Starosta Grodziski
WO.0065-35/10

Zarządzenie Nr .....3..... /2010

Starosty Grodziskiego

z dnia .30. grudnia 2010.....

w sprawie wprowadzenia i wdrożenia do stosowania procedur i instrukcji obowiązujących pracowników Starostwa pracujących w Systemie Informatycznym.

Na podstawie art. 34 ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (t.j. Dz. U. 2001 nr 142 poz. 1592 z późn. zmianami) oraz ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2002 r., Nr 101, poz. 926 ze zmianami) zarządzam co następuje:

§ 1

Wprowadza się następujące procedury korzystania z Systemu Informatycznego:

1. Procedurę rozpoczynania, zawieszania i kończenia pracy w Systemie Informatycznym.
2. Instrukcję korzystania ze sprzętu komputerowego
3. Procedurę zabezpieczenie systemu przed samoistnym zainstalowaniem i działaniem nieuprawnionego oprogramowania oraz osób trzecich.
4. Procedura tworzenia kopii zapasowych, ich przechowywania i niszczenia.

§ 2

Zarządzenie wchodzi z dniem 01.01.2011r.

STAROSTA
Marek Wieżbicki

Nie ma wad pod względem prawnym

PRAWNIK
Jan Morwiński

Załącznik 1.
do Zarządzenia Nr ..3./2010.....
Starosty Grodziskiego
z dnia .....30.12.2010.....

Procedura rozpoczynania, zawieszania i kończenia pracy w Systemie Informatycznym

Dokument przeznaczony jest do stosowania w Starostwie Powiatu Grodziskiego

Pomieszczenia, w których przetwarzane są dane osobowe muszą być zamykane na czas nieobecności osób w nich pracujących i w sposób uniemożliwiający dostęp do nich osób trzecich. Podczas nieobecności osób zatrudnionych przy informatycznym przetwarzaniu danych osobowych pomieszczenia, w których przetwarzane są dane, nie mogą być udostępniane osobom postronnym. Po wejściu należy sprawdzić stan pomieszczenia. W przypadku stwierdzenia śladów nieuprawnionego wejścia do pomieszczenia, należy postępować zgodnie z „Instrukcją postępowania w przypadku naruszenia bezpieczeństwa".

Przed rozpoczęciem pracy w systemie informatycznym należy:

1. upewnić się, że na stanowisku, na którym przetwarzane są dane osobowe ekran monitora jest tak ustawiony, aby osoby nieupoważnione nie miały dostępu do informacji na nich wyświetlanych,
2. włączyć komputer,
3. uwierzytelnić się w Systemie Informatycznym przy pomocy nazwy użytkownika i hasła,
4. po pozytywnym przejściu procesu uwierzytelnienia użytkownik uzyskuje prawo dostępu do SI.

Zasady zawieszania i wznawiania pracy w Systemie Informatycznym:

1. w przypadku przerwania pracy należy stosować wygaszacz ekranu blokowany hasłem,
2. stanowisko komputerowe z uruchomionym systemem lub aplikacją nie może pozostać bez kontroli pracującego na nim pracownika, zanim nie zacznie działać wygaszacz ekranu blokowany hasłem,
3. przed wznowieniem pracy należy wprowadzić odpowiednie hasło.

Zasady kończenia pracy w systemie:

1. użytkownik ma obowiązek zamykania sesji aplikacji, Systemu i wyłączania komputera po zakończeniu pracy,
2. przed opuszczeniem pomieszczenia dokumenty i nośniki informacji należy schować w zamkniętej szafie,
3. sprawdzić czy wszystkie urządzenia elektryczne zostały wyłączone, pozamykane na klucz wszystkie szafy oraz czy zamknięte zostały okna,
4. zamknąć drzwi na klucz.

5. Czas pracy na urządzeniach informatycznych jest tożsamy z godzinami pracy Starostwa, wynikającymi z Regulaminu Organizacyjnego Starostwa Powiatu Grodziskiego.
6. Na pracę na urządzeniach informatycznych poza godzinami pracy Starostwa konieczna jest zgoda Administratora Danych Osobowych - Starosty Powiatu Grodziskiego.

Załącznik 2.
do Zarządzenia Nr ...3/2010...
Starosty Grodziskiego
z dnia ...30.12.2010...

Instrukcja korzystania ze sprzętu komputerowego

Dokument przeznaczony jest do stosowania w Starostwie Powiatu Grodziskiego

I. Cel instrukcji

Celem instrukcji jest określenie zasad korzystania ze sprzętu komputerowego przez użytkowników Systemu Informatycznego w Starostwie Powiatu Grodziskiego.

II. Odpowiedzialność

Za przestrzeganie zasad, zawartych w instrukcji odpowiadają:
1. użytkownicy,
2. Administrator Systemu Informatycznego,
3. Administrator Bezpieczeństwa Informacji.

III. Zakres stosowania

Stosowanie instrukcji obowiązuje wszystkich użytkowników Systemu Informatycznego.

