Załącznik do Zarządzenia
Starosty Powiatu Żyrardowskiego
Nr 36/10 z dnia 31.12.2010r.

Polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych Starostwa Powiatowego w Żyrardowie

STAROSTA
inż. Wojciech Szustakiewicz

Opracował : Artur Foks

Administrator Bezpieczeństwa Informacji

SPIS TREŚCI:

§ 1.

Podstawa prawna

Niniejszy dokument reguluje sprawy ochrony danych osobowych przetwarzane w Starostwie Powiatowym w Żyrardowie i jest zgodny z następującymi aktami prawnymi:
1) ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002r., Nr 101, poz. 926 wraz z późniejszymi zmianami),
2) rozporządzeniem 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),

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 operatorów, 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 możemy podzielić na: nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu), nieuprawniony dostęp do systemu z jego wnętrza, nieuprawniony przekaz danych, pogorszenie jakości sprzętu i oprogramowania, 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 itp.

ZABEZPIECZENIE DANYCH OSOBOWYCH

1. Administratorem danych osobowych zawartych i przetwarzanych w systemach informatycznych Starostwa Powiatowego w Żyrardowie jest Starosta.

2. 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.

3. Do zastosowanych 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 (komputer centralny, serwerownia) poprzez zastosowanie systemu kontroli dostępu,
4) wyposażenie pomieszczeń w szafy dające gwarancję bezpieczeństwa dokumentacji,

4. 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.

5. Niezależnie od niniejszych zasad opisanych w dokumencie „Polityka bezpieczeństwa w Starostwie Powiatowym" 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 systemie.

6. Wykaz pomieszczeń w których przetwarzane są dane osobowe oraz opis systemów informatycznych Starostwa Powiatowego w Żyrardowie i ich zabezpieczeń zawiera załącznik nr 1 do niniejszego dokumentu.

7. W celu ochrony przed utratą danych w Starostwie Powiatowym w Żyrardowie stosowane są następujące zabezpieczenia:

1) ochrona sprzętu komputerowego przed zanikiem zasilania poprzez stosowanie zasilaczy zapasowych UPS,
2) ochrona serwerów przed zanikiem zasilania poprzez stosowanie zasilaczy zapasowych UPS,
3) ochrona przed utratą zgromadzonych danych przez robienie kopii zapasowych na dodatkowym komputerze i płytach CD, z których w przypadku awarii odtwarzane są dane i oprogramowanie biurowe
4) ochrona przed awarią podsystemu dyskowego przez używanie macierzy dyskowych.

Uszkodzenie jakiegokolwiek z dysków zestawu nie spowoduje utraty danych, a nawet zatrzymania pracy systemu (zastosowanie elementów hotswap i hotspare).

Zabezpieczenia przed nieautoryzowanym dostępem do baz danych Starostwa:

1) wszystkie gniazdka lokalnej sieci komputerowej są galwanicznie oddzielone od szkieletu sieci komputerowej. Podłączenie (zkrosowanie) danego użytkownika do sieci komputerowej dokonuje Administrator Bezpieczeństwa Informacji.
2) aby uzyskać dostęp do zasobów sieci, należy zwrócić się do Administratora Bezpieczeństwa z odpowiednim wnioskiem w którym podane będą dane nowego użytkownika oraz zasoby jakie ma on mieć udostępnione.
3) w systemie informatycznym Starostwa zastosowano podwójną autoryzację użytkownika. Pierwszej autoryzacji należy dokonać w momencie uzyskania dostępu do serwera Starostwa, podając login użytkownika i hasło. Drugiej autoryzacji należy dokonać Uruchamiając program użytkowy, podając login użytkownika i hasło. Dostęp do wybranej bazy danych Starostwa uzyskuje się dopiero po poprawnym podwójnym zalogowaniu się do systemu informatycznego Urzędu.

Zabezpieczenia przed nieautoryzowanym dostępem do baz danych Starostwa Powiatowego w Żyrardowie poprzez internet.

W zakresie dostępu z sieci wewnętrznej Starostwa do sieci rozległej Internet zastosowano środki ochrony przed podsłuchiwaniem, penetrowaniem i atakiem z zewnątrz. Zastosowano firewall, który ma za zadanie uwierzytelnianie źródła przychodzących wiadomości oraz filtrowanie pakietów w oparciu o adres IP, numer portu i inne parametry. Ściana ogniowa składa się z bezpiecznego systemu operacyjnego i filtra pakietów. Ruch pakietów, który firewall przepuszcza jest określony przez administratora.

