Niniejszy załącznik uwzględnia:
- zarządzenie (pierwotne) Nr 18/04 Starosty z 28.12.2004 r.
- zarządzenie zmieniające Nr 33/09 z 10.12.2009 r.
- zarządzenie zmieniające Nr 51/2011 z 25.10.2011 r.

Załącznik Nr 2
do Zarządzenia Nr 18/04
Starosty Toruńskiego
z dnia 28 grudnia 2004r.

INSTRUKCJA

określająca sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji, zwana dalej „instrukcją"

Spis treści:

Rozdział 1
Postanowienia ogólne

§ 1

1. „**Instrukcja zarządzania systemem informatycznym** w Starostwie Powiatowym w Toruniu", zwana dalej „**Instrukcją"**, opracowana została zgodnie z wymogami określonymi w § 5 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).
2. Niniejsza Instrukcja, jest wewnętrznym dokumentem wydanym przez Starostę Toruńskiego i przeznaczona jest dla osób zatrudnionych przy przetwarzaniu danych osobowych w Urzędzie oraz ich przełożonych, którzy nadzorują przetwarzanie danych osobowych.
3. Przestrzeganie postanowień niniejszej Instrukcji służyć ma zapewnieniu poufności, integralności, rozliczalności, dostępności i niezawodności przetwarzania danych w systemach.

§ 2

Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych musi zapoznać się z:

- ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.);
- Polityką bezpieczeństwa przetwarzania danych osobowych w Starostwie Powiatowym w Toruniu;
- niniejszą Instrukcją.

§ 3

Określenia i skróty użyte w Instrukcji oznaczają:

1) **Administrator Danych Osobowych,** zwany dalej **ADO –** Starostę Toruńskiego;
2) **Administrator Bezpieczeństwa Informacji**, zwany dalej **ABI –** osoba wyznaczona przez ADO, nadzorująca przestrzeganie zasad ochrony przetwarzanych danych osobowych oraz monitorowanie sytuacji zagrażających ich bezpieczeństwu. *Zadania ABI określa załącznik nr 1 do niniejszej instrukcji;*
3) **Lokalny Administrator Bezpieczeństwa Informacji,** zwany dalej **LABI** - rolę LABI pełnią Naczelnicy Wydziałów oraz pracownicy na samodzielnych stanowiskach pracy. Osoby te odpowiedzialne są za bezpieczeństwo zbiorów danych osobowych, w odniesieniu do zbiorów danych istniejących w danej komórce organizacyjnej, w których przetwarzana jest dana grupa informacji. *Zadania LABI określa załącznik nr 2 do niniejszej instrukcji;*
4) **Lokalny Administrator Bezpieczeństwa Informacji,** zwany dalej **LABI/AI –** Naczelnik Wydziału Organizacyjnego i Spraw Obywatelskich, odpowiedzialny za wdrażanie organizacyjnych środków ochrony danych osobowych przetwarzanych w systemach informatycznych bądź w sposób papierowy;
5) **Administrator Systemu Informatycznego**, zwany dalej **ASI –** osoba wyznaczona przez ABI, odpowiedzialna za zapewnienie ciągłości i poprawności działania systemu oraz wdrażanie technicznych środków ochrony przewidzianych w tych systemach. *Zadania ASI określa załącznik nr 3 do niniejszej instrukcji;*

5a) **Administrator Bezpieczeństwa Informacji PEFS 2007**, zwany dalej **ABI PEFS 2007 –** osoba wyznaczona przez ADO, odpowiedzialna za zbieranie i aktualizację danych, zarządzanie użytkownikami, zabezpieczanie oraz przekazywanie danych zawartych w formularzu PEFS na podstawie umów o dofinansowaniu poszczególnych projektów; [1)]

