoczęcia i zakończenia pracy w systemie informatycznym

§26.

1. Użytkownik systemu informatycznego Urzędu musi być zarejestrowany przez administratora systemu jako użytkownik odpowiedniej aplikacji.
2. Włączając komputer w celu podjęcia pracy użytkownik dokonuje autoryzacji zgodnie z poleceniami wydawanymi przez system komputerowy ukazującymi się na ekranie monitora.
3. W przypadku pojawienia się trudności w autoryzacji, pomimo prawidłowo wykonanych czynności, użytkownik zobowiązany jest skontaktować się z administratorem systemu.
4. Jeżeli autoryzacja przebiegła prawidłowo, użytkownik dokonuje wyboru aplikacji, w której zamierza pracować.

§27.

Obowiązkiem każdego pracownika jest dbałość o nie pozostawianie stanowiska informatycznego z dostępem do systemów bazodanowych, bez należytego zabezpieczenia i w tym:

1. opuszczając stanowisko pracy należy wylogować się z systemu,
2. przy krótkotrwałych przerwach w pracy należy zablokować stację roboczą.

§28.

Kończąc pracę w systemie użytkownik zamyka wszystkie otwarte aplikacje, a następnie zamyka system postępując zgodnie z ukazującymi się na ekranie monitora komunikatami.

V. Obszary przetwarzania danych

§29.

W celu zapewnienia bezpiecznych warunków przetwarzania danych w systemach Urzędu określa się obszary przetwarzania danych jako:

1. obiekty, wydzielone pomieszczenia lub części pomieszczeń, w których przetwarzane są dane (także w postaci tradycyjnej – papierowej),
2. części obiektów, w których znajdują się informatyczne urządzenia wyjścia (np. monitory, drukarki itp.).

§30.

Pomieszczenie określone jako obszar przetwarzania danych powinno spełniać następujące warunki:

1. być wyposażone w zamek mechaniczny lub elektroniczny zamykany każdorazowo, gdy opuszczają je pracownicy zatrudnieni przy przetwarzaniu danych,
2. jeżeli pomieszczenie znajduje się na parterze, lub istnieje możliwość podglądu z zewnątrz, ekrany monitorów umieszcza się w sposób uniemożliwiający taki podgląd,
3. monitory komputerów, na których wykonuje się przetwarzanie danych powinny być ustawione w sposób uniemożliwiający ich podgląd osobom nieuprawnionym.

§31.

Wydzielona część pomieszczenia określona jako obszar przetwarzania danych powinna spełniać następujące warunki:

1. wyposażenie (meble) w tej części pomieszczenia muszą być tak ustawione, aby uniemożliwić lub istotnie utrudnić dostęp do tego obszaru osobom nieuprawnionym,
2. monitory komputerów, na których dokonuje się przetwarzania danych powinny być ustawione w sposób uniemożliwiający ich podgląd osobom nieuprawnionym.

§32.

1. Lokalni Administratorzy Danych (naczelnicy komórek organizacyjnych Urzędu), sporządzają imienne wykazy pracowników komórki organizacyjnej aktualnie zatrudnionych przy przetwarzaniu danych (Załącznik nr 2 do Instrukcji).
2. Lokalni Administratorzy Danych wykazy określone w ust. 1 przekazują do dnia 15-go każdego miesiąca wg stanu na miesiąc poprzedni, Administratorowi Bezpieczeństwa Informacji.

§33.

Nadzór nad przestrzeganiem zasad ochrony przetwarzanych danych sprawuje Administrator Bezpieczeństwa Informacji.

VI. Opis metod i harmonogram sporządzania kopii bezpieczeństwa

§34.

1. Jedynie administrator systemów informatycznych jest upoważniony do sporządzania kopii zabezpieczających plików aplikacji i baz danych oraz systemów operacyjnych i ponosi pełną odpowiedzialność w tym zakresie.
2. Z kopii bezpieczeństwa mogą być odtwarzane zbiory danych, uprawnienia użytkowników i ustawienia związane ze specyfiką i uwarunkowaniami systemów Urzędu.
3. Odtwarzania dokonuje administrator systemu.

§35.

