BIP Starostwa Powiatowego w Skarżysku-Kamiennej

Zarządzenie nr 80/2007

2008-01-14

ZARZĄDZENIE nr 80/2007
Starosty Powiatu Skarżyskiego
z dnia 4 grudnia 2007 roku
w sprawie: Polityki bezpieczeństwa i Instrukcji zarządzania i użytkowania systemów informatycznych oraz baz danych w zakresie wymogów bezpieczeństwa przetwarzania danych osobowych w Starostwie Powiatowym w Skarżysku-Kamiennej

Działając na podstawie art. 36 ust 2 Ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz.U. z 2004 r. nr 33 poz. 285 z późn. zm.) oraz § 3 ust. 3 Rozporządzenia MSWiA 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)zarządzam, co następuje:
§ 1
1.Ustalam Politykę bezpieczeństwa Starostwa Powiatowego w Skarżysku-Kamiennej stanowiącą załącznik nr 1 do niniejszego zarządzenia
2. Ustalam Instrukcję zarządzania i użytkowania systemów informatycznych oraz baz danych w zakresie wymogów bezpieczeństwa przetwarzania danych osobowych stanowiącą załącznik nr 2 do niniejszego zarządzenia
§ 2

Wykonanie zarządzenia powierzam Administratorowi Bezpieczeństwa Informacji
§ 3
Zarządzenie wchodzi w życie z dniem podpisania.

Starosta Powiatu Skarżyskiego

Jerzy Żmijewski

Załącznik Nr 1 do Zarządzenia Nr 80/2007
Starosty Skarżyskiego z dnia 4 grudnia 2007r.

POLITYKA BEZPIECZEŃSTWA
INFORMACJI

W ZAKRESIE PRZETWARZANIA DANYCH

OSOBOWYCH

w

STAROSTWIE POWIATOWYM W SKARŻYSKU-KAMIENNEJ

Skarżysko-Kamienna 2007 rok
SPIS TREŚCI

I. ZASADY OGÓLNE

§1.
Polityka Bezpieczeństwa danych osobowych zgodnie z wymogami obowiązujących w tym zakresie aktów prawnych określa bezpieczny sposób przetwarzania danych i dostępu do informacji zawierających dane osobowe w Starostwie Powiatowym w Skarżysku-Kamiennej.
§2.
Użyte w Polityce Bezpieczeństwa określenia oznaczają:
1. Starostwo - Starostwo Powiatowe w Skarżysku-Kamiennej,
2. Komórka organizacyjna - wydział lub komórki organizacyjna starostwa,
3. Dane osobowe - wszelkie informacje pozwalające zidentyfikować osoby fizyczne,
4. Przetwarzanie danych osobowych - gromadzenie, utrwalanie (przechowywanie), opracowywanie, zmienianie, udostępnianie i usuwanie danych osobowych, zwłaszcza systemach informatycznych,
5. Użytkownik - osoba upoważniona do przetwarzania danych osobowych,
6. Administrator systemu - osoba upoważniona do zarządzania systemem

informatycznym,
7. System informatyczny - system przetwarzania danych w Starostwie Powiatowym w Skarżysku-Kam. wraz z zasobami ludzkimi, technicznymi oraz finansowymi, który dostarcza i rozprowadza informacje,
8. Zabezpieczenie systemu informatycznego – to wdrożenie środków ochrony przed nieuprawnionym dostępem, modyfikacją, zniszczeniem oraz ujawnieniem lub pozyskaniem danych osobowych, a także stosowanych środków administracyjnych, technicznych w tym zakresie.

II. DEFINICJA BEZPIECZEŃSTWA INFORMACJI

§3.
1. Utrzymanie bezpieczeństwa przetwarzanych przez Starostwo informacji rozumiane jest jako zapewnienie ich poufności, integralności i dostępności na odpowiednim poziomie.
2. Pojęcia w odniesieniu do informacji i aplikacji:
1) Poufność informacji - rozumiana jako zapewnienie, że tylko uprawnieni pracownicy mają dostęp do informacji,
2) Integralność informacji - rozumiana jako zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania,
3) Dostępność informacji - rozumiane jako zapewnienie, ze osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne,
4) Zarządzanie ryzykiem - rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych.

III. ZAKRES

§4.
Politykę Bezpieczeństwa stosuje się do danych osobowych i wszystkich systemów informatycznych starostwa zawierających i przetwarzających te dane.

§5.
1. W systemie informacyjnym Starostwa przetwarzane są informacje służące do wykonywania zadań z zakresu administracji publicznej.
2. Informacje te są przetwarzane i składowane zarówno w postaci manualnej jak i elektronicznej.
§6.
1. Dokumenty Polityki Bezpieczeństwa Informacji mają zastosowanie do całego systemu informacyjnego Starostwa w szczególności do:
1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są informacje podlegające ochronie,
2) informacji będących własnością Starostwa lub klientów Starostwa, o ile zostały przekazane na podstawie umów,
3) wszystkich lokalizacji - budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie,
4) wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, konsultantów, stażystów i innych osób mających dostęp do informacji podlegających ochronie.
2. Do stosowania zasad określonych przez dokumenty Polityki Bezpieczeństwa zobowiązani są wszyscy pracownicy w rozumieniu Kodeksu Pracy, konsultanci, stażyści oraz inne osoby mające dostęp do informacji podlegających ochronie.

§7.
Informacje niejawne nie są objęte zakresem niniejszej Polityki.

IV. STRUKTURA DOKUMENTÓW POLITYKI BEZPIECZENSTWA INFORMACJI

§8.
1. Dokumenty Polityki Bezpieczeństwa Informacji ustanawiają metody zarządzania oraz wymagania niezbędne do zapewnienia skutecznej i spójnej ochrony przetwarzanych informacji.
2. Zestaw dokumentów Polityki Bezpieczeństwa Informacji składa się z:
1) Niniejszego dokumentu Polityki Bezpieczeństwa Informacji,
2) Instrukcji zarządzania systemami informatycznymi w zakresie wymogów bezpieczeństwa przetwarzania danych osobowych, opisującej sposób zarządzania systemami przetwarzania danych osobowych w Starostwie,
3) Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych, opisującej tryb postępowania w sytuacjach naruszenia zabezpieczenia zasobów danych osobowych, zaobserwowanych prób naruszenia tego zabezpieczenia, a także uzasadnionego podejrzenia o przygotowywanej próbie naruszenia.

