ZARZĄDZENIE NR 57/2009
STAROSTY TUCHOLSKIEGO
z dnia 4 grudnia 2009.

w sprawie wprowadzenia „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Starostwie Powiatowym w Tucholi"

Na podstawie Art.36 ust 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity opublikowany w Dz.U. 2002 r. nr 101 poz.926 ze zm.) w związku z §3 i §4 ust. 1 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100 poz.1024)

zarządzam, co następuje:

§ 1. 1. W celu uregulowania spraw związanych z ochroną danych osobowych zgodnie z wymaganiami wynikającymi z obowiązujących w tym zakresie przepisów wprowadzam **„Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Starostwie Powiatowym w Tucholi"**, stanowiącą załącznik do niniejszego zarządzenia.

2. Dokument, o którym mowa w § 1 ust. 1, obowiązuje wszystkich pracowników zatrudnionych w Starostwie Powiatowym przy przetwarzaniu tych danych.
3. Postanowienia polityki bezpieczeństwa, w których jest mowa o „pracownikach": stosuje się odpowiednio także do innych osób urzędowo upoważnionych przez Starostę do takiego dostępu do zbiorów danych osobowych, który umożliwia dokładniejsze zapoznanie się z tymi danymi, w szczególności do osób wdrażających i konserwujących systemy przetwarzania danych osobowych, osób odbywających w Starostwie aplikację lub praktykę zawodową albo szkolenie, studentów zbierających materiały do prac dyplomowych itp.

§2. Traci moc Zarządzenie Starosty Tucholskiego Nr 29/2005 z dnia 21 października 2005 r. w sprawie wprowadzenia „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Starostwie Powiatowym w Tucholi"

§3. Wykonanie zarządzenia powierza się Administratorowi Bezpieczeństwa Informacji.

§ 4. Zarządzenie wchodzi w życie z dniem podjęcia.

STAROSTA TUCHOLSKI
Piotr Mowiński

Załącznik nr 1 do Zarządzenia
Starosty Tucholskiego nr 57/2009
z dnia 4 grudnia 2009r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W STAROSTWIE POWIATOWYM W TUCHOLI

§1.

INFORMACJE OGÓLNE

Dane przetwarzane w systemie informatycznym Starostwa Powiatowego w Tucholi podlegają ochronie z uwagi na obowiązujące przepisy prawa. Zachowanie bezpieczeństwa systemów informatycznych i danych w nich przetwarzanych jest wspólnym obowiązkiem wszystkich użytkowników systemu informatycznego Starostwa. Niniejszy dokument reguluje sprawy ochrony danych osobowych zawartych w systemie informatycznym oraz zasady zabezpieczenia dokumentów elektronicznych eksploatowanych systemach informatycznych Starostwa Powiatowego w Tucholi.

1. Systemy informatyczne Starostwa Powiatowego w Tucholi służą jedynie do wykonywania zadań służbowych.
2. Dostęp do systemu informatycznego Starostwa Powiatowego w Tucholi jest przyznawany pracownikom wyłącznie na czas pozostawania w stosunku zatrudnienia. Zakres dostępu do zasobów informatycznych wynika z zakresu czynności pracownika.
3. Niedozwolone jest wykorzystywanie dostępu do przydzielonych im zasobów informatycznych w celach sprzecznych z obowiązującymi przepisami prawnymi. Dotyczy to szczególnie przepisów związanych z ochroną danych osobowych, dóbr osobistych oraz ochroną własności intelektualnych.
4. Służbowe informacje, dokumenty i korespondencja służbowa, które są przetwarzane w systemach informatycznych są własnością Starostwa Powiatowego w Tucholi. Przełożeni mają prawo zażądać udostępnienia ich treści.
5. Niniejszy dokument jest w szczególności zgodny z następującymi aktami prawnymi:

1) ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. Nr 101, z 2002 r., poz. 926),

2) ustawą o ochronie informacji niejawnych z dnia 22 stycznia 1999 r. (Dz. U. Nr 11, poz. 95 z późn. zm.),

3) rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024),

Odpowiednie zabezpieczenia, ochrona przetwarzanych danych oraz niezawodność funkcjonowania są podstawowymi wymogami stawianymi współczesnym systemom informatycznym. Dokument „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Starostwie Powiatowym w Tucholi", zwany dalej „Instrukcją", wskazujący sposób zabezpieczenia systemów informatycznych, przeznaczony jest dla osób zatrudnionych przy przetwarzaniu tych danych. „Instrukcja" obowiązuje wszystkich pracowników, stażystów i praktykantów odpowiednio pracujących lub odbywających praktykę w Starostwie Powiatowym w Tucholi.

