Załącznik Nr 1
do Zarządzenia Nr 62/2006
Starosty Gryfińskiego
z dnia 30 czerwca 2006 r.

Instrukcja

określająca sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Starostwie Powiatowym w Gryfinie

Opracował: Administrator Bezpieczeństwa Informacji

Czerwiec 2006

Rozdział 1

Postanowienia ogólne

§ 1. Niniejsza instrukcja, zwana dalej *Instrukcją*, jest wewnętrznym dokumentem w Starostwie Powiatowym w Gryfinie i ma zastosowanie do wszelkich danych osobowych znajdujących się, bądź mogących znajdować się w systemie informatycznym oraz dokumentacji papierowej.

§ 2. *Instrukcja* określa:
1) sposób przydziału haseł dla użytkowników i częstotliwości ich zmiany oraz wskazuje osobę odpowiedzialną za te czynności;
2) sposób rejestrowania i wyrejestrowywania użytkowników oraz wskazuje osobę odpowiedzialną za te czynności;
3) procedury rozpoczęcia i zakończenia pracy;
4) metodę i częstotliwość tworzenia kopii awaryjnych;
5) metodę i częstotliwość sprawdzania obecności wirusów komputerowych oraz metodę ich usuwania;
6) sposób i czas przechowywania nośników informacji, w tym kopii informatycznych i wydruków;
7) sposób dokonywania przeglądów i konserwacji systemu i zbioru danych osobowych;
8) sposób postępowania w zakresie komunikacji w sieci komputerowej LAN.

§ 3. Ilekroć w niniejszej Instrukcji jest mowa o:
1) **danych osobowych** – rozumie się przez to, że każda informacja dotycząca osoby fizycznej, pozwalająca na określenie tożsamości tej osoby;
2) **przetwarzaniu danych** – rozumie się przez to, wszelkie operacje wykonywane na danych osobowych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;
3) **administratorze danych osobowych** – rozumie się przez to, Starostę Gryfińskiego, zwanego dalej *ADO*;
4) **administratorze bezpieczeństwa informacji** – rozumie się przez to wyznaczoną osobę odpowiedzialną za nadzorowanie przestrzegania zasad ochrony danych osobowych przetwarzanych w systemach informatycznych, zwany dalej *ABI*;
5) **osobie upoważnionej lub użytkowniku** – rozumie się przez to osobę posiadającą upoważnienie wydane przez *ADO* i dopuszczoną w zakresie w nim wskazanym, jako użytkownika do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych lub uprawniona we wskazanym zakresie do dostępu do dokumentacji Starostwa Powiatowego w Gryfinie;
6) **osobie trzeciej** – rozumie się przez to każdą osobę nieupoważnioną i przez to nieuprawnioną do dostępu do danych osobowych lub zbiorów tych danych. Osobą trzecią jest również osoba posiadająca upoważnienie wydane przez *ADO* w zakresie czynności przekraczających ramy udzielonego jej upoważnienia;
7) **systemie informatycznym** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i urządzeń programowych zastosowanych w celu przetwarzania danych;

8) **zabezpieczeniu systemu informatycznego** – rozumie się przez to wdrożenie w Starostwie stosowanych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą.

§ 4. Instrukcja ma na celu zapewnienie procedur i właściwych warunków zarządzania systemem informatycznym dla ochrony zgromadzonych tam danych, jak również jednolitych i bezpiecznych zasad korzystania z danych osobowych przetwarzanych w systemie informatycznym oraz w dokumentacji papierowej.

§ 5. Realizację zamierzeń określonych w § 4 gwarantuje następująca strategia:
1) przeszkolenie użytkowników w zakresie ochrony danych osobowych oraz zaznajomienie z przepisami dotyczącymi ochrony danych osobowych;
2) korzystanie z oprogramowania systemowego i użytkowego spełniającego wysokie standardy;
3) wykorzystanie w systemie informatycznym zabezpieczeń gwarantujących nienaruszoną pracę systemu, w tym najnowszych wersji oprogramowania antywirusowego;
4) przypisanie użytkownikom określonych atrybutów pozwalających na ich identyfikację (hasła i identyfikatory);
5) ocena ewentualnych zagrożeń bezpieczeństwa systemu informatycznego i ryzyk związanych z jego obsługą;
6) wdrożenie zabezpieczeń o charakterze fizycznym pomieszczeń, stosownie do zagrożeń i ryzyk wynikających z oceny, o której mowa w pkt 5;
7) stałe monitorowanie wdrożonych zabezpieczeń w celu identyfikacji podatnych na zagrożenia obszarów i słabości zabezpieczeń;
8) okresowe sprawdzanie przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych osobowych oraz podejmowanie niezbędnych działań dla likwidacji słabych ogniw w systemie zabezpieczeń.