V. DOSTĘP DO INFORMACJI

§9.
Wszystkie osoby, których rodzaj wykonywanej pracy będzie wiązał się z dostępem do danych osobowych, przed przystąpieniem do pracy, podlegają przeszkoleniu w zakresie obowiązujących przepisów prawa dotyczących ochrony danych osobowych oraz obowiązujących w Starostwie zasad ochrony danych osobowych.

§10.
Zakres czynności dla osoby dopuszczonej do przetwarzania danych osobowych powinien określać zakres odpowiedzialności tej osoby za ochronę danych osobowych w stopniu odpowiednim do zadań tej osoby realizowanych przy przetwarzaniu tych danych.

§11.
Udostępnianie danych osobowych podmiotom upoważnionym do ich otrzymania, na podstawie przepisów prawa, powinno odbywać się wg określonych odrębnymi przepisami procedur postępowania.

VI. ZARZĄDZANIE DANYMI OSOBOWYMI

§12.
Administratorem danych osobowych Starostwa jest Starosta Powiatu Skarżyskiego.

§13.
1. Za bezpieczeństwo danych osobowych Starostwa, odpowiadają
1) Administrator danych osobowych - Starosta Powiatu Skarżyskiego,
2) Administrator Bezpieczeństwa Informacji Starostwa.
2. Administrator Bezpieczeństwa Informacji Starostwa realizuje politykę bezpieczeństwa

informacji, ma prawo wydawać instrukcje regulujące kwestie związane z ochroną danych w strukturach Starostwa.
3. W umowach zawieranych przez Starostwo winny znajdować się postanowienia zobowiązujące podmioty zewnętrzne do ochrony danych udostępnionych przez Starostwo.

§14.
1. Obowiązki wynikające z ustawy o ochronie danych osobowych Starosta Powiatu Skarżyskiego powierza lokalnym administratorom danych, naczelnikom wydziałów w zakresie podległych im pracowników.
2. Naczelnicy komórek organizacyjnych Starostwa odpowiadają za realizację wymagań obowiązujących przepisów prawa, dotyczących ochrony danych osobowych z obowiązkiem współdziałania z Administratorem Bezpieczeństwa Informacji w tym zakresie.
3. Naczelnicy komórek organizacyjnych Starostwa zobowiązani są do zapoznania podległych pracowników z treścią, ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych {Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.) z Polityką Bezpieczeństwa Informacji w zakresie przetwarzania danych osobowych, Instrukcją zarządzania systemami informatycznymi w zakresie wymogów bezpieczeństwa przetwarzania danych osobowych oraz Instrukcją postępowania w sytuacji naruszenia ochrony danych osobowych.
4. Zapoznanie się z dokumentami określonymi w ust. 3 pracownicy Starostwa potwierdzają podpisem na indywidualnym zakresie czynności osoby zatrudnionej przy przetwarzaniu danych osobowych.

§15.
Ochrona zasobów danych osobowych Starostwa jako całości przed ich nieuprawnionym użyciem lub zniszczeniem jest jednym z podstawowych obowiązków pracowników Starostwa.

VII. ZAKRESY ODPOWIEDZIALNOŚCI.

§16.
Za bezpieczeństwo informacji odpowiedzialny jest każdy pracownik Starostwa.

§17.
Administrator bezpieczeństwa informacji w starostwie powiatowym w Skarżysku-Kam.:
1. odpowiada za realizacje. ustawy o ochronie danych osobowych w zakresie dotyczącym Administratora Bezpieczeństwa Informacji,
2. sprawuje nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których dane są. przetwarzane oraz kontrolą przebywających w nich osób,
3. określa strategię zabezpieczania systemów informatycznych starostwa,
4. sprawuje nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych,
5. sprawuje nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych na których zapisane są. dane osobowe,
6. identyfikuje i analizuje zagrożenia oraz ryzyko, na które narażone może być przetwarzanie danych osobowych w systemach informatycznych starostwa,
7. określa potrzeby w zakresie zabezpieczenia systemów informatycznych, w których przetwarzane są dane osobowe,
8. sprawuje nadzór nad bezpieczeństwem danych zawartych w komputerach przenośnych,

dyskach wymiennych, laptopach, w których przetwarzane są dane osobowe,
9. sprawuje nadzór nad obiegiem oraz przechowywaniem dokumentów i wydawnictw zawierających dane osobowe,
10. monitoruje działanie zabezpieczeń wdrożonych w celu ochrony danych osobowych w systemach informatycznych,
11. sprawuje nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane oraz kontrolę dostępu do danych,
12. opiniuje wniosek naczelnika wydziału o przyznaniu danemu użytkownikowi identyfikatora oraz praw dostępu do informacji chronionych w danym systemie przetwarzania,
13. powiadamia administratora systemu o konieczności utworzenia identyfikatora użytkownika w systemie oraz zmianie/nadaniu uprawnień dostępu użytkownika do systemu,
14. prowadzi ewidencje. baz danych w systemach informatycznych, w których przetwarzane są dane osobowe,
15. prowadzi ewidencję osób zatrudnionych przy przetwarzaniu danych osobowych w systemach informatycznych,
16. prowadzi ewidencję miejsc przetwarzania danych osobowych w systemach informatycznych,
17. prowadzi rejestr zbiorów danych osobowych starostwa (przetwarzanych metodą tradycyjna lub w systemach informatycznych).