Potrzeba jego opracowania wynika z § 3 rozporządzenia Prezesa Rady Ministrów z dnia 25 lutego 1999 roku w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych (Dz. U. Nr 18 póz. 162) oraz § 3 i 4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, póz. 1024).

1. „Instrukcja" określa w szczególności:

1) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności;

2) stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;

3) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;

4) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;

5) sposób, miejsce i okres przechowywania:

a)elektronicznych nośników informacji zawierających dane osobowe,

b) kopii zapasowych,

6) sposób zabezpieczenia systemu informatycznego przed działalnością złośliwego oprogramowania,

7) procedury w przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego,

8) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

3. Wykonywanie postanowień tego dokumentu ma zapewnić właściwą reakcję, ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa systemów oraz zapewnić właściwy tryb działania w celu przywrócenia bezpieczeństwa danych przetwarzanych w systemie informatycznym Urzędu.

4. Administrator Danych, którym jest Starosta, swoją decyzją wyznacza Administratora Bezpieczeństwa Informacji danych zawartych w systemach informatycznych Urzędu, zwanego dalej „Administratorem Bezpieczeństwa" oraz osobę upoważnioną do zastępowania „Administratora Bezpieczeństwa".

5. „Administrator bezpieczeństwa" realizuje zadania w zakresie ochrony danych, a w szczególności:

- ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach systemów informatycznych Urzędu,
- podejmowania stosownych działań zgodnie z niniejszą „Instrukcją" w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia danych znajdujących się w systemie informatycznym,
- niezwłocznego informowania Administratora Danych lub osoby przez niego upoważnionej o przypadkach naruszenia przepisów ustawy o ochronie danych osobowych,
- nadzoru i kontroli systemów informatycznych służących do przetwarzania danych osobowych i osób przy nim zatrudnionych.

6. Osoba zastępująca Administratora Bezpieczeństwa powyższe zadania realizuje w przypadku nieobecności Administratora Bezpieczeństwa.

7. Osoba zastępująca składa Administratorowi Bezpieczeństwa sprawozdanie z podejmowanych działań w czasie jego zastępstwa.

§2.

PRZYJMOWANIE I SZKOLENIE UŻYTKOWNIKA SYSTEMU INFORMATYCZNEGO STAROSTWA POWIATOWEGO W TUCHOLI

1. Szkolenie podstawowe dotyczące bezpieczeństwa danych informatycznych obejmuje wszystkich pracowników oraz osób nowoprzyjętych do pracy w Starostwie Powiatowym w Tucholi

2. Tematyka szkoleń obejmuje:

1) przepisy i instrukcje wewnętrzne dotyczące ochrony danych archiwizacji zasobów i przechowywania nośników, niszczenie wydruków i zapisów na nośnikach magnetycznych i optycznych

2) Zakresy obowiązków pracowników związanych bezpośrednio z bezpieczeństwem danych i ochroną systemów na poszczególnych stanowiskach.

Przyjęcie użytkownika do systemu informatycznego Starostwa Powiatowego w Tucholi polega na określeniu przez administratora bezpieczeństwa tożsamości osoby, nadaniu mu odpowiedniego loginu i hasła i wskazaniu odpowiednich uprawnień w systemie informatycznym. Login i hasło w zależności od wymagań ustalonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100 poz. 1024) ustala Administrator Bezpieczeństwa. Wszystkie loginy i hasła są przekazywanie ustnie. Użytkownik systemu nie może przekazywać innym osobom informacji o ww. uprawnieniach, hasłach, loginach itp. W czasie nieobecności pracownika uprawnienia, hasła i login do systemu muszą być przekazane ustnie osobie zastępującej danego pracownika.

Po wygaśnięciu zatrudnienia pracownika administrator danych oraz administrator bezpieczeństwa odnotowują wykreślenia użytkownika z systemu informatycznego Starostwa Powiatowego w Tucholi. Login i hasło takiego użytkownika są usuwane z systemu w sposób uniemożliwiający jego odtworzenie.

Rozpoczęcie pracy użytkownika w systemie/aplikacji następuje po poprawnym uwierzytelnieniu użytkownika (zalogowaniu się do systemu /aplikacji).