Rozdział 2

Pomieszczenia lub części pomieszczeń, tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego

§ 6. 1. W pomieszczeniach, w których znajduje się stacjonarny sprzęt komputerowy służący do eksploatowania na bieżąco zbiorów danych osobowych, nie mogą być przechowywane kopie awaryjne.

2. Przebywanie wewnątrz pomieszczeń, o których mowa w ust. 1, osób nieuprawnionych do dostępu do danych osobowych jest dopuszczalne tylko za zgodą *ADO* lub w obecności osoby upoważnionej do przetwarzania danych osobowych.

3. Pomieszczenia, o których mowa w ust. 1, powinny być zamykane na czas nieobecności w nich osób upoważnionych, w sposób uniemożliwiający dostęp do nich osób trzecich.

Rozdział 3

Sposób przydziału identyfikatorów i haseł dla użytkowników i częstotliwości ich zmiany

§ 7. Mając na względzie, iż system informatyczny przetwarzający dane osobowe powinien być wyposażony w mechanizmy uwierzytelniania użytkownika oraz kontroli dostępu do tych danych – dla każdej osoby upoważnionej ustalany jest odrębny identyfikator i hasło. Bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła. Hasła dostępu i identyfikatory przyznawane są indywidualnie dla każdego z użytkowników i znane są tylko właścicielowi.

§ 8. Identyfikator użytkownika:
1) jest niepowtarzalny;
2) po wyrejestrowaniu użytkownika z systemu informatycznego nie jest przydzielany innej osobie;
3) nie podlega zmianie, z wyjątkiem sytuacji, gdy zostanie ujawniony;
4) użytkownicy zobowiązani są do zachowania w tajemnicy ustalonych dla nich identyfikatorów;
5) jest wpisywany do ewidencji osób zatrudnionych przy przetwarzaniu danych wraz z imieniem i nazwiskiem użytkownika;
6) za ochronę identyfikatora odpowiada *ABI*.

§ 9. Hasło użytkownika:
1) jest przydzielane indywidualnie dla każdego z użytkowników i znane tylko użytkownikowi, który się nim posługuje;
2) zostaje zmienione przy pierwszym zastosowaniu (zalogowaniu użytkownika) po przydzieleniu przez *ABI*;
3) nie jest zapisywane w systemie w postaci jawnej;
4) jest zmieniane raz na miesiąc;
5) jest utrzymywane w tajemnicy, również po upływie jego ważności.

§ 10. 1. Osobą odpowiedzialną w Starostwie Powiatowym w Gryfinie za sposób przydziału haseł dla użytkowników i częstotliwość ich zmiany jest *ABI* , który je rejestruje.
2. Hasło *ABI* przechowywane jest w zapieczętowanej kopercie, w Kancelarii Tajnej.

§ 11. Przydziału i zmiany haseł dokonuje się w następujący sposób:
1) wymogiem niezbędnym jest przydział haseł alfanumerycznych skonstruowanych co najmniej z 6 (sześciu) znaków;
2) hasła są zmieniane przez każdego z użytkowników co najmniej raz na miesiąc; system informatyczny „wymusza” zmianę haseł, informując o upływie ich ważności;
3) zachowując wymóg zmieniania haseł każdego z użytkowników co najmniej raz na miesiąc, hasła użytkowników nie mogą się powtarzać;
4) hasła nie mogą składać się z kombinacji znaków mogących prowadzić do odszyfrowania ich przez osoby trzecie (nieupoważnione);
5) niezależnie od wymogu zmieniania haseł każdego z użytkowników co najmniej raz na miesiąc, hasło winno być zmienione przez użytkownika niezwłocznie w przypadku powzięcia podejrzenia lub stwierdzenia, że z hasłem mogły zapoznać się osoby trzecie.

§ 12. 1. Użytkownik odpowiedzialny jest za wszystkie czynności wykonane przy użyciu hasła, którym się posługuje lub posługiwał.

2. Użytkownik obowiązany jest utrzymywać hasła, którymi się posługuje lub posługiwał, w ścisłej tajemnicy, co obejmuje, w szczególności dołożenie przez niego wszelkich starań w celu uniemożliwienia zapoznania się przez osoby trzecie z hasłem nawet po ustaniu jego ważności, czy też użycia hasła przez te osoby.

3. W przypadku powzięcia przez użytkownika podejrzenia lub stwierdzenia, że z hasłem mogły zapoznać się osoby trzecie, obowiązany jest on niezwłocznie zmienić hasło i powiadomić o tym *ABI*.