1. Przyjmuje się zasadę, iż kopie bezpieczeństwa nie powinny być przechowywane w tym samym pomieszczeniu, w których przechowywane są zbiory danych eksploatowane na bieżąco.
2. Nośniki zawierające kopie bezpieczeństwa przechowywane są w sejfie ogniotrwałym.
3. Dostęp do kopii bezpieczeństwa może posiadać wyłącznie administrator systemu, a w razie jego nieobecności: Administrator Bezpieczeństwa Informacji oraz Administrator Danych Urzędu.

§36.

1. Co najmniej raz na kwartał administrator systemu dokonuje sprawdzenia zasobów kopii bezpieczeństwa pod kątem ich przydatności do odtworzenia danych w przypadku awarii systemu.
2. Kopie bezpieczeństwa, które uległy uszkodzeniu, lub zdezaktualizowały się, podlegają bezzwłocznemu zniszczeniu.
3. Zniszczenia kopii bezpieczeństwa lub innego nośnika zawierającego dane, dokonuje się komisyjne na polecenie Administratora Bezpieczeństwa Informacji. Z wykonanych czynności sporządza się protokół zniszczenia (wzór protokołu w załączniku nr 7 do niniejszej Instrukcji).

§37.

Opisu czynności sporządzania, okresowego sprawdzania, niszczenia kopii bezpieczeństwa, jak też odtwarzania danych z tych kopii, dokumentuje się w „Dzienniku ewidencji kopii bezpieczeństwa", który przechowywany jest przez administratora systemu (wzór dziennika w załączniku nr 8 do niniejszej Instrukcji).

§38.

Nadzór nad procesem sporządzania, przechowywania i niszczenia kopii bezpieczeństwa sprawuje Administrator Bezpieczeństwa Informacji.

§39.

Sposób i częstotliwość tworzenia awaryjnych kopii systemu operacyjnego serwerów:

1. Kopia systemu operacyjnego powinna być wykonywana po każdej modyfikacji, zmianie, konfiguracji i instalacji nowej wersji oprogramowania.
2. Powinny istnieć przynajmniej dwa zestawy takiej kopii zapisywane naprzemiennie, kopie takie powinny być okresowo sprawdzane pod kątem ich przydatności – prawidłowości wykonania oraz możliwości odtwarzania.

§40.

Metoda i częstotliwość tworzenia awaryjnych kopii danych:

1. Pełna kopia zabezpieczająca plików aplikacji i bazy danych systemów wykonywana jest raz w tygodniu.
2. Przyrostowa kopia zabezpieczająca wykonywana jest codziennie.
3. Każda kopia powinna zostać opisana w taki sposób, by zawierała następujące informacje:
   1) data wykonania,
   2) nazwa systemu informatycznego,
   3) nazwa zbioru danych.

§41.

Zobowiązuje się pracowników urzędu do zapisywania ważnych zasobów na dysku sieciowym.

VII. Opis metod oraz harmonogram sprawdzania obecności wirusów i ich usuwanie

§42.

1. Bieżące sprawdzanie obecności wirusów komputerowych realizuje się przez stosowanie oprogramowania monitorującego występowanie wirusów.
2. Sprawdzaniu obecności wirusów podlegają wszystkie informatyczne nośniki danych.
3. Sprawdzanie obecności wirusów na dyskach serwerów przeprowadza administrator systemów.
4. Administrator systemu zobowiązany jest do zapewnienia systematycznej aktualizacji programu antywirusowego.
5. Sprawdzanie obecności wirusów na dyskach stacji roboczej odbywa się automatycznie po uruchomieniu komputera.

§43.

1. O wykryciu wirusa na stacji roboczej użytkownik powiadamia administratora systemu.
2. W przypadku problemów z usunięciem wirusa ze stacji roboczej użytkownik nie podejmuje dalszych działań do czasu przybycia administratora systemu.
3. Administrator systemu o przypadku stwierdzenia szczególnie groźnych lub trudnych do usunięcia wirusów komputerowych powiadamia Administratora Bezpieczeństwa Informacji.

§44.

Po dokonanej naprawie lub konserwacji należy przeprowadzić proces sprawdzenia pod kątem występowania wirusów.

§45.