Zakończenie pracy użytkownika w systemie /aplikacji następuje po wykonaniu procedury zakończenia pracy (wylogowaniu się z systemu/aplikacji). Niedopuszczalne jest zakończenie pracy bez wykonania pełnej i poprawnej procedury zamknięcia lub przez wyłączenie napięcia zasilającego. Po zakończeniu pracy pracownik porządkuje swoje stanowisko pracy wyłączając możliwość dostępu osób nieupoważnionym. Rozpoczynanie i zakończenie pracy systemu i aplikacji musi być prowadzone zgodnie z instrukcją zawartą w dokumentacji sytemu/aplikacji.

§3.

ZABEZPIECZENIA

1. Za bieżące utrzymanie i prawidłową eksploatację systemów informatycznych stacji roboczej odpowiada użytkownik systemu. Wszelkie prace dotyczące instalacji, aktualizacji, rekonfiguracji, deinstalację systemów informatycznych mogą być przeprowadzone tylko przez Informatyka. W wyjątkowych sytuacjach ww. prace mogą być wykonane przez inną osobę za pisemną zgodą Informatyka.
2. Instalację nowego oprogramowania i poprawek (patchy) na serwerach Starostwa Powiatowego w Tucholi wykonuje Informatyk.
3. Instalację nowego oprogramowania oraz poprawek na osobistych komputerach PC może wykonywać informatyk. W przypadku samodzielnych instalacji, użytkownik musi powiadomić administratora i uzyskać jego pisemną zgodę na jej przeprowadzenie.
4. Informatyk starostwa zobowiązany jest do inwentaryzacji instalowanego oprogramowania.
5. Zakazuje się instalowania i używania oprogramowania:
    a) bez posiadania wymaganej przez producenta lub autora licencji
    b) pochodzącego z nieznanego źródła
    c) z nośników nie sprawdzonych programem antywirusowym
    d) utrudniającego pracę innym użytkownikom
    e) wpływającego negatywnie na pracę w sieci.

§4.

ZARZĄDZANIE HASŁAMI

1. W celu ochrony systemów informatycznych należy wykorzystać wchodzące w ich skład mechanizmy zarówno sprzętowe jak i programowe. Użytkownik systemu informatycznego starostwa musi posiadać własny identyfikator i hasło dostępu.
2. Niedopuszczalne jest korzystanie z tego samego identyfikatora i hasła przez więcej niż jednego pracownika.
3. Niedopuszczalne jest używanie tego samego hasła do kilku różnych kont.
4. Niedopuszczalne jest występowanie użytkowników sytemu nie chronionych hasłem.
5. Hasła wpisywane z klawiatury nie mogą pojawiać się w formie jawnej na ekranie monitorów. Wymagane są hasła składające się z co najmniej 8 znaków będących kombinacją dużych i małych liter, cyfr i znaków specjalnych.

6. Hasło nie powinno zawierać żadnych informacji, które można kojarzyć z użytkownikiem komputera np. nie może bazować na danych osobistych użytkownika tj. nazwisko, inicjały, imiona marka lub numer samochodu. Hasło również nie może być nazwą użytkownika systemu, nazwą własną rzeczy, (nawet pisanym wspak), datą i nie może posiadać odpowiednika znaczeniowego w języku polskim i popularnych językach obcych. Hasło nie może być sekwencją kolejnych liter z klawiatury np. :asdfghjk" lub qwertyui".
7. Hasła należy zmieniać nie rzadziej niż raz na 30 dni. W przypadku gdy istnieje podejrzenie, że hasło mogła poznać osoba nieupoważniona użytkownik zobowiązany jest do natychmiastowej zmiany hasła.
8. Hasła stanowią tajemnicę. Nie należy ich zapisywać ani udostępniać nikomu. Należy pamiętać, że każdy z użytkowników jest odpowiedzialny za operacje w systemach informatycznych wykonywane z użyciem identyfikatorów i haseł. Odchodząc od stacji roboczej użytkownik powinien zablokować stację roboczą np. poprzez hasło w wygaszaczu ekranu.

§5.

SIEĆ INTERNET

Internet jest jednym z ważniejszych mediów wykorzystywany do komunikacji pomiędzy jednostkami administracji publicznej oraz petentami urzędu. Jednocześnie jest jednym z głównych zagrożeń dla bezpieczeństwa systemu informatycznego. Dlatego zaleca się zachowanie szczególnej ostrożności przy pracy z wykorzystaniem sieci internet i ścisłe stosowanie się do poniższych zasad.