6) **Osoba upoważniona lub użytkownik systemu**, zwany dalej **użytkownikiem –** osoba posiadająca upoważnienie wydane przez ADO lub osobę upoważnioną przez niego i dopuszczona w zakresie w nim wskazanym, jako użytkownik do przetwarzania danych osobowych w określonym systemie informatycznym Urzędu. **Użytkownikiem** może być pracownik, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej bądź osoba odbywająca staż lub przygotowanie zawodowe w Urzędzie;
7) **Przełożony użytkownika**, zwany dalej **przełożonym –** Naczelnik Wydziału Urzędu;
8) **System informatyczny,** zwany dalej **systemem -** to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych wraz z pracownikami upoważnionymi do obsługi systemu, który dostarcza i rozprowadza informacje;
9) **Zabezpieczenie systemu informatycznego** – wdrożenie przez Administratora stosownych środków organizacyjnych i technicznych w celu zabezpieczenia zasobów oraz ochrony danych przed dostępem, modyfikacją ujawnieniem, pozyskaniem lub zniszczeniem przez osobę trzecią;
10) **Przetwarzanie danych osobowych** – wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza tych, które są wykonywane w systemach informatycznych.

Rozdział 2
Obowiązki pracownicze wynikające z ochrony danych osobowych

§ 4

1. Obowiązek przestrzegania tajemnicy danych osobowych dotyczy wszystkich pracowników, którzy mają dostęp do informacji o charakterze danych osobowych.
2. Naruszenie zasad ochrony danych osobowych, w efekcie którego nastąpiło udostępnienie danych osobie nie upoważnionej, jest ciężkim naruszeniem obowiązków pracowniczych.
3. Kierownicy komórek organizacyjnych Urzędu są zobowiązani do:
   1) zastosowania niezbędnych środków technicznych i organizacyjnych, określonych w przepisach powszechnie obowiązujących w celu zapewnienia ochrony przetwarzania danych osobowych;
   2) kontroli przestrzegania zasad i sposobu wykonywania operacji przetwarzania danych przez podległych pracowników;
   3) sygnalizowania niezgodności aktów prawnych oraz aktów wewnętrznych Urzędu z przepisami ustawowymi w zakresie ochrony danych osobowych;
   4) zwracania się do ABI, w przypadku istotnych wątpliwości co do stosowania przepisów prawnych z zakresu ochrony danych osobowych
4. Czynności przetwarzania danych osobowych może dokonywać jedynie pracownik upoważniony przez ADO, w zakresie indywidualnych obowiązków pracowniczych.
5. Osoba upoważniona przez ADO, jest zobowiązana do:
   1) zapoznania się z przepisami prawa w zakresie ochrony danych osobowych;
   2) stosowania określonych przez ADO procedur i środków, mających na celu zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym;
   3) zachowania szczególnej staranności w trakcie wykonywania operacji przetwarzania danych w celu ochrony interesów osób, których dane dotyczą;

[1)] Zm. zarządz. Nr 51/2011 z dnia 25.10.2011 r.

4) podporządkowanie się poleceniom przełożonego i przestrzegania ustalonych przez niego szczegółowych zasad i procedur.

Rozdział 3
Postępowanie przy upoważnianiu osób do przetwarzania danych osobowych

§ 5

1. W przypadku przyjęcia do pracy nowego pracownika, którego zakres obowiązków obejmować będzie przetwarzanie danych osobowych, bezpośredni przełożony obowiązany jest:
   a) zapoznać użytkownika z przepisami dotyczącymi ochrony danych osobowych, po zapoznaniu się z którymi użytkownik składa oświadczenie, *którego treść stanowi* ***załącznik nr 6*** ***do niniejszej instrukcji***;
   b) zwrócić się do ABI o wydanie wskazanej osobie upoważnienia do przetwarzania danych osobowych, w celu akceptacji – na wniosku, *którego treść stanowi* ***załącznik nr 4*** *do niniejszej Instrukcji*.
2. Wniosek o którym mowa w ust. 1 lit. b należy stosować odpowiednio w przypadku zmiany stanowiska bądź zakresu obowiązków pracowniczych, zmiany uprawnień w systemie albo odebrania uprawnień w systemie. W tych przypadkach przełożony komórki organizacyjnej i samodzielne stanowiska pracy zobowiązani są bezzwłocznie skierować wniosek o wydanie bądź cofnięcie upoważnienia administratora danych.
3. ABI w przypadku braku uwag przekazuje wniosek ze swoją adnotacją do LABI/AI, o którym mowa w § 3 pkt 4 w celu zapoznania użytkownika z przepisami o ochronie danych osobowych oraz przygotowania upoważnienia. Wykonując swe zadania współpracuje również z ASI.
4. LABI/AI odpowiedzialny za ochronę danych osobowych w zakresie wymogów o charakterze organizacyjnym:
   a) przygotowuje użytkownikowi upoważnienie do przetwarzania danych osobowych w zakresie określonym we wniosku przełożonego (*wzór upoważnienia w* ***załączniku nr 5*** ***do niniejszej instrukcji***);
   b) wpisuje dane użytkownika do „Ewidencji osób upoważnionych do przetwarzania danych osobowych", według *wzoru stanowiącego* ***załącznik nr 7*** ***do instrukcji;***
   c) podpisuje wniosek wraz z ASI;
   d) opracowuje projekty zarządzeń, instrukcji i wytycznych ABI dotyczących przetwarzania danych osobowych w Urzędzie;
   e) prowadzi korespondencję z Generalnym Inspektorem Ochrony Danych Osobowych.
5. Wypowiedzenie umowy o pracę jest równocześnie cofnięciem upoważnienia ADO do przetwarzania danych. W takiej sytuacji upoważnienie traci moc z datą rozwiązania umowy o pracę.
6. W postępowaniu przy upoważnianiu osób do przetwarzania danych osobowych zawartych w formularzach PEFS mają zastosowanie odrębne przepisy zawarte w obowiązującej wersji Instrukcji wypełniania formularza PEFS 2007 dla PO KL.[2)]