Informatyczne nośniki informacji pochodzenia zewnętrznego podlegają sprawdzeniu programem antywirusowym przed rozpoczęciem korzystania z nich.

§46.

1. Nadzór nad prawidłowym funkcjonowaniem oprogramowania antywirusowego sprawuje administrator systemu.
2. Administrator systemu zobowiązany jest do przeprowadzania systematycznej kontroli antywirusowej serwerów.

VIII. Ogólne zasady i odpowiedzialność przy instalacji oprogramowania

§47.

1. Administrator systemu zobowiązany jest prowadzić dziennik czynności technologicznych każdego serwera. W dzienniku tym opisuje się wszystkie czynności podejmowane w ramach jego administrowania, w szczególności związane z bezpieczeństwem danych (wzór dziennika w załączniku nr 9).
2. Do instalacji i modyfikacji oprogramowania na serwerach uprawniony jest wyłącznie administrator systemów.
3. O konieczności instalacji lub modyfikacji oprogramowania na serwerach decyduje Informatyk.
4. Na serwerach może być instalowane tylko oprogramowanie, na które Urząd posiada licencję.
5. Oprogramowanie testowe może być instalowane wyłącznie na wydzielonych serwerach.
6. W szczególnych przypadkach dopuszcza się instalowanie na serwerze oprogramowania testowego, wyłącznie za pisemną zgodą Informatyka.
7. Oprogramowanie testowe, określone w ust. 6 odinstalowuje się bezzwłocznie po zakończeniu testowania.
8. Podczas prowadzenia testów oprogramowania określonego w ust. 6, praca systemu jest na bieżąco monitorowana przez administratora systemu.
9. Administrator systemu prowadzący, test oprogramowania określonego w ust. 6 informuje Informatyka o stwierdzonych nieprawidłowościach.

§48.

1. Instalowanie oprogramowania testowego i bezpłatnego dopuszcza się pod warunkiem:
   1) otrzymania zgody na instalację od Informatyka,
   2) dokonania tego wyłącznie na stacjach roboczych będących w bezpośredniej dyspozycji komórki Informatyki.
2. O instalacji powiadamia się Administratora Bezpieczeństwa Informacji.

§49.

Instalację lub modyfikację oprogramowania na serwerze lub stacji roboczej odnotowuje się na liście oprogramowania instalowanego.

§50.

1. Administrator Bezpieczeństwa Informacji prowadzi wykaz oprogramowania dopuszczonego do

używania w Urzędzie.

2. Kontroli podlega rodzaj oprogramowania oraz ilość licencji zakupionych przez Urząd.
3. Przed dopuszczeniem do zainstalowania oprogramowania testowego lub bezpłatnego Administrator Bezpieczeństwa Informacji sprawdza i nadzoruje legalność procesu instalacji oprogramowania.

§51.

Zabrania się użytkownikom dokonywania samodzielnej instalacji jakiegokolwiek oprogramowania. Instalacji oprogramowania dokonują wyłącznie pracownicy komórki Informatyki.

§52.

Na wszystkich komputerach w urzędzie dopuszcza się instalację tylko legalnego, licencjonowanego oprogramowania.

§53.

Wprowadza się następujące zasady korzystania z oprogramowania:

1. Oryginalne dokumenty licencyjne oraz nośniki każdego oprogramowania przechowywane są w komórce Informatyki w zamkniętej szafie. Nośniki oprogramowania nie mogą znajdować się w żadnym innym miejscu, a szczególnie nie mogą być kopiowane, wypożyczane lub w żaden sposób przekazywane osobom trzecim. Dotyczy to również kodów aktywacyjnych produktów.
2. Każdy z pracowników zobowiązany jest do podpisania karty użytkownika (wzór w załączniku nr 10).
3. Zabrania się użytkownikom wykonywania kopii oprogramowania.
4. Wszyscy pracownicy zobowiązani są do pracy na legalnym oprogramowaniu oraz otrzymują wyraźny zakaz instalacji i użytkowania oprogramowania pochodzącego ze źródeł innych niż komórka Informatyki.
5. Konieczne zakupy oprogramowania muszą być konsultowane z Informatykiem.
6. Do podstawowych obowiązków pracownika należy korzystanie z oprogramowania w związku z wykonywaniem obowiązków pracowniczych, zgodnie z obowiązującymi przepisami prawa oraz wyłącznie w celach wykonywania obowiązków pracowniczych. Zabrania się korzystania z jakiegokolwiek oprogramowania do którego urząd nie jest uprawniony, w czasie pracy, w miejscu pracy ani przy użyciu sprzętu Urzędu.