4. Naruszenie przez użytkownika postanowień ust. 2 lub 3 może stanowić podstawę dla pociągnięcia użytkownika do odpowiedzialności dyscyplinarnej, odszkodowawczej lub karnej w trybie i na zasadach przewidzianych przepisami prawa.

5. Użytkownicy obowiązani są utrzymywać hasła w tajemnicy również po upływie ich ważności.

Rozdział 4

Sposób rejestrowania i wyrejestrowywania użytkowników

§ 13. 1. Rejestracji i wyrejestrowania użytkowników dokonuje *ABI*, który w imieniu *ADO* prowadzi ich ewidencję (wzór stanowi załącznik nr 1 do *Instrukcji*), w oparciu o gromadzone wnioski (wzór stanowi załącznik nr 2 do *Instrukcji*) o przyznanie i/lub modyfikację uprawnień.

2. Jakakolwiek zmiana w zakresie informacji zawartych w ewidencji podlega natychmiastowemu odnotowaniu.

§ 14. Dana osoba jest rejestrowana w systemie informatycznym, jako użytkownik po spełnieniu następujących warunków:

1) uzyskaniu przez *ABI* informacji koniecznych do zdefiniowania dla danej osoby jej profilu jako użytkownika oraz jej uprawnień. Informacji takich udziela osoba odpowiedzialna pod względem merytorycznym, co do charakteru pracy danej osoby, mającej być użytkownikiem;
2) uzyskaniu przez tę osobę upoważnienia (wzór stanowi załącznik nr 3 do *Instrukcji*) wydanego przez *ABI* dopuszczającego daną osobę w zakresie w nim wskazanym, jako użytkownika, do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych.

§ 15. Osoba upoważniona do dostępu i przetwarzania danych osobowych podpisuje oświadczenie (wzór stanowi załącznik nr 4 do *Instrukcji*) o obowiązku zachowania danych w tajemnicy. Obowiązek ten trwa również po ustaniu zatrudnienia.

§ 16. Upoważnienie, o którym mowa w § 14 oraz oświadczenie, o którym mowa w § 15 pracownik prowadzący sprawy kadrowe dołącza do akt osobowych pracownika.

§ 17. 1. Z chwilą zarejestrowania w systemie informatycznym, zgodnie z postanowieniami § 14, dana osoba jest informowana przez *ABI* o ustalonym dla niej identyfikatorze i konieczności posługiwania się hasłami.

2. Bez spełnienia wymogów wynikających z § 14, *ABI* nie może zarejestrować jakiejkolwiek osoby w systemie informatycznym.

§ 18. Użytkownik jest wyrejestrowywany z systemu informatycznego, na podstawie wniosku o wyrejestrowanie użytkownika (wzór stanowi załącznik nr 5 do *Instrukcji*), w każdym przypadku utraty przez niego uprawnień do dostępu do danych osobowych, co ma miejsce w przypadku:

1) ustania zatrudnienia tego użytkownika w Starostwie – o czym informację *ABI* uzyskuje od pracownika prowadzącego sprawy kadrowe,
2) zmiany zakresu obowiązków tego użytkownika – o czym informację *ABI* uzyskuje od pracownika prowadzącego sprawy kadrowe lub bezpośredniego przełożonego użytkownika.

§ 19. W przypadkach wskazanych w § 18, co do użytkownika, który utracił uprawnienia do dostępu do systemu informatycznego, *ABI* dokonuje niezwłocznie następujących czynności:

1) blokuje jego profil, co powoduje, że osoba ta nie ma możliwości „zalogowania się" do sieci lub aplikacji;
2) wyrejestrowuje jego identyfikator;
3) unieważnia jego hasło;
4) podejmuje inne stosowne działania w celu zapobieżenia dalszemu dostępowi tej osoby do danych osobowych w Starostwie.

§ 20. 1. Identyfikator, który utracił ważność nie może być ponownie przydzielony innemu użytkownikowi.

2. *ABI* obowiązany jest gromadzić odrębnie identyfikatory, które utraciły ważność.

Rozdział 5

Procedury rozpoczęcia i zakończenia pracy

§ 21. Przed przystąpieniem do pracy w systemie użytkownik obowiązany jest dokonać sprawdzenia stanu urządzeń komputerowych służących do przetwarzania danych osobowych oraz dokonać oględzin swojego stanowiska pracy, ze szczególnym uwzględnieniem czy nie zaszły okoliczności wskazujące na naruszenie ochrony danych osobowych.

