Załącznik Nr 1
do Zarządzenia Nr 61/2006
Starosty Gryfińskiego
z dnia 30 czerwca 2006 r.

Polityka bezpieczeństwa

systemów informatycznych służących do przetwarzania danych osobowych

w Starostwie Powiatowym w Gryfinie

Opracował: Administrator Bezpieczeństwa Informacji

Czerwiec 2006

Spis treści

Wprowadzenie

Niniejszy dokument opisuje reguły dotyczące bezpieczeństwa danych osobowych zawartych w systemach informatycznych w Starostwie Powiatowym w Gryfinie. Opisane reguły określają granice dopuszczalnego zachowania wszystkich użytkowników systemów informatycznych wspomagających pracę Starostwa. Dokument zwraca uwagę na konsekwencje, jakie mogą ponosić osoby przekraczające określone granice oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń.

Odpowiednie zabezpieczenia, ochrona przetwarzanych danych oraz niezawodność funkcjonowania są podstawowymi wymogami stawianymi współczesnym systemom informatycznym.

Dokument *Polityka bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Starostwie Powiatowym w Gryfinie*, zwany dalej *Polityką bezpieczeństwa*, wskazujący sposób postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych w systemach informatycznych, przeznaczony jest dla osób zatrudnionych przy przetwarzaniu tych danych.
Potrzeba jego opracowania wynika z § 3 rozporządzenia Prezesa Rady Ministrów dnia 25 lutego 1999 roku w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych (Dz.U. Nr 18, poz. 162 z 1999r.) oraz § 3 i 4 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 z 2004r.).

1. *Polityka bezpieczeństwa* określa tryb postępowania w przypadku, gdy:
   1) stwierdzono naruszenie zabezpieczenia systemu informatycznego,
   2) stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci informatycznej mogą wskazywać na naruszenie zabezpieczeń tych danych.

2. *Polityka bezpieczeństwa* obowiązuje wszystkich pracowników Starostwa Powiatowego w Gryfinie.

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 systemach informatycznych Starostwa.

4. Administrator danych osobowych, którym jest Starosta, w drodze zarządzenia, wyznacza Administratora Bezpieczeństwa Informacji, zwanego dalej *ABI* oraz osobę upoważnioną do zastępowania *ABI*.

5. *ABI* realizuje zadania w zakresie ochrony danych osobowych, a w szczególności:
   1) ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach systemów informatycznych,
   2) podejmowania stosownych działań zgodnie z niniejszą *Polityką bezpieczeństwa* w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia danych znajdujących się w systemie informatycznym,

3) niezwłocznego informowania Administratora danych osobowych lub osoby przez niego upoważnionej o przypadkach naruszenia przepisów ustawy o ochronie danych osobowych,
4) nadzoru i kontroli systemów informatycznych służących do przetwarzania danych osobowych i osób przy nim zatrudnionych.

6. Osoba zastępująca *ABI* powyższe zadania realizuje w przypadku nieobecności *ABI*.

7. Osoba zastępująca składa *ABI* relację z podejmowanych działań w czasie jego zastępstwa.

Niniejszy dokument jest zgodny z następującymi aktami prawnymi:
1) ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz.U. Nr 101, poz. 926 z późn. zm.),
2) ustawą z dnia 22 stycznia 1999 roku o ochronie informacji niejawnych (Dz.U. Nr 11, poz. 95 z późn. zm.),
3) rozporządzeniem Prezesa Rady Ministrów dnia 25 lutego 1999 roku w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych (Dz.U. Nr 18, poz. 162).

Rozdział 1

Opis zdarzeń naruszających ochronę danych osobowych

§ 1. Podział zagrożeń:
1) zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych;
2) zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki użytkowników, administratora, awarie sprzętowe, błędy oprogramowania), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych;
3) zagrożenia zamierzone, świadome i celowe – najpoważniejsze zagrożenia, naruszenia poufności danych, zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy, zagrożenia te dzielimy na:
   a) nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu),
   b) nieuprawniony dostęp do systemu z jego wnętrza,
   c) nieuprawniony przekaz danych,
   d) pogorszenie jakości sprzętu i oprogramowania,
   e) bezpośrednie zagrożenie materialnych składników systemu.

§ 2. Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe to głównie:
1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu, jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.;

2) niewłaściwe parametry środowiska, jak np.: nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych;
3) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru;
4) pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu;
5) jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie;
6) nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie;
7) stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji);
8) nastąpiła niedopuszczalna manipulacja danymi osobowymi w systemie;
9) ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń;
10) praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych – np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.;
11) ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. *bocznej furtki*, itp.;
12) podmieniono lub zniszczono nośniki z danymi osobowymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane osobowe;
13) rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.).

