ZARZĄDZENIE NR 0050.142.2012
BURMISTRZA WYRZYSKA

z dnia 30 listopada 2012 r.

w sprawie ochrony danych osobowych w Urzędzie Miejskim w Wyrzysku.

Na podstawie art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z póź. zm.) oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji, przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024) zarządzam, co następuje:

§ 1. Wprowadza się „Politykę bezpieczeństwa i instrukcję zarządzania systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Miejskim w Wyrzysku.", stanowiącą załącznik do zarządzenia.

§ 2. Traci moc Zarządzenie Nr 69/2005 Burmistrza Wyrzyska z dnia 18 lipca 2005 r. w sprawie „Polityki bezpieczeństwa i instrukcji zarządzania systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Miejskim w Wyrzysku."

§ 3. Wykonanie zarządzenia powierza się Administratorowi Bezpieczeństwa Informacji.

§ 4. Zarządzenie wchodzi w życie z dniem wydania.

Załącznik do Zarządzenia Nr 0050.142.2012
Burmistrza Wyrzyska
z dnia 30 listopada 2012 r.

Polityka bezpieczeństwa i instrukcja zarządzania systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Miejskim w Wyrzysku.

Rozdział 1.
Postanowienia ogólne.

§ 1. Stosowane definicje i określenia:

1) **dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden z kilku specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne;
2) **zbiór danych osobowych (ZDO) -** każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony (jego części znajdują się w różnych miejscach) lub podzielony funkcjonalnie (przetwarzany za pomocą programów realizujących różne funkcje);
3) **przetwarzanie danych osobowych** – jakiekolwiek operacje wykonywane na danych osobowych, takie jak **zbieranie,** utrwalanie, przechowywanie, opracowywanie, udostępnianie i usuwanie; zwłaszcza takie, które wykorzystuje się w systemach informatycznych;
4) **system informatyczny** – system przetwarzania informacji wraz ze związanymi z nimi ludźmi oraz zasobami technicznymi i finansowymi, które dostarcza i rozprowadza informacje. W szczególności systemem informacyjnym może być system, w którym nie będzie żadnego komputera, a wyłącznie dokumenty papierowe, skoroszyty oraz ludzie tam pracujący, wyposażenie pokoi, czy też organizacja pracy. Ochronie podlegają nie tylko informacje osobowe, ale także ludzie, zasoby techniczne i finansowe;
5) **bezpieczeństwo systemu informatycznego** – wdrożenie 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;

6) **Administrator Danych Osobowych (ADO)** – organ, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania danych osobowych. Administratorem danych jest Burmistrz, który ponosi pełnię odpowiedzialności wynikającej z przepisów ustawy o ochronie danych osobowych w odniesieniu do zbiorów danych osobowych znajdujących się w jego ustawowej dyspozycji;
7) **Administrator Bezpieczeństwa Informacji (ABI)** – należy przez to rozumieć pracownika urzędu wyznaczonego przez Administratora Danych Osobowych do nadzorowania przestrzegania zasad ochrony oraz wymagań w zakresie ochrony, wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych;
8) **Administrator Systemów Informatycznych (ASI)** – należy przez to rozumieć pracownika lub pracowników Informatyki odpowiedzialnych za stosowanie technicznych i organizacyjnych środków ochrony danych osobowych;
9) **Właściciel Zbioru Danych Osobowych (WZDO)** – osoba kierująca komorką organizacyjną lub samodzielne stanowiska, odpowiedzialna za ochronę danych osobowych przetwarzanych na stanowisku lub w podległej komórce. Jest ona zobowiązana zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy o ochronie danych osobowych oraz nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.
10) **osoba upoważniona lub użytkownik systemu** – osoba posiadająca upoważnienie wydane przez ADO **lub** osoba uprawniona przez niego i dopuszczona jako użytkownik do przetwarzania danych osobowych w systemie informatycznym danej komórki organizacyjnej, w zakresie wskazanym w upoważnieniu, zwana dalej użytkownikiem;
11) **osoba uprawniona** – osoba posiadająca uprawnienie wydane przez ADO na mocy którego **wykonuje** w jego imieniu określone czynności;
12) **sieć Lokalna (LAN)** – lokalna sieć teleinformatyczna;
13) **sieć rozległa (WAN)** – rozległa sieć teleinformatyczna;
14) **identyfikator użytkownika (LOGIN)** – ciąg znaków literowych i cyfrowych, lub innych, jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
15) **hasło (Password)** – ciąg znaków literowych cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
16) **zalogowanie** – uwierzytelnienie, czyli działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;

17) **odbiorcy danych -** rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:

a) **osoby,** której dane dotyczą,

b) **osoby,** upoważnionej do przetwarzania danych,

c) **przedstawiciela,** o którym mowa w art. 31a ustawy o ochronie danych osobowych,

d) **podmiotu,** o którym mowa w art. 31 ustawy o ochronie danych osobowych,

e) **organów** państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

18) **zwrotna informacja telefoniczna** – czynności polegająca na:

a) przyjęciu wniosku telefonicznego o udostępnienie danych wraz z informacją o tożsamości, **nazwie** komórki organizacyjnej, nazwie zamiejscowej komórki organizacyjnej, nazwie podległej jednostce organizacyjnej, numerze telefonu wnioskodawcy,

b) oddzwonienie ze stosowna informacją bądź danymi, po uprzednim sprawdzeniu **prawdziwości** i autentyczności wnioskodawcy.

Rozdział 2.
Zasady postępowania przy przetwarzaniu danych osobowych

§ 2. 1. Administrator Danych Osobowych, zarządzeniem wyznacza Administratora Bezpieczeństwa Informacji dla danych przetwarzanych w Urzędzie Miejskim, zwanego dalej Administratorem Bezpieczeństwa Informacji oraz osobę upoważnioną do zastępowania Administratora Bezpieczeństwa Informacji.

2. Administrator Danych Osobowych jest zobowiązany do:

1) czuwania nad tym, by będące w jego posiadaniu dane osobowe były przetwarzane zgodnie z prawem;
2) zastosowania niezbędnych środków technicznych i organizacyjnych w celu zapewnienia ochrony przetwarzanych w Urzędzie Gminy danych osobowych;
3) sprawowania kontroli nad bezpieczeństwem oraz sposobem przetwarzania danych;
4) rejestracji w Głównym Inspektoracie Ochrony Danych Osobowych, zbiorów danych przed przystąpieniem do ich przetwarzania, prowadzenia ewidencji osób zatrudnionych przy przetwarzaniu danych.

§ 3. 1. Administrator Bezpieczeństwa Informacji realizuje zadania w zakresie ochrony danych, a w szczególności:

1) ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach systemów informatycznych Urzędu Miejskiego;
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 służących do przetwarzania danych osobowych i osób przy nim zatrudnionych;
5) opracowania i wdrożenia programu szkolenia w zakresie zabezpieczenia systemu informatycznego.

2. Osoba zastępująca Administratorowi Bezpieczeństwa Informacji powyższe zadania realizuje tylko w przypadku nieobecności Administratorowi Bezpieczeństwa Informacji.

3. Osoba zastępująca składa Administratorowi Bezpieczeństwa Informacji relację z podejmowanych działań w czasie jego zastępstwa.

§ 4. Właściciel zbioru danych osobowych jest odpowiedzialny za:

1) dopuszczanie do przetwarzania danych wyłącznie osób upoważnionych,
2) kontrolę przestrzegania zasad przetwarzania danych osobowych,
3) opracowanie zakresu czynności osób zatrudnionych przy przetwarzaniu danych uwzględniając obowiązki wynikające z ustawy o ochronie danych osobowych,
4) przekazywanie do ABI informacji o zmianie lub powstaniu nowej lokalizacji miejsc przetwarzania danych osobowych,
5) przygotowanie i aktualizację, we współpracy z ABI zasad zapewniających ciągłość procesów związanych z przetwarzaniem zbioru danych osobowych, którego jest właścicielem.

§ 5. Kierownicy referatów i osoby zatrudnione na samodzielnych stanowiskach pracy Urzędu Miejskiego są zobowiązani do:

1) współdziałania z Administratorem Bezpieczeństwa Informacji w zakresie przestrzegania instrukcji o której mowa w rozdziale 7;

2) sprawowania nadzoru nad pracą podległych pracowników w zakresie wykonywania czynności służbowych w sposób zapewniający ochronę danych osobowych;
3) zwracania się do administratora danych o rozstrzygnięcie w przypadku istotnych wątpliwości co do stosowania przepisów prawnych zakresu danych osobowych;
4) niezwłocznego zawiadomienia ADO o konieczności utworzenia nowego zbioru danych osobowych, wymagającego rejestracji.

§ 6. Pracownik upoważniony przez ADO do przetwarzania danych osobowych, jest zobowiązany do:
1) odbycia wewnętrznego szkolenia dotyczącego przetwarzania i ochrony danych osobowych;
2) zapoznania się z przepisami prawa w zakresie ochrony danych osobowych;
3) stosowania określonych przez administratora danych, procedur i środków mających na celu zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym;
4) zachowania szczególnej staranności w trakcie wykonywania operacji przetwarzania danych w celu ochrony interesów osób, których te dane dotyczą;
5) podporządkowania się poleceniom administratora bezpieczeństwa informacji oraz właściwego kierownika, w zakresie ochrony danych.

§ 7. Czynności przetwarzania danych osobowych może dokonywać jedynie pracownik upoważniony przez Administratora Danych Osobowych. Wzór upoważnienia stanowi załącznik nr 3 do niniejszego dokumentu.

§ 8. Bezpośredni nadzór nad przetwarzaniem danych osobowych w komórkach organizacyjnych Urzędu Miejskiego sprawują kierownicy referatów tych komórek, a w przypadku pracowników na samodzielnych stanowiskach Burmistrz, Sekretarz Gminy – każdy w swoim pionie.

§ 9. Pracownik, któremu administrator danych osobowych udzielił upoważnienia, o którym mowa w §5 jest zobowiązany do podpisania oświadczenia. Wzór oświadczenia stanowi załącznik nr 4 do niniejszego dokumentu.

§ 10. 1. W przypadku zatrudnienia nowego pracownika, zmiany stanowiska, zmiany zakresu obowiązków pracowniczych, utworzenia nowego zbioru danych osobowych, zmiany sposobu przetwarzania danych lub w innych przypadkach, które wpływają bezpośrednio na rodzaj i zakres przetwarzania danych, kierownik referatu jest zobowiązany bezzwłocznie skierować wniosek do administratora danych osobowych o wydanie lub cofnięcie upoważnienia. W przypadku samodzielnych stanowisk pracy cofnięcia lub wydania upoważnienia dokonuje administrator danych. Wzór pisma o cofnięciu upoważnienia stanowi załącznik nr 5 do niniejszego dokumentu.

2. Procedura nadawania/cofania uprawnień do przetwarzania danych osobowych:

1) przełożony użytkownika będącego pracownikiem Urzędu Miejskiego w Wyrzysku składa wniosek o nadanie/cofnięcie uprawnień dla użytkownika systemu. Wniosek zawiera dokładny opis uprawnień, które powinny zostać nadane/cofnięte oraz okres (od...do…). Wniosek składa się do ABI. Wzór wniosku stanowi załącznik nr 1 do niniejszego dokumentu;
2) w przypadku użytkowników niebędących pracownikami Urzędu Miejskiego w Wyrzysku, wniosek przygotowuje ABI;
3) ABI przygotowuje upoważnienie do przetwarzania danych osobowych dla użytkownika systemu. Upoważnienie przygotowane jest na piśmie w dwóch egzemplarzach (wzór upoważnienia stanowi załącznik nr 3);
4) administrator podpisuje upoważnienie do przetwarzania danych osobowych i przekazuje ABI;
5) po potwierdzeniu odbioru upoważnienia przez użytkownika systemu ASI rejestruje użytkownika oraz okres, na który upoważnienie zostało nadane w ewidencji osób uprawnionych. Wzór Ewidencji osób uprawnionych znajduje się w załączniku nr 12;

3. Wypowiedzenie umowy o pracę jest równoznaczne z cofnięciem upoważnienia do przetwarzania danych osobowych.

§ 11. 1. W obiegu wewnętrznym między referatami, samodzielnymi stanowiskami pracy a także pracownikami jednostek podległych Urzędowi Miejskiemu wprowadza się następujące zasady udostępniania danych osobowych:

1) informacje zawierające dane powszechnie dostępne może udostępnić pracownik przetwarzający dane w formie bezpośredniej lub telefonicznej, po sprawdzeniu tożsamości w procedurze „zwrotnej informacji telefonicznej”;
2) zgodę na udostępnienie danych osobowych w szerszym zakresie wyraża ADO.

2. W obiegu zewnętrznym zgodę na udostępnienie danych osobowych wyraża administrator danych zgodnie z powszechnie obowiązującymi przepisami.

§ 12. Obowiązek przestrzegania tajemnicy danych osobowych spoczywa na wszystkich pracownikach, którzy mają do nich dostęp, również po ustaniu stosunku pracy.

§ 13. ADO może przenieść obowiązek utrzymywania lub przetwarzania zbioru/zbiorów danych osobowych, na podmiot trzeci jednak musi się to odbyć za pośrednictwem stosownej umowy oraz z zachowaniem reguł bezpieczeństwa danych opisanych w niniejszym dokumencie.