§ 22. 1. Każdy użytkownik rozpoczynający pracę obowiązany jest „zalogować się" do systemu komputerowego posługując się swoim identyfikatorem i hasłem, dokładając jednocześnie szczególnej staranności w tym, aby przy tych czynnościach osoby trzecie nie powzięły wiadomości o treści używanego przez niego hasła. Następnie po podaniu dodatkowego identyfikatora i hasła użytkownik ma możliwość „zalogowania się" do aplikacji zawierających dane osobowe.

2. Bez wykonania procedury opisanej w ust. 1 jakakolwiek praca w systemie komputerowym nie jest możliwa.

§ 23. 1. Maksymalna ilość prób wprowadzenia hasła przy logowaniu się do systemu wynosi 3 (trzy).

2. Po przekroczeniu liczby prób logowania system blokuje dostęp do zbioru danych na poziomie danego użytkownika.

3. Użytkownik informuje *ABI* o zablokowaniu dostępu do zbioru danych.

4. *ABI* ustala przyczyny zablokowania systemu oraz w zależności od zaistniałej sytuacji, podejmuje odpowiednie działania.

§ 24. 1. W przypadku bezczynności użytkownika na komputerze stacjonarnym przez okres dłuższy niż 5 minut automatycznie włączany jest wygaszasz ekranowy.

2. Wygaszacze ekranowe powinny być zaopatrzone w hasła. Regulacje odnoszące się do haseł używanych przez użytkownika przy logowaniu, stosuje się odpowiednio do haseł wygaszacza.

3. Przed opuszczeniem miejsca pracy, użytkownik obowiązany jest poczekać, aż zaktywizuje się wygaszacz, samem zaktywizować wygaszacz lub w inny sposób zablokować stację roboczą.

4. W przypadku, gdy przerwa w pracy trwa dłuższy okres, oraz kończąc pracę użytkownik obowiązany jest „wylogować się" z aplikacji i systemu komputerowego. Sprawdzić czy nie zostały pozostawione bez zamknięcia nośniki informacji. Opuszczając stanowisko użytkownik zamyka używane przez niego szafy i pomieszczenia, w których przechowuje się dokumentację i nośniki informacji.

§ 25. W przypadku zauważenia przez użytkownika naruszenia zabezpieczenia systemu informatycznego, zauważenia, że stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci komputerowej LAN mogą wskazywać na naruszenie zabezpieczeń danych osobowych, użytkownik ten obowiązany jest niezwłocznie poinformować o tym fakcie *ABI* lub swojego przełożonego.

Rozdział 6

Metoda i częstotliwość tworzenia kopii zapasowych oraz likwidacja nośników informacji

§ 26. Wszyscy pracownicy zobowiązaniu są przestrzegać terminów sporządzania kopii zapasowych oraz okresowo dokonywać kontroli możliwości odczytu danych zapisanych na tych kopiach.

§ 27. Kopie zapasowe są:
1) tworzone na odpowiednio opisanych oznakowanych nośnikach magnetycznych,
2) raz w miesiącu sprawdzane pod kątem ich dalszej przydatności do odtworzenia danych w przypadku awarii systemu informatycznego,
3) przechowywane w innych pomieszczeniach niż zbiory danych osobowych eksploatowane na bieżąco,
4) przechowywane w szafie zamykanej na klucz, sejfie lub innym miejscu odpowiednio zabezpieczonym, do którego mogą mieć dostęp wyłącznie osoby upoważnione przez *ADO*.

§ 28. 1. Kopiowanie danych na nośniki informacji i robienie wydruków tych danych jest zabronione, chyba, że konieczność ich sporządzenia wynika z nałożonego na użytkownika zakresu obowiązków i jest uzasadniona potrzebą ich wykonania oraz dozwolona przepisami prawa.

2. Wykorzystywanie nośników informacji lub wydruków w innym celu niż wskazany w ust. 1 jest zakazane.

§ 29. 1. Kopie zapasowe po ustaniu ich użyteczności są bezzwłocznie usuwane.

2. Kopie dzienne kasowane są po 1 tygodniu.

3. Kopie tygodniowe kasowane są po 1 miesiącu.

4. Kopie miesięczne nie są niszczone.

5. Kopie zapasowe, które uległy uszkodzeniu podlegają natychmiastowemu zniszczeniu.

6. Niszczenia kopii zapasowych na nośnikach magnetycznych dokonuje *ABI* i/lub upoważniona przez niego osoba.

7. Z nośników magnetycznych dane należy usunąć w sposób uniemożliwiający ich odczytanie, a w przypadku, gdy usunięcie danych nie jest możliwe, nośniki podlegają zniszczeniu w stopniu uniemożliwiającym dostęp do zawartych na nich danych.