Firewall zapisuje do logu fakt zaistnienia wyjątkowych zdarzeń i śledzi ruch pakietów przechodzących przez nią. Dostęp do sieci jest ustalony indywidualnie dla każdego użytkownika na podstawie wniosku.

Oprócz filtra pakietów (firewall) zastosowano również system wykrywający obecność wirusów w poczcie elektronicznej.

W efekcie zapewnione jest:

1) zabezpieczenie sieci przed atakiem z zewnątrz poprzez blokowanie wybranych portów,
2) filtrowanie pakietów i blokowanie niektórych usług,
3) objęcie ochroną antywirusową wszystkich danych ściąganych z Internetu na stacjach lokalnych,
4) zapisywanie logów połączeń użytkowników z siecią Internet

3. Postanowienia końcowe.

1) do pomieszczeń w których następuje przetwarzanie danych osobowych mają dostęp tylko uprawnione osoby bezpośrednio związane z nadzorem nad serwerami lub aplikacjami. Dostęp ten powinien być kontrolowany za pomocą drzwi z zamkiem.
2) zabezpieczenie przed nieuprawnionym dostępem do danych, prowadzone jest przez Administratora Bezpieczeństwa zgodnie z przyjętymi procedurami nadawania uprawnień do systemu informatycznego.
3) osoby mające dostęp do danych powinny posiadać zaświadczenie o przebytym szkoleniu z zakresu ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997r. (Dz. U. Nr 133, poz. 883 z późn. zm.).
4) w pomieszczeniach w których znajdują się serwery powinna być zamontowana klimatyzacja, która zapewnia właściwą temperaturę i wilgotność powietrza dla sprzętu komputerowego
5) w pobliżu wejścia do pomieszczenia z serwerami i innym urządzeniami znajduje się gaśnica, która okresowo jest napełniana i kontrolowana przez specjalistę.
6) większość urządzeń w serwerowni umieszczona jest w szafach serwerowych i sieciowych.

KONTROLA PRZESTRZEGANIA ZASAD ZABEZPIECZENIA DANYCH OSOBOWYCH

1. Administrator danych lub osoba przez niego wyznaczona, którą jest „Administrator Bezpieczeństwa Informacji" sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych wynikających z ustawy o ochronie danych osobowych oraz zasad ustanowionych w niniejszym dokumencie.

2. Administrator Bezpieczeństwa sporządza półroczne plany kontroli zatwierdzone przez Starostę i zgodnie z nimi przeprowadza kontrole oraz dokonuje kwartalnych ocen stanu bezpieczeństwa danych osobowych.

1. Na podstawie zgromadzonych materiałów, o których mowa w ust. 2, Administrator Bezpieczeństwa sporządza roczne sprawozdanie i przedstawia Administratorowi danych (Staroście).

POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

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 Administratora Bezpieczeństwa.

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

3. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych Administratora Bezpieczeństwa 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 Administratora Bezpieczeństwa lub osoby upoważnionej.

1. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych, Administrator Bezpieczeństwa lub osoba go zastępująca:

1) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy Starostwa,
2) może żądać 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 powiadamia o zaistniałym naruszeniu Administratora danych ,
2) nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba, ze specjalistami spoza urzędu.

6. Administrator Bezpieczeństwa 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.

7. Raport, o którym mowa w ust. 6, Administrator Bezpieczeństwa niezwłocznie przekazuje Administratorowi danych (Staroście), a w przypadku jego nieobecności osobie uprawnionej.

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

9. Zaistniałe naruszenie może stać się przedmiotem szczegółowej, zespołowej analizy prowadzonej przez Kierownictwo urzędu, Administratora Bezpieczeństwa Informacji, Pełnomocnika ds. Ochrony Informacji Niejawnych.

10. Analiza, o której mowa w ust. 9, 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.

MONITOROWANIE ZABEZPIECZEŃ

1. Prawo do monitorowania systemu zabezpieczeń posiadają , zgodnie z zakresem czynności:
   a) Administrator Danych,
   b) Administrator Bezpieczeństwa Informacji.

2. W ramach kontroli należy zwracać szczególna uwagę na:

   a) okresowe sprawdzanie kopii bezpieczeństwa pod względem przydatności do możliwości odtwarzania danych,
   b) kontrola ewidencji nośników magnetycznych i optycznych,
   c) kontrola właściwej częstotliwości zmiany haseł .