Rozdział 4
Postępowanie w przypadku utworzenia nowego zbioru danych osobowych

§ 6

1. W przypadku konieczności utworzenia nowego zbioru danych, wynikającej z obowiązków nałożonych przepisami ustawy, nowymi zasadami bądź też podpisanymi

[2)] Zm. zarządz. Nr 51/2011 z dnia 25.10.2011 r.

zobowiązaniami Naczelnik Wydziału i samodzielne stanowiska pracy zobowiązani są niezwłocznie – nie później niż w ciągu 7 dni – poinformować o tym fakcie ABI.[3)]

2. Informacja, o której mowa w ust. 1 powinna zawierać dane jak we wniosku dot. zgłoszenia zbioru danych do rejestracji, określonym rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. Nr 100, poz. 1025):
   1) nazwę zbioru (ewidencji);
   2) podstawę prawną utworzenia nowego zbioru danych;
   3) metodę katalogowania (system komputerowy, metoda tradycyjna);
   4) zakres danych zawartych w zbiorze (np. imię, nazwisko, PESEL);
   5) informacje o skazaniu, orzeczeniu o ukaraniu, mandatach karnych;
   6) orzeczeniach wydanych w postępowaniu administracyjnym;
   7) sposób zbierania danych osobowych;
   8) podmioty, którym dane osobowe będą udostępniane.

Rozdział 5
Nadawanie uprawnień do przetwarzania danych i rejestrowanie tych uprawnień w systemie informatycznym

§ 7

1. W Urzędzie ASI jest osoba zatrudniona na stanowisku informatyka, odpowiedzialna za zapewnienie ciągłości i poprawności działania systemu oraz wdrażanie technicznych środków ochrony przewidzianych w tych systemach.[4)]
2. ASI rejestruje użytkownika w systemie i nadaje mu określone uprawnienia.
3. Pracownik którego zakres obowiązków obejmuje dostęp i prace w systemie informatycznym w którym przetwarzane są dane osobowe otrzymuje od ASI:
   1) uprawnienia do pracy w systemie, a w szczególności unikalny login (identyfikator) i hasło z możliwością samodzielnej zmiany (jeśli system informatyczny to umożliwia);
   2) login (identyfikator) i hasło - z możliwością zmiany - do pracy w sieci komputerowej, jeśli system do przetwarzania danych osobowych znajduje się w sieci komputerowej ;
   3) hasło do komputera - hasło BIOS - jeśli jest to komputer typu PC.
4. W przypadku gdy pracownik Urzędu zmienił stanowisko pracy bądź ustał stosunek pracy, jego indywidualne hasła i uprawnienia do pracy w przetwarzaniu danych osobowych są wycofywane przez:
   1) skasowanie konta użytkownika;
   2) zmianę uprawnień odpowiednich do zakresu obowiązków.
5. Osobą odpowiedzialną za nadawanie i cofanie uprawnień jest ASI.

Rozdział 6
Metody i środki uwierzytelnienia w systemie oraz procedury związane z ich zarządzaniem i użytkowaniem.