8. Z nośników podlegających zniszczeniu nie wolno sporządzać wydruków.

9. Jeżeli dysk twardy jest uszkodzony i nie ma możliwości skasowania z niego danych osobowych należy wymontować go z komputera i fizycznie zniszczyć.

10. Likwidacji wydruków dokonuje się przy użyciu przeznaczonych do tego celu urządzeń (np. niszczarek).

11. Urządzenia, dyski lub inne informatyczne nośniki informacji, zawierające dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie, czego dokonać można poprzez zniszczenie ich w sposób trwały, tj. przez ich mechaniczne zniszczenie.

12. Urządzenia, dyski lub inne informatyczne nośniki informacji, zawierające dane osobowe, przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymania danych osobowych, pozbawia się zapisu tych danych.

13. Trwałego niszczenia zbędnych nośników informacji i wydruków komputerowych dokonuje się na bieżąco w czasie pracy, nie później jednak niż przed opuszczeniem stanowiska pracy.

§ 30. Wydruki komputerowe z sytemu zawierającego dane osobowe są:

1) sporządzane jedynie dla celów operacyjnych;
2) odpowiednio opisane i oznakowane;
3) elementem archiwum papierowego i podlegają zasadom dotyczącym przetwarzania danych osobowych w systemie archiwum papierowego;
4) przechowywane są w odpowiednich szafach i używane do celów operacyjnych przez określony czas wykorzystywania.

Rozdział 7

Metoda i częstotliwość sprawdzania obecności wirusów komputerowych oraz metoda ich usuwania

§ 31. Na bieżące i bezpośrednie sprawdzanie obecności zagrożeń typu wirusy, robaki, trojany itp. pozwala oprogramowanie antywirusowe automatycznie monitorujące system w trakcie załączania, wczytywania danych z zewnętrznych nośników informacji lub poprzez sieć LAN.

§ 32. 1. Nadzór nad instalowaniem nowego oprogramowania antywirusowego oraz nad bieżącą jego aktualizacją sprawuje *ABI* lub wyznaczone przez niego osoby.

2. Kontrola antywirusowa jest przeprowadzana na wszystkich nośnikach magnetycznych i optycznych, służących zarówno do przetwarzania danych osobowych w systemie, jak i do celów instalacyjnych.

3. Oprogramowanie antywirusowe jest systematycznie aktualizowane.

§ 33. 1. O każdorazowym wykryciu wirusa przez oprogramowanie antywirusowe użytkownik obowiązany jest niezwłocznie poinformować swojego przełożonego.

2. W razie niemożności usunięcia wirusa, *ABI* ma obowiązek niezwłocznego przedstawienia *ADO* lub wyznaczonej przez niego osobie, propozycji działań zaradczych.

3. W sytuacji korzystania z usług specjalistów zewnętrznych należy podjąć działania uniemożliwiające tym osobom dostęp do danych osobowych. Osoby te mogą dokonywać operacji na „zainfekowanym" komputerze wyłącznie pod nadzorem *ABI* lub upoważnionej przez niego osoby.

§ 34. 1. Po usunięciu wirusa *ABI* sprawdza system informatyczny oraz przywraca go do pełnej funkcjonalności i sprawności.

2. *ABI*, jeżeli zachodzi taka konieczność, wnioskuje do *ADO* o zakup nowego oprogramowania antywirusowego.

3. *ABI* prowadzi rejestr przypadków zainfekowania komputerów i nośników wykorzystywanych do przetwarzania danych osobowych w systemie.

4. Procedura opisana w paragrafach niniejszego rozdziału ma odpowiednie zastosowanie także do przypadków awarii systemu spowodowanych błędami oprogramowania antywirusowego, bądź błędami użytkownika.

Rozdział 8

Wymagania sprzętowo-organizacyjne w zakresie ochrony przetwarzanych danych osobowych

§ 35. Sprzęt obsługujący zbiory danych osobowych składa się z komputerów stacjonarnych klasy PC, zlokalizowanych w wydzielonych pomieszczeniach siedziby *ADO*.

§ 36. 1. Prowadzona przez Starostwo baza danych osobowych przetwarzana jest na serwerze.

2. Serwer powinien być umieszczony w pomieszczeniu, do którego wejście zabezpieczone jest elektronicznym zamkiem szyfrowym oraz posiada własne zabezpieczenia:

1) zamykaną część dostępu do dysków twardych oraz napędów CD/DVD i FDD,
2) mechanizm blokujący dostęp do dysków twardych.