§ 14. Przetwarzanie danych osobowych sprzeczne z przepisami ustawy o ochronie danych osobowych może stanowić ciężkie naruszenie obowiązków pracowniczych.

§ 15. Zbiory danych osobowych przetwarzane przez pracowników Urzędu Miejskiego w Wyrzysku nie mogą być udostępniane do celów komercyjnych.

§ 16. 1. Jeżeli zachodzi taka konieczność dopuszcza się przetwarzanie danych osobowych w systemie informatycznym poza zbiorem danych w plikach (np. MS Word, MS Excell) poza bazą danych, znajdującą się w określonym systemie informatycznym.

2. Zgodę na przetwarzanie danych w formie w takiej sytuacji wydaje właściciel ZDO wg wzoru upoważnienia określonego w Załączniku Nr 2

3. Dane przetwarzane w plikach mogą stanowić kopie części bazy znajdującej się w systemie lub być nową celową ewidencją tworzoną na potrzeby realizacji zadań związanych z przetwarzaniem danych osobowych przez uprawnionych pracowników.

4. Dostęp do plików z danymi powinien być ograniczony jedynie do osoby tworzącej taki plik na swojej stacji roboczej. W tej sytuacji pliki:

1) nie mogą być udostępnione przez sieć komputerową innym użytkownikom;
2) możliwe są do otwarcia jedynie po zalogowaniu się na profil danego użytkownika;
3) muszą być chronione hasłem, jeżeli mają być dostępne dla innych Użytkowników;

5. W sytuacji umieszczenia plików z danymi osobowymi na serwerze plików, dostęp do niego powinien być ograniczony do określonej grup uprawnionych użytkowników.

6. Grupę użytkowników określa dany Właściciel ZDO.

7. ASI jest obowiązany określić szczegółowe zasady zabezpieczenia plików z danymi osobowymi znajdującymi się w komputerach pracowników lub na serwerze plików.

8. Zbiory danych osobowych znajdujące się w oprogramowaniach pocztowych danego użytkownika (książki adresowe), tworzone przez niego jedynie w celach ułatwienia kontaktu, chronione są hasłem dostępowym do programu pocztowego.

Rozdział 3.
Opis zdarzeń naruszających ochronę danych osobowych

§ 17. 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 systemu informatycznego, 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:

   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.

§ 18. 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 silnego 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 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 zakłócenie 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 np. login użytkownika i jego hasło;
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" (backdoor), itp.;
12) podmieniono, lub zniszczono nośniki z danymi osobowymi bez odpowiedniego upoważnienia lub w inny sposób niedozwolony skasowano lub skopiowano dane osobowe;
13) rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylogowano się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, prace na danych osobowych w celach prywatnych, itp.).

§ 19. Za naruszenie ochrony uważa się również stwierdzone nieprawidłowości w zakresie bezpieczeństwa 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.

Rozdział 4.
Zabezpieczenie danych osobowych

§ 20. Administrator Danych Osobowych jest zobowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w systemach informatycznych Urzędu Miejskiego, 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.

§ 21. 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. wyżej;
3) szczególne zabezpieczenie centrum przetwarzania danych (komputer centralny, serwerownia) poprzez zastosowanie systemu kontroli dostępu;
4) wyposażenie pomieszczeń w szafy dające gwarancję bezpieczeństwa dokumentacji.

§ 22. 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 w/w ustępie, w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochrona danych osobowych;
3) kontrolowanie otwierania i zamykania pomieszczeń, w którym są przetwarzane dane osobowe, polegające na otwarciu pomieszczenia przez pierwszą osobę, która rozpoczyna pracę oraz zamknięciu pomieszczenia przez ostatnią wychodzącą osobę.

§ 23. Niezależnie od niniejszych zasad opisanych w dokumencie „Polityka bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Miejskim w Wyrzysku” 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.

§ 24. Wykaz pomieszczeń w których przetwarzane są dane osobowe stanowi załącznik nr 6 do niniejszego dokumentu.

§ 25. Wykaz zbiorów przetwarzanych elektronicznie lub w inny sposób stanowi załącznik nr 7 a i b do niniejszego dokumentu.

§ 26. Opis struktury zbiorów danych

1) Przetwarzanie odbywa się częściowo na serwerze, częściowo na stacjach roboczych użytkowników (dostęp możliwy wyłącznie ze specjalizowanego oprogramowania klienckiego).
2) SWDO (System Wydawania Dowodów Osobistych) znajduje się na komputerach dostarczonych przez Ministerstwo i dostęp do zbioru danych przez osoby upoważnione przez Ministerstwo jest możliwy tylko z tych stanowisk.

§ 27. Sposób przepływu danych pomiędzy systemami stanowi załącznik nr 8 do niniejszego dokumentu.

§ 28. Opis rejestracji baz danych stanowi załącznik nr 9 do niniejszego dokumentu.

§ 29. Właściciele zbiorów danych osobowych są zobowiązani do niezwłocznego przekazywania do ABI informacji o zmianie lub powstaniu nowej lokalizacji miejsc przetwarzania danych osobowych.

§ 30. 1. W celu ochrony przed utratą danych w Urzędzie Miejskim w Wyrzysku stosowane są następujące zabezpieczenia:
1) wyodrębniony obwód zasilania sprzętu komputerowego;
2) ochrona serwerów przed zanikiem (wahaniami) zasilania poprzez stosowanie zasilaczy zapasowych UPS;
3) ochrona newralgicznych elementów sieciowych (switchy) przed zanikiem zasilania;
4) ochrona przed utratą zgromadzonych danych przez robienie codziennych kopii zapasowych na taśmach magnetycznych, dyskach przenośnych lub płytach CD/DVD, z których w przypadku awarii odtwarzane są dane i system operacyjny;
5) ochrona przed awarią podsystemu dyskowego poprzez używanie macierzy dyskowych (mirroring).

2. Zabezpieczenia przed nieautoryzowanym dostępem do baz danych Urzędu Miejskiego w Wyrzysku:

1) wszystkie gniazdka lokalnej sieci komputerowej są galwanicznie oddzielone od szkieletu sieci komputerowej. Podłączenie (zkrosowanie) danego użytkownika do szkieletu sieci komputerowej dokonuje Administratora Systemów Informatycznych, lub osoba przez niego upoważniona;
2) aby uzyskać dostęp do zasobów sieci, należy zwrócić się do Administratora Bezpieczeństwa z wnioskiem w którym podane będą dane nowego użytkownika oraz zasoby jakie mają być udostępnione;
3) w systemie informatycznym Urzędu Miejskiego w Wyrzysku zastosowano podwójną autoryzację użytkownika. Pierwszej autoryzacji należy dokonać w momencie uzyskania dostępu do serwera

Urzędu podając login oraz hasło, drugiej autoryzacji należy dokonać uruchamiając program użytkowy, podając login użytkownika oraz hasło. Dostęp do wybranej bazy danych uzyskuje się dopiero po poprawnym podwójnym zalogowaniu się do systemu informatycznego.

3. Zabezpieczenia przed nieautoryzowanym dostępem do baz danych Urzędu Gminy poprzez Internet.

4. W zakresie dostępu do sieci wewnętrznej Urzędu Miejskiego w Wyrzysku z rozległej sieci Internet zastosowano środki ochrony przed podsłuchiwaniem, penetrowaniem i atakiem z zewnątrz.

5. Zastosowano firewall na routerze, który ma za zadanie uwierzytelnianie źródła przychodzących pakietów oraz ich filtrowanie w oparciu o adres IP i inne parametry. Zablokowano wszystkie nieużywane porty celem zmniejszenia potencjalnych luk, które mogą być wykorzystane przez osobę próbującą uzyskać nieautoryzowany dostęp do sieci wewnętrznej. Ruch pakietów, oraz otwarte porty zostały określone przez Administratora Bezpieczeństwa.

6. Firewall zapisuje do logu fakt zaistnienia wyjątkowych zdarzeń i śledzi ruch pakietów przechodzących przez router. dostęp do sieci zewnętrznej jest ustalony indywidualnie na wniosek pisemny, lub ustny użytkownika. Oprócz filtra pakietów (firewall) zastosowano system wykrywający obecność wirusów w poczcie elektronicznej.

7. Pozostałe stosowane zabezpieczenia:

1) do pomieszczeń w których następuje przetwarzanie danych osobowych mają dostęp tylko uprawnione osoby bezpośrednio związane z nadzorem nad serwerami, lub aplikacjami;
2) zabezpieczenie przed nieuprawnionym dostępem do danych, prowadzone jest przez ABI 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;
4) w pomieszczeniach w których znajdują się serwery jest zamontowana klimatyzacja, która zapewnia właściwą temperaturę i wilgotność powietrza dla sprzętu komputerowego;
5) w pobliżu wejścia do pomieszczenia z serwerami i innymi urządzeniami znajduje się gaśnica, która jest okresowo napełniana i kontrolowana przez stosownego specjalistę.

Rozdział 5.
Kontrola przestrzegania zasad zabezpieczenia danych osobowych

§ 31. Administrator Danych Osobowych 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.

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

§ 33. Na podstawie zgromadzonych materiałów o których mowa w §32 ABI sporządza roczne sprawozdanie i przedstawia ADO.

Rozdział 6.
Środki organizacyjne i techniczne

§ 34. 1. Dostęp do danych osobowych mogą mieć tylko i wyłącznie pracownicy posiadający pisemne, imienne upoważnienia podpisane przez Administratora Danych Osobowych.

2. Każdy z pracowników powinien zachować szczególną ostrożność przy przetwarzaniu, przenoszeniu wszelkich danych osobowych.

3. Należy chronić dane przed wszelkim dostępem do nich osób nieupoważnionych.

4. Pomieszczenia, w których są przetwarzane dane osobowe, muszą być zamykane na klucz.

5. Dostęp do kluczy powinni posiadać tylko upoważnieni pracownicy.

6. Dostęp do pomieszczeń możliwy jest tylko i wyłącznie w godzinach pracy urzędu. W wypadku, gdy jest wymagany poza godzinami pracy - możliwy jest tylko na podstawie ustnego lub pisemnego zezwolenia Administratora Danych Osobowych.

7. Dostęp do pomieszczeń, w których są przetwarzane dane osobowe mogą mieć tylko upoważnieni pracownicy urzędu.

8. W przypadku pomieszczeń do których dostęp mają również osoby nieupoważnione, mogą przebywać w tych pomieszczeniach TYLKO w obecności osób upoważnionych, i tylko w czasie wymaganym na wykonanie niezbędnych czynności.

9. Szafy w których przechowywane są dane osobowe muszą być zamykane na klucz.

10. Klucze do tych szaf powinni posiadać tylko upoważnieni pracownicy.

11. Szafy z danymi powinny być otwarte tylko na czas potrzebny na dostęp do danych a następnie powinny być zamykane.

12. Dane osobowe w formie papierowej mogą znajdować się na biurkach tylko na czas niezbędny na dokonanie czynności służbowych a następnie muszą być chowane do szaf.

§ 35. 1. Dostęp do komputerów na których są przetwarzane dane osobowe mogą mieć tylko upoważnieni pracownicy urzędu.

2. Stacje komputerowe na których przetwarzane są dane osobowe powinny mieć tak ustawione monitory, aby nie miały wglądu w dane osoby nieupoważnione.

3. Każdy plik w którym są zawarte dane osobowe powinien być zabezpieczony hasłem jeśli nie jest to przetwarzanie danych w systemie informatycznym.

4. W przypadku przetwarzania danych osobowych na komputerach przenośnych (notebook) należy zachować szczególną ostrożność przy ich przewożeniu.

5. Po zakończeniu pracy komputery (notebook) takie powinny być zabezpieczone w zamykanych na klucz szafach.

6. Komputerów tych nie należy wynosić poza budynek.

7. W wypadku potrzeby wyniesienia (np. notebooka) wcześniej należy dane osobowe przenieść na komputer stacjonarny w miejscu pracy.

8. Nie należy udostępniać osobom nieupoważnionym tych komputerów.

9. W przypadku potrzeby przeniesienia danych osobowych pomiędzy komputerami należy dokonać tego z zachowaniem szczególnej ostrożności i za zgodą ABI.

10. Nośniki użyte do tego należy wyczyścić (skasować nieodwracalnie/zniszczyć), aby nie zostały na nich dane osobowe.

11. W wypadku niemożliwości skasowania danych z nośnika (płyta CD/DVD) należy taką płytę zniszczyć fizycznie (np. za pomocą odpowiedniej niszczarki).

12. W przypadku wykorzystania do przenoszenia dysków, dane należy kasować z tych dysków.

13. Niezabezpieczonych danych osobowych nie należy przesyłać drogą elektroniczną.

14. Sieć komputerowa powinna być zabezpieczona przed wszelkim dostępem z zewnątrz.

15. Do zabezpieczenia sieci należy stosować:

1) firewall;
2) adresowanie stacji roboczych tylko adresami prywatnymi, nieroutowalnymi;
3) systemy wykrywania włamań IDS;
4) logowanie wszelkich zdarzeń w dziennikach systemowych na serwerach i stacjach roboczych;
5) systemy antywirusowe i antyszpiegowskie;
6) zabezpieczenia skrzynek poczty elektronicznej hasłami „trudnymi” (min. 8 znaków w tym litery, cyfry, znaki dodatkowe);
7) zabezpieczenie przed dostępem na zewnątrz ze stacji roboczych do innych usług niż WWW, (zasada blokowania wszystkie i przepuszczania określonych usług w tym przypadku http, czyli port 80);
8) dostęp do poczty elektronicznej tylko na serwerach autoryzowanych przez Urząd Miejski;
9) zabezpieczenia stacji roboczych poprzez hasła w BIOS, w systemach MS Windows 2000, i wyższych (autoryzacja użytkownika, login + hasło);
10) zabezpieczenie wszelkich systemów teleinformatycznych hasłami „trudnymi” (min. 8 znaków w tym litery, cyfry, znaki dodatkowe) zmienianymi minimum raz na 60 dni;
11) ustawienie odpowiednich poziomów dostępu dla odpowiednich użytkowników w systemach teleinformatycznych, zmiany mogą zostać przeprowadzone tylko i wyłącznie przez administratora danego systemu (polityka ograniczonego zaufania).