§18.
Lokalni administratorzy danych osobowych zobowiązani są. do przestrzegania wszystkich przepisów ustawy o ochronie danych, w szczególności poprzez:
1. określanie indywidualnych obowiązków i odpowiedzialności osób zatrudnionych przy przetwarzaniu danych osobowych, wynikających z ustawy o ochronie danych osobowych,
2. zapoznawanie osób zatrudnionych przy przetwarzaniu danych osobowych z przepisami obowiązującymi w tym zakresie,
3. wykonywania zaleceń Administratora Bezpieczeństwa Informacji Starostwa Powiatowego w Skarżysku-Kam. w zakresie ochrony danych osobowych,
4. wdrażanie i nadzorowanie przestrzegania Polityki bezpieczeństwa informacji,
5. wdrażanie i nadzorowanie przestrzegania instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
6. działanie zgodnie z instrukcją postępowania w sytuacji naruszenia ochrony danych osobowych,
7. stwarzanie warunków organizacyjnych i technicznych umożliwiających spełnienie wymogów wynikających z obowiązywania ustawy o ochronie danych osobowych,
8. odpowiedzialność za poprawność merytoryczną danych gromadzonych w systemach informacyjnych,
9. określanie, które osoby i na jakich prawach mają dostęp do danych informacji,
10. przygotowanie zgłoszeń rejestracji Zbiorów Danych do Generalnego Inspektoratu Danych Osobowych, jeżeli mają one charakter danych osobowych i przekazanie do Administratora Bezpieczeństwa Informacji. Praca Lokalnych Administratorów Danych Osobowych jest nadzorowana pod względem bezpieczeństwa przez Administratora Bezpieczeństwa Informacji.

§ 19
Administrator Systemu Informatycznego odpowiedzialny jest za:
1. bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz

baz danych,
2. optymalizacje wydajności systemu informatycznego baz danych,
3. instalacje i konfiguracje sprzętu sieciowego i serwerowego,
4. instalacje i konfiguracje oprogramowania systemowego, sieciowego i oprogramowania bazodanowego,
5. konfiguracje i administrację oprogramowaniem systemowym, sieciowym oraz bazodanowym zabezpieczającym dane chronione przed nieupoważnionym dostępem,
6. współpracę z dostawcami usług oraz sprzętu sieciowego i serwerowego oraz zapewnienie zapisów dotyczących ochrony danych osobowych,
7. zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego, sieciowego,
8. zarządzanie kopiami awaryjnymi danych w tym danych osobowych oraz zasobów umożliwiających ich przetwarzanie,
9. przeciwdziałanie próbom naruszenia bezpieczeństwa informacji,
10. przyznawanie na wniosek Lokalnego Administratora Danych, za zgodą Administratora Bezpieczeństwa Informacji ściśle określonych praw dostępu do informacji w danym systemie,
11. wnioskowanie do Administratora Bezpieczeństwa Informacji w sprawie procedur bezpieczeństwa i standardów zabezpieczeń,
12. zarządzanie licencjami, procedurami ich dotyczącymi,
13. prowadzenie profilaktyki antywirusowej.
Praca Administratorów Systemów Informatycznych jest nadzorowana pod względem bezpieczeństwa przez Administratora Bezpieczeństwa Informacji.

VIII. PRZETWARZANIE DANYCH OSOBOWYCH

§20.
Systemy informatyczne służące do przetwarzania danych osobowych, muszą spełniać wymogi obowiązujących aktów prawnych regulujących zasady gromadzenia i przetwarzania danych osobowych.

§21.
Do tworzenia kopii bezpieczeństwa danych osobowych w postaci elektronicznej służą indywidualne systemy archiwizowania dla poszczególnych systemów przetwarzania.

§22.
Kopie bezpieczeństwa oraz dokumenty papierowe zawierające dane osobowe przechowuje się w warunkach uniemożliwiających dostęp do nich osobom nieuprawnionym.

IX. ARCHIWIZOWANIE INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE

§23.
Zasady archiwizacji i brakowania dokumentów reguluje Rozporządzenie Ministra Kultury z dnia 16 września 2002 r. w sprawie postępowania z dokumentacją zasad jej klasyfikacji i kwalifikowania oraz zasad i trybu przekazywania materiałów archiwalnych do archiwów państwowych (Dz. U. Nr 167, poz. 1375).

Załącznik nr.2 do Zarządzenia nr 80/2007
Starosty Skarżyskiego z dnia 4 grudnia 2007r.

INSTRUKCJA ZARZĄDZANIA I UŻYTKOWANIA SYSTEMÓW INFORMATYCZNYCH ORAZ BAZ DANYCH

W ZAKRESIE WYMOGÓW BEZPIECZEŃSTWA

PRZETWARZANIA DANYCH OSOBOWYCH

w

STAROSTWIE POWIATOWYM W SKARŻYSKU-KAMIENNEJ

SKARŻYSKO-KAMIENNA 2007 rok SPIS TREŚCI str. Postanowienia ogólne 3

I . POSTANOWIENIA OGÓLNE

§1.
Instrukcja określa procedury zarządzania systemami informatycznymi w zakresie przetwarzania danych osobowych, zwanych dalej danymi, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji w Starostwie Powiatowym w Skarżysku-Kam. zwanym dalej Starostwem.
1. Zawarte w instrukcji procedury mają na celu podniesienie poziomu bezpieczeństwa systemów informatycznych oraz określenie odpowiedzialności pracowników Starostwa za prawidłowe działanie tych systemów i bezpieczeństwo przetwarzanych w nim danych.
2. Instrukcja pozwala stosować ujednolicone zasady ochrony danych w systemach i sieciach informatycznych Starostwa.

§ 2.
Instrukcja w szczególności zawiera:
1. Procedurę rozpoczęcia i zakończenia pracy w systemach informatycznych,
2. Procedurę przydziału haseł dla użytkowników i częstotliwość ich zmiany.