3. Serwer przetwarzający dane osobowe w zbiorze danych powinien być zabezpieczony zasilaczem awaryjnym o mocy przynajmniej 780 W z oprogramowaniem do automatycznego wyłączenia i restartu serwera w przypadku przekroczenia czasu podtrzymania zasilania z automatycznym, bezpiecznym wyłączeniem bazy danych osobowych.

§ 37. 1. Ekrany monitorów ustawione są do wewnątrz pomieszczeń wydzielonych do przetwarzania danych osobowych, w taki sposób, by uniemożliwić wgląd lub spisanie zawartości aktualnie wyświetlanej na ekranie monitorów.

2. Programy zainstalowane na komputerach stacjonarnych i przenośnych obsługujących przetwarzanie danych osobowych użytkowane są z zachowaniem praw autorskich i posiadają licencje.

3. Decyzję o instalacji oprogramowania systemowego oraz oprogramowania użytkowego obsługującego przetwarzanie danych osobowych podejmuje *ADO*.

4. Używanie sprzętu komputerowego przez użytkownika w trakcie przetwarzania danych osobowych do innych celów jest zabronione.

§ 38. 1. Stały dostęp do pomieszczeń Starostwa mają tylko użytkownicy oraz pracownicy upoważnieni przez *ADO*.

2. Osoby trzecie mogą przebywać w tych pomieszczeniach wyłącznie w obecności co najmniej jednego upoważnionego użytkownika.

3. W trakcie prac technicznych wykonywanych przez osoby trzecie, przetwarzanie danych osobowych na wydzielonych stanowiskach jest zabronione, a sprzęt komputerowy musi być wyłączony.

Rozdział 9

Sposób dokonywania przeglądów i konserwacji systemu i zbiorów danych osobowych

§ 39. Przeglądy i konserwacje sprzętu komputerowego dokonuje się w miarę potrzeb wynikających z obciążenia sprzętu komputerowego, warunków zewnętrznych, w których eksploatowane są dane urządzenia oraz ważności sprzętu dla funkcjonowania całości systemu informatycznego.

§ 40. 1. Prace dotyczące przeglądów, konserwacji i napraw wymagające autoryzowanych firm zewnętrznych, są wykonywane przez uprawnionych przedstawicieli tych firm (serwisantów) pod nadzorem *ABI* lub upoważnionej przez niego osoby, bez możliwości dostępu do danych osobowych.

2. W przypadku konieczności dostępu do danych osobowych przez serwisantów, podpisują oni oświadczenie o zachowaniu tajemnicy (zgodnie z art. 39 ust. 2 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych).

3. Urządzenia, dyski lub inne informatyczne nośniki informacji, przeznaczone do napraw, gdzie wymagane jest zaangażowanie autoryzowanych podmiotów zewnętrznych, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem *ABI* lub upoważnionej przez niego osoby.

Rozdział 10

Sposób postępowania w zakresie komunikacji w sieci komputerowej LAN

§ 41. 1. Korzystanie z zasobów sieci komputerowej LAN jest dozwolone jedynie po właściwym podaniu identyfikatora i hasła użytkownika. Po zalogowaniu użytkownik uzyskuje dostęp tylko do tych zasobów, które są mu niezbędne do wykonania prac w zakresie jego obowiązków i wynikających z nich uprawnień.

2. W przypadku awarii systemu lub z innych przyczyn powstanie możliwość dostępu do innych zasobów sieci komputerowej, niż te, które są przypisane danemu użytkownikowi, nie dozwolone jest przeglądanie tych zasobów. Powstanie takiej sytuacji należy niezwłocznie zgłosić *ABI* lub upoważnionej przez niego osobie.

3. Wprowadzenie do systemu informatycznego informacji z zewnątrz, w tym danych osobowych, jest dopuszczalne tylko przy stwierdzeniu legalności i wiarygodności źródeł informacji i tylko przez użytkownika w zakresie jego obowiązków i wynikających z nich uprawnień.

4. Konfiguracja systemu informatycznego jest dokonywana wyłącznie przez *ABI* lub upoważnione przez niego osoby.

5. W celu uniemożliwienia niekontrolowanej wymiany informacji, w tym danych osobowych, lub modyfikacji systemu informatycznego zapewniona jest optymalna konfiguracja komputerowych stanowisk pracy.

6. Pliki zawierające dane osobowe powinny znajdować się jedynie na serwerach, gdzie podlegają ochronie przez mechanizmy bezpieczeństwa systemu operacyjnego (np. uwierzytelnianie).