1. Zabronione jest korzystanie z usług dostępu do internetu, w sposób który narusza przepisy krajowe i międzynarodowe. Taki charakter ma na przykład naruszenie prywatności, praw autorskich, własności intelektualnej lub wszelkie użycie, które narusza prawa osób trzecich i/lub może służyć działalności przestępczej.
2. Internet jest siecią ogólnie dostępną, dlatego przy przesyłaniu danych służbowych za jego pośrednictwem zaleca się szyfrowanie informacji, w sposób uniemożliwiający ich odczytanie przez osoby niepowołane.
3. Dostęp do Internetu z sieci Starostwa Powiatowego w Tucholi może być realizowany tylko za pośrednictwem routera dostępowego. Zabronione jest używanie modemów podłączonych do komputerów pracujących w sieci, w celu zestawiania wyżej wymienionych połączeń. Modemy można wykorzystać jedynie do zestawiania bezpośrednich połączeń po uzyskaniu pisemnej zgody informatyka starostwa.

4. Zaleca się wyłączenie opcji zapamiętywania identyfikatorów, haseł i formularzy przez przeglądarki internetowe.
5. Korzystanie z serwisów i zasobów internetowych dozwolone jest w zakresie wykonywania zadań służbowych.
6. Zabrania się korzystania z usług internetu dla celów prywatnych. Wszelkie potrzeby prywatnego skorzystania z takich usług należy skonsultować z kierownikiem jednostki lub naczelnikiem wydziału i uzyskać zgodę.

§6.

KORESPONDENCJA ELEKTRONICZNA

1. Uprawnionymi do obsługi głównego konta ogólnego e-mail oraz elektronicznej skrzynki podawczej są osoby upoważnione przez Starostę Tucholskiego. Pozostałe konta służbowe o adresach imiennych pracowników starostwa obsługują osoby na których są założone konta. Korzystanie z kont służbowych imiennych dozwolone jest wyłącznie w zakresie wykonywania zadań służbowych.
2. Zabrania się otwierania załączników poczty elektronicznej pochodzącej od nieznanych nadawców.
3. Nie zaleca się otwierania podejrzanych lub nieznanych załączników, dokumentów elektronicznych np. z rozszerzeniami (exe, src, pif itp.).
4. Usługa poczty elektronicznej nie może być wykorzystywana do wysyłania wiadomości o charakterze komercyjnym, reklam handlowych, ogłoszeń petycji o próśb o podpisy oraz wiadomości politycznych i religijnych – do osób, które sobie tego nie życzyły.
5. Zabrania się odpowiadania na niechciane wiadomości (spam).
6. Dostęp do skrzynki na serwerze powinien odbywać się przez autoryzację hasłem.
7. Postępowanie z pocztą przychodzącą:
    a) drukować i składać na sekretariat starostwa wszystkie oficjalne pisma których nadawcą są:
        - jednostki organizacyjne Starostwa,
        - urzędy państwowe i samorządowe,
        - instytucje naukowe,
        - firmy i przedsiębiorstwa,
        - odbiorcy drewna,

- pozostałe instytucje oraz osoby prywatne bezpośrednio zwracające się do starostwa.

b) załączniki w formie plików można udostępnić właściwym pracownikom przez:
   - przeniesienie na ich serwer lokalny folder Company lub przesłać pocztą wewnętrzną.

§7.

SIEĆ LOKALNA

1. Zabrania się podłączania do sieci informatycznej Starostwa Powiatowego w Tucholi innych komputerów, pamięci USB i innych urządzeń informatycznych nie będących własnością starostwa bez pisemnej zgody Informatyka.
2. Dostęp zdalny do sieci Starostwa Powiatowego w Tucholi może być realizowany tylko z komputerów posiadających odpowiednie i właściwie skonfigurowane oprogramowanie. Minimalne wymagania dla komputerów określa każdorazowo informatyk.
3. Dostęp zdalny do sieci Starostwa Powiatowego w Tucholi wymaga pisemnej i elektronicznej autoryzacji wyznaczonej przez Informatyka.

§8.

OCHRONA ANTYWIRUSOWA

Należy stosować takie systemy zabezpieczające programy i bazy danych przed wirusami, które nie dopuszczają do zainfekowania a równocześnie posiadają możliwość wykrywania wirusów, trojanów, snifferów itp. już zagnieżdżonych w systemie, usuwają je i zabezpieczają przed wystąpieniem następnych.