3. Zasady rejestrowania i wyrejestrowywania użytkowników .
4. Metody oraz harmonogram tworzenia kopii bezpieczeństwa,
5. Procedurę 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.
Użyte w instrukcji terminy i określenia 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. Starostwo - Starostwo Powiatowe w Skarżysku-Kam,
4. Komórka organizacyjna - odpowiednio komórki organizacyjne Starostwa.
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 - Starosta Powiatu Skarżyskiego,
7. ABI - Administrator Bezpieczeństwa Informacji,
8. Administrator systemu - osoba zarządzająca bieżącą pracą systemu informatycznego i zbiorami danych w Starostwie Powiatowym w Skarżysku.
9. Systemy informatyczne Starostwa 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 Starostwa, 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 Starostwa - wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym pozyskiwaniem, gromadzeniem i przetwarzaniem,
13. Użytkownik - użytkownik systemu informatycznego czyli:
1. osoba zatrudniona przy przetwarzaniu danych w Starostwie, która posiada upoważnienie do obsługi systemu oraz urządzeń wchodzących w jego skład, a także osoba przetwarzająca dane w toku wykonywania umowy cywilnoprawnej zawartej ze Starostwem (np. umowy zlecenia, umowy o dzieło, itp.),
2. pracownik innego podmiotu, który świadczy usługi związane z pracą, w systemie Starostwa na podstawie odrębnych umów z tym podmiotem (np. serwis, zlecenie przetwarzania danych, itp.),
14. Gromadzenie danych - zbieranie danych (bazy danych) na nośnikach elektronicznych oraz wydrukach danych.

§ 4.
Za bezpieczeństwo danych osobowych Starostwa, odpowiadają:
1. Administrator Danych Osobowych - Starosta Powiatu Skarżyskiego,
2. Administrator Bezpieczeństwa Informacji Starostwa.

§ 5.
Ochrona zasobów danych Starostwa jako całości, przed ich nieuprawnionym użyciem lub zniszczeniem jest jednym z podstawowych obowiązków każdego pracownika Starostwa. Muszą zatem być przestrzegane zasady i obowiązki w tym zakresie tzn.:
1. Osoby zatrudnione przy przetwarzaniu danych (także poza systemami) są zobowiązane do szczególnej dbałości o zachowanie poufności i dostępu do danych gromadzonych: w bazach danych, kartotekach, skorowidzach itp.
2. Obowiązkiem każdego pracownika Starostwa jest zachowanie tajemnicy służbowej, w tym ochrony danych osobowych gromadzonych i przetwarzanych przez Starostwo. Obowiązek ten istnieje również po ustaniu zatrudnienia.

§ 6.
Obowiązki wynikające z ustawy o ochronie danych osobowych Starosta Powiatu Skarżyskiego powierza administratorom systemów oraz naczelnikom wydziałów w zakresie podległych im pracowników.

§ 7.
1. Obszary przetwarzania danych w obiektach i pomieszczeniach Starostwa 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 tradycyjnych kartotek należy w nich stosować szczególne środki ostrożności, w tym:
1) monitory powinny być usytuowane tak, aby ekrany były niewidoczne dla osób nieuprawnionych,
2) 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,
5) drukarki i urządzenia peryferyjne powinny być usytuowane tak, aby znajdowały się z dala od przestrzeni, po której poruszają się osoby nieuprawnione,
6) naczelnicy komórek organizacyjnych określą szczegółowe zasady: wzywania pomocy przez pracownika w przypadku bezpośredniego zagrożenia ich życia lub zdrowia, próby pozyskania danych osobowych oraz w szczególnych przypadkach ogłoszenia alarmu.

§ 8.
Systemy informatyczne w Starostwie powinny wymuszać autoryzację osoby przystępującej do pracy na zbiorach danych osobowych.

§ 9.
Odpowiedzialność za ochronę danych zawartych na komputerach przenośnych oraz innych przenośnych

urządzeniach umożliwiających gromadzenie danych, spoczywa wyłącznie na dysponentach tych urządzeń. Minimalnym wymaganym zabezpieczeniem każdego komputera PC w Starostwie jak również komputera przenośnego jest ograniczenie dostępu do tego komputera hasłem (hasło na BIOS, Windows, wygaszacz ekranu).

§ 10.
1. Dane wyeksportowane z systemu do komputera lokalnego lub przenośnego 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.
Wszelkie informacje zawierające dane, udostępniane podmiotom zewnętrznym Starostwa, mogą zostać przekazane tylko za pośrednictwem kancelarii ogólnej Starostwa, w której odnotowywany jest zakres podmiotowy i przedmiotowy udostępnienia. W uzasadnionych przypadkach dane mogą, być przesyłane drogę 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 lub Głównego Specjalisty ds. Informatyzacji,
4) logowania się w systemie jako inny użytkownik,
5) samodzielnego wgrywania oprogramowania,
6) wynoszenia dokumentacji w tym nośników elektronicznych zawierających dane, poza obszar jednostki organizacyjnej,
7) instalowania na komputerach starostwa 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 łamiącym zabezpieczenia programów przed nielegalnym kopiowaniem, korzystania z „czatów" internetowych, ściągania plików muzycznych oraz filmów.
2. Odwiedzanie stron internetowych jest monitorowane przez komórkę informatyki starostwa.
3. Identyfikator i hasło osoby, która utraciła uprawnienia do korzystania z systemu należy bezzwłocznie unieważnić.
4. Identyfikator osoby, która utraciła uprawnienia i została wyrejestrowana z systemu nie może być przydzielony innej osobie.
5. Dostęp do poszczególnych elementów systemów bazodanowych powinien być realizowany tylko w zakresie określonym nadanymi uprawnieniami, po wydaniu upoważnienia użytkownikowi.