SZKOLENIA

1. Wszyscy pracownicy Starostwa mają obowiązek brać udział w szkoleniach ,
2. Szkolenie powinno dotyczyć:
   a) obowiązujących przepisów i instrukcji wewnętrznych dotyczących ochrony danych osobowych, sposobu niszczenia wydruków i zapisów na nośnikach magnetycznych i optycznych,
   b) przedstawienie zasad ochrony danych osobowych dotyczących bezpośrednio wykonywanych obowiązków na stanowisku pracy.

NISZCZENIE WYDRUKÓW I ZAPISÓW NA NOŚNIKACH MAGNETYCZNYCH

1. Nośniki magnetyczne przekazywane na zewnątrz powinny być pozbawione zapisów zawierających dane osobowe.,
2. Niszczenie poprzednich zapisów powinno odbywać się poprzez wymazywanie informacji oraz formatowanie nośnika,
3. Poprawność przygotowania nośnika magnetycznego powinna być sprawdzona przez Administratora Bezpieczeństwa Informacji,
4. Uszkodzone nośniki magnetyczne przed ich wyrzuceniem należy fizycznie zniszczyć poprzez przecięcie, przełamanie itp.
5. Wydruki po wykorzystaniu należy zniszczyć w mechanicznej niszczarce do papieru.
6. Komputery powinny być utylizowane.

ARCHIWIZACJA DANYCH

1. Dane programów biurowych kopiowane są codziennie,
2. Kopie awaryjne danych zapisywanych w programach wykonywane są w systemie tygodniowym,
3. Odpowiedzialnym za wykonywanie kopii danych i kopii awaryjnych jest Administrator Bezpieczeństwa Informacji,
4. Na koniec danego miesiąca wykonywane są kopie bezpieczeństwa z całego programu przetwarzającego dane. Nośniki z kopiami bezpieczeństwa przechowywane są w szafie zabezpieczonej zamkiem,
5. Kopie awaryjne przechowywane są w wyznaczonym pomieszczeniu,
6. Płyty CD , na których przechowuje się kopie awaryjne niszczy się w sposób mechaniczny , tak by nie można było użyć ich ponownie,
7. Administrator Bezpieczeństwa Informacji odpowiedzialny jest za dokonywanie wymiany kopii awaryjnych na aktualne,
8. Administrator Bezpieczeństwa Informacji dokonuje okresowej weryfikacji kopii bezpieczeństwa pod kątem ich czytelności i odtwarzalności

Komputery na których przetwarzane są dane osobowe nie mają bezpośredniego dostępu do sieci publicznej. Dostęp do sieci publicznej realizowany jest poprzez sprzętowo programowe rozwiązania zapewniające bezpieczeństwo dostępu. Polega ono na translacji adresów NAT na sprzętowym urządzeniu typu router. Drugim poziomem zabezpieczeń jest Microsoft ISA Server, za pośrednictwem którego udzielany jest bezpieczny dostęp do sieci publicznej.

POSTANOWIENIA KOŃCOWE

1. 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.

2. Administrator Bezpieczeństwa 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 4 do niniejszego dokumentu.

3. 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 Administratora Bezpieczeństwa.

4. Orzeczona kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia administratora bezpieczeństwa informacji nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926) oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

5. W sprawach nie uregulowanych niniejszym dokumentem mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926), 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) oraz rozporządzenie Ministra Sprawiedliwości z dnia 28 kwietnia 2004 r. 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).

6. Niniejsza „Polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Starostwie Powiatowym w Żyrardowie" wchodzi w życie z dniem jej podpisania przez Starostę.

STAROSTA

inż. Wojciech Szustakiewicz

Załącznik nr 1 do „ Polityki bezpieczeństwa"

Granice obszarów oraz osoby i wydziały , które przetwarzają dane osobowe.