§ 8

1. **W Urzędzie stosuje się następujące metody i środki uwierzytelniania**:
   1) zabezpieczenie na poziomie BIOS-u – indywidualne hasło użytkownika pozwalające włączyć komputer w celu załadowania systemu operacyjnego;
   2) login i hasło do systemu Novell i Windows, przydzielane indywidualnie każdemu użytkownikowi systemu, znane jest tylko użytkownikowi - hasło składa się z unikalnego zestawu co najmniej 8 znaków, zawiera małe litery oraz cyfry;

[3)] Zm. zarządz. Nr 51/2011 z dnia 25.10.2011 r.
[4)] zm. zarządz. Nr 33/09 z dn. 10.12.2009 r.

3) karty elektroniczne (inteligentne) – indywidualne karty, bez których obsługa konta w systemie operacyjnym i zalogowanie się jest niemożliwe;
4) login i hasło do systemu operacyjnego, jeśli system operacyjny komputera posiada wbudowany mechanizm uwierzytelniania.

2. Każdy użytkownik systemu jest zobowiązany nie udostępniać nikomu swoich haseł dostępu, nie przechowywać ich zapisanych w widocznym i łatwo dostępnym miejscu. Hasło nie może być ujawnione nawet po utracie przez nie ważności.
3. Zmiana hasła do systemu następuje nie rzadziej, niż co 90 dni oraz niezwłocznie w przypadku podejrzenia, że hasło mogło zostać ujawnione.[5)]
4. Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów.
5. W Urzędzie rejestr haseł dostępu do komputerów - hasła BIOS - przechowuje ASI.

§ 9

Hasła dostępu są zmieniane:

1) do programów - co miesiąc automatycznie, chyba że funkcja taka nie jest zaimplementowana w programie, wtedy zmiana następuje ręcznie przez administratora systemu na wniosek użytkownika lub w przypadku naruszenia bezpieczeństwa, chyba że odrębne przepisy wymagają ważności hasła przez określony czas;
2) do sieci Novell – samodzielnie przez ASI co 90 dni.[6)]

Rozdział 7
Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie przeznaczone dla użytkowników systemów

§ 10

1. Procedura rozpoczęcia pracy:

1) w celu rozpoczęcia pracy w systemie informatycznym użytkownik obowiązany jest do podania wszystkich wymaganych identyfikatorów i haseł dostępu do systemu;
2) zabrania się wpisywania hasła lub jego zmiany w obecności innych osób;
3) hasło nie może być zapisywane lub przechowywane w miejscu dostępnym dla osób nieuprawnionych;
4) w przypadku zagubienia hasła użytkownik musi skontaktować się z ASI w celu uzyskania nowego hasła.

2. Procedura zawieszenia pracy w systemie:

1) w trakcie pracy, przy każdorazowym opuszczeniu stanowiska komputerowego, należy dopilnować, aby na ekranie nie były wyświetlane dane osobowe;
2) przy opuszczaniu pokoju na dłuższy czas należy zaktywizować wygaszacz ekranu, wyłączyć monitor lub w inny sposób zablokować stację roboczą np. wyjęcie karty elektronicznej.

3. Procedura zakończenia pracy w systemie:

1) zamknięcie aplikacji,
2) zamknięcie systemu operacyjnego,
3) wyłączenie stacji roboczej.

Rozdział 8
Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

---

[5)] zm. zarządz. Nr 33/09 z dn. 10.12.2009 r.
[6)] zm. zarządz. Nr 33/09 z dn. 10.12.2009 r.

§ 11

1. Kopie zapasowe zbiorów danych osobowych są tworzone codziennie po zakończeniu dnia pracy przez ASI dla całego systemu z wyłączeniem systemu CEPiK (Centralna Ewidencja Pojazdów i Kierowców), dla którego tworzone są oddzielne kopie zapasowe przez wyznaczonych przez przełożonego pracowników.
2. Nośnikiem są taśmy magnetyczne i optyczne.
3. ASI sprawuje nadzór nad wykonywaniem kopii zapasowych, weryfikuje ich poprawność oraz sprawdza okresowo pod kątem ich dalszej przydatności.