Zmniejszenie ryzyka zarażenia wirusem systemów informatycznych wymaga przestrzegania następujących zasad:

1. Każdy komputer PC wpięty do sieci powinien posiadać aktywną ochronę antywirusową.
2. Skaner antywirusowy powinien pracować w trybie skanowania plików i poczty w czasie rzeczywistym.
3. Każdy program antywirusowy powinien posiadać aktualną bazę danych wirusów.
4. Użytkownikom nie wolno wyłączać programu ochrony antywirusowej. Program antywirusowy może wyłączyć jedynie administrator na czas przeprowadzania czynności konserwacyjnych wymagających takiego postępowania.

5. Nie można uruchamiać na komputerze dyskietek, płyt lub innych elektronicznych nośników informacji nieznanego pochodzenia (pochodzących z zewnątrz) bez uprzedniego sprawdzenia tych nośników za pomocą programu antywirusowego. W systemie informatycznym starostwa można używać pamięci USB wyłącznie zarejestrowane w metryczce stanowiska komputerowego.
6. Po każdej naprawie i konserwacji komputera należy stosować aktualnie najnowsze wersje programów antywirusowych.

§9.

POSTĘPOWANIE NA WYPADEK AWARII SYSTEMU

1. Każdą zauważoną awarię, „zawieszenie się" systemu oraz wszelkie niesprawne działanie komputerów PC oraz sprzętu peryferyjnego należy natychmiast zgłosić do Informatyka.
2. Wszelkie postępowanie w celu ustalenia ewentualnych przyczyn powstania awarii oraz zlikwidowania jej skutków lub „odwieszenia" systemu dokonuje Informatyk. Zabrania się wszystkim osobom podejmowania jakichkolwiek prób samodzielnej naprawy systemu lub sprzętu.

§10.

MONITOROWANIE ZABEZPIECZEŃ

1. Do monitorowania systemu zabezpieczeń, stosownie do swojego zakresu czynności zobligowani są:

a) Administrator Danych

b) Administrator Bezpieczeństwa Informacji

2. W ramach monitoringu należy przeprowadzać następujące działania:

a) okresowe sprawdzanie kopii bezpieczeństwa pod względem przydatności do odtworzenia danych,

b) kontrola ewidencji nośników magnetycznych i optycznych,

c) sprawdzania częstotliwości zmian haseł,

3. Administrator Bezpieczeństwa sporządza roczne plany kontroli zatwierdzone przez Administratora Danych i zgodnie z nimi przeprowadza kontrole oraz dokonuje kwartalnych ocen stanu bezpieczeństwa danych osobowych.

4. Na podstawie zgromadzonych materiałów, o których mowa w pkt. 3. Administrator Bezpieczeństwa sporządza roczne sprawozdanie i przedstawia Administratorowi Danych.

§11.

ARCHIWIZACJA DANYCH INFORMATYCZNYCH STAROSTWA (KOPIE BEZPIECZEŃSTWA)

1. Informatyk starostwa zobowiązany jest do tworzenia kopii bezpieczeństwa danych przetwarzanych w systemie informatycznym na serwerach starostwach i innych nośnikach danych. Serwery oraz poszczególne stacje robocze powinny być zabezpieczone urządzeniami podtrzymującymi zasilanie (UPS), co umożliwi funkcjonowanie systemu w przypadku awarii zasilania.
2. Informatyk tworzy następujące rodzaje kopii bezpieczeństwa:
   a) kopia wszystkich systemów operacyjnych, aplikacji i baz danych serwerów – wykonywana jest codziennie na dyskach twardych archiwizacyjnych serwera.
   b) kopia dokumentów elektronicznych stacji roboczych - wykonywana codziennie na serwerze oraz na taśmach streamera
   c) kopie partycji głównych i systemów operacyjnych (tzw. „lustra systemu" poszczególnych stacji roboczych - wykonywane są raz na pół roku na zewnętrzny dysk twardy.
3. Użytkownicy systemu informatycznego starostwa zobowiązani są do przechowywania własnych dokumentów elektronicznych typu pliki *.doc, *.xls., *.ppt itp wyłącznie w folderze Moje dokumenty. Powyższe pliki są automatycznie archiwizowane na serwery starostwa codziennie przy logowaniu i wylogowaniu systemów stacji roboczych. Pozostałe dokumenty elektroniczne i ustawienia systemowe stacji roboczej podlegają archiwizacji tylko w przypadku zgłoszenia tego Informatykowi. Takie zgłoszenie jest odnotowywane metryczce stanowiska komputera.
4. Kopie bezpieczeństwa powinny być regularnie (nie rzadziej niż raz na 30 dni) sprawdzane pod kątem ich przydatności do odtworzenia danych w przypadku awarii systemu.
5. Nośniki informacji na których są składowane informacje przechowuje się w innych pomieszczeniach niż pomieszczenia w których odbywa się przetwarzanie informacji. Kopia wszystkich danych informatycznych serwerów oraz pozostałe kopie bezpieczeństwa przechowywane są w sejfie ogniotrwałym. Ponadto informatyk przekazuje raz w miesiącu kopie bezpieczeństwa danych do innego budynku Starostwa tj. do Kancelarii Tajnej Starostwa.