IX. Procedura i okres przechowywania nośników informacji, w tym kopii elektronicznych i wydruków.

§54.

1. Nośniki informacji, w tym kopie elektroniczne i wydruki zawierające dane nie mogą być dostępne dla osób nieuprawnionych.
2. Dane z magnetycznych nośników informacji usuwa się bezzwłocznie po ich wykorzystaniu służbowym, w sposób trwały.
3. Zabrania się sporządzania kopii baz danych na dyskach twardych stacji roboczych lub w folderach ogólnodostępnych w systemach Urzędu.

§55.

1. Użytkownik dokonujący wydruku jest właścicielem wytworzonego dokumentu.
2. Użytkownik dokonujący wydruku na drukarce sieciowej, zobowiązany jest udać się niezwłocznie do pomieszczenia usytuowania drukarki i przejąć drukowany dokument.
3. Kopie błędne, nadmiarowe czy z innych powodów niepotrzebne należy niezwłocznie zniszczyć.
4. Wydruki, które nie podlegają archiwizacji należy niezwłocznie zniszczyć.
5. Każdy pracownik, który napotka wydruk, nośnik elektroniczny, czy inny dokument pozostawiony bez dozoru jest zobowiązany zabezpieczyć go i przekazać Administratorowi Bezpieczeństwa Informacji.

§56.

1. Wydruki zawierające dane sporządzane w oparciu o systemy Urzędu podlegają szczególnej ochronie, a w szczególności niedopuszczalne jest:
   1) pozostawianie wydruków zawierających dane, z możliwością dostępu do nich osób nieuprawnionych,
   2) wyrzucania nieudanych lub próbnych wydruków do kosza.

X. Procedura i harmonogram dokonywania przeglądów i konserwacji systemów oraz zbiorów danych.

§57.

Przeglądu i konserwacji systemu i zbioru danych dokonuje administrator systemu.

§58.

1. Przegląd systemu polega na sprawdzeniu jego konfiguracji oraz sprawdzeniu logów systemowych, ze szczególnym uwzględnieniem logów bezpieczeństwa.
2. Przeglądu systemu dokonuje się codziennie.
3. W przypadku stwierdzenia nieprawidłowości w systemie, administrator systemu usuwa je, wykorzystując dostępne narzędzia i odnotowuje ten fakt w dzienniku pracy serwera (wzór w załączniku nr 9 do niniejszej Instrukcji).
4. Jeżeli stwierdzone nieprawidłowości wskazują na działanie osób nieuprawnionych w systemie, administrator systemu podejmuje czynności zgodnie z zapisami „Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych w Urzędzie".

§59.

1. Przegląd zbiorów danych polega na:
   1) sprawdzeniu dostępu do zbiorów danych na poziomie użytkowników o różnych prawach dostępu,
   2) ocenie stanu zbiorów danych,
   3) sprawdzeniu ustawień dostępu dla poszczególnych użytkowników.
2. Przeglądu zbiorów danych dokonuje się codziennie.
3. W przypadku stwierdzenia nieprawidłowości w stanie zbiorów danych lub naruszenia praw dostępu, administrator systemu powiadamia o zaistniałym fakcie Administratora Bezpieczeństwa Informacji, a następnie podejmuje działania zmierzające do usunięcia nieprawidłowości i zidentyfikowania osoby, która doprowadziła do ich powstania.
4. W przypadku wykrycia użytkowników nieuprawnionych, których działania mogły doprowadzić do: przeglądania, przenikania, wnioskowania, zniekształcania, powtarzania, wstawiania, niszczenia, kradzieży, modyfikacji, szpiegostwa, blokowania usług systemu, itp., administrator systemu podejmuje czynności zgodnie z zapisami „Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych w Urzędzie".

XI. Zasady wyposażania i eksploatacji stacji roboczych

§60.