§ 13.
1. Osoby zatrudnione w Starostwie potwierdzają własnoręcznym podpisem zapoznanie się z instrukcją dotyczącą przetwarzania danych osobowych.
2. Osoby zatrudnione w Starostwie podlegają, szkoleniu w zakresie ochrony danych, po którym otrzymują, upoważnienie do obsługi systemów informatycznych w zakresie przetwarzania danych.
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.
2) ewidencję osób upoważnionych do przetwarzania danych osobowych w systemach informatycznych.
3) ewidencję miejsc przetwarzania danych osobowych w systemach informatycznych i sposobu ich zabezpieczania,
4) rejestr zbiorów danych osobowych starostwa (przetwarzanych metodą tradycyjną lub w systemach informatycznych).
2. Naczelnicy wydziałów (lokalni administratorzy danych) zobowiązani są do przekazywania do administratora bezpieczeństwa informacji danych o nowych użytkownikach systemów lub zmianach dotyczących kont użytkowników.
3. O zamiarze wypowiedzenia umowy o pracę lub ustaniu stosunku pracy z osobą zatrudnioną w Starostwie, właściwa ds. pracowniczych komórka organizacyjna Starostwa powiadamia Administratora Bezpieczeństwa Informacji.
4. Administrator Bezpieczeństwa Informacji niezwłocznie powiadamia o faktach wynikających z ust. 3, osobą odpowiedzialną za nadawanie haseł i kodów dostępu. Kody dostępu i hasła są, likwidowane w ciągu 24 godzin od ustania uprawnień lub zatrudnienia.

Procedury i metody zapewniające bezpieczeństwo systemów informatycznych i baz danych.

I. Procedura rejestrowania i wyrejestrowywania użytkowników

§ 1.

1. Każdy pracownik Starostwa korzystający z systemu informatycznego lub innego oprogramowania rejestruje się jako użytkownik.
2. Niedopuszczalna jest praca w systemie na koncie innego użytkownika.

§2.

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

§3.

1. Nadawanie i rozszerzanie uprawnień użytkowników koordynuje Administrator Bezpieczeństwa

Informacji.
2. Administrator systemu w porozumieniu z Administratorem Bezpieczeństwa Informacji nadaje, nadzoruje i wycofuje uprawnienia.

§ 4.
Identyfikator użytkownika powinien spełniając 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.

II. Procedura budowy i przydziału haseł dla administratorów
systemów i użytkowników oraz częstotliwość ich zmiany.

§1.
Określa się następujące zasady tworzenia haseł.
1. hasło powinno mieć nie mniej niż 8 znaków,
2. hasło powinno 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 powinno 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.

§ 2.
Określa się następujące zasady korzystania z haseł:
1. nie wolno powtórnie używać hasła raz użytego,
2. hasło znane jest tylko użytkownikowi,
3. przy wpisywaniu hasta nie jest ono wyświetlane na ekranie,
4. użytkownik odpowiada za systematyczną zmianę haseł.

§ 3.
Niedopuszczalne jest:
1. jakiekolwiek notowanie hasła,
2. podawanie swojego hasła innym użytkownikom bądź osobom nieuprawnionym do pracy w systemie lub nie posiadającym uprawnień do przetwarzania danych.

§ 4.
1. Hasła w systemach Starostwa zmienia się nie rzadziej niż raz w miesiącu.
2. Powyższe zalecenie jest obowiązujące w Starostwie niezależnie od tego czy użytkownik przetwarza dane.

§ 5.
1. Administrator systemu tworzy i zmienia hasła zgodnie z zasadami określonymi w niniejszej instrukcji.

2. Hasła do serwerów lub aktywnych urządzeń sieci i istotnych programów konfiguracyjnych, administrator systemów umieszcza w zapieczętowanych kopertach i składa w obecności Administratora Bezpieczeństwa Informacji w w zabezpieczonej szafie (sejfie) .
3. Otwarcie koperty określonej w ust. 2 może nastąpić w przypadku:
1) kontroli przez Starostę (Głównego Specjalistę ds. Informatyzacji),
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 Główny Specjalista ds. Informatyzacji,
4) innych sytuacji nie określonych w Instrukcji postępowania za zgodą Administratora Danych.

§ 6.
1. Hasło lokalnego administratora stacji roboczych pozostaje w wyłącznej dyspozycji komórki Informatyki.
2. Zabrania się nadawania użytkownikom stacji roboczych uprawnień administratora stacji roboczej.

§ 7.
Na stacjach lokalnych (roboczych) winny działać procedury automatycznego wymuszania haseł przez zainstalowane tam systemy.

III. Procedura rozpoczęcia i zakończenia pracy w systemie informatycznym.

§ 1.
Postanowienia ogólne.

1. Każdy użytkownik zobowiązany jest racjonalnie korzystać ze wszystkich zasobów wspólnych, do których posiada dostęp (np. moc obliczeniowa, pojemność dysku, czas zajmowania zasobów przyporządkowanych różnym aplikacjom, sieci komputerowe) oraz przestrzegać zaleceń właściwych dla każdego stanowiska pracy.
2. Za podłączenie sprzętu do wewnętrznych oraz zewnętrznych sieci łączności, gniazd elektrycznych i logicznych itp. odpowiada administrator systemów. Dokonywanie jakichkolwiek zmian w istniejących podłączeniach przez użytkowników bez zgody administratora systemu jest zabronione.
2. Zabronione jest samowolne podłączanie urządzeń elektrycznych do instalacji zasilającej okablowania strukturalnego (sieci elektrycznej przeznaczonej do zasilania komputerów).Każdy użytkownik komputera (stacji roboczej) odpowiada za jego stan i bieżącą eksploatację.
3. Zabrania się przechowywania na dyskach lokalnych i sieciowych plików z danymi nie związanymi bezpośrednio z zakresem wykonywanych obowiązków służbowych.
4. Zabrania się korzystania z prywatnych nośników elektronicznych (dyskietki, CD, dyski zewnętrzne).
5. Za uruchamianie oraz wyłączanie serwerów odpowiedzialni są administratorzy systemów.