§12.

NISZCZENIE WYDRUKÓW I ZAPISÓW NA NOŚNIKACH MAGNETYCZNYCH

1. Nośniki magnetyczne (dyski twarde, pamięci USB przekazywane na zewnątrz powinny być pozbawione zapisów zawierających dane osobowe i inne niepubliczne dokumenty elektroniczne. Niszczenie poprzednich zapisów powinno odbywać się poprzez nadpisanie informacji odpowiednim programem informatycznym.
2. Uszkodzone nośniki magnetyczne przed ich likwidację należy fizycznie zniszczyć (przeciąć, przełamać itp.).
3. Po wykorzystaniu wydruki komputerowe zawierające dane osobowe i inne niejawne informacje powinny być niszczone poprzez niszczarkę dokumentów odpowiedniej kategorii (DIN3).

§13.

ZABEZPIECZENIE POMIESZCZEŃ

1. Pomieszczenia, w których stoi serwer zawierający dane osobowe są zabezpieczone poprzez wzmocnione drzwi, okna z roletami antywłamaniowymi oraz system alarmowy i przeciwpożarowy.
2. Dostęp do komputerów, w których są przetwarzane dane osobowe powinien być ograniczony. Dodatkowo komputer taki powinien być usytuowany w taki sposób aby nie było możliwe przeczytanie wyświetlanych na monitorze danych przez osoby niepowołane.
3. Po zakończeniu pracy wszystkie pomieszczenia, w których przetwarza się te dane są zamykane. Klucze do pomieszczeń przechowuje się zgodnie z obowiązującymi w starostwie zasadami.

§14.

ZASADY POSTĘPOWANIA NA WYPADEK POŻARU, POWODZI, INNYCH KLĘSK ŻYWIOŁOWYCH.

1. Podstawowym obowiązkiem jest ratowanie życia i nie narażanie na utratę zdrowia pracowników.

2. Ważne nośniki informatyczne (taśmy, dyski, i inne nośniki informatyczne zawierające składowania systemów informatycznych, baz danych nośniki dystrybucyjne oprogramowania itp.) należy spakować w niepalne, wodoodporne pojemniki i niezwłocznie umieścić je Kancelarii Tajnej Starostwa lub jeśli jest to niemożliwe w bezpiecznym miejscu.
3. Jeśli pozwolą na to warunki – przenieść sprzęt komputerowy w bezpieczne miejsce.
4. Po naprawieniu szkód i odtworzeniu sprzętu komputerowego i oprogramowania informatycznego odtwarza się dane z zarchiwizowanych danych informatycznych pozwalające na ponowne podjęcie zadań starostwa.

§15.

ZASADY POSTĘPOWANIA NA WYPADEK KRADZIEŻY, ZNISZCZENIA SPRZĘTU.

W przypadku stwierdzenia kradzieży lub zniszczenia sprzętu należy:

1. Zabezpieczyć stanowisko pracy tak, aby uniemożliwić dalsze działania destrukcyjne (wyłączyć komputer, zamknąć pomieszczenie itp.)
2. Jeśli to możliwe zabezpieczyć ślady przestępstwa: opuścić pomieszczenie niczego nie dotykając, zastosować wszystkie dostępne środki ochrony pomieszczeń (kraty, zamki, system alarmowy, itp.)
3. Niezwłocznie powiadomić Informatyka i Naczelnika Wydziału lub Starostę Tucholskiego.

STAROSTA TUCHOLSKI
Piotr Mówiński