§ 36. Należy przestrzegać zapisów "Instrukcji Zarządzania Sprzętem Komputerowym" która jest przedstawiona w załączniku nr 13.

§ 37. Wymogi systemu teleinformatycznego:
1) system informatyczny służący do przetwarzania danych osobowych wyposażony jest w mechanizmy uwierzytelniania użytkownika oraz kontroli dostępu do tych danych;
2) identyfikator użytkownika wraz z jego imieniem i nazwiskiem wpisuje się do ewidencji osób upoważnionych do przetwarzania danych osobowych prowadzonej przez Właścicieli ZDO;
3) identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego nie powinien być przydzielany innej osobie;
4) identyfikator osoby, która utraciła uprawnienia dostępu do danych osobowych, należy bezzwłocznie wyrejestrować z systemu informatycznego, w którym są one przetwarzane, unieważnić jej hasło oraz podjąć stosowne działania w celu zapobieżenia dalszemu dostępowi tej osoby do danych osobowych;
5) ekrany monitorów stanowisk dostępu do danych osobowych powinny być automatycznie wyłączane po upływie, co najwyżej 5 minut nieaktywności użytkownika, a po wykonaniu „akcji” przez użytkownika (np. poruszenie myszą), komputer powinien domagać się podania loginu i hasła użytkownika;

6) w pomieszczeniach, w których przebywają osoby postronne, monitory stanowisk dostępu do danych osobowych powinny być ustawione w taki sposób, żeby uniemożliwić tym osobom wgląd w te dane.

Rozdział 7.
Instrukcja określająca sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem bezpieczeństwa informacji.

§ 38. Określenie sposobu przydziału haseł dla użytkowników i częstotliwość ich zmiany oraz wskazanie osoby odpowiedzialnej za te czynności.

1) hasło nie powinno zawierać mniej niż 8 znaków;
2) hasło nie może być takie samo jak identyfikator;
3) hasło musi być zmieniane przynajmniej raz na 60 dni przez użytkownika, Administratora Systemów Informatycznych lub automatycznie przez system;
4) użytkownikowi nie wolno zapisywać hasła na papierze;
5) użytkownik jest zobowiązany do utrzymania hasła w tajemnicy, również po utracie jego ważności,
6) komputery nie pracujące w sieci muszą mieć hasło założone na BIOS;
7) w przypadku czasowego opuszczenia stanowiska pracy, użytkownik powinien wylogować się z systemu, lub uruchomić wygaszacz ekranu zabezpieczony hasłem;
8) za gospodarkę hasłami odpowiedzialny jest Administratora Systemów Informatycznych;
9) hasło przy wpisywaniu nie może być wyświetlane na ekranie;

§ 39. Określenie sposobu rejestrowania i wyrejestrowania użytkowników oraz wskazanie osoby odpowiedzialnej za te czynności:

1) Administratora Systemów Informatycznych prowadzi ewidencję osób upoważnionych do przetwarzania danych, zawierającą ich identyfikatory, załącznik nr 12 do niniejszego dokumentu;
2) rejestracji użytkowników w systemie dokonuje Administratora Systemów Informatycznych, lub osoba przez niego upoważniona;
3) zarejestrować można wyłącznie osoby, które administrator danych wpisał do ewidencji osób upoważnionych do przetwarzania danych;
4) wyłączenie z ewidencji osób upoważnionych do przetwarzania danych, obliguje Administratora Systemów Informatycznych do odebrania dostępu do danych osobowych;
5) zalecane jest aby identyfikator składał się z nazwiska i pierwszej litery imienia.

§ 40. Procedury rozpoczęcia i zakończenia pracy.

1) ASI w porozumieniu z kierownikiem referatu, ustala czas pracy użytkownikom systemu, na pracę poza godzinami funkcjonowania urzędu musi wyrazić zgodę na piśmie kierownik jednostki, w formie upoważnienia jednorazowego lub stałego;
2) w pomieszczeniach gdzie przyjmowani są klienci, monitory powinny być tak ustawione, aby uniemożliwić osobie niepowołanej wgląd w dane;
3) dopuszcza się pozostawianie włączonego serwera w nocy, jeżeli pomieszczenie w którym on pracuje wyposażone jest w sprawny system powiadamiania p-poż, UPS oraz alarm antywłamaniowy;
4) kontrola wprowadzanych danych prowadzona jest na bieżąco na każdym stanowisku merytorycznym, nadzór prowadzi kierownik danej komórki organizacyjnej;
5) o przekazywaniu danych osobowych innym podmiotom decyduje ADO;
6) osoby, których dane są przetwarzane powinny mieć możliwość zapoznania się, na tablicy ogłoszeń, z przysługującymi im prawami wynikającymi z ustawy o ochronie danych osobowych.

§ 41. Metoda i częstotliwość tworzenia kopii awaryjnych:
1) za sporządzanie i bezpieczeństwo kopii odpowiedzialny jest ASI, lub osoba przez niego upoważniona;
2) kopii należy dokonywać poprzez przegrywanie (backup) całej bazy danych;
3) w każdej chwili powinno być dostępnych jednocześnie pięć kopii: z ostatniego dnia, tygodnia,miesiąca, kwartału i roku. Kopie dzienne i tygodniowe należy zapisywać na dysku twardym a pozostałe na CD/DVD, bądź innym nośniku niemodyfikowalnym;
4) kopie awaryjne może tworzyć jedynie Administrator Systemów Informatycznych, lub osoba przez niego upoważniona;
5) w czasie tworzenia kopii awaryjnej przez administratora, dostęp do bazy dla wszystkich użytkowników powinien być zablokowany;
6) dyski wymienne z kopiami bezpieczeństwa powinny być wyjęte z komputera w czasie bieżącej pracy;
7) ASI lub administrator systemu wykonuje backup lub archiwizacje systemu wykorzystując jak najlepiej swoje umiejętności;

§ 42. Wprowadza się praktyczne zalecenia odnośnie do wykonania kopii bezpieczeństwa:
1) przeprowadzić składowanie informacji regularnie;
2) używać różnych typów nośników danych;
3) kopie umieszczać w różnych, oddalonych od siebie miejscach;
4) najlepiej do składowania wybrać tak nośnik, aby mógł w całości pomieścić kopie danych;
5) przed składowaniem danych sprawdzić je programem antywirusowym;

6) dokładnie opisywać składowane dane;
7) trzymać nośniki z kopiami z daleka od źródeł pola magnetycznego i miejsc nasłonecznionych;
8) sprawdzić, czy składowanie przebiegło prawidłowo;
9) upewnić się, że nośnik jest niezależny od urządzenia, tzn. że dane mogą być przywrócone nie tylko na komputerze, z którego były pobrane;
10) regularnie konserwować urządzenia do składowania;

§ 43. Metody i częstotliwość sprawdzania obecności wirusów komputerowych oraz sposoby ich usuwania:
1) za ochronę antywirusową odpowiedzialny jest Administratora Systemów Informatycznych;
2) do ochrony antywirusowej należy stosować program antywirusowy, zainstalowany na komputerze, gdzie odbierana jest poczta elektroniczna i sprawdzane są wszystkie nośniki wymienne, przed ich uruchomieniem w sieci oraz na komputerach stacjonarnych;
3) sprawdzanie dostępnymi programami antywirusowymi odbywać się powinno przynajmniej raz w miesiącu (zalecane jest codzienne skanowanie komputera);
4) zalecane jest wykorzystanie programów pracujących w tle;
5) przy kontroli szczególną uwagę należy zwrócić na makra (dokumenty pakietów biurowych);
6) każdą przesyłkę otrzymaną za pomocą transmisji danych (e-mail, ftp) należy sprawdzić programem antywirusowym;
7) korzystanie z zewnętrznych nośników i źródeł informacji (dyskietek, dysków wymiennych, płyt CD, Internetu, poczty elektronicznej) może mieć miejsce wyłącznie po uzyskaniu zgody ABI;

§ 44. Sposób i czas przechowywania nośników informacji, w tym kopii zapasowych i wydruków:
1) nie należy magazynować zbędnych plików i wydruków, kopie bezpieczeństwa po upływie okresu przechowywania muszą być skasowane, lub fizycznie zniszczone w sposób uniemożliwiający odczytanie danych;
2) za zniszczenie zbędnych wydruków i innych dokumentów zawierających dane osobowe odpowiedzialny jest kierownik referatu, za skasowanie danych, lub zniszczenie nośników elektronicznych, odpowiedzialny jest ASI;
3) zbędne dokumenty konwencjonalne (papierowe) powinny być zniszczone w niszczarce dokumentów lub przekazane do utylizacji firmie uprawnionej;
4) kopie bezpieczeństwa na nośnikach wymiennych powinny być przechowywane w zamkniętej metalowej szafie;
5) kopie na nośnikach wymiennych nie powinny być przechowywane w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych eksploatowanych na bieżąco;

6) kopie awaryjne sprawdza się pod kątem ich dalszej przydatności do odtworzenia danych w przypadku awarii systemu – co najmniej jednorazowo po przegraniu danych;
7) wydruki należy przechowywać w pomieszczeniach, uniemożliwiających dostęp do nich przez osoby niepowołane;
8) kopie przechowuje się co najmniej:
   a) dzienne przez siedem dni,
   b) tygodniowe przez kolejny tydzień,
   c) miesięczne przez kolejny miesiąc,
   d) kwartalne przez kolejny kwartał,
   e) roczne przez cały kolejny rok od daty sporządzenia;
9) osoba użytkująca przenośny komputer, służący do przetwarzania danych osobowych w celu zapobieżenia dostępowi do tych danych osobie niepowołanej, powinna zabezpieczyć dostęp do komputera hasłem i nie zezwalać na używanie komputera osobom, komputera nie należy pozostawiać w samochodzie.

§ 45. Należy przestrzegać zapisów "Instrukcji Zarządzania Oprogramowaniem" która jest przedstawiona w załączniku nr 14.

§ 46. Sposób dokonywania przeglądów i konserwacji systemu i zbioru danych osobowych:
1) przeglądu i konserwacji dokonuje ABI, lub osoba przez niego upoważniona, przynajmniej dwa razy w roku;
2) zasilacz UPS powinien zapewnić automatyczne zakończenie pracy i wyłączenie serwerów przy zaniku lub nadmiernym wahaniu napięcia – min. czas podtrzymania pracy wynosi 5 min;
3) w przypadku przekazywania komputera z dyskiem lub innym nośnikiem danych osobowych do naprawy, należy nośnik zdemontować, zabezpieczyć dostęp hasłem, dokonać naprawy w obecności osoby upoważnionej przez administratora danych lub przekazać do naprawy firmie z która Urząd podpisuje odpowiednie dokumenty przekazania zbioru danych z zastrzeżeniem co do przetwarzania i wykorzystywania tych danych w przypadku przekazania nośnika innemu podmiotowi należy dane nieodwracalnie skasować;
4) o wszelkich nieprawidłowościach, awariach, próbie lub naruszeniu bezpieczeństwa danych osobowych, użytkownik powinien niezwłocznie powiadomić ABI;
5) do wydzielonej sieci energetycznej zasilającej system komputerowy nie wolno podłączać żadnych innych urządzeń (czajników elektrycznych, odkurzaczy, radioodbiorników);

6) zabronione jest dokonywanie napraw sprzętu komputerowego samodzielnie przez pracowników urzędu;

§ 47. Sposób postępowania w zakresie komunikacji w sieci komputerowej:

1) system informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych, lub logicznych zabezpieczeń, chroniących przed nieuprawnionym dostępem zgodnie z załącznikiem do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 Kwietnia 2004 poz. 1024 (Dz.U. Nr. 100, poz. 1024);
2) przy przydzielaniu uprawnień obowiązuje zasada „wszystko co nie jest dozwolone, jest zabronione”;
3) Administrator Bezpieczeństwa Informacji z Administratorem Danych Osobowych określi zasoby dostępne dla każdego użytkownika;
4) użytkownicy powinni być przydzielani do odpowiedniej grupy roboczej, automatycznie w procesie logowania np. za pomocą skryptu logowania;
5) dostęp do serwerowni ma tylko ASI i pracownicy przez niego upoważnieni;
6) dostęp do konsoli serwera winien być zabezpieczony hasłem (min. 12 znaków, dostępnych w tablicy ASCII);
7) ASI winien monitorować pracę w sieci za pomocą dostępnego oprogramowania narzędziowego i plików .log (plik z informacjami przekazywanymi przez system/program dla użytkownika);
8) w pomieszczeniu, gdzie ustawiony jest serwer może pracować tylko ASI, lub osoby przez niego upoważnione;
9) nie wolno instalować na żadnym z komputerów w sieci urzędowej własnego oprogramowania bez zgody ASI;
10) użytkownicy nieuprawnieni nie powinni mieć dostępu do zasobów systemowych serwera, katalogów roboczych, danych i woluminów z poziomu systemu operacyjnego;
11) dostęp do archiwalnych plików pocztowych, mających status poufnych (informacje handlowe) należy zabezpieczyć hasłem;
12) wszystkie listy otrzymane pocztą elektroniczną należy przekazywać do kancelarii;
13) w celu zwiększenia bezpieczeństwa transmisji danych osobowych należy stosować kryptografie;
14) w czasie korzystania z Internetu za pośrednictwem linii komutowanej, stacja powinna być fizycznie odłączona od sieci lokalnej;
15) uczestnictwo w internetowych grupach dyskusyjnych dozwolone jest jedynie za zgodą ASI;
16) komunikacja w sieci lokalnej musi umożliwiać identyfikację pracujących użytkowników.