§ 2
1. Rozpoczynanie i kończenie pracy we wszystkich systemach informatycznych winno odbywać się zgodnie z zaleceniami administratorów systemów i naczelników komórek organizacyjnych.
3. Każdy użytkownik przed rozpoczęciem pracy w systemach informatycznych zobowiązany jest do zapoznania się z właściwymi podręcznikami lub instrukcjami (opracowanymi dla tych systemów).
4. Użytkownik systemu informatycznego Starostwa musi być zarejestrowany przez administratora

systemu jako użytkownik odpowiedniej aplikacji.
5. Włączając komputer (w celu podjęcia pracy) użytkownik dokonuje autoryzacji zgodnie z poleceniami wydawanymi przez system komputerowy ukazującymi się na ekranie monitora.
6. W przypadku pojawienia się trudności w autoryzacji, pomimo prawidłowo wykonanych czynności, użytkownik zobowiązany jest skontaktować się z administratorem systemu.
7. W wypadku konieczności odejścia od komputera należy zablokować możliwość jego użytkowania. Jeżeli nie ma możliwości zablokowania komputer należy wyłączyć.
8. Po zakończeniu pracy należy wylogować się z aplikacji oraz systemu operacyjnego (zamknąć uruchomione aplikacje) następnie zamknąć system operacyjny (wyłączyć komputer) . Komputera nie należy wyłączać, jeżeli są takie zalecenia administratora sieci (systemu).

IV. Obszary przetwarzania danych

§ 1.
W celu zapewnienia bezpiecznych warunków przetwarzania danych w systemach Starostwa 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 sie informatyczne urządzenia wyjścia (np. monitory, drukarki itp.).

§ 2.
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.
Wydzielona część pomieszczenia określona jako obszar przetwarzania danych powinna spełniać następujące warunki;
1. wyposażenie (meble) w tej części pomieszczenia musza, 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.

§ 4.
1. Lokalni Administratorzy Danych (Naczelnicy komórek organizacyjnych Starostwa), sporządzają imienne wykazy pracowników swojej komórki organizacyjnej aktualnie zatrudnionych przy przetwarzaniu danych.
2. Lokalni Administratorzy Danych (Naczelnicy komórek organizacyjnych Starostwa) wykazy określone w ust. 1 przekazują Administratorowi Bezpieczeństwa Informacji.
3. Zmiany dotyczące osób przetwarzających dane Naczelnicy komórek organizacyjnych Starostwa przekazują do dnia 15-go każdego miesiąca wg stanu na miesiąc poprzedni Administratorowi Bezpieczeństwa Informacji.

§ 5.
Nadzór nad przestrzeganiem zasad ochrony przetwarzanych danych sprawuje Administrator Bezpieczeństwa Informacji.

V. Opis metod i harmonogram sporządzania kopii bezpieczeństwa

§ 1.
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 Starostwa.
3. Odtwarzania dokonuje administrator systemu.

§ 2.
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 lub szafie odpowiednio zabezpieczonej.
3. Dostęp do kopii bezpieczeństwa może posiadać wyłącznie administrator systemu, a w razie jego nieobecności: Administrator Bezpieczeństwa Informacji oraz Administrator Danych Starostwa.

§ 3.
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 w porozumieniu z Administratorem Bezpieczeństwa Informacji. Z wykonanych czynności sporządza się protokół zniszczenia.

§ 4.
Opisu czynności sporządzania, okresowego sprawdzania. niszczenia kopii bezpieczeństwa, jak też odtwarzania danych z tych kopii, dokumentuje się w ,,Ewidencji kopii bezpieczeństwa', która przechowywana jest przez administratora systemu.

§ 5.
Nadzór nad procesem sporządzania, przechowywania i niszczenia kopii bezpieczeństwa sprawuje Administrator Bezpieczeństwa Informacji.

§ 6.
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.

§ 7.
Metoda i częstotliwość tworzenia awaryjnych kopii danych;
1. Pełna kopia zabezpieczająca plików aplikacji i bazy danych systemów wykonywana jest raz w tygodniu.
2. Przyrostowa (częściowa) kopia zabezpieczająca wykonywana jest codziennie.
3. Wykonane kopie powinny być odpowiednio opisane (nazwa serwera,

bazy danych, data)

§ 8.
Zobowiązuje się pracowników starostwa do zapisywania ważnych zasobów na dysku sieciowym.

VI. Procedura wykrywania i usuwania wirusów
w systemach informatycznych.

§ 1.
Procedura przeznaczona jest dla administratorów i użytkowników sieci informatycznej oraz indywidualnych stanowisk komputerowych Starostwa.

§ 2.
Ochrona antywirusowa realizowana jest przy użyciu stosowanego w Starostwie licencjonowanego oprogramowania antywirusowego, zwanego dalej oprogramowaniem. Oprogramowanie antywirusowe instalowane jest na:
1) wszystkich stacjach roboczych,
2) wyznaczonych serwerach..
§ 3.
Administrator systemu dokonuje instalacji i konfiguracji oprogramowania antywirusowego zgodnie z posiadanymi licencjami oraz zachowaniem zasad maksymalnego bezpieczeństwa

§ 4.
Administrator sprawuje kontrolę nad poprawnością funkcjonowania oprogramowania antywirusowego oraz nadzoruje proces automatycznej aktualizacji oprogramowania.

§ 5.
Zaleca się, aby wszyscy użytkownicy zwracali uwagę na następujące objawy, które mogą świadczyć o obecności wirusów komputerowych:
1) nagłe spowolnienie pracy systemu,
2) nieoczekiwany restart komputera,
3) dziwne efekty dźwiękowe,
4) nieznane nowe pliki lub foldery,
5) znaczne zmniejszenie się wolnego miejsca na dysku,
6) pojawianie się komunikatów nie związanych bezpośrednio z
wykorzystywaną do pracy aplikacją.
7) inne podejrzane sytuacje.

§ 6.
Użytkownicy poczty elektronicznej zobowiązani są do zwrócenia szczególnej uwagi na wiadomości:
1) pochodzące od nieznanych nadawców,
2) zawierające dziwną treść,
3) zawierające załączniki z nieznanymi plikami.