POKÓJ NR od 101 do 115 – I piętro	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Wydział Finansowo-Księgowy (Kasa) Wydział Organizacyjny Wydział Komunikacji, Transportu i Dróg Publicznych Wydział Rozwoju i Budownictwa Stanowisko ds. Zarządzania Kryzysowego, Ochrony Ludności i Spraw Obronnych Pełnomocnik ds. Ochrony Informacji Niejawnych Pomieszczenie gospodarcze

POKÓJ NR od 201 do 215 – II piętro	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Starosta Powiatu Wicestarosta Powiatu Członek Zarządu Powiatu Przewodniczący Rady Powiatu Sekretarz Powiatu Skarbnik Powiatu Pełnomocnik ds. Kontroli Wewnętrznej Pełnomocnik ds. Społeczeństwa Informacyjnego Pełnomocnik ds. Zamówień Publicznych Pełnomocnik ds. Promocji i Współpracy z U.E. Zespół Radców Prawnych Wydział Organizacyjny Wydział Oświaty, Kultury, Sportu i Turystyki Wydział Ochrony Środowiska i Rolnictwa Wydział Finansowo-Księgowy

POKÓJ NR od 303 do 316 – III piętro	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Powiatowy Rzecznik Konsumentów Wydział Geodezji i Gospodarki Nieruchomościami

Osoby mające prawo wglądu do danych osobowych w kartotekach z uwagi na wykonywane zakresy czynności	
1.	Administrator Danych
2.	Sekretarz Powiatu
3.	Administrator Bezpieczeństwa Informacji
4.	Radca Prawny
5.	Audytor Wewnętrzny
6.	Pełnomocnik ds. Ochrony Informacji Niejawnych

Uwaga!

1. Obsługa techniczna urzędu, (sprzątaczki , pracownicy gospodarczy podpisują oświadczenie , którego wzór stanowi załącznik nr 6 do „Polityki bezpieczeństwa".
2. Osoby odbywające staż, praktykę mają wgląd do danych osobowych oraz do systemu informatycznego na podstawie upoważnienia (zał. nr 6) nadanego przez Administratora oraz oświadczenia (zał. nr 5).

Załącznik nr 2 do „ Polityki bezpieczeństwa" - Opis struktur zbiorów danych.

Zgłoszenia zbioru danych należy dokonać na formularzu, którego wzór stanowi załącznik do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. Nr 229, poz. 1536). Stosownie do art. 41 ust. 1 ustawy o ochronie danych osobowych, zgłoszenie zbioru danych do rejestracji powinno zawierać:

1. wniosek o wpisanie zbioru do rejestru zbiorów danych osobowych,
2. oznaczenie podmiotu prowadzącego zbiór i adres jego siedziby lub miejsca zamieszkania, w tym numer identyfikacyjny rejestru podmiotów gospodarki narodowej, jeżeli został mu nadany, oraz podstawę prawną upoważniającą do prowadzenia zbioru, a w przypadku podmiotu, o którym mowa w art. 31a, oznaczenie tego podmiotu i adres jego siedziby lub miejsce zamieszkania,
3. cel przetwarzania danych,

3a. opis kategorii osób, których dane dotyczą, oraz zakres przetwarzanych danych,

4. sposób zbierania oraz udostępniania danych,

4a. informację o odbiorcach lub kategoriach odbiorców, którym dane mogą być przekazywane,

5. opis środków technicznych i organizacyjnych zastosowanych w celach określonych w art. 36-39,
6. informację o sposobie wypełniania warunków technicznych i organizacyjnych, określonych w przepisach, o których mowa w art. 39a,
7. informację dotyczącą ewentualnego przekazywania danych do państwa trzeciego.

Zgłoszenie powinno zawierać wszystkie informacje, o których mowa w art. 41 ust. 1 pkt 1-7 ustawy być podpisane przez administratora danych (np. osobę fizyczną prowadzącą działalność gospodarczą jednoosobowo) lub inną osobę upoważnioną do reprezentowania wnioskodawcy.
Zgłoszenie można również przesłać pocztą lub złożyć w Biurze Generalnego Inspektora Ochrony Danych Osobowych (ul. Stawki 2, 00-193 Warszawa). Od lipca 2006 r. zgłoszenia można dokonać także drogą elektroniczną z użyciem bezpiecznego podpisu elektronicznego. Zgłoszenie można również dokonać drogą elektroniczną bez użycia podpisu elektronicznego, a następnie uzupełnić zgłoszenie w formie papierowej. Aplikacja umożliwiająca skuteczne dokonanie zgłoszenia drogą elektroniczną znajduje się na stronie internetowej Generalnego Inspektora Ochrony Danych Osobowych w systemie.

Wykaz zbiorów zgłoszonych do Generalnego Inspektora Ochrony Danych Osobowych, znajduje się u Administratora Bezpieczeństwa Informacji.