Rozdział 8.
Instrukcja postępowania w sytuacji naruszenie ochrony danych osobowych

§ 48. Niniejsze zasady określają tryb postępowania w przypadku gdy:

1) stwierdzono naruszenie zabezpieczenia systemu informatycznego lub naruszenie zabezpieczenia zbioru danych osobowych zebranych i przetwarzanych w innej formie;
2) stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej, mogą wskazywać na naruszenie zabezpieczeń tych danych;

§ 49. O naruszeniu ochrony danych osobowych mogą świadczyć w szczególności następujące symptomy:

1) brak możliwości uruchomienia przez użytkownika aplikacji pozwalającej na dostęp do danych osobowych;
2) brak możliwości zalogowania się do tej aplikacji;
3) ograniczone, w stosunku do normalnej sytuacji, uprawnienia użytkownika aplikacji (np. brak możliwości wykonywania pewnych operacji normalnie dostępnych użytkownikowi) lub uprawnienia poszerzone w stosunku do normalnej sytuacji;
4) wygląd aplikacji inny niż normalnie;
5) inny zakres danych niż normalnie dostępny dla użytkownika - dużo więcej lub dużo mniej danych;
6) znaczne spowolnienie działania systemu informatycznego;
7) pojawienie się nie standardowych komunikatów generowanych przez system informatyczny;
8) ślady włamania lub prób włamania do obszaru, w którym przetwarzane są dane osobowe;
9) ślady włamania lub prób włamania do pomieszczeń, w których odbywa się przetwarzanie danych osobowych, w szczególności do serwerowni oraz do pomieszczeń, w których przechowywane są nośniki kopii awaryjnych;
10) włamanie lub próby włamania do szafek, w których przechowywane są w postaci elektronicznej lub papierowej - nośniki danych osobowych;
11) zagubienie lub kradzież nośnika danych osobowych;
12) zagubienie lub kradzież nośnika materiału;
13) kradzież sprzętu informatycznego, w którym przechowywane były dane osobowe;
14) informacja z systemu antywirusowego o zainfekowaniu systemu informatycznego wirusami;
15) fizyczne zniszczenie lub podejrzenie zniszczenia elementów systemu informatycznego przetwarzającego dane osobowe na skutek przypadkowych lub celowych działań albo zaistnienia siły wyższej;

16) podejrzenie nieautoryzowanej modyfikacji danych osobowych przetwarzanych w systemie informatycznym.

§ 50. O ujawnieniu danych osobowych decyduje:

1) dane osobowe zostają ujawnione, gdy stają się znane w całości lub części pozwalającej na określenie osobom nie uprawnionym tożsamości osoby, której dane dotyczą;
2) w stosunku do danych, które zostały zagubione, pozostawione bez nadzoru poza obszarem bezpieczeństwa należy przeprowadzić postępowanie wyjaśniające, czy dane osobowe należy uznać za ujawnione.

§ 51. Każdy pracownik Urzędu Miejskiego biorący udział w przetwarzaniu danych osobowych w systemie informatycznym jest odpowiedzialny za bezpieczeństwo tych danych:

1) w szczególności osoba, która zauważyła zdarzenie mogące być przyczyną naruszenia ochrony danych osobowych lub mogących spowodować naruszenie bezpieczeństwa danych, zobowiązana jest do natychmiastowego poinformowania Administratora Bezpieczeństwa Informacji lub innej osoby wskazanej przez niego;
2) osoba zatrudniona w Urzędu Miejskiego, która stwierdzi lub podejrzewa naruszenie zabezpieczenia ochrony danych osobowych w systemie informatycznym (lub przetwarzanych w inny sposób), powinna niezwłocznie poinformować o tym Administratora Bezpieczeństwa Informacji lub osobę zatrudnioną przy przetwarzaniu danych osobowych, albo inną upoważnioną przez niego osobę;
3) Administrator Bezpieczeństwa Informacji jest odpowiedzialny za przygotowanie i opublikowanie wykazu osób, które mogą być informowane w przypadku wystąpienia zagrożenia danych osobowych;
4) w przypadku niemożliwości zawiadomienia Administratora Bezpieczeństwa Informacji lub osób przez niego upoważnionych, pracownik winien powiadomić bezpośredniego przełożonego.

§ 52. Informacja o pojawieniu się zagrożenia lub wystąpieniu zagrożenia danych osobowych.

1) informacja przekazywana jest przez pracownika osobiście, telefonicznie lub pocztą elektroniczną;
2) informacja, o której mowa w w/w podpunkcie powinna zawierać imię i nazwisko osoby zgłaszającej oraz zauważone symptomy zagrożenia;
3) w przypadku gdy zgłoszenie o podejrzeniu zaistnienia incydentu otrzyma osoba inna niż ABI, jest ona obowiązana poinformować o tym fakcie ABI;
4) pracownik może zostać poproszony przez ABI o potwierdzenie zauważonego faktu na piśmie.

§ 53. Czynności „pierwszej reakcji” użytkownika zgłaszającego naruszenie:

1) do czasu przybycia Administratora Bezpieczeństwa Informacji lub upoważnionej przez niego osoby, zgłaszający:

a) niezwłocznie podejmuje czynności niezbędne do powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnia w działaniu również ustalenie przyczyn lub sprawców,

b) zabezpiecza dostęp do miejsca lub urządzenia przez osoby trzecie,

c) wstrzymuje pracę na komputerze na którym zaistniało naruszenie ochrony oraz nie uruchamia bez koniecznej potrzeby komputerów i innych urządzeń, których funkcjonowanie w związku naruszeniem ochrony zostało wstrzymane,

d) nie zmienia położenia przedmiotów, które pozwalają stwierdzić naruszenie ochrony lub odtworzyć jej okoliczności,

e) podejmuje, stosownie do zaistniałej sytuacji, inne niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych,

f) podejmuje inne działania przewidziane określone w instrukcjach technicznych i technologicznych stosownie do objawów i komunikatów towarzyszących naruszeniu,

g) wstępnie udokumentować zaistniałe naruszenie;

2) Dokonywanie zmian w miejscu naruszenia ochrony jest dopuszczalne jeżeli zachodzi konieczność ratowania osób lub mienia albo zapobieżenia grożącemu niebezpieczeństwu.

§ 54. Administrator Bezpieczeństwa Informacji lub osoba przez niego upoważniona, niezwłocznie po uzyskaniu sygnału o naruszeniu danych osobowych, powinien:

1) zapoznać się z zaistniałą sytuacją i dokonać wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy Urzędu Miejskiego;
2) zapisać wszelkie informacje związane z danym zdarzeniem;
3) na bieżąco wygenerować i wydrukować wszystkie możliwe dokumenty i raporty, które mogą pomóc w ustaleniu okoliczności zdarzenia;
4) przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, zwłaszcza do określenia skali zniszczeń i metody dostępu do danych osoby niepowołanej;
5) dokonać fizycznego odłączenia urządzeń i segmentów sieci, które mogły umożliwić dostęp do bazy danych osobie nie uprawnionej;
6) wylogować użytkownika podejrzanego o naruszenie zabezpieczenia ochrony danych;
7) dokonać zmiany hasła na konto ABI i użytkownika, poprzez które uzyskano nielegalny dostęp w celu uniknięcia ponownej próby włamania;

8) zażądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem;
9) rozważyć możliwość i potrzebę powiadomienia o zaistniałym naruszeniu ADO;
10) nawiązać bezpośredni kontakt, jeżeli zachodzi taka potrzeba, ze specjalistami spoza Urzędu;
11) zamknąć i opieczętować urządzeń, w których przechowywane są dane osobowe w formie cyfrowej.

§ 55. Administrator Bezpieczeństwa Informacji podejmuje działania zmierzające do wyjaśnienia zgłoszonego zdarzenia. W szczególności może on dokonywać, w zależności od zgłoszonego zdarzenia:
1) wizji lokalnej w zakresie adekwatnym do rodzaju zgłoszonego zdarzenia;
2) przeprowadzenia wywiadów z pracownikami w celu ustalenia zaistniałych faktów;
3) przeprowadzenia analizy poprawności funkcjonowania systemu informatycznego, jeżeli zgłoszone zdarzenie było związane z nieprawidłowym jego funkcjonowaniem;
4) przeprowadzenia analizy zapisu zdarzeń w systemie informatycznym z uwzględnieniem zapisu operacji realizowanych przez użytkowników;
5) przeprowadzenia analizy danych przetwarzanych w systemie informatycznym, jeżeli zgłoszone zdarzenie mogło być spowodowane utratą dostępności lub integralności przetwarzanych danych;
6) sporządzenia dokumentacji fotograficznej;
7) zabezpieczenia danych przetwarzanych w systemie informatycznym dotkniętym incydentem, w szczególności danych konfiguracyjnych tego systemu;
8) zebrania innych materiałów pozwalających na wyjaśnienie przyczyn zaistnienia incydentu, jego charakteru i potencjalnych skutków.

§ 56. Po wykonaniu czynności, o których mowa w §55, Administrator Bezpieczeństwa Informacji jest zobowiązany do podjęcia kroków w celu:
1) wyjaśnienia zdarzenia - w szczególności czy miało miejsce naruszenie ochrony danych osobowych;
2) wyjaśnienia przyczyn naruszenia bezpieczeństwa danych osobowych i zebranie ewentualnych dowodów - w szczególności, gdy zdarzenie było związane z celowym działaniem pracowników bądź osób trzecich;
3) zabezpieczenia systemu informatycznego przed dalszym rozprzestrzenianiem się zagrożenia;
4) usunięcie skutków incydentu i przywrócenie pierwotnego stanu systemu informatycznego (to jest sprzed incydentu).

§ 57. 1. W szczególności działania związane z usuwaniem skutków incydentu mogą obejmować:
1) przeprowadzenie naprawy sprzętu informatycznego;
2) rekonfigurację sprzętu informatycznego;

3) wprowadzenie poprawek do oprogramowania;
4) rekonfigurację oprogramowania;
5) odtworzenie danych z kopii awaryjnych;
6) modyfikację danych w celu odtworzenia ich integralności;
7) wycofanie z użycia materiału kryptograficznego;
8) inne naprawy urządzeń wchodzących w skład infrastruktury informatycznej wspomagających lub zabezpieczających działanie systemu informatycznego.

2. Administratora Systemów Informatycznych może odstąpić od usuwania skutków incydentu, jeżeli został on spowodowany działaniem celowym, a całkowite wyjaśnienie zdarzenia i wyciągnięcie konsekwencji wobec sprawców jest istotniejsze niż przerwa w działaniu systemu. Istniejący stan systemu informatycznego jest niezmieniany w celach dowodowych do czasu wyjaśnienia sprawy.

3. Przy usuwaniu skutków incydentu z wykorzystaniem odtwarzania danych z kopii awaryjnych Administratora Systemów Informatycznych obowiązany jest upewnić się, że odtworzone dane zostały zapisane przed wystąpieniem incydentu - w szczególności dotyczy to przypadków odtwarzania systemu po infekcji wirusowej.

4. Osoby upoważnione:

1) w sytuacjach wyjątkowych wszystkie powyżej opisane działania związane z usuwaniem skutków incydentu i wyjaśnianiem jego przyczyn mogą być realizowane przez osoby upoważnione przez Administratora Bezpieczeństwa Informacji;
2) ABI odpowiada za sporządzenie listy pracowników mających prawo do podejmowania odpowiednich kroków w razie wystąpienia incydentu w sytuacji, gdy nie mogą one być wykonane osobiście przez niego.

5. Raporty i powiadomienia:

1) ABI określa, na podstawie przeprowadzonych wyjaśnień, przyczyny zaistnienia incydentu;
2) jeżeli incydent był spowodowany celowym działaniem, ABI jest zobowiązany do pisemnego powiadomienia Burmistrza Wyrzyska - Administratora Danych lub Sekretarza Gmin;
3) Burmistrz Wyrzyska - Administrator Danych lub Sekretarz Gminy, biorąc pod uwagę charakter zdarzenia, może poinformować organy uprawnione do ścigania przestępstw o fakcie celowego naruszenia bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym.

6. Korzystanie z urządzeń po naruszeniu ochrony.Zgodę na uruchomienie komputerów i innych urządzeń lub dokonanie zmian w miejscu naruszenia ochrony wyraża ABI lub osoba przez niego upoważniona.