Wiadomości takie mogą zawierać wirusy komputerowe i dlatego nie należy
otwierać zawartych w nich załączników ani przesyłać wiadomości innym
adresatom.

§ 7.
Dokumenty pakietu Microsoft Office zawierające makra mogą być uruchamiane jeżeli pochodzą z zaufanego źródła. W pozostałych przypadkach należy otworzyć dokument bez uruchamiania makra.

§ 8.
Administrator systemu zobowiązany jest do zapewnienia systematycznej aktualizacji programu antywirusowego.
Przypadki wykrycia w systemie wirusa komputerowego, który nie został usunięty automatycznie przez oprogramowanie użytkownik zobowiązany jest zgłaszać administratorowi. Użytkownik dokonuje zgłoszenia ustnie lub na piśmie administratorowi sieci (aplikacji) .

§ 9.
W przypadku wykrycia wirusa należy zwrócić uwagę na następujące zagadnienia:
1) Przed przystąpieniem do czynności usunięcia wirusa komputerowego administrator odłącza zawirusowane urządzenie od systemu informatycznego.
2) W przypadku stwierdzenia szczególnie groźnych lub trudnych do usunięcia wirusów lub innych istotnych problemów administrator systemu informuje Administratora Bezpieczeństwa Informacji.
3) Ponowne włączenie urządzenia do systemu informatycznego możliwe jest dopiero, gdy czynności naprawcze przyniosą pozytywny rezultat i powinno zostać wykonane przez administratora, który podjął czynności naprawcze.

§ 10.
Użytkownicy zobowiązani są do kontrolowania pod kątem obecności wirusów komputerowych wszystkich elektronicznych nośników informacji wpływających z zewnątrz do Starostwa. Informację na temat sposobu wykonania kontroli nośnika uzyskać można u administratora.

§ 11.
W przypadku stwierdzenia świadomego wprowadzenia wirusa do systemu informatycznego administrator systemu zobowiązany jest zgłosić ten fakt jako naruszenie bezpieczeństwa danych osobowych, zgodnie z zarządzeniem Starosty.

VII. Ogólne zasady i odpowiedzialność przy korzystaniu
i instalacji oprogramowania.

§ 1.
1. Administrator systemu odpowiada za dokumentowanie czynności technologicznych każdego serwera związane z bezpieczeństwem danych.
2. Do instalacji i modyfikacji oprogramowania na serwerach uprawniony jest wyłącznie administrator systemów.
3. O konieczności instalacji lub modyfikacji oprogramowania na serwerach decyduje Informatyk w porozumieniu z Głównym Specjalistą ds. Informatyzacji.
4. Na serwerach może być instalowane tylko oprogramowanie, na które Starostwo posiada licencje.
5. Dopuszcza się instalowania oprogramowania testowego na serwerze na czas wykonywania testu. Oprogramowanie to należy bezzwłoczne usunąć po zakończeniu testów. O instalacji powiadamia się Administratora Bezpieczeństwa Informacji.
6. Podczas prowadzenia testów oprogramowania określonego w ust. 5, praca systemu jest na bieżąco monitorowana przez administratora systemu.
7. Administrator Bezpieczeństwa Informacji prowadzi wykaz oprogramowania dopuszczonego do używania w Starostwie.
8. Kontroli podlega rodzaj oprogramowania oraz ilość licencji zakupionych przez Starostwo.
9. Przed dopuszczeniem do zainstalowania oprogramowania testowego lub bezpłatnego Administrator

Bezpieczeństwa Informacji sprawdza i nadzoruje legalność procesu instalacji oprogramowania.
10. Zabrania się użytkownikom dokonywania samodzielnej instalacji jakiegokolwiek oprogramowania. Instalacji oprogramowania dokonują wyłącznie pracownicy komórki Informatyki.
11. Na wszystkich komputerach w starostwie dopuszcza się instalacji tylko legalnego licencjonowanego oprogramowania.

§ 2.
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, którą przekazuje pracownikowi Główny Specjalista ds. Informatyzacji.
3. Zabrania sie 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 Głównym Specjalista ds. Informatyzacji.
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 Starostwo nie jest uprawnione
(w czasie pracy, w miejscu pracy ani przy użyciu sprzętu Starostwa).

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

§ 1.
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 ogólnodostępnych dyskach twardych stacji roboczych (folderach) w systemach Starostwa.

§ 2.
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.

§ 3.
Wydruki zawierające dane sporządzane w oparciu o systemy Starostwa 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, bez dokładnego ich zniszczenia.

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

§ 1.
Przeglądu i konserwacji systemu i zbioru danych dokonuje administrator systemu.

§ 2.
1. Przegląd systemu polega na sprawdzeniu jego konfiguracji oraz sprawdzeniu i logów systemowych, ze szczególnym uwzględnieniem logów bezpieczeństwa.
2. Przeglądu systemu dokonuje sie codziennie.
3. W przypadku stwierdzenia nieprawidłowości w systemie, administrator systemu usuwa je, wykorzystując dostępne narzędzia i odnotowuje ten fakt w dzienniku pracy serwera.
4. Jeżeli stwierdzone nieprawidłowości wskazują na działanie osób nieuprawnionych w systemie, administrator systemu podejmuje czynności zgodnie z zapisami określonymi w rozdziale XI niniejszej instrukcji.

§ 3.
1. Przegląd zbiorów danych polega na:
1) sprawdzeniu dostępu do zbiorów danych na poziomie użytkowników o różnych prawach dostępu,
2) ocenie stanu zbiorów danych.
2. Sprawdzeniu ustawień dostępu dla poszczególnych użytkowników.
3. Przeglądu zbiorów danych dokonuje sie wyrywkowo.
4. 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.
5. W przypadku wykrycia użytkowników nieuprawnionych, których działania mogły doprowadzić do: przeglądania, zniekształcania, powtarzania, wstawiania, niszczenia, kradzieży, modyfikacji, szpiegostwa, blokowania usług systemu, itp., administrator systemu podejmuje czynności zgodnie z zapisami rozdziału XI niniejszej instrukcji.