7. Na stacjach roboczych użytkowników dane osobowe nie są przechowywane.

8. Nieuzasadnione kopiowanie przez użytkowników plików z serwerów na stacje robocze użytkowników, dyskietki i inne nośniki jest zabronione.

9. Wszelkie pliki z danymi osobowymi przesyłane na zewnątrz Starostwa przez łącza publiczne muszą być zaszyfrowane lub chronione hasłem.

Rozdział 11

Zasady korzystania z komputerów przenośnych

§ 42. 1. Komputery przenośne, używane do przetwarzania danych osobowych, powinny być zabezpieczone podczas transportu oraz zabezpieczone przed dostępem do tych danych osób nieuprawnionych.

2. W szczególności należy:

1) zabezpieczyć dostęp do komputera hasłem;
2) nie zezwalać na używanie komputera osobom nieupoważnionym do dostępu do danych osobowych;
3) pliki z danymi osobowymi należy zaszyfrować lub chronić hasłem.

Rozdział 12

Postępowanie w zakresie przypadku naruszenia zabezpieczenia systemu ochrony danych osobowych

§ 43. 1. Do czasu przybycia *ABI* zgłaszający:

1) zabezpiecza dostęp do miejsca naruszenia ochrony lub urządzenia przez osoby trzecie;
2) wstrzymuje pracę na komputerze, na którym zaistniało naruszenie ochrony oraz nie uruchamia bez koniecznej potrzeby komputerów i innych urządzeń, które w związku z naruszeniem ochrony zostały wstrzymane;
3) nie zmienia położenia przedmiotów, które pozwolą stwierdzić naruszenie ochrony lub odtworzyć jego okoliczności;
4) podejmuje, stosownie do zaistniałej sytuacji, inne niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych.

2. Zgodę na uruchomienie komputerów i innych urządzeń wyraża *ABI*.

3. Po zaistnieniu okoliczności wskazujących na naruszenie ochrony, osoba zatrudniona przy przetwarzaniu danych może kontynuować pracę dopiero po otrzymaniu zgody *ABI*.

4. Dokonywanie zmian w miejscu naruszenia ochrony bez uzyskania zgody, o której mowa w ust. 1 pkt 3 jest dopuszczalne, jeżeli zachodzi konieczność ratowania osób lub mienia albo zapobieżenia grożącemu niebezpieczeństwu.

5. Okoliczności i przyczyny naruszeń ochrony ustala zespół, w którego skład wchodzi *ABI* oraz pracownik obsługujący stanowisko pracy, na którym nastąpiło naruszenie ochrony.

6. Niezwłocznie po otrzymaniu wiadomości o naruszeniu ochrony zespół, o którym mowa w ust 5, przystępuje do ustalenia okoliczności i przyczyn tego naruszenia, a w szczególności:

1) dokonuje oględzin miejsca naruszenia, bądź urządzenia, w którym wykryto naruszenie oraz bada inne okoliczności, które mogły mieć wpływ na powstanie naruszenia ochrony;
2) wysłuchuje relacji osób, które mogą wnieść nowe fakty dla wyjaśnienia sytuacji;
3) jeżeli jest to konieczne, sporządza szkic lub wykonuje fotografie miejsca naruszenia ochrony;
4) podejmuje decyzje o toku dalszego postępowania, stosownie do zakresu naruszenia lub zasadności podejrzenia naruszenia ochrony i w przypadkach uzasadnionych niezwłocznie powiadamia *ADO*.

7. Zespół, o którym mowa w ust. 5 sporządza protokół oględzin, który stanowi podstawę do:

1) ustalenia skali stwierdzonych naruszeń ochrony, przyczyn ich powstania, skutków, jakie wywołują lub mogą wywołać, w odniesieniu do stanu zabezpieczenia danych osobowych lub ich zbiorów;
2) wyciągnięcia wniosków, zwłaszcza co do podjęcia określonych działań organizacyjnych i technicznych.

8. Protokół oględzin, o którym mowa w ust. 7, zespół, o którym mowa w ust. 5, przedstawia Staroście, który podejmuje decyzję o koniecznych działaniach organizacyjnych i technicznych.

9. *ABI* w przypadkach określonych w *Instrukcji* podejmuje kroki zmierzające do likwidacji naruszeń ochrony i zapobieżenia wystąpieniu ich w przyszłości, w tym celu:

1) w miarę możliwości przywraca stan zgodny z zasadami zabezpieczenia systemu;
2) relacjonuje Staroście przedsięwzięte czynności;
3) o ile taka potrzeba zachodzi, postuluje wprowadzenie nowych form zabezpieczenia systemu, a w razie ich wprowadzenia zaznajamia z nimi osoby zatrudnione przy przetwarzaniu danych.