Rozdział 9
Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych

§ 12

1. Elektroniczne nośniki informacji:

1. Dane osobowe w postaci elektronicznej przetwarzane w systemie informatycznym, zapisane na dyskietkach, taśmach magnetycznych czy dyskach twardych nie są wynoszone poza siedzibę Urzędu, z wyłączeniem zbiorów (np. formularz PEFS) przekazywanych na podstawie odrębnych umów związanych z realizacją projektów.[7)]
2. Wymienne elektroniczne nośniki informacji są przechowywane w pokojach stanowiących obszar przetwarzania danych osobowych, określony w Polityce bezpieczeństwa przetwarzania danych osobowych.
3. Po zakończeniu pracy przez użytkowników systemu, wymienne elektroniczne nośniki informacji są przechowywane w zamykanych szafach biurowych lub kasetkach.
4. W przypadku uszkodzenia lub zużycia nośnika zawierającego dane osobowe należy go fizycznie zniszczyć.
5. Dyski twarde z danymi osobowymi należy niszczyć zgodnie z obowiązującymi w Urzędzie przepisami dotyczącymi gospodarki środkami trwałymi oraz wartościami niematerialnymi.

2. Kopie zapasowe

1. Taśmy magnetyczne i optyczne z kopiami zapasowymi zbiorów danych osobowych oraz oprogramowania i narzędzi programowych zastosowanych do przetwarzania danych są przechowywane przez ASI i odpowiednio zabezpieczone.
2. Po okresie obowiązującego okresu przechowywania kopie podlegają komisyjnej likwidacji poprzez ich fizyczne zniszczenie.

3. Wydruki

1. Wszelkie wydruki, zawierające dane osobowe, należy przechowywać w miejscu uniemożliwiającym ich odczyt przez osoby nieuprawnione, w zamkniętych szafach lub pomieszczeniach.
2. Wydruki, zawierające dane osobowe, po upływie czasu ich przydatności należy zniszczyć w stopniu uniemożliwiającym ich odczytanie np. przez pocięcie w niszczarce dokumentów.
3. Dane osobowe zapisane w formie papierowej innej niż wydruki z systemu informatycznego (pisma, ankiety itp.) są przechowywane na podobnych zasadach co wydruki.

[7)] Zm. zarządz. Nr 51/2011 z dnia 25.10.2011 r.

Rozdział 10

Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego.

§ 13

1. Ochrona antywirusowa

1. Za ochronę antywirusową odpowiada ASI.
2. Ochrona antywirusowa jest realizowana przez oprogramowanie antywirusowe instalowane na serwerach i stacjach roboczych użytkowników.
3. Oprogramowanie antywirusowe jest uaktualniane automatycznie, co najmniej raz na 2 dni.[8)]
4. Dane zawarte na nośnikach zewnętrznych (np. dyskietki) muszą być każdorazowo sprawdzone przez użytkownika poprzez program antywirusowy przed wprowadzeniem do systemu.
5. W celu zabezpieczenia systemu Urząd wykorzystuje:
   1) oprogramowanie Esest Smart Security Business Edition na stacjach roboczych i serwerach wewnątrz sieci lokalnej, [9)]
   2) w przypadku poczty elektronicznej oprogramowanie antywirusowe zabezpiecza operator serwera na którym znajduje się poczta zewnętrzna Urzędu.

2. Ochrona przed nieautoryzowanym dostępem do sieci lokalnej

1. ASI jest odpowiedzialny za aktywowanie i poprawne konfigurowanie specjalistycznego sprzętu i oprogramowania monitorującego wymianę danych na styku:
   a) sieci lokalnej i sieci rozległej,
   b) stanowiska komputerowego użytkownika systemu i pozostałych urządzeń wchodzących w skład sieci lokalnej.