7. Czynności końcowe - obserwacja:

1) System informatyczny, którego prawidłowe działanie zostało odtworzone, powinien zostać poddany szczegółowej obserwacji w celu stwierdzenia całkowitego usunięcia symptomów incydentu. W czasie jej trwania użytkowanie systemu informatycznego powinno być ograniczone do niezbędnego minimum;
2) Okres kwarantanny, o którym mowa powyżej, jest uzależniony charakterem incydentu i specyfiką systemu informatycznego - jest on każdorazowo określany przez Administratora Bezpieczeństwa Informacji;

8. Czynności końcowe - dokumentacja:

1) ABI dokumentuje w raporcie każdy zaistniały przypadek naruszenia ochrony danych osobowych;
2) dokumentacja, o której mowa powyżej, obejmuje następujące informacje:

a) imię i nazwisko osoby zgłaszającej incydent,

b) imię i nazwisko osoby przyjmującej zgłoszenie incydentu,

c) datę i godzinę przyjęcia zgłoszenia incydentu,

d) określenie czasu i miejsca incydentu,

e) opis zgłoszonego incydentu oraz okoliczności towarzyszące,

f) przyczyny wystąpienia naruszenia,

g) opis podjętych działań naprawczych,

h) wyniki przeprowadzonego badania wyjaśniającego,

i) ocenę skuteczności przeprowadzonego postępowania naprawczego,

j) podjęte środki techniczne, organizacyjne i dyscyplinarne w celu zapobiegania w przyszłości naruszenia ochrony danych osobowych,

9. wzór raportu, o którym mowa w §57 ust. 8, określa załącznik nr 10 do Polityki Bezpieczeństwa,

10. Czynności końcowe - analiza,Administrator Bezpieczeństwa Informacji w oparciu o posiadaną dokumentację, odpowiedzialny jest za przeprowadzenie przynajmniej raz w roku analizy zaistniałych incydentów w celu:

1) określenia skuteczności podejmowanych działań wyjaśniających i naprawczych.
2) określenia wymagań działań zwiększających bezpieczeństwo systemu informatycznego i minimalizujących ryzyko zaistnienia incydentów.
3) określenia potrzeb w zakresie szkoleń użytkowników systemu informatycznego przetwarzającego dane osobowe.

Rozdział 9.
Postanowienia końcowe

§ 58. 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 nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie dyscyplinarne.

§ 59. Administrator Bezpieczeństwa Informacji 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 11 do niniejszego dokumentu.

§ 60. 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.

§ 61. Orzeczona kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia Administratora Bezpieczeństwa Informacji nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą o ochronie danych osobowych oraz możliwość wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

§ 62. W sprawach nieuregulowanych niniejszym dokumentem mają zastosowanie przepisy ustawy o ochronie danych osobowych, rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych oraz rozporządzenia Ministra Sprawiedliwości 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.

§ 63. Niniejsza „Polityka bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Miejskim w Wyrzysku” wchodzi w życie z dniem jej wydania.

Załącznik Nr 1
do Polityki bezpieczeństwa i instrukcji zarządzania systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Miejskim w Wyrzysku.

(WZÓR)

Wyrzysk, dnia .....

……./.....

WNIOSEK

o nadanie/cofnięcie uprawnień do przetwarzania danych osobowych

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

Pani/Pana .....

Pracownika.....

.....

do wykonywania czynności związanych z przetwarzaniem danych osobowych w zakresie:.

.....

.....

.....

.....

.....

na okres od ..... do .....

.....

Podpis

Administratora Danych Osobowych

Załącznik Nr 2
do Polityki bezpieczeństwa i instrukcji zarządzania systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Miejskim w Wyrzysku.

(WZÓR)

Data nadania upoważnienia: .....

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH POZA BAZĄ DANYCH SYSTEMU INFORMATYCZNEGO URZĘDU MIEJSKIEGO W WYRZYSKU

1. Upoważniam Panią/Pana .....
zatrudnioną/-ego na stanowisku: .....
w Urzędzie Miejskim w Wyrzysku do przetwarzania poza bazą danych systemu informatycznego następujących danych osobowych:
- .....
- .....
- .....
- .....
- .....
- .....

(zakres upoważnienia: wskazanie kategorii danych, które może przetwarzać określona w upoważnieniu osoba, lub rodzaj czynności lub operacji, jakich może dokonywać na danych osobowych)

2. Identyfikator: .....

3. Okres trwania upoważnienia: .....
(okres obowiązywania upoważnienia)

Wystawił: .....
(podpis Właściciela Zbioru Danych Osobowych)

4. Osoba upoważniona do przetwarzania danych, objętych zakresem, o którym mowa wyżej, jest zobowiązana do zachowania ich w tajemnicy, nie kopiowania ich i nie udostępniania, również po ustaniu zatrudnienia oraz zachowania w tajemnicy informacji o ich zabezpieczeniu.

Data i podpis osoby upoważnionej: .....

Załącznik Nr 3
do Polityki bezpieczeństwa i instrukcji zarządzania systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Miejskim w Wyrzysku.

(WZÓR)

...., dnia ..... r.

(pieczątka)

UPOWAŻNIENIE NR .....

z dnia .....

Na podstawie art. 37 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.) upoważniam Panią/a ….....
zatrudnioną/ego w .....
na stanowisku ….....
do przetwarzania danych osobowych.

Zadania i czynności do wykonania:

1. Przestrzeganie zasad określonych w instrukcji określającej sposób zarządzania systemem informatycznym i ręcznym. (Rozdział VI)
2. Przestrzeganie zasad określonych w instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych. (Rozdział VII)
3. Przestrzeganie zachowania w tajemnicy danych osobowych uzyskanych w okresie zatrudnienia w związku z upoważnieniem do przetwarzania danych osobowych, także po ustaniu stosunku pracy.
4. W szczególności przetwarzanie danych osobowych w następujących zbiorach danych (numer i nazwa): .....
5. Ochrona danych osobowych w systemie informatycznym i ręcznym, a w szczególności przeciwdziałanie dostępowi osób niepowołanych oraz przeciwdziałanie w przypadku wykrycia naruszeń zabezpieczeń systemu zgodnie z ustawą o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.).

....

(data i podpis Administratora Danych Osobowych) (data i podpis pracownika)

Załącznik Nr 4
do Polityki bezpieczeństwa i instrukcji zarządzania systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Miejskim w Wyrzysku.

(WZÓR)

.....
(imię i nazwisko)

.....
(referat)

OŚWIADCZENIE

Oświadczam, że zapoznałem(łam) się z przepisami prawa dotyczącymi ochrony danych osobowych, a w szczególności z ustawą z 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. 2002 Nr 101, poz. 926 ze zm.) oraz rozporządzeniem ministra spraw wewnętrznych i administracji z 29 kwietnia 2004 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemu informatyczne, służące do przetwarzania danych osobowych (Dz. U Nr 100, poz. 1024) i zobowiązuję się do ich przestrzegania.

Oświadczam ponadto, że zapoznałem(łam) się z Polityką bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Miejskim w Wyrzysku wprowadzoną zarządzeniem nr ..... Burmistrza Miejskim w Wyrzysku z dnia ..... r. oraz Instrukcją przetwarzania danych osobowych.

Świadomy(a) odpowiedzialności porządkowej i karnej oświadczam, że znane mi dane osobowe będę przetwarzać zgodnie z prawem, i nie dopuszczę do bezprawnego naruszenia tajemnicy również w sytuacji, gdy ustanie moje zatrudnienie w:

Urząd Miejskim w Wyrzysku
ul. Bydgoska 29
89-300 Wyrzysk
Otrzymałem(łam) dnia:

.....
(podpis pracownika)

....., dnia ..... r.

Załącznik Nr 5
do Polityki bezpieczeństwa i instrukcji zarządzania systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Miejskim w Wyrzysku.

(WZÓR)

WYCOFANIE UPOWAŻNIENIA

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

.....

.....

.....

cofam upoważnienie

Pana/Pani .....

zatrudnionego/zatrudnionej w .....

na stanowisku.....

do przetwarzania danych osobowych, wynikającego z zakresu obowiązków pracowniczych.

.....

(data i podpis Administratora Danych Osobowych)

Otrzymałem(łam) dnia:

.....

(podpis pracownika)

....., dnia ..... r.

Załącznik Nr 6
do Polityki bezpieczeństwa i instrukcji zarządzania systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Miejskim w Wyrzysku.

Wykaz budynków, pomieszczeń lub części pomieszczeń w których przetwarzane są dane.

Lp.	Budynek	Nr pokoju	Referat/Sam. stanowisko	Określenie części pomieszczenia, w którym przetwarza się, lub archiwizuje dane.
1	UMW	1	Referat Organizacyjny	
2	UMW	2	Skarbnik Gminy	
3	UMW	3	Referat Finansowo-Księgowy	
4	UMW	4	Referat Finansowo-Księgowy	
5	UMW	5	Referat Finansowo-Księgowy	
6	UMW	7	Wieloosobowe stanowiska ds. obsługi budżetu gminy	
7	UMW	8	Stanowisko ds. ewidencji ludności Stanowisko ds. dowodów osobistych i ochrony danych osobowych	
8	UMW	10	Kierownik USC Zastępca kierownika USC	
9	UMW	11	Główny Księgowy Referat Finansowo-Księgowy	
10	UMW	15	Stanowisko ds. kontroli zarządczej	
11	UMW	16	Referat Organizacyjny	
12	UMW	17	Burmistrz Wyrzyska	

Załącznik Nr 7A
do Polityki bezpieczeństwa i instrukcji zarządzania systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Miejskim w Wyrzysku.

Wykaz zbiorów przetwarzanych elektronicznie

Lp.	Referat/Sam. stanowisko	Nazwa urządzenia i program zastosowany do przetwarzania (urządzenie/ system/ program)	Nazwa zbioru/ Cel przetwarzania
1	Sekretarz Miasta i Gminy	Komputer PC/Windows XP Pro/LibreOffice	Oświadczenia majątkowe
2	Stanowisko ds wojskowych, OC, obronnych i ochr. przeciwpożarowej	Komputer PC/Windows XP Pro/ LibreOffice	Ewidencja strażaków biorących udział w akcjach ratunkowych
3	Sekretarz Miasta i Gminy	Komputer PC/Windows XP Pro/ LibreOffice	Wybory ławników sądowych
4	Referat Finansowo-Księgowy Referat Gospodarki Nieruchomościami, Rolnictwa i Leśnictwa	Komputer PC/ Windows XP Pro/ POGRUN	Zwrot podatku akcyzowego zawartego w cenie oleju napędowego
5	Stanowisko ds gospodarki komunalnej	Komputer PC/ Windows XP Pro/eGmina	Nadawanie numerów porządkowych nieruchomości
6	Referat Gospodarki Nieruchomościami, Rolnictwa i Leśnictwa	Komputer PC/ Windows XP Pro/ EGW	Przekształcenie prawa użytkowania wieczystego w prawo własności
7	Pracownicy merytoryczni Urzędu Miejskiego w Wyrzysku	Komputer PC/ Windows XP Pro/ Proton	System elektronicznej skrzynki podawczej i elektronicznego obiegu dokumentów PROTON
8	Kierownik i Zastępca Kierownika USC	Komputer PC/ Windows XP Pro/ PB_USC	Urząd Stanu Cywilnego
9	Stanowisko ds. ewidencji ludności Stanowisko ds. dowodów osobistych i ochrony danych osobowych	Komputer PC/ Windows XP Pro/ ELUD+ Komputer PC/ Windows 7 Pro/ ELUD+	Ewidencja Ludności i Dowody Osobiste
10	Referat Finansowo-Księgowy	Komputer PC/ Windows XP Pro/ WIP	Wymiar i windykacja należności podatku rolnego i podatków lokalnych
11	Stanowisko ds. dodatków mieszkaniowych i oświetlenia gminy	Komputer PC/ Windows XP Pro/ NDM	Dodatki Mieszkaniowe
12	Referat Gospodarki Nieruchomościami, Rolnictwa i Leśnictwa	Komputer PC/ Windows XP Pro/ EGR Komputer PC/ Windows XP Pro/ EGW	Ewidencja gruntów, budynków, ewidencja użytkowników wieczystych