IV. Treść instrukcji

1. Sprzęt komputerowy przydzielany jest użytkownikowi na podstawie protokołu przekazania, który za potwierdzeniem odbioru, sporządzają pracownicy Wydziału Finansowego Starostwa.
2. Każdemu użytkownikowi nadawany jest - przez ASI - login (nazwa użytkownika) oraz hasło, na podstawie których następuje procedura uwierzytelnienia w SI.
3. Hasło użytkownika objęte jest tajemnicą i znane wyłącznie jego właścicielowi.
4.Użytkownik jest zobowiązany do zmiany hasła nie rzadziej niż raz w miesiącu, odpowiedzialność za zmianę hasła ponosi jego właściciel.
5. Użytkownika obowiązuje bezwzględny zakaz używania powierzonego mu sprzętu do celów innych niż służbowe.
6. Użytkownika obowiązuje bezwzględny zakaz instalowania własnego oprogramowania.
7. Używanie w Starostwie prywatnych nośników danych zawierających informacje niewiadomego pochodzenia powoduje zagrożenie SI:
- wirusami,
- koniami trojańskimi,
- robakami internetowymi.
7. Po zakończeniu pracy w Systemie Informatycznym użytkownik zobowiązany jest do wylogowania się.
8. Za powierzony sprzęt komputerowy i przestrzeganie zasad dotyczących korzystania z niego odpowiada użytkownik.

Załącznik 3
do Zarządzenia Nr 3/2010
Starosty Grodziskiego
z dnia ..... 30.12.2010 ....

Zabezpieczenie systemu przed samoistnym zainstalowaniem i działaniem nieuprawnionego oprogramowania

Dokument przeznaczony jest do stosowania w Starostwie Powiatu Grodziskiego

I. Cel procedury

Celem procedury jest określenie zasad zabezpieczenia Systemu Informatycznego Starostwa przed samoistnym zainstalowaniem i działaniem nieuprawnionego oprogramowania.

II. Odpowiedzialność

1. Za przestrzeganie zasad zawartych w procedurze odpowiadają:
   a. wszyscy pracownicy merytoryczni zatrudnieni w Starostwie Powiatu Grodziskiego,
   b. informatycy.

III. Zakres stosowania procedury

1. Procedurę stosuje się do wszystkich stanowisk komputerowych znajdujących się w sieci wewnętrznej Starostwa.

IV. Treść procedury

1. Program antywirusowy, skanowanie systemu:
a. na wszystkich komputerach znajdujących się w sieci wewnętrznej należy zainstalować oprogramowanie antywirusowe,
b. w przypadku wykrycia wirusa przez program, użytkownik powinien niezwłocznie zgłosić tę sytuację do Administratora Systemu Informatycznego oraz postępować zgodnie ze wskazaniami oprogramowania antywirusowego,
c. wprowadzenie informacji do sieci z nośnika zewnętrznego na stanowisku może mieć miejsce tylko po wcześniejszym zeskanowaniu tego nośnika właściwym programem antywirusowym.

2. Zabezpieczenie systemu przed nieuprawnionym dostępem:
   a. stosowanie haseł dostępu do komputerów i do systemu zgodnie z polityką bezpieczeństwa, min. 8 znaków z wykorzystaniem liter, cyfr i znaków specjalnych, np. #, $, %.
   b. diagnostyka systemu pod kątem naruszenia bezpieczeństwa oraz stabilności systemów z wykorzystaniem logów systemowych i aplikacyjnych.

3. Urządzenia zabezpieczające system przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej:
a. stosowanie zasilaczy bezprzerwowych do serwerów oraz komputerów zapisujących

przetwarzane dane,
b. stosowanie filtrów przeciwprzepięciowych do każdego stanowiska komputerowego.

4. Regularne, zgodnie z opracowaną procedurą wykonywanie kopii bezpieczeństwa danych.
5. Przechowywanie kopii w sposób uniemożliwiający ich zniszczenie równocześnie z systemem komputerowym.

Załącznik 4.
do Zarządzenia Nr 3/2010
Starosty Grodziskiego
z dnia 30.12.2010

Procedura tworzenia kopii zapasowych, ich przechowywania i niszczenia

Dokument przeznaczony jest do stosowania w Starostwie Powiatu Grodziskiego

I. Cel procedury

Celem procedury jest określenie zasad tworzenia kopii zapasowych umożliwiających pełne odtworzenie funkcjonalności Systemu Informatycznego.

II. Odpowiedzialność

Za przestrzeganie zasad wymienionych w procedurze odpowiadają osoby upoważnione przez Administratora Danych Osobowych, tj. Administrator Systemu Informatycznego i Informatyk.

III. Zakres i warunki stosowania

Procedurę stosuje się do Systemu Informatycznego, zainstalowanego w Starostwie Powiatu Grodziskiego.