Rozdział 11

Zasady i sposób odnotowywania w systemie informacji: komu, kiedy i w jakim zakresie dane osobowe ze zbiorów zostały udostępnione

§ 14

1. Odbiorcą danych jest każdy, komu udostępnia się dane osobowe, z wyłączeniem:
   a) osoby, której dane dotyczą,
   b) osoby użytkownika systemu lub innej osoby upoważnionej do przetwarzania danych osobowych w Urzędzie,
   c) przedstawiciela, o którym mowa w art. 31a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych,
   d) podmiotu, któremu powierzono przetwarzanie danych,
   e) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.
2. Generalnie użytkownik nie ma prawa udostępniania danych osobowych innym odbiorcom, aniżeli wymienieni w ust. 1 lit. a-e, chyba że wynika to z przepisów szczególnych.
3. Fakt udostępnienia danych osobowych innym odbiorcom odnotowuje się w systemie informatycznym.
4. Odnotowanie obejmuje informacje o:

[8)] zm. zarządz. Nr 33/09 z dn. 10.12.2009 r.
[9)] zm. zarządz. Nr 33/09 z dn. 10.12.2009 r.

a) nazwie jednostki organizacyjnej lub imieniu i nazwisku osoby, której udostępniono dane,
b) zakresie udostępnianych danych,
c) dacie udostępnienia,

5. Obowiązek odnotowania w/w informacji spoczywa na użytkowniku systemu, w tym celu wypełnia on odpowiednie pole w bazie danych osobowych.
6. Na żądanie osoby, której dane zostały udostępnione, informacje o udostępnieniu danych są zamieszczane w raporcie z systemu informatycznego, a raport przekazywany tej osobie.

Rozdział 12
Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych

§ 15

1. O przeprowadzanych przeglądach, konserwacjach i naprawach systemu w każdym przypadku informowany jest ASI, który powinien być przy nich obecny.
2. Przeglądy i konserwacja urządzeń:
   1) przeglądy i konserwacja urządzeń wchodzących w skład systemu informatycznego powinny być wykonywane w terminach określonym przez producenta sprzętu,
   2) nieprawidłowości ujawnione w trakcie tych działań powinny być niezwłocznie usunięte, a ich przyczyny przeanalizowane. O fakcie ujawnienia nieprawidłowości należy zawiadomić ABI.
   3) za terminowość przeprowadzenia przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada ASI.
3. Przegląd programów i narzędzi programowych przeprowadzany jest w następujących przypadkach:
   a) zmiany wersji oprogramowania serwera plików;
   b) zmiany wersji oprogramowania stanowiska komputerowego użytkownika systemu;
   c) zmiany systemu operacyjnego serwera plików;
   d) zmiany systemu operacyjnego stanowiska komputerowego użytkownika systemu;
   e) wykonania zmian w projekcie systemu spowodowanych koniecznością naprawy, konserwacji lub modyfikacji systemu.
4. Przegląd przeprowadza projektant systemu w obecności ASI.
3. Za prawidłowość przeprowadzenia przeglądów i konserwacji systemu odpowiada ASI.
4. W przypadku stwierdzenia uszkodzenia urządzenia, dyski i inne informatyczne nośniki danych zawierające dane osobowe przed ich przekazaniem do naprawy innemu podmiotowi pozbawiane są zawartości.
5. W przypadku likwidacji urządzenia, dyski i inne informatyczne nośniki danych zawierające dane osobowe są niszczone w sposób uniemożliwiający odczytanie danych.
6. Naprawa wymienionych urządzeń zawierających dane osobowe, jeżeli nie można danych usunąć, wykonywana jest pod nadzorem ABI lub ASI.

Rozdział 13
Przetwarzanie danych osobowych w zbiorach doraźnych

§ 16

1. Dostęp do danych osobowych powinien odbywać się poprzez aplikację. Gdy zachodzi potrzeba zapisania danych w innym formacie np. dane w postaci pliku arkusza kalkulacyjnego, można tego dokonać w doraźnym zbiorze danych osobowych pod warunkiem, że zapisane dane będą należycie chronione, tj.

1) uniemożliwi się dostęp do danych osobom nieuprawnionym,
2) uniemożliwi się zmiany danych, a tym samym zafałszowanie informacji pochodzących z systemu,
3) zabezpieczy się bezpośredni dostęp do danych hasłem.

2. Doraźny zbiór danych osobowych należy usunąć z nośnika danych, na którym został utworzony lub zniszczyć nośnik, nie później niż 3 dni po wykorzystaniu danych.
3. Zawiadamiać ABI w przypadku podejrzenia lub stwierdzenia dostępu do zbioru osób nieuprawnionych.
4. Przetwarzać dane w pokojach stanowiących obszar przetwarzania danych osobowych w systemie informatycznym.