§ 3. Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, dyskietkach w formie niezabezpieczonej, płytach CD lub DVD, pamięciach USB itp.

Rozdział 2

Zabezpieczenie danych osobowych

§ 4. Administratorem danych osobowych zawartych i przetwarzanych w systemach informatycznych Starostwa Powiatowego w Gryfinie jest Starosta.

§ 5. Administrator danych osobowych jest obowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w systemach informatycznych Starostwa, a w szczególności:
1) zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym;
2) zapobiegać przed zabraniem danych przez osobę nieuprawnioną;

3) zapobiegać przetwarzaniu danych z naruszeniem ustawy oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych.

§ 6. Do zastosowania środków technicznych należy:
1) przetwarzanie danych osobowych w wydzielonych pomieszczeniach położonych w strefie administracyjnej;
2) zabezpieczenie wejścia do pomieszczeń, o których mowa w pkt 1;
3) szczególne zabezpieczenie centrum przetwarzania danych (serwery, pomieszczenie serwerowni) poprzez zastosowanie systemu kontroli dostępu;
4) wyposażenie pomieszczeń w szafy dające gwarancję bezpieczeństwa dokumentacji.

§ 7. Do zastosowanych środków organizacyjnych należą przede wszystkim następujące zasady:
1) zapoznanie każdej osoby z przepisami dotyczącymi ochrony danych osobowych, przed dopuszczeniem jej do pracy przy przetwarzaniu danych osobowych;
2) przeszkolenie osób, o których mowa w pkt. 1, w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochroną danych osobowych;
3) kontrolowanie otwierania i zamykania pomieszczeń, w których są przetwarzane dane osobowe, polegające na otwarciu pomieszczenia przez pierwszą osobę, która rozpoczyna pracę oraz zamknięciu pomieszczenia przez ostatnią wychodzącą osobę.

§ 8. Niezależnie od niniejszych zasad opisanych w dokumencie *Polityka bezpieczeństwa* w zakresie bezpieczeństwa mają zastosowanie wszelkie wewnętrzne regulaminy lub instrukcje dotyczące bezpieczeństwa ludzi i zasobów informacyjnych oraz indywidualne zakresy zadań osób zatrudnionych przy przetwarzaniu danych osobowych w określonym zakresie.

§ 9. Wzór wykazu pomieszczeń, w których przetwarzane są dane osobowe oraz wzór opisu systemów informatycznych i ich zabezpieczeń zawiera załącznik nr 1 do niniejszego dokumentu. Pełny wykaz pomieszczeń oraz opis systemów informatycznych znajduje się w posiadaniu *ABI*.

Rozdział 3

Kontrola przestrzegania zasad zabezpieczenia danych osobowych

§ 10. *ABI* sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych wynikających z ustawy o ochronie danych osobowych oraz zasad ustanowionych w niniejszym dokumencie.

§ 11. 1. *ABI* sporządza półroczne plany kontroli zatwierdzone przez Starostę i zgodnie z nimi przeprowadza kontrole oraz dokonuje kwartalnych ocen bezpieczeństwa danych osobowych.

2. Na podstawie zgromadzonych materiałów, o których mowa w ust. 1, *ABI* sporządza roczne sprawozdanie i przedstawia Administratorowi danych osobowych.

Rozdział 4

Postępowanie w przypadku naruszenia ochrony danych osobowych

§ 12. 1. W przypadku stwierdzenia naruszenia:
1) zabezpieczenia systemu informatycznego;
2) technicznego stanu urządzeń;
3) zawartości zbioru danych osobowych;
4) ujawnienia metody pracy lub sposobu działania programu;
5) jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych;
6) innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. zalanie, pożar, itp.)

każda osoba zatrudniona przy przetwarzaniu danych osobowych jest obowiązana niezwłocznie powiadomić o tym fakcie *ABI*.

2. W razie niemożliwości zawiadomienia *ABI* lub osoby przez niego upoważnionej, należy powiadomić bezpośredniego przełożonego.

3. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych *ABI* lub upoważnionej przez niego osoby, należy:
1) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców;
2) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia;
3) zaniechać, o ile to możliwe, dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę;
4) podjąć inne działania przewidziane i określone w instrukcjach technicznych i technologicznych stosownie do objawów i komunikatów towarzyszących naruszeniu;
5) podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej;
6) zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku;
7) udokumentować wstępnie zaistniałe naruszenie;
8) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia *ABI* lub osoby upoważnionej.

4. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych, *ABI* lub osoba upoważniona:
1) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy;
2) może zażądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem;
3) rozważa celowość i potrzebę powiadamiania o zaistniałym naruszeniu Administratora danych osobowych;
4) nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba, ze specjalistami spoza Starostwa.

5. *ABI* dokumentuje zaistniały przypadek naruszenia oraz sporządza raport wg wzoru stanowiącego załącznik nr 2, który powinien zawierać w szczególności:
1) wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpytanych w związku z naruszeniem,

2) określenie czasu i miejsca naruszenia i powiadomienia,
3) określenie okoliczności towarzyszących i rodzaju naruszenia,
4) wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania,
5) wstępną ocenę przyczyn wystąpienia naruszenia,
6) ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.

6. Raport, o którym mowa w ust. 5, *ABI* niezwłocznie przekazuje Administratorowi danych osobowych, a w przypadku jego nieobecności osobie uprawnionej.

§ 13. Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu *ABI* zasięga niezbędnych opinii i proponuje postępowanie naprawcze, a w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych.

§ 14. 1. Zaistniałe naruszenie może stać się przedmiotem szczegółowej, zespołowej analizy prowadzonej przez Kierownictwo Starostwa, *ABI*, Pełnomocnika ds. Ochrony Informacji Niejawnych.

2. Analiza, o której mowa w ust. 1, powinna zawierać wszechstronną ocenę zaistniałego naruszenia, wskazanie odpowiedzialnych, wnioski, co do ewentualnych przedsięwzięć proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.

Rozdział 5

Postanowienia końcowe

§ 15. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie dyscyplinarne.

§ 16. *ABI* zobowiązany jest prowadzić ewidencję osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych wg wzoru stanowiącego załącznik nr 3 do niniejszego dokumentu. Pełny wykaz osób znajduje się w posiadaniu *ABI*.

§ 17. 1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, w szczególności przez osobę, która wobec naruszenia zabezpieczenia systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym *ABI*.

2. Orzeczona kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia *ABI* nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz.U. Nr 101, poz. 926 z późn. zm.) oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

§ 18. W sprawach nie uregulowanych niniejszym dokumentem mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz.U. Nr 101, poz. 926 z późn. zm.), 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) oraz rozporządzenie Ministra Sprawiedliwości z dnia 28 kwietnia 2004 roku w sprawie sposobu technicznego przygotowania systemów i sieci do przekazywania informacji – do gromadzenia wykazów połączeń telefonicznych i innych przekazów informacji oraz sposobów zabezpieczenia danych informatycznych (Dz.U. Nr 100, poz. 1023).

Załącznik nr 1 do Polityki bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Starostwie Powiatowym w Gryfinie

Wzór wykazu pomieszczeń, w których przetwarzane są dane osobowe oraz wzór opisu systemów informatycznych i ich zabezpieczeń.

1. Wzór wykazu pomieszczeń, w których przetwarzane są dane osobowe.

Lp.	Nr pokoju	Komórka organizacyjna	Program do przetwarzania

2. Wzór opisu systemów informatycznych (zbiorów danych osobowych) oraz programy zastosowane do przetwarzania tych danych.

Lp.	Nazwa zbioru (opis)	Program do przetwarzania

3. W celu ochrony danych osobowych stosowane są następujące zabezpieczenia:
   1) odrębne zasilanie sprzętu komputerowego, jeżeli pozwoli na to rozwiązanie architektury sieci elektrycznej w budynku,
   2) ochrona serwerów i stacji roboczych przed zanikiem zasilania poprzez zastosowanie zasilaczy awaryjnych UPS,
   3) ochrona przed utratą zgromadzonych danych przez robienie kopii zapasowych na taśmach magnetycznych, z których w przypadku awarii odtwarzane są dane oraz okresowe próby odtwarzania danych z kopii,

   4) zabezpieczenie przed nieautoryzowanym dostępem do baz danych:
      a) podłączenie danego użytkownika do sieci komputerowej dokonuje *ABI*,
      b) w celu uzyskania dostępu do zasobów sieci należy zwrócić się do *ABI* z odpowiednim wnioskiem, w którym podane będą dane nowego użytkownika oraz zasoby, jakie ma on mieć udostępnione,
      c) w systemie informatycznym Starostwa zastosowano podwójną autoryzację użytkownika. Pierwszej autoryzacji należy dokonać w momencie uzyskania dostępu do serwera, podając login użytkownika i hasło. Drugiej autoryzacji należy dokonać uruchamiając program użytkowy, podając również login użytkownika i hasło. Dostęp do wybranej bazy danych uzyskuje się dopiero po poprawnym podwójnym zalogowaniu się do systemu informatycznego Starostwa.
      d) dostęp do stacji roboczej zabezpieczony poprzez wprowadzone na poziomie BIOS-u hasło dostępu do komputera, odrębne dla użytkownika oraz dla administratora (tylko wówczas, gdy wersja BIOS-u pozwala na określenie odrębnych haseł) oraz poprzez zastosowanie wygaszacza ekranowego, który po upływie określonego czasu bezczynności użytkownika wygasza monitor

i jednocześnie uruchamia blokadę, która uniemożliwia kontynuowanie pracy na komputerze bez podania właściwego hasła.