IV. Treść Procedury

W celu zapewnienia bezpieczeństwa pracy Systemu Informatycznego i możliwości odtworzenia danych po wystąpieniu awarii, wprowadzony zostaje następujący harmonogram wykonywania poszczególnych kopii zabezpieczających:

1. Pełna kopia danych z serwerów Starostwa wykonywana jest pięć razy w tygodniu na taśmach magnetycznych, które przechowywane są 7 dni, a następnie ponownie nadpisywane. Kopia wykonywana jest automatycznie (przez zdefiniowany proces w oprogramowaniu do wykonywania kopii zapasowych). Obsługa procesu kopiowania polega na codziennej wymianie nośnika danych (taśmy magnetycznej) oraz kontroli poprawności wykonania kopii na serwer służący do wykonywania kopii zapasowych (backup'owy). Za nadzór nad tworzeniem kopii odpowiedzialni są Administrator Systemu Informatycznego i Informatyk.
2. Wykonywanie kopii danych zgromadzonych na komputerach użytkowników odbywa się za pomocą serwera usług katalogowych, a następnie zabezpieczane zostają poprzez tworzenie pełnych kopii z serwerów, o których mowa w punkcie 1.
3. W przypadku, gdy użytkownik nie jest objęty usługą katalogową sam zabezpiecza dane przetwarzane podczas pracy, poprzez kopiowanie ich na dysk CD - R, CD - RW, DVD, DVD - RW, pamięci przenośne USB lub inny nośnik umożliwiający zapis.-

Nośniki zabezpieczane są i przechowywane przez użytkownika do czasu wykonania następnych kopii. W przypadku, gdy kopiowane dane przestają być przydatne nośniki są niszczone lub nadpisywane nowymi danymi.

4. W celu zminimalizowania ryzyka utraty danych kopie należy wykonywać nie rzadziej niż raz na tydzień.
5. Za wykonywanie kopii danych odpowiedzialni są pracownicy Starostwa Powiatu Grodziskiego przetwarzający je.

V. Nadzór nad kopiami

1. Kopie danych są okresowo sprawdzane pod kątem ich przydatności – prawidłowości wykonania i możliwości odtworzenia.
2. Każda kopia opisana jest w sposób umożliwiający identyfikację danych na niej zapisanych, tj. na etykiecie nośnika w następujący sposób :

a. data wykonania kopii,
b. numer kolejny nośnika,
c. typ kopii: kopia pełna, przyrostowa,
d. nazwa jednostki organizacyjnej,
e. nazwa Systemu Informatycznego / zbioru danych.

3. Wykonanie kopii bezpieczeństwa Administrator Systemu Informatycznego odnotowuje w rejestrze tworzonych kopii bezpieczeństwa, prowadzonym w formie elektronicznej lub pisemnej.
4. Rejestr kopii bezpieczeństwa zawiera następujące informacje o nośniku:

a. data wykonania,
b. typ kopii,
c. oznaczenie Systemu Informatycznego / zbioru danych,
d. uwagi.

5. Nośniki danych wykorzystywane do sporządzania kopii posiadają określoną trwałość - ilość pojedynczych zapisów:

a. taśmy magnetyczne - około 50 cykli kopiowania,
b. dyski CD - RW, DVD – RW - około 1000 cykli kopiowania.

6. Inne nośniki służące do wykonywania kopii należy używać zgodnie z zaleceniami producenta.
7. Kopie serwerów produkcyjnych: serwer z aplikacjami Wydziału Finansowego, Elektronicznym Obiegiem Dokumentów, usług katalogowych z danymi użytkowników przechowywane są w metalowej, zamykanej szafie w serwerowni.
8. Taśmy z kopiami raz w tygodniu transportowane są do Wydziału Komunikacji, gdzie deponowane są w szafie metalowej.
9. Transport kopii, ze względu na dane osobowe, odbywa się w specjalnie przygotowanej do tego celu walizce, posiadającej odpowiednie zabezpieczenia chroniące przed kradzieżą.

VI. Niszczenie nośników.

1. W przypadku awarii uniemożliwiającej dalsze wykorzystywanie nośnika lub po przekroczeniu liczby dozwolonych cykli kopiowania na danym nośniku należy go zniszczyć.
2. W przypadku niszczenia nośników o dużej pojemności lub posiadających trwałe obudowy, tj. dysk twardy serwera, taśma magnetyczna Administrator Systemu Informatycznego w porozumieniu z Administratorem Bezpieczeństwa Informacji powołuje komisję, która dokonuje zniszczenia nośnika ***metodą gwarantującą uniemożliwienie odzyskania danych***:
    a. taśmy magnetyczne należy wyjąć z obudowy i zniszczyć w niszczarce poprzez rozdrobnienie.
    b. dyski twarde należy rozkręcić wyjąć z nich części zawierające dane (talerze) następnie zniszczyć je poprzez rozdrobnienie.

    Po zniszczeniu nośników o dużej pojemności lub posiadających trwałe obudowy sporządzany jest protokół przechowywany przez Administrator Systemu Informatycznego.
3. Płyty CD-R, CD-RW, DVD-R, DVD-RW, dyskietki należy zniszczyć w niszczarce poprzez rozdrobnienie.
4. Pamięci przenośne typu flesz należy zniszczyć poprzez rozdrobnienie, zgniecenie.

Mechaniczne zniszczenie jest metodą gwarantującą zniszczenie danych na nośnikach.