Rozdział 14
Postępowanie w sytuacjach naruszenia zbioru danych osobowych

§ 17

Użytkownik systemu informatycznego zobowiązany jest niezwłocznie zawiadomić przełożonego oraz ABI lub ASI o każdym naruszeniu zabezpieczenia systemu polegającym na:

1) naruszeniu hasła dostępu (system nie reaguje na hasło lub je ignoruje – usunięty mechanizm hasła),
2) częściowym lub całkowitym braku bazy danych,
3) braku możliwości uruchomienia właściwej aplikacji (programu komputerowego),
4) zmianie położenia komputerów,
5) kradzieży z pomieszczenia.

§ 18

1. Użytkownik do momentu przybycia ABI, lub osoby przez niego upoważnionej powinien:
   a) zabezpieczyć dostęp do pomieszczenia lub urządzenia;
   b) powstrzymać się od rozpoczęcia lub kontynuowania jakichkolwiek czynności mogących spowodować zatarcie śladów, bądź dowodów naruszenia ochrony;
   c) zatrzymać pracę na komputerze, na którym zaistniało naruszenie ochrony oraz nie uruchamiać innych urządzeń, które mogą mieć związek z naruszeniem ochrony;
   d) podjąć, stosownie do zaistniałej sytuacji działania, które zapobiegną ewentualnej utracie danych osobowych.

§ 19

1. ABI lub ASI, po otrzymaniu zawiadomienia o naruszeniu zabezpieczenia systemu informatycznego powinien niezwłocznie:
   1) powiadomić ADO,
   2) przeprowadzić postępowanie wyjaśniające w celu ustalenia okoliczności naruszenia i osoby odpowiedzialnej za naruszenie,
   3) określić dokładnie rodzaj, sposób oraz rozmiar naruszeń zabezpieczenia systemu informatycznego,
   4) podjąć działania zabezpieczające system przed ponownym naruszeniem,
   5) sporządzić notatkę służbową z przebiegu zdarzenia, która obejmuje:
      a) dane osoby stwierdzającej naruszenie ochrony;
      b) datę, godzinę i miejsce naruszenia ochrony;
      c) rodzaj naruszenia ochrony;
      d) czas powiadomienia o zdarzeniu;
      e) opis podjętych czynności;
      f) wnioski do realizacji.
2. Notatkę o której mowa w ust. 1, ABI przekazuje ADO lub osobie upoważnionej.

§ 20

ADO po zapoznaniu się z pisemną informacją w sprawie, ocenia stopień przyczynienia się pracownika do powstania naruszenia obowiązku ochrony danych i stosuje wobec osoby odpowiedzialnej za powstały stan rzeczy sankcje dyscyplinarne, do odsunięcia od pracy na stanowisku na którym przetwarza się dane podlegające ochronie włącznie.

§ 21

W przypadku kradzieży z pomieszczenia, w którym znajdują się komputery, należy niezwłocznie powiadomić o tym fakcie Policję.

§ 22

W przypadku naruszenia zabezpieczenia systemu informatycznego przed przystąpieniem do dalszej pracy, należy dokonać zmiany haseł i identyfikatorów.

§ 23

Zgodę na ponowne uruchomienie komputera lub innych urządzeń oraz kontynuowanie przetwarzania danych, wyraża ABI.

Rozdział 15
Ogólne zasady korzystania z sieci teleinformatycznej Urzędu

§ 24

1. Sieć komputerowa Starostwa służy wymianie informacji oraz wspomaga zarządzanie Urzędem.
2. Z sieci komputerowej mogą korzystać wyłącznie pracownicy Starostwa oraz stażyści odbywający staże i przygotowanie zawodowe w Starostwie, w zakresie swoich obowiązków służbowych.
3. Zabrania się bez powiadamiania ASI i osoby odpowiedzialnej za środki trwałe dokonywać zmiany lokalizacji jakiegokolwiek z elementu danego zestawu komputerowego.
4. Zestaw komputerowy należy wykorzystywać zgodnie z przeznaczeniem służbowym. W szczególności zabrania się ściągania plików i innych form danych elektronicznych z Internetu, wykraczających poza służbowe cele.