Rozdział 13

Postanowienia końcowe

§ 44. Osoba zatrudniona przy przetwarzaniu danych osobowych za naruszenie obowiązków wynikających z niniejszej *Instrukcji* i przepisów o ochronie danych osobowych ponosi odpowiedzialność przewidzianą Kodeksem Pracy oraz wynikającą z ustawy, o której mowa w § 45 *Instrukcji*.

§ 45. W sprawach nie uregulowanych Instrukcją zastosowanie mają przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r. Nr 101, poz. 926 – tekst jednolity z późn. zm.).

Załącznik Nr 1
do Instrukcji określającej sposób zarządzania
systemem informatycznym służącym
do przetwarzania danych osobowych
w Starostwie Powiatowym w Gryfinie

Ewidencja osób upoważnionych do pracy w systemie informatycznym Starostwa Powiatowego w Gryfinie oraz upoważnionych do przetwarzania danych osobowych

L.p.	Nazwisko, imię	System/aplikacja	Zakres upoważnienia do przetwarzania danych osobowych (określenie nazwy zbioru danych osobowych lub systemu jednoznacznie identyfikującego zbiór)	Data nadania upoważnienia	Data ustania upoważnienia	Identyfikator użytkownika

Załącznik Nr 2
do Instrukcji określającej sposób zarządzania
systemem informatycznym służącym
do przetwarzania danych osobowych
w Starostwie Powiatowym w Gryfinie

Wniosek o przyznanie/modyfikację uprawnień użytkownika w systemie informatycznym Starostwa Powiatowego w Gryfinie

.....
Wydział/Biuro

Lp.	Nazwisko i imię pracownika	Nr pokoju	System/ podsystem	Zakres dostępu do funkcji i słowników systemu (opcjonalnie)	Czas dostępu do systemów (określone dni, godziny)	Identyfikator (wypełnia administrator systemu)

Wnioskuję o dopisanie w/w użytkownika/ów do wymienionych podsystemów oraz o wydanie upoważnienia do przetwarzania danych osobowych.

Gryfino, dnia .....

.....
Podpis Naczelnika/Kierownika

Załącznik Nr 3
do Instrukcji określającej sposób zarządzania
systemem informatycznym służącym
do przetwarzania danych osobowych
w Starostwie Powiatowym w Gryfinie

UPOWAŻNIENIE
do przetwarzania danych osobowych

Na podstawie art. 37 ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 roku (Dz. U. z 2002 r., Nr 101, poz. 926 - tekst jednolity z późn. zm.) upoważniam:

Panią/Pana .....

Zatrudnioną/ego w .....

Do przetwarzania danych osobowych wynikających z zakresu obowiązków pracowniczych z wyłączeniem udostępniania danych osobowych oraz do następujących zbiorów danych osobowych:

.....

.....

.....

.....

.....

.....

.....

.....

Gryfino, dnia ..... …….....

Podpis Administratora Danych Osobowych

1. Upoważnienie wydaje się na czas nieokreślony.
2. Rozwiązanie stosunku pracy powoduje wygaśnięcie upoważnienia.

Załącznik Nr 4
do Instrukcji określającej sposób zarządzania
systemem informatycznym służącym
do przetwarzania danych osobowych
w Starostwie Powiatowym w Gryfinie

…….....
Imię i nazwisko pracownika

…….....
Stanowisko

…….....
Wydział/Referat

OŚWIADCZENIE

Oświadczam, że w związku z przetwarzaniem danych osobowych wynikającym z wykonywanych przeze mnie czynności służbowych zobowiązuję się do zapoznania i przestrzegania:

1. ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 roku (Dz. U. z 2002 r., Nr 101, poz. 926 - tekst jednolity z późn. zm.),
2. obowiązującej Instrukcji określającej sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Starostwie Powiatowym w Gryfinie.

Gryfino, dnia .....

…….....
Podpis pracownika

Załącznik Nr 5
do Instrukcji określającej sposób zarządzania
systemem informatycznym służącym
do przetwarzania danych osobowych
w Starostwie Powiatowym w Gryfinie

.....
Wydział/Biuro

Wniosek o wyrejestrowanie użytkownika z systemu informatycznego Starostwa Powiatowego w Gryfinie

Proszę o wyrejestrowanie użytkownika .....
z systemu informatycznego. (Imię i nazwisko)

Przyczyną wyrejestrowania jest:

.....

.....

.....

.....

Systemy/podsystemy/aplikacje, z których należy wyrejestrować użytkownika:

.....

.....

.....

.....

Gryfino, dnia ....
Podpis Naczelnika/Kierownika