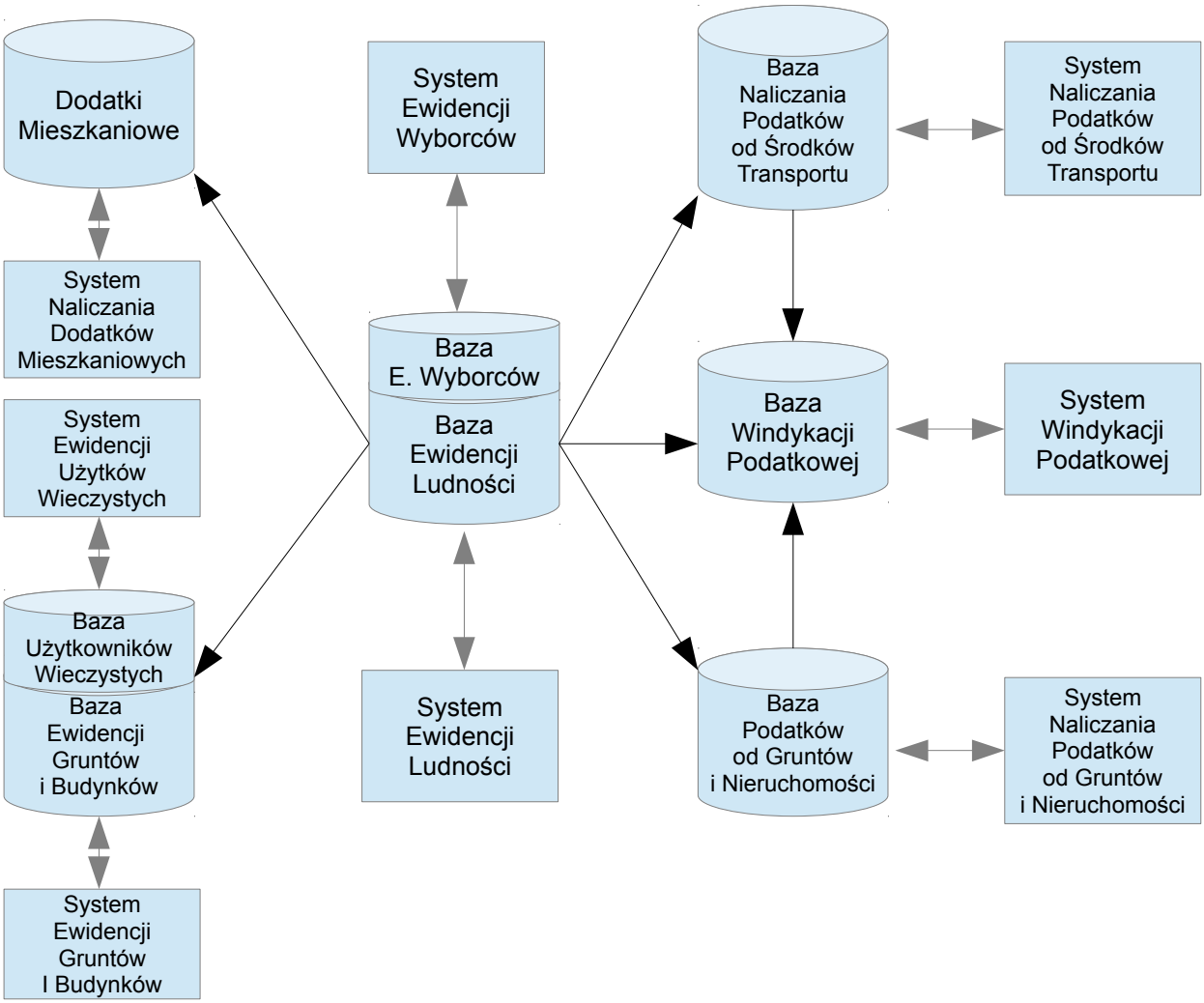
Załącznik Nr 7B
do Polityki bezpieczeństwa i instrukcji zarządzania systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Miejskim w Wyrzysku.

Wykaz zbiorów przetwarzanych w inny sposób niż elektronicznie

Lp.	Referat/Sam. stanowisko	Rodzaj danych/ Cel przetwarzania	Nazwa zbioru
1	Referat Organizacyjny	Realizacja zadań ustawowych	Ewidencja sołtysów i rad sołeckich
2	Referat Gospodarki Nieruchomościami, Rolnictwa i Leśnictwa	Realizacja zadań ustawowych	Usuwanie drzew i krzewów
3	Referat Organizacyjny	Realizacja zadań ustawowych	Archiwum Zakładowe
4	Referat Gospodarki Nieruchomościami, Rolnictwa i Leśnictwa	Realizacja zadań ustawowych	Ewidencja kart wieczystych użytkowników i dzierżawców
5	Stanowisko ds wojskowych, OC, obronnych i ochr. przeciwpożarowej	Realizacja zadań ustawowych	Wykaz przedpoborowych, rejestr przedpoborowych, lista poborowych
6	Referat Organizacyjny	Realizacja zadań ustawowych	Dziennik korespondencji
7	Stanowisko ds. dowodów osobistych i ochrony danych osobowych	Realizacja zadań ustawowych	Ewidencja zezwoleń na sprzedaż napojów alkoholowych
8	Wieloosobowe stanowisko ds. ochrony środowiska i zamówień publicznych	Realizacja zadań ustawowych	Rejestr oferentów ubiegających się o udzielenie zamówień publicznych i złożenie oferty
9	Stanowisko ds. dodatków mieszkaniowych i oświetlenia gminy	Realizacja zadań ustawowych	Ewidencja mieszkań komunalnych
10	Sekretarz Miasta i Gminy	Realizacja zadań ustawowych	Rejestr skarg i wniosków
11	Straż Miejska Wyrzysk	Realizacja zadań ustawowych	Rejestr osób popełniających wykroczenia drogowe i kierowanych postępowań mandatowych
12	Wieloosobowe stanowisko ds. zagospodarowania przestrzennego	Realizacja zadań ustawowych	Rejestr wydanych decyzji o warunkach zabudowy i zagospodarowania terenu
13	Inspektor ds. oświaty, zdrowia, kultury i sportu	Realizacja zadań ustawowych	Ewidencja osób realizujących obowiązek nauki.
14	Inspektor ds. oświaty, zdrowia, kultury i sportu	Realizacja zadań ustawowych	Dofinansowania kosztów kształcenia pracowników młodocianych

Załącznik Nr 8
do Polityki bezpieczeństwa i instrukcji zarządzania systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Miejskim w Wyrzysku.

Schemat blokowy połączeń bazami oprogramowania



Załącznik Nr 9
do Polityki bezpieczeństwa i instrukcji zarządzania systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Miejskim w Wyrzysku.

Opis rejestracji baz danych

W przypadku konieczności przetwarzania danych w nowej bazie danych, wymagana jest konsultacja z Administratorem Bezpieczeństwa Informacji (ABI). W przypadku konieczności rejestracji bazy danych w Generalnym Inspektoracie Danych Osobowych, rejestracja następuje na wniosek danego referatu.

1. Właściciel ZDO zgłasza ABI zamiar utworzenia nowego zbioru danych osobowych.

Dokumentacja winna zawierać:

1) nazwę bazy;
2) imię i nazwisko, stanowisko osoby tworzącej;
3) datę utworzenia;
4) ewentualną datę zakończenia przetwarzania danych;
5) podstawę prawną przetwarzania;
6) cel przetwarzania;
7) listę osób przetwarzających dane;
8) zakres danych osobowych zawartych w bazie;
9) przewidywany czas użytkowania bazy (stały, okresowy, jednorazowy);
10) informacje o ewentualnym przekazywaniu danych (komu, kiedy, w jakim celu, pod stawa prawna, jaki zakres przekazania danych);
11) dodatkowe ważne informacje (zmiany osób uprawnionych itp.).

2. ABI przygotowuje projekt zgłoszenia zbioru danych osobowych do rejestracji GIODO, jeżeli takie zgłoszenie jest ustawowo wymagane, na podstawie obowiązującego wzoru wniosku określonego w Rozporządzeniu do u.o.d.o.

3. ASI w uzgodnieniu z ABI określa warunki techniczne dotyczące zabezpieczeń w systemie informatycznym, o których mowa w części E i F zgłoszenia zbioru danych osobowych do rejestracji GIODO.

4. ABI sprawdza opisane w części E i F zgłoszenia zbioru danych osobowych do rejestracji GIODO warunki techniczne dotyczące zabezpieczeń w systemie informatycznym, a w przypadku niewystarczającego poziomu zabezpieczeń występuje z wnioskiem do ASI o podniesienie poziomu zabezpieczeń.

5. Przygotowany przez ABI projekt zgłoszenia zbioru danych osobowych do rejestracji GIODO parafują Właściciel ZDO oraz ASI.

6. ABI przedkłada wniosek o rejestrację zbioru danych osobowych Administratorowi i zgłasza go do GIODO.

7. Tryb określony w niniejszym paragrafie stosuje się odpowiednio w razie konieczności aktualizacji zgłoszenia zbioru danych osobowych do rejestracji GIODO.

8. Właściciel ZDO zgłasza w ciągu 5 dni wszelkie zmiany dotyczące przetwarzania danych w zarejestrowanym zbiorze danych osobowych do ABI.

9. ASI zgłasza w ciągu 5 dni wszelkie zmiany dotyczące sposobu przetwarzania danych osobowych oraz ich zabezpieczeń w systemie informatycznym.

10. ABI przygotowuje aktualizację zgłoszenia zbioru danych osobowych do GIODO w terminie 30 dni od dnia dokonania zmiany w zbiorze, na podstawie obowiązującego wzoru określonego w Rozporządzeniu do u.o.d.o.

11. Wniosek aktualizacyjny zgłoszenie zbioru danych osobowych do rejestracji GIODO parafuje Właściciel ZDO oraz ASI.

12. ABI przedkłada Administratorowi do podpisania wniosek aktualizacyjny zgłoszenie zbiór danych osobowych i wysyła go do GIODO.

Każdy referat powinien prowadzić dokumentację opisującą bazy danych osobowych przetwarzanych w referacie.

Załącznik Nr 10
do Polityki bezpieczeństwa i instrukcji zarządzania systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Miejskim w Wyrzysku.

(WZÓR)

Raport nr ...../.....

z naruszenia bezpieczeństwa systemu informatycznego

w Urzędzie Miejskim w Wyrzysku

Osoba powiadamiająca o zaistniałym zdarzeniu:

.....

(Imię i Nazwisko, stanowisko służbowe, nazwa użytkownika jeśli występuje)

Osoba przyjmująca zgłoszenie o zaistniałym zdarzeniu:

.....

(Imię i Nazwisko, stanowisko służbowe, nazwa użytkownika jeśli występuje)

Lokalizacja zdarzenia:

.....

(np. nr pokoju; nazwa pomieszczenia)

Rodzaj naruszenia bezpieczeństwa, oraz okoliczności towarzyszące:

.....

.....

.....

Podjęte działania:

.....

.....

.....

Przyczyny wystąpienia zdarzenia:

.....

.....

.....

Postępowanie wyjaśniające:

.....

.....

Ocena skuteczności przeprowadzonego postępowania naprawczego:

.....

.....

.....

Podjęte środki techniczne, organizacyjne i dyscyplinarne w celu zapobiegania w przyszłości podobnym naruszeniom ochrony danych osobowych:

.....

.....

.....

.....

….....

(data, podpis Administratora Bezpieczeństwa Informacji)

Załącznik Nr 11
do Polityki bezpieczeństwa i instrukcji zarządzania systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Miejskim w Wyrzysku.

(WZÓR)

Wykazu osób które zapoznały się z „Polityką bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Miejskim w Wyrzysku.”

Wykaz osób, które zostały zapoznane z „Polityką bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Miejskim w Wyrzysku”, przeznaczonej dla osób zatrudnionych przy przetwarzaniu tych danych.
Przyjąłem/am/ do wiadomości i stosowania zapisy Polityki bezpieczeństwa.

Nr upoważnienia	Nazwisko i Imię	Data nadania	Upoważniający	Data odebrania	Odbierający

.....

(data, podpis Administratora Bezpieczeństwa Informacji)

Załącznik Nr 12
do Polityki bezpieczeństwa i instrukcji zarządzania systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Miejskim w Wyrzysku.

(WZÓR)

Ewidencja osób upoważnionych do przetwarzania danych.

LP.	**Imię**	**Nazwisko**	**Identyfikator**

.....

(data, podpis Administratora Bezpieczeństwa Informacji)

Załącznik Nr 13
do Polityki bezpieczeństwa i instrukcji zarządzania systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Miejskim w Wyrzysku.

Instrukcja zarządzania sprzętem komputerowym

Rozdział 1.
Procedura zgłaszania zapotrzebowania na sprzęt komputerowy.

§ 1. Zgłoszenie ASI zapotrzebowania na sprzęt komputerowy poprzez wypełnienie formularza zapotrzebowania stanowiący załącznik Nr 1 do Instrukcji Zarządzania Systemem Komputerowym.

§ 2. ASI konsultuje zgłoszenie z Sekretarzem Mista i Gminy

§ 3. Decyzje o zakupie oraz o trybie zakupu podejmuje Burmistrz.

§ 4. Jeżeli nie jest to pilny zakup , ale został pozytywnie zaopiniowany przez ASI i Sekretarza Miasta i Gminy, to zostaje on wpisany do Rejestru Zapotrzebowania Sprzętu Komputerowego.

Rozdział 2.
Procedura zakupu sprzętu komputerowego.

§ 5. Na początku roku kalendarzowego, po przyjęciu budżetu, ASI wraz Sekretarzem Miasta i Gminy decydują o strategii zakupów inwestycyjnych. Analizowany jest Rejestr Zapotrzebowania na Sprzęt Komputerowy i podejmowane są decyzje o kolejności zakupów,

§ 6. Zakupy sprzętu komputerowego dokonywane są w oparciu o ustawę o zamówieniach publicznych,

§ 7. ASI przygotowuje Specyfikacje Istotnych Warunków Zamówienia, która jest zatwierdzana przez Burmistrza,

§ 8. Rozstrzygnięcie postępowania przetargowego regulują odrębne przepisy,

§ 9. W sytuacjach awaryjnych (nagła awaria sprzętu, itp.) procedura przewiduje zakupy z wolnej ręki.

Rozdział 3.
Procedura przyjęcia do ewidencji sprzętu komputerowego.

§ 10. Każdorazowo po zakupie sprzętu komputerowego ASI wprowadza jego parametry do Ewidencji Sprzęty Komputerowego prowadzonej w sposób elektroniczny i nadaje mu numer inwentarzowy.