Załącznik nr 3 do „Polityki bezpieczeństwa „

W z ó r

R a p o r t
z naruszenia bezpieczeństwa systemu informatycznego
w Starostwie Powiatowym

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:

.....
(np. 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 4 do „ Polityki bezpieczeństwa „

W z ó r

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

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

Nazwisko i Imię	Komórka organizacyjna	Data, podpis

Załącznik nr 5 do „Polityki bezpieczeństwa".

W z ó r

.....
/imię i nazwisko pracownika/

.....

.....
/stanowisko/

OŚWIADCZENIE

1. Stwierdzam własnoręcznym podpisem, że znana jest mi treść przepisów :
   a) o ochronie tajemnic prawnie chronionych stanowiących tajemnicę służbową wynikającą z Kodeksu Pracy,
   b) o ochronie danych osobowych wynikająca z ustawy o ochronie danych osobowych (Dz.U.Nr 133, poz.833 ze zm.) ,
   c) o odpowiedzialności karnej za naruszenie ochrony danych osobowych.

2. Zobowiązuję się nie ujawniać wiadomości, z którymi zapoznałem/am się w trakcie wykonywanych czynności służbowych .

.....
(podpis pracownika)

.....
(podpis złożono w obecności)

Załącznik nr 6 do „Polityki bezpieczeństwa".

W z ó r

Miejscowość, data

U P O W A Ż N I E N I E Nr

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

upoważniam Pana Imię Nazwisko

zatrudnioną na stanowisku (stanowisko) - (Wydział)

do przetwarzania danych osobowych, obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych

w Starostwie Powiatowym w Żyrardowie

Upoważnienie wydaje się na czas zatrudnienia. Z dniem podpisania przedmiotowego upoważnienia przez pracownika, wszystkie wydane wcześniej upoważnienia dotyczące przetwarzania danych osobowych w Starostwie Powiatowym tracą swoją moc.

Administrator Bezpieczeństwa Informacji

Załącznik nr 7 do „Polityki bezpieczeństwa".

Wniosek

W z ó r **o założenie profilu/nadanie uprawnień/modyfikację uprawnień ***

Dane użytkownika

Nazwisko	
Imię	
Stanowisko służbowe	
Wydział	
Telefon stacjonarny	
e-mail	
Nr upoważnienia dot. obsługi systemu informatycznego w zakresie przetwarzania danych osobowych	

Wnioskuję o :

założenie profilu i nadanie uprawnień*)

modyfikację uprawnień na wymienione poniżej*)

zablokowanie profilu*)

Wnioskowane uprawnienia do systemu

……

(nazwa bazy danych) [1]

Uprawnienie, które ma być przyznane pracownikowi, należy zaznaczyć w pierwszej kolumnie znakiem „x".

TAK	Nazwa	Opis uprawnienia	Uwagi
	Z	Pełne prawa do zarządzania bazą	
	W	Pełne prawa do edycji danych (w tym drukowania, usuwania)	
	N	Prawo do zakładania nowych kont	
	M	Prawo do dodawania i modyfikacji danych	
	P	Prawo do przeglądania danych na ekranie	
	D	Prawo do drukowania danych	
	A	Prawo do wykonywania kopii archiwalnych	
	INNE		

Wniosek o nadanie / modyfikację uprawnień złożył :

Nazwisko i imię : Dnia / /

_____ : _____

Podpis : _____

Oświadczam, że zostałem przeszkolony z zasad bezpieczeństwa przetwarzania danych osobowych i zobowiązuję się do ich przestrzegania.	Data, podpis użytkownika profilu
Upoważniam w/w pracownika do obsługi systemu informatycznego w zakresie przetwarzania danych osobowych zgodnie z Ustawą o ochronie danych osobowych z dnia 29.08.1997 r.(Dz. U. z 2002 r. nr 101, poz. 926 z późn. zm.)	Data, podpis Administratora Bezpieczeństwa Informacji

Nadanie / modyfikację uprawnień wykonał :

Nazwisko i imię : _____ : Dnia / / _____

Podpis : _____

NADANO IDENTYFIKATOR : | | | | | | | | | |

* - niepotrzebne skreślić
1 - nazwa bazy danych z załącznika nr 1 do Instrukcji zarządzania systemami informatycznymi w zakresie wymogów bezpieczeństwa przetwarzania danych osobowych w Ministerstwie Środowiska