5) zabezpieczenie przed nieautoryzowanym dostępem do baz danych poprzez Internet:
   a) w zakresie dostępu z sieci lokalnej Starostwa do sieci rozległej Internet zastosowano środki ochrony przed podsłuchiwaniem, penetrowaniem i atakiem z zewnątrz,
   b) zastosowano firewall (ścianę ogniową), która ma za zadanie uwierzytelnianie źródła przychodzących wiadomości oraz filtrowanie pakietów w oparciu o adres IP, numer portu i inne parametry. Firewall składa się z bezpiecznego systemu operacyjnego i filtra pakietów. Ruch pakietów, który firewall przepuszcza jest określony przez *ABI*. Firewall zapisuje w logu fakt zaistnienia wyjątkowych zdarzeń i śledzi ruch pakietów przechodzących przez nią, a dostęp do sieci jest ustalony indywidualnie dla każdego użytkownika na podstawie wniosku,
   c) zastosowano system wykrywający obecność wirusów, trojanów i robaków internetowych w poczcie elektronicznej,
   d) zastosowano ochronę antywirusową wszystkich danych ściąganych z Internetu na stacjach roboczych.
6) ochrona przed awarią systemu dyskowego serwerów poprzez zastosowanie macierzy dyskowych, uszkodzenie jakiegokolwiek z dysków systemu dyskowego nie spowoduje utraty danych, a nawet zatrzymania pracy systemu,
7) postanowienia końcowe:
   a) do pomieszczeń, w których następuje przetwarzanie danych osobowych mają dostęp tylko uprawnione osoby bezpośrednio związane z nadzorem nad serwerami lub aplikacjami. Dostęp do serwerowi powinien być kontrolowany za pomocą drzwi z elektronicznym zamkiem szyfrowym,
   b) zabezpieczenie przed nieuprawnionym dostępem do danych, prowadzone jest przez *ABI* zgodnie z przyjętymi procedurami nadawania uprawnień do systemu informatycznego,
   c) osoby mające dostęp do danych powinny posiadać zaświadczenie o przebytym szkoleniu z zakresu ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz.U. Nr 101, poz. 926 z późn. zm.),
   d) w pomieszczeniach, w których znajdują się serwery zamontowane są czujniki dymu oraz czujniki ruchu,
   e) w pomieszczeniach, w których znajdują się serwery powinna być zamontowana klimatyzacja, która zapewnia właściwą temperaturę i wilgotność powietrza dla sprzętu komputerowego,
   f) w pobliżu wejścia do pomieszczeń z serwerami i innymi urządzeniami znajduje się gaśnica, która okresowo jest napełniana i kontrolowana przez specjalistę,
   g) większość urządzeń w serwerowi umieszczona jest w szafach serwerowych i sieciowych.

Załącznik nr 2 do Polityki bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Starostwie Powiatowym w Gryfinie

RAPORT
z naruszenia bezpieczeństwa systemu informatycznego
w Starostwie Powiatowym w Gryfinie

1. Data: ……..……..…….. Godzina: ……..…….....
   (dd.mm.rrrr) (00:00)
2. Osoba powiadamiająca o zaistniałym zdarzeniu:

……..
(Imię, nazwisko, stanowisko służbowe, nazwa użytkownika (jeśli występuje))
3. Lokalizacja zdarzenia:

……..
(budynek, nr pokoju, nazwa pomieszczenia)
4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

……..

……..
5. Podjęte działania:

……..

……..
6. Przyczyny wystąpienia zdarzenia:

……..

……..
7. Postępowanie wyjaśniające:

……..

……..

……..……..
Data, podpis Administratora Bezpieczeństwa Informacji

Załącznik nr 3 do Polityki bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Starostwie Powiatowym w Gryfinie

Wzór wykazu osób, które zostały zapoznane z *Polityką bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Starostwie Powiatowym w Gryfinie*, przeznaczonej dla osób zatrudnionych przy przetwarzaniu tych danych.

Przyjąłem/am do wiadomości i stosowania zapisy *Polityki bezpieczeństwa*.

Imię i nazwisko	**Komórka organizacyjna**	**Data, podpis**