X. Zasady wymiany informacji w sieci komputerowej.

§ 1.
1. Użytkownik systemów informatycznych Starostwa zobowiązany jest do prawidłowego rozpoczęcia i zakończenia pracy w systemie.
2. System Starostwa powinien być przygotowany do bezpiecznego przekazywania informacji pomiędzy poszczególnymi komórkami organizacyjnymi i uprawnionymi podmiotami zewnętrznymi za pośrednictwem poczty elektronicznej z obowiązkiem szyfrowania.
Zabrania się wykorzystywania poczty elektronicznej do przekazywania informacji nie związanej z zagadnieniami służbowymi.

XI. Zasady postępowania w sytuacji naruszenia ochrony
danych osobowych.
§ 1.
Postanowienia ogólne.
1. Zasady dotyczą postępowania w sytuacji naruszenia ochrony danych osobowych gromadzonych i przetwarzanych zarówno w zbiorach informatycznych, jak i w zbiorach manualnych. Zasady stosuje się także w przypadku, gdy stwierdzono naruszenie zabezpieczeń sprzętu informatycznego, sieci

komputerowej, systemu alarmowego i zabezpieczenia pomieszczeń, w których przetwarzane są dane.
2. Przez naruszenie ochrony danych osobowych rozumie się niezgodne z przepisami ustawy o ochronie danych i rozporządzeń wykonawczych, przetwarzanie danych (zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie) oraz usuwanie (zmiana lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą).
3. Osobami bezpośrednio odpowiedzialnymi za zgodną z prawem ochronę danych osobowych i ich zabezpieczenie są:
- pracownicy upoważnieni do przetwarzania danych osobowych,
- naczelnicy komórek organizacyjnych,
- administrator bezpieczeństwa informacji – w przypadku naruszenia systemów informatycznych.
§ 2.
Tryb postępowania w sytuacji naruszenia ochrony danych osobowych.
1. Każdy pracownik, który podejmie wiadomość lub stwierdzi naruszenie ochrony danych osobowych, jest zobowiązany do natychmiastowego poinformowania o tym bezpośredniego przełożonego, a gdy dotyczy to danych utrwalonych w zbiorach informatycznych administratora bezpieczeństwa informacji (stosowny zapis w dzienniku ABI).
2. Gdy stan urządzeń, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci teleinformatycznej mogą wskazać na naruszenie zabezpieczenia tych baz, to fakt ten należy zgłosić administratorowi bezpieczeństwa informacji (stosowny zapis w dzienniku ABI).
3. Administrator bezpieczeństwa informacji razem z Naczelnikiem komórki organizacyjnej doraźnie usuwają przyczynę naruszenia systemu informatycznego, sprawdzają cały system i dokonują wpisu do dziennika ABI.
4. W przypadku naruszenia bezpieczeństwa danych osobowych w zbiorach naturalnych naczelnik komórki organizacyjnej sporządza protokół, który powinien zawierać:
- kto zgłosił, kiedy(data), o której godzinie,
- na czym polega naruszenie ochrony danych osobowych,
- zabezpieczone dowody naruszenia danych,
- propozycje wniosków co do dalszego trybu postępowania, w tym dotyczących zmiany systemu ochrony danych.
5. Protokół (dziennik ABI) przedstawia się niezwłocznie Administratorowi Danych Osobowych.
6. Administratorowi Danych Osobowych wdraża postępowanie wyjaśniające. Jeżeli stwierdzone zostanie naruszenie ochrony danych osobowych z winy pracownika wszczyna się postępowanie dyscyplinarne (wg odrębnych przepisów). Jeżeli naruszenie ochrony danych wyczerpuje znamiona przestępstwa określone w art. 49-52 i 54 ustawy sporządza się doniesienie (wniosek) do odpowiednich organów ścigania.
7. Administrator Bezpieczeństwa Informacji przeprowadza niezwłocznie analizę systemu i wprowadza dodatkowe zabezpieczenia w celu zmniejszenia zagrożenia i podatności systemu komputerowego na naruszenie bezpieczeństwa informacji.
XII. Postanowienia końcowe
§ 1.
Przestrzeganie postanowień niniejszej Instrukcji przez użytkowników systemów stanowi podstawę bezpiecznego posługiwania się systemami Starostwa.

§ 2.
Instrukcja nie może być wynoszona z obiektów Starostwa, powielana w części lub całości bez zgody Administratora Bezpieczeństwa Informacji.

§ 3.
1. Postanowienia niniejszej Instrukcji mogą być modyfikowane zarządzeniem Starosty wraz ze zmianami w systemach informatycznych Starostwa.

2. Propozycje zmian może składać pisemnie każdy pracownik Starostwa korzystając z drogi służbowej lub bezpośrednio do Administratora Bezpieczeństwa Informacji.

§ 4.
Administrator Bezpieczeństwa Informacji okresowo monitoruje przestrzeganie przez pracowników Starostwa zasad i przepisów ochrony danych osobowych.

§ 5.
W kwestiach nie uregulowanych niniejszą Instrukcją, mają zastosowanie unormowania Regulaminu Pracy Starostwa, przepisy Kodeksu Pracy i Ustawy o ochronie danych osobowych wraz z aktami wykonawczymi.

SPIS ZAŁĄCZNIKÓW:

1. Wniosek o wydanie uprawnienia użytkownikowi zasobów dostępnych na platformach systemowych.
2. Zgłoszenie wykrycia wirusa w systemie – raport.
3. Indywidualny zakres czynności osoby zatrudnionej przy przetwarzaniu danych osobowych.

Data wytworzenia : 2008-01-14 01:00, Autor : Starosta Skarżyski, Data publikacji : 2008-01-14 01:00, Osoba udostępniająca na stronie : Karina Wiśniewska, Data ostatniej modyfikacji : 2012-12-07 09:33, Osoba modyfikująca : Cezary Przeworski