§ 25

1. Sporządzanie kopii zapasowych:
   1) wszystkie ważniejsze dane, w celu ich zabezpieczenia i ochrony przed utratą należy archiwizować na serwerze Starostwa lub sporządzać kopie na nośnikach elektronicznych;
   2) użytkownik powinien archiwizować dokumenty do wydziałowego katalogu znajdującego się na serwerze Starostwa;
   3) użytkownik ponosi odpowiedzialność za zabezpieczenie danych przed ich utratą;
   4) kopie dokumentów ze stacji roboczej należy wykonywać co najmniej raz w tygodniu, a przy dokumentach szczególnie ważnych - codziennie;
   5) bazy danych z zintegrowanych systemów informatycznych podlegają ochronie na oddzielnych zasadach, określonych dla każdego systemu.

§ 26

1. Prawa i obowiązki użytkowników sieci teleinformatycznej Urzędu:

1) Użytkownicy mogą korzystać z następujących zasobów sieciowych:
   a) dostępu do Internetu;
   b) kont poczty elektronicznej;
   c) możliwości zmiany własnego hasła dostępu do poczty;
   d) dostępu do własnych zasobów sieci lokalnej.
2) Użytkownicy są zobowiązani:
   a) do codziennego porządkowania zasobów swojej stacji roboczej, usuwanie plików zbędnych, zakładanie w określonym porządku katalogów i podkatalogów;
   b) przeprowadzać defragmentację twardego dysku conajmniej raz w miesiącu;
   c) sprawdzać funkcjonowanie systemu ochrony antywirusowej po uruchomieniu stacji roboczej;
   d) skanować zewnętrzne nośniki elektroniczne przed ich otwarciem na zawartość wirusów;
   e) zgłaszać niezwłocznie ASI uwagi w przypadku podejrzeń pojawienia się wirusa, z którym nie radzi sobie system ochrony komputerowej;
   f) dbać o bezpieczeństwo swoich zasobów komputerowych poprzez stosowanie odpowiednich haseł zabezpieczających dostęp do własnego komputera i nie przekazywanie ich osobom trzecim;
   g) zachować szczególną ostrożność przy pracy z pocztą elektroniczną. W przypadku jakichkolwiek wątpliwości, szczególnie w przypadku załączników poczty elektronicznej, należy przed uruchomieniem skontaktować się z ASI;
   h) stosować się do zaleceń osób odpowiedzialnych za stan informatyczny w Starostwie w zakresie korzystania z sieci komputerowej.
3) Użytkownikom sieci komputerowej nie wolno:
   a) udostępniać swojego konta pocztowego osobom trzecim;
   b) wykorzystywać swojego konta i dostępu do Internetu w celu ściągania nielegalnego oprogramowania i zasobów Internetu (filmów, gier itp.), które są potencjalnym zagrożeniem dla całej sieci komputerowej;
   c) zachowywać się wobec innych użytkowników sieci lokalnej i Internetu w sposób odbiegający od powszechnie przyjętych norm obyczajowych i moralnych oraz norm prawnych (np. blokowanie łącza, aplikacji, łamanie praw autorskich innych osób, itp.);
   d) podejmować działań powodujących zakłócenia w pracy sieci lokalnej (np. ingerować w konfigurację sieci lokalnej lub działać na szkodę zasobów sieci).

Rozdział 16
Postanowienia końcowe

§ 27

Zabrania się:
a) samodzielnego instalowania oprogramowania, zarówno licencjonowanego jak i nielegalnego oraz darmowego oraz jego używanie;
b) samodzielnego naprawiania uszkodzeń mechanicznych, związanych ze złym funkcjonowaniem zestawu komputerowego;
c) montażu i demontażu urządzeń komputerowych;
d) podłączania dodatkowych urządzeń elektrycznych do listwy zasilającej komputer, bez uzgodnienia z administratorem sieci.

§ 28

1. Każdy pracownik zatrudniony przy przetwarzaniu danych osobowych w systemie, zobowiązany jest zapoznać się z niniejszą Instrukcją i stosować jej przepisy na swoim stanowisku pracy.
2. W obszarach w których nie przetwarza się danych osobowych w systemach informatycznych przepisy niniejszej Instrukcji stosuje się odpowiednio.

§ 29

W sprawach nieuregulowanych niniejszą Instrukcją mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) i rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku 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).

§ 30

Wszelkie zmiany Instrukcji mogą być wprowadzane tylko na podstawie zarządzeń Administratora Danych Osobowych.