§ 11. ASI wypełnia zgłoszenie sprzętu komputerowego do Wydziału Finansowego prowadzącego Ewidencję Środków Trwałych, które stanowi załącznik Nr 2 do Instrukcji Zarządzania Sprzętem Komputerowym.

§ 12. Wydział Finansowy wprowadza do Ewidencji Środków Trwałych zakupiony sprzęt komputerowy.

Rozdział 4.
Procedura instalacji sprzętu komputerowego na stanowisku pracy.

§ 13. Przed instalacją sprzętu komputerowego na stanowisku pracy ASI sprawdza działanie urządzeń, aby w razie problemów zgłosić reklamacje.

§ 14. Po zainstalowaniu sprzętu komputerowego na stanowisku pracy ASI dokonuje instruktarzu pracownika i zapoznaniu z ewentualnymi nowymi funkcjami urządzeń i programów zainstalowanych na komputerze.

Rozdział 5.
Procedura zmiany lokalizacji\osoby użytkującej sprzęt komputerowy

§ 15. W razie zmiany lokalizacji, zmiany osoby użytkującej sprzęt komputerowy ASI aktualizuje wszystkie rejestry i ewidencje dotyczące tego pracownika i sprzętu komputerowego.

§ 16. O zmianie osoby przypisanej do sprzętu komputerowego bądź lokalizacji urządzeń ASI powiadamia poprzez wypełnienie Protokołu Przeniesienia znajdującego się w załączniku nr 3 Instrukcji zarządzania sprzętem komputerowym, a Wydział Finansowy dokonuje aktualizacji w Ewidencji Środków Trwałych.

Rozdział 6.
Procedura likwidacji sprzętu komputerowego.

§ 17. Jeśli sprzęt komputerowy:

1) Jest uszkodzony i jego naprawa jest nieopłacalna lub niemożliwa;
2) Jest przestarzały i niespełna wymagań technicznych zainstalowanego oprogramowania w Urzędzie;
3) Został uszkodzony a zakup nowego podzespołu naruszałby umowę licencyjną oprogramowania dołączoną do tego sprzętu;

to zostaje on poddany Procedurze likwidacji.

§ 18. Sprzęt komputerowy do likwidacji typuje ASI i w porozumieniu Sekretarzem Miasta i Gminy oraz Burmistrzem przygotowuje Wniosek typowania sprzętu komputerowego do likwidacji, stanowiący załącznik Nr 4 do Instrukcji Zarządzania Sprzętem Komputerowym. Wniosek ten jest przekazany do Wydziału Finansowego, który powołuje Komisję likwidacyjną.

§ 19. Komisja likwidacyjna składająca się z trzech członków dokonuje likwidacji sprzętu komputerowego.

§ 20. Komisja sporządza Protokół likwidacji sprzętu komputerowego w dwóch egzemplarzach dla Wydziału Finansowego i ASI.

§ 21. Wydział Finansowy wykreśla z Ewidencji Środków Trwałych zlikwidowany sprzęt komputerowy. Także ASI zaznacza w swojej Ewidencji sprzętu komputerowego, że dane urządzenie zostało zlikwidowane.

Rozdział 7.
Procedura utylizacji sprzętu komputerowego.

§ 22. Po zgromadzeniu odpowiedniej ilości zlikwidowanego sprzętu komputerowego zostaje on poddany Procedurze utylizacji.

§ 23. W wyniku wewnętrznych konsultacji zostaje wyłoniona firma utylizacyjna.

§ 24. ASI przekazuje firmie utylizacyjnej zlikwidowany sprzęt komputerowy a następnie sporządzany zostaje w dwóch egzemplarzach protokół przekazania sprzętu komputerowego do utylizacji.

§ 25. Firma utylizacyjna jest zobowiązana do przekazania Urzędowi Protokołu utylizacji sprzętu komputerowego.

§ 26. Wydział Finansowy prowadzi Ewidencję utylizowanego sprzętu komputerowego, którego kopię posiada ASI.

Rozdział 8.
Procedura przekazania sprzętu komputerowego do podmiotów zewnętrznych.

§ 27. W określonych przypadkach zachodzi możliwość przekazania sprzętu komputerowego podmiotowi zewnętrznemu. Odbywa się to za pomocą Uchwały Rady Miejskiej.

IX. Procedura konserwacji i rozbudowy sprzętu komputerowego.

§ 28. ASI dokonuje okresowej konserwacji sprzętu komputerowego.

§ 29. Jeżeli procedura konserwacji nie przeszkadza w znaczący sposób w funkcjonowaniu Urzędu może ona być dokonywana w godzinach pracy, w przeciwnym wypadku po zakończeniu pracy Urzędu.

§ 30. ASI dokonuje rozbudowy/modernizacji sprzętu komputerowego zgodnie z zasadami bezpieczeństwa BHP oraz zgodnie z przepisami licencyjnymi oprogramowania zainstalowanego na rozbudowywanym/modernizowanym komputerze.

Załącznik nr 1 do

Instrukcji zarządzania sprzętem komputerowym

(WZÓR)

Wyrzysk dnia ……r.

Zapotrzebowanie na sprzęt komputerowy

Imię i nazwisko: .....

Referat: .....

e-mail: .....

Zgłasza zapotrzebowanie na sprzęt komputerowy.

1. Opis zapotrzebowania.

Rodzaj sprzętu	*
Jednostka Centralna	
Monitor	
Drukarka	
Skaner	
Klawiatura	
Mysz	
Nagrywarka	
UPS	
Dysk Twardy	
Czytnik Kart Pamięci	
**……	

*- właściwe zaznaczyć X

** - wpisz rodzaj sprzętu

2. Przyczyna zapotrzebowania na nowy sprzęt komputerowy:

.....

.....

.....

.....

……

Podpis pracownika

Załącznik nr 2 do

Instrukcji zarządzania sprzętem komputerowym

(WZÓR)

	Przyjęcie Środka Trwałego		
	Numer	Data	**OT**
pieczęć			

Nazwa:		
Dostawca - Wykonawca	I. Wartość rozliczenia	
	1. Wartość nabycia lub wytworzenia	zł
	2. Koszty _____	zł
Numer i data dowodu dostawy	3. Koszty _____	zł
	Razem	zł
Miejsce użytkowania lub przeznaczenia	II Wartość szacunkowa	
		zł

Podpis zespołu przyjmującego	Podpis osoby, której powierza się pieczę nad przyjętym środkiem trwałym

Uwagi:	Ilość załączków

Polecenie księgowania

Numer	Data	Stopa % umożenia		
Symbol układu klasyfikacyjnego	Konto **WINIEN**	Kwota	Kwota **MA**	
Nr inwentarzowy	**Zaksięgowano**			
	podpis		data	
Stanowisko kosztów				

……

Podpis ASI

Załącznik nr 3 do

Instrukcji zarządzania sprzętem komputerowym

(WZÓR)

<table>
<tr><td colspan="3">Komórka Organizacyjna</td><td colspan="6">Zmiana miejsca użytkowania
Środka trwałego MT
Przedmiotu nietrwałego MN Nr</td></tr>
<tr><td colspan="3">Dnia przeniesiono</td><td colspan="6">Nr inwentarzowy</td></tr>
<tr><td colspan="9">Uzasadnienie</td></tr>
<tr><td>Jedn. miary</td><td>Ilość</td><td>Cena</td><td>Wartość</td><td colspan="5" rowspan="2"></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="4" rowspan="2">Przeniesiono</td><td colspan="5">Księgowość</td></tr>
<tr><td colspan="5">Stanowisko kosztów</td></tr>
<tr><td colspan="4">Skąd</td><td colspan="5"></td></tr>
<tr><td colspan="4">Dokąd</td><td colspan="5"></td></tr>
<tr><td colspan="2">Zlecił</td><td colspan="2">Przekazał</td><td colspan="2">Przyjął</td><td colspan="3"></td></tr>
<tr><td>Data</td><td>Podpis</td><td>Data</td><td>Podpis</td><td>Data</td><td>Podpis</td><td>Rodzaj ewidencji</td><td>Data</td><td>Podpis</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

.....

Podpis ASI

Załącznik nr 4 do
Instrukcji zarządzania sprzętem komputerowym
(WZÓR)

Wyrzysk dnia …….r.

Urząd Miejski w Wyrzysku
ul. Bydgoska 29
89-300 Wyrzysk

Protokół typowania do likwidacji sprzętu komputerowego

W dniu …….r. skierowano do likwidacji następujący sprzęt komputerowy:

Lp.	Rodzaj sprzętu	NUMER INWENTARZOWY	Powód wytypowania do likwidacji
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			

……
Sporządził

Załącznik Nr 14
do Polityki bezpieczeństwa i instrukcji zarządzania systemów informatycznych służących do przetwarzania danych osobowych w Urzędzie Miejskim w Wyrzysku.

Instrukcja Zarządzania Oprogramowaniem

§ 1. Uznając wagę legalnego i etycznego użytkowania oprogramowania, przyjmuje się niniejszą instrukcję jako drogowskaz dla naszych pracowników używających oprogramowania zarówno legalnie jak i w sposób etyczny. Wszystkie zasoby oprogramowania są wykorzystywane w w ramach obowiązków służbowych i nie są używane przez pracowników we własnych celach.

§ 2. 1. Urząd Miejski w Wyrzysku posiada licencjonowane egzemplarze programów komputerowych różnych producentów oprogramowania. Licencjonowane i zarejestrowane egzemplarze programów zostały zainstalowane na komputerach oraz sporządzono odpowiednie kopie zapasowe oprogramowania zgodnie z warunkami umów licencyjnych. Bez pisemnej zgody producenta oprogramowania nie wolno wykonywać żadnych dodatkowych kopii programów ani też ich dokumentacji.

2. Poza oprogramowaniem komercyjnym w Urzędzie Miejskim w Wyrzysku wykorzystuje się oprogramowanie darmowe, czyli freeware, oraz na licencji GPL.

3. ASI prowadzi Rejestr oprogramowania zainstalowanego na poszczególnych stacjach roboczych, a w przypadku instalacji dodatkowych programów ASI dokonuje aktualizacji w Rejestrze oprogramowania.

§ 3. 1. Urząd Miejski w Wyrzysku wyposażył stanowiska komputerowe pracowników w legalne oprogramowanie. Używanie oprogramowania pochodzącego z jakiegokolwiek innego źródła, bez konsultacji z ASI może stanowić zagrożenie dla bezpieczeństwa Urzędu Miejskiego w Wyrzysku oraz grozić może wszczęciem postępowania prawnego – używanie takiego oprogramowania jest ściśle zabronione.

2. Pracownicy są zobowiązani do zapoznania się z odpowiednimi przepisami o ochronie praw autorskich oraz kodeksu karnego przedstawionymi im przez ASI. Przepisy te mówią o odpowiedzialności pracownika w przypadku korzystania z nielegalnego oprogramowania.

§ 4. 1. Programy zainstalowane przez pracowników Urzędu Miejskiego w Wyrzysku w celu pobierania danych (plików mp3, filmów, itp.) stanowią ogromne zagrożenie dla bezpieczeństwa sieci oraz jej wydajności. Wykorzystywanie tego rodzaju oprogramowania jest zabronione.

2. Pracownik w porozumieniu oświadcza, iż nie będzie korzystał z zainstalowanego oprogramowania do nielegalnych celów oraz, że nie będzie używał szkodliwych i niebezpiecznych programów (typu p2p, torrentów itp.) w miejscu pracy, gdzie wykorzystywałby je do zabronionych celów. Oświadczenie pracownika Urzędu Miejskiego w Wyrzysku stanowi Część C załącznika nr 3 z Porozumienia do Instrukcji zarządzania Oprogramowaniem.

§ 5. 1. W niektórych przypadkach umowa licencyjna pozwala na sporządzenie dodatkowej kopii określonego programu, przeznaczonej do użytkowania na komputerze przenośnym lub komputerze domowym wykorzystywanym do celów służbowych. Pracownicy nie mogą wykonywać dodatkowych kopii oprogramowania lub dokumentacji.

2. Łamanie, czy obchodzenie zabezpieczeń oprogramowania jest dopuszczalne wtedy i tylko wtedy, gdy chcemy wykonać jedną kopię danego oprogramowania do celów zabezpieczenia się w przypadku zniszczenia oryginalnego nośnika programu.

3. Niedopuszczalne jest wykonanie więcej niż jednej kopii oprogramowania. Chyba, że umowa licencyjna na to pozwala.

§ 6. 1. Urząd Miejski w Wyrzysku zastrzega sobie prawo do ochrony swojej reputacji i swoich inwestycji w programy komputerowe poprzez ustanowienie wewnętrznych mechanizmów kontroli zapobiegających wykonywaniu lub użytkowaniu nielegalnych kopii oprogramowania. Mechanizmy te obejmują częste, regularne kontrole sposobu wykorzystywania oprogramowania, zapowiedziane i niezapowiedziane przeglądy zawartości służbowych komputerów umożliwiające stwierdzenie zgodności zainstalowanego oprogramowania z umowami licencyjnymi, usuwanie wszelkich programów zainstalowanych na służbowych komputerach, dla których nie da się stwierdzić ważności licencji lub przedstawić jej dowodu, a także podjęcie postępowania dyscyplinarnego – łącznie ze zwolnieniem z pracy – w stosunku do pracowników naruszających postanowienia niniejszych zasad użytkowania oprogramowania.