1. Zasadność zakupu sprzętu komputerowego oraz oprogramowania podlega ocenie i akceptacji przez Informatyka.
2. Informatyk nadzoruje proces zakupu sprzętu komputerowego oraz oprogramowania.
3. Instalacja sprzętu komputerowego na stanowiskach pracy wykonywana jest przez pracowników komórki Informatyki.
4. Każdy z pracowników, którego stanowisko pracy zostało wyposażone w sprzęt komputerowy zobowiązany jest podpisać oświadczenie ze specyfikacją powierzonego sprzętu komputerowego oraz oprogramowania (wzór w załączniku nr 11).
5. Przeniesienia sprzętu do innych pomieszczeń wykonywane będą przez pracowników komórki Informatyki na wniosek Naczelnika Wydziału. Zabrania się samodzielnego przenoszenia sprzętu przez innych pracowników.
6. Zmiana osoby odpowiedzialnej za powierzony sprzęt musi być zgłoszona przez Naczelnika Wydziału do komórki Informatyki.
7. Użytkownicy ponoszą odpowiedzialność materialną za powierzony im sprzęt komputerowy.
8. Zasady korzystania przez pracowników z oprogramowania Urzędu zostały opisane w §53.

XII. Zasady wymiany informacji w sieci komputerowej

§61.

1. Użytkownik systemu Urzędu zobowiązany jest do prawidłowego rozpoczęcia i zakończenia pracy w systemie.
2. System Urzędu powinien być przygotowany do przekazywania informacji pomiędzy poszczególnymi komórkami organizacyjnymi i uprawnionymi podmiotami zewnętrznymi za pośrednictwem poczty elektronicznej z obowiązkiem szyfrowania.
3. Zabrania się wykorzystywania poczty elektronicznej do przekazywania dokumentów zawierających dane, bez kodu dostępu.

XIII. Postanowienia końcowe

§62.

Przestrzeganie postanowień niniejszej Instrukcji przez użytkowników systemów stanowi podstawę bezpiecznego posługiwania się systemami Urzędu.

§63.

Instrukcja nie może być wynoszona z obiektów Urzędu, powielana w części lub całości bez zgody Administratora Bezpieczeństwa Informacji.

§64.

1. Postanowienia niniejszej Instrukcji mogą być modyfikowane zarządzeniem Burmistrza wraz ze zmianami w systemach informatycznych Urzędu.
2. Propozycje zmian może składać pisemnie każdy pracownik Urzędu korzystając z drogi służbowej lub bezpośrednio do Administratora Bezpieczeństwa Informacji.

§65.

Administrator Bezpieczeństwa Informacji okresowo monitoruje przestrzeganie przez pracowników Urzędu zasad i przepisów ochrony danych osobowych.

§66.

W kwestiach nie uregulowanych niniejszą Instrukcją mają zastosowanie unormowania Regulaminu Pracy Urzędu, przepisy Kodeksu Pracy i Ustawy o ochronie danych osobowych wraz z aktami wykonawczymi.

XIV. Spis załączników

Załącznik nr 1 - Ewidencja baz danych w systemach informatycznych, w których przetwarzane są dane osobowe

Załącznik nr 2 - Ewidencja osób upoważnionych do przetwarzania danych osobowych w systemach informatycznych

Załącznik nr 3 - Wykaz miejsc przetwarzania danych osobowych w systemach informatycznych

Załącznik nr 5 – Indywidualny zakres czynności osoby zatrudnionej przy przetwarzaniu danych osobowych

Załącznik nr 6 – Upoważnienie do obsługi systemu informatycznego w zakresie przetwarzania danych osobowych

Załącznik nr 7 – Protokół zniszczenia kopii bezpieczeństwa / innych nośników zawierających dane osobowe

Załącznik nr 8 – Dziennik ewidencji kopii bezpieczeństwa

Załącznik nr 9 – Dziennik pracy systemu serwera

Załącznik nr 10 – Oświadczenie (odpowiedzialność za sprzęt komputerowy oraz oprogramowanie)

Załącznik nr 11 – Wniosek o założenie profilu/nadanie uprawnień/modyfikację uprawnień

BURMISTRZ

w.z.
mgr inż. Mariusz Witek
Zastępca Burmistrza