2. Mechanizmy kontroli wewnętrznej określa „Procedura audytu\inwentaryzacji oprogramowania”.

§ 7. 1. Procedura zgłaszania zapotrzebowania na oprogramowanie:

1) zgłoszenie ASI zapotrzebowania na oprogramowanie odbywa się poprzez wypełnienie formularza "zapotrzebowania na oprogramowanie", stanowiący załącznik Nr 1 do Instrukcji Zarządzania Oprogramowaniem;
2) ASI konsultuje zgłoszenie z Sekretarzem Miasta i Gminy;
3) decyzje o zakupie oprogramowania podejmuje Burmistrz;
4) jednocześnie tworzony jest Rejestr Zapotrzebowania na oprogramowanie, do którego trafiają zgłoszenia pracowników, jeżeli ich zgłoszenie nie wymaga natychmiastowej realizacji;

2. Procedura zakupu oprogramowania komputerowego:

1) ASI kontaktuje się z dystrybutorem oprogramowania w celu uzgodnienia szczegółów zakupu oprogramowania i licencji;
2) dostawca dostarcza nośnik z oprogramowaniem, licencję oraz fakturę zakupu, które stanowią podstawę legalności oprogramowania;
3) w przypadku przedłużenia licencji, opieki autorskiej bądź aktualizacji oprogramowania ASI pisemnie kontaktuje się z odpowiednimi dystrybutorami;
4) wszelkie zakupy oprogramowania zatwierdza Burmistrz i Sekretarz Miasta i Gminy.

3. Procedura przyjęcia do Ewidencji Oprogramowania Komputerowego:

1) po zakupie oprogramowania komputerowego ASI wpisuje je do Ewidencji Oprogramowania Komputerowego oraz przypisuje mu odpowiedni komputer;
2) ASI wypełnia zgłoszenie oprogramowania do Wydziału Finansowego. Zgłoszenie to stanowi załącznik Nr 2 do Instrukcji Zarządzania Oprogramowaniem;
3) ASI aktualizuje Metrykę Komputera, w której znajdują się parametry komputera wraz zainstalowanym na nim oprogramowaniem, wzór Metryki znajduje się w części B załącznika Nr 3 do Instrukcji Zarządzania Oprogramowaniem;
4) wszystkie licencje, płyty instalacyjne i dowody zakupu oprogramowania przechowywane są w biurze nr 31 na II piętrze w Urzędzie Miejskim w Wyrzysku.

4. Procedura instalacji oprogramowania:

1) proces instalacji dokonuje tylko ASI lub pracownik firmy zewnętrznej, ale tylko i wyłącznie w obecności ASI;
2) ASI zapoznaje pracownika z nowo zainstalowanym oprogramowaniem i poucza o legalnym wykorzystaniu oprogramowania.

5. Procedura aktualizacji oprogramowania:

1) W przypadku, kiedy pozwala na to licencja programu aktualizacja może być darmowa, wykonuje ją pracownik lub ASI;

2) W przypadku programów o określonym czasie licencji i płatnej aktualizacji, ASI wypełnia stosowne wnioski o aktualizacje oprogramowania.

6. Procedura likwidacji oprogramowania:

1) W przypadku licencji OEM, program jest likwidowany razem ze sprzętem komputerowym.
2) Programy, które są uważane za nieprzydatne mogą zostać zlikwidowane po trzech latach ich nieużytkowania.

7. Procedura audytu\inwentaryzacji oprogramowania:

1) procedura inwentaryzacji oprogramowania odbywa się raz w roku. Przeprowadza ją ASI, a wyniki przedstawia Sekretarz Miasta i Gminy;
2) jeżeli zostaną wykryte jakieś nieprawidłowości zastosowane zostaną odpowiednie procedury;
3) ASI po inwentaryzacji aktualizuje Ewidencję Oprogramowania Komputerowego.

8. Procedura podpisania Porozumienia pomiędzy Burmistrzem a Pracownikiem:

1) W związku z wprowadzeniem Polityki Bezpieczeństwa i Instrukcji Zarządzania Oprogramowaniem każdy pracownik jest zobowiązany do podpisania Porozumienia, które określa odpowiedzialność pracownika za użytkowany komputer i zainstalowane na nim oprogramowanie;
2) porozumienie składa się z trzech części: A, B i C. Część A stanowi wstęp do porozumienia, w części B znajduje się Metryka Komputera, za który pracownik jest odpowiedzialny, natomiast część C jest oświadczeniem pracownika o nie wykorzystywaniu zainstalowanego oprogramowania do nielegalnych celów oraz o nie korzystaniu ze szkodliwych i niebezpiecznych programów (typu p2p, torrentów itp.) w miejscu pracy, gdzie wykorzystywałby je do zabronionych celów, użytkowaniu i posługiwaniu się sprzętem komputerowym;
3) lista programów jest aktualizowana po ewentualnych zakupach oprogramowania;
4) Porozumienie zostaje sporządzone w dwóch egzemplarzach po jednej dla stron;
5) Wzór Porozumienia stanowi załącznik Nr 3 do Instrukcji Zarządzania Oprogramowaniem;
6) ASI prowadzi rejestr osób, które podpisały porozumienie. Wzór rejestru stanowi załącznik nr 4 do Instrukcji zarządzania oprogramowaniem.

Załącznik nr 1 do

Instrukcji zarządzania oprogramowaniem

(WZÓR)

Wyrzysk dnia ……r.

Zapotrzebowanie na oprogramowanie komputerowe

Imię i nazwisko: …….....

Wydział: ……

E-mail: ……

Zgłasza zapotrzebowanie na oprogramowanie komputerowe.

1. Opis zapotrzebowania.

Rodzaj lub nazwa oprogramowania komputerowego	*
Edytor tekstu	
Arkusz kalkulacyjny	
Program do tworzenia prezentacji	
Program graficzny	
RADIX	
Legislator	
Podpis elektroniczny	
**……	

*- właściwe zaznaczyć X

** - wpisz rodzaj oprogramowania

2. Opis przeznaczenia programu:

……

……

……

……

……

Podpis pracownika

Załącznik nr 2 do

Instrukcji zarządzania oprogramowaniem

(WZÓR)

	Przyjęcie Środka Trwałego		
	Numer	Data	**OT**
pieczęć			

Nazwa:		
Dostawca - Wykonawca	I. Wartość rozliczenia	
	1. Wartość nabycia lub wytworzenia	zł
	2. Koszty _____	zł
Numer i data dowodu dostawy	3. Koszty _____	zł
	Razem	zł
Miejsce użytkowania lub przeznaczenia	II Wartość szacunkowa	
		zł
Podpis zespołu przyjmującego	Podpis osoby, której powierza się pieczę nad przyjętym środkiem trwałym	
Uwagi:	Ilość załączków	

Polecenie księgowania

Numer	Data	Stopa % umożenia		
Symbol układu klasyfikacyjnego	Konto **WINIEN**	Kwota	Kwota **MA**	
Nr inwentarzowy	**Zaksięgowano**			
	podpis	data		
Stanowisko kosztów				

……

Podpis ASI

Załącznik nr 3 do
Instrukcji zarządzania oprogramowaniem

(WZÓR)

Część A

POROZUMIENIE

Niniejsze porozumienie (zwane dalej „Porozumieniem") zostało zawarte w dniu …..... w Wyrzysku pomiędzy Urzędem Miejskim z siedzibą w Wyrzysku reprezentowaną/ego przez Burmistrza Wyrzyska …..... (zwaną/ego dalej „Pracodawcą") oraz Panią/Panem …..... (zwaną/ym dalej „Pracownikiem").

Wstęp:

(A) Pracownik zatrudniony jest przez Pracodawcę na podstawie umowy o pracę.

(B) Pracodawca wyposażył stanowisko pracy Pracownika w oprogramowanie, na używanie, którego nabył licencję („Oprogramowanie"). Odpowiednie przepisy regulują w sposób szczegółowy zasady korzystania z Oprogramowania.

(C) Pracownik korzysta z komputera/notebooka i oprogramowania w związku z wykonywaniem obowiązków pracowniczych w miejscu pracy.

(D) Porozumienie składa się z części A – ogólnej, części B - metryki komputera, w której znajduje się wykaz sprzętu i zainstalowanego dozwolonego oprogramowania i części C - oświadczeniu pracownika o nie wykorzystywaniu zainstalowanego oprogramowania do nielegalnych celów oraz o nie korzystaniu ze szkodliwych i niebezpiecznych programów (typu p2p, torrentów itp.) w miejscu pracy, gdzie wykorzystywałby je do zabronionych celów, użytkowaniu i posługiwaniu się sprzętem komputerowym.

1. Pracodawca i Pracownik uzgadniają, że do podstawowych obowiązków Pracownika należy korzystanie z Oprogramowania w związku z wykonywaniem obowiązków pracowniczych, zgodnie z obowiązującymi przepisami prawa oraz wyłącznie w celach wykonywania obowiązków pracowniczych jak również nie korzystanie z jakiegokolwiek Oprogramowania komputerowego, do używania którego Pracodawca nie jest uprawniony, w czasie pracy, w miejscu pracy ani przy użyciu sprzętu Pracodawcy.
2. Pracodawca i Pracownik uzgadniają, że naruszenie przez Pracownika jego podstawowych obowiązków pracowniczych w zakresie wskazanym powyżej, może stanowić podstawę do podjęcia przez Pracodawcę przysługujących mu środków prawnych, a w szczególności, może stanowić przyczynę uzasadniającą wypowiedzenie przez Pracodawcę umowy o pracę, łączącej Pracodawcę z Pracownikiem, lub rozwiązanie przez Pracodawcę tejże umowy o pracę bez wypowiedzenia, z winy pracownika, zgodnie z przepisami ustawy z dnia 26 czerwca 1974 r. Kodeks Pracy (tekst jedn.: Dz. U. z 1998 r., Nr 21, póz. 94, ze zm.).
3. Niniejsze Porozumienie zostało sporządzone w trzech egzemplarzach, po jednym dla każdej ze stron i dla Administratora Systemu Informatycznego. Zmiana, uzupełnienie oraz rozwiązanie niniejszego Porozumienia za zgodą obu stron wymaga formy pisemnej pod rygorem nieważności.
4. Pracownik oświadcza, iż jest świadomy odpowiedzialności karnej, o której mowa w artykułach: 278 § 2, 293 w związku z 291 oraz 292 ustawy z dnia 6 czerwca 1997 r. kodeks karny, (tekst jednolity - Dz. U. z 1997, Nr 88, póz. 553, ze zmianami) oraz odpowiedzialności karnej i cywilnej przewidzianej w artykułach 116 i nast. ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (tekst jednolity - Dz. U. z 2000, Nr 80, póz. 904, ze zmianami) za niezgodne z prawem korzystanie, rozpowszechnianie, utrwalanie, uzyskiwanie lub zwielokrotnianie Oprogramowania.

Burmistrz Wyrzyska

…..
podpis pracownika

podpis osoby upoważnionej
do reprezentowania Pracodawcy

Część B

Nazwa użytkownika: ….....
Nazwa komputera: .....
DOMENA: ….....
Adres IP:192.168.___.___

Specyfikacja sprzętowa (hardware) i oprogramowania (software).

System operacyjny	
Procesor:	
Nazwa płyty głównej:	
Pamięć:	
Dysk twardy:	
Karta graficzna:	
Karta dźwiękowa:	
Numer inwentarzowy:	

Licencje komercyjne

L.p	Nazwa programu	Producent programu	Licencja (ID)	Sprzedawca programu	Data zakupu	Numer faktury
1.						
2.						
3.						
4.						
5.						

Licencje freeware, GPL

L.p	Nazwa programu	Producent programu
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		

Przyjmuję do użytkowania wyżej wymieniony sprzęt i oprogramowanie.

…… ……
Podpis ASI data i podpis użytkownika

Część C

Pracownik nie może korzystać z nielegalnie nabytych plików i oprogramowania, plików mp3 oraz szkodliwych, niebezpiecznych programów (np typu p2p, torrent, czy też nabytych z nielegalnego źródła plików) w miejscu pracy, gdzie wykorzystywałby ich do zabronionych celów.

Pracownik oświadcza, iż nie będzie instalował żadnego oprogramowania, bez wcześniejszej konsultacji z Administratorem Systemu Informatycznego.

W przypadku, gdy użytkownik pracuje na komputerze przenośnym (notebook, netbook) nie jest dopuszczalne by wynosił go poza teren miejsca pracy, ze względów na bezpieczeństwo informacji znajdujących się na dyskach twardych.

Użytkownik odpowiada za uszkodzenia wynikłe podczas złego/nieprawidłowego eksploatowania sprzętu.

Wszelkie urządzenia magazynujące dane (pendrive, karty pamięci, przenośne dyski twarde) zakupione do celów służbowych, mają być używane do celów służbowych i nie mogą być używane, czy wynoszone poza teren Urzędu Miejskiego w Wyrzysku.

Oświadczam, iż zapoznałem(am) się z porozumieniem i będę się stosować do wyżej wymienionych zaleceń oraz jestem świadomy(ma) odpowiedzialności karnej, o której mowa w artykułach: 278 § 2, 293 w związku z 291 oraz 292 ustawy z dnia 6 czerwca 1997r. kodeks karny, (tekst jednolity - Dz. U. z 1997, Nr 88, póz. 553, ze zmianami) oraz odpowiedzialności karnej i cywilnej przewidzianej w artykułach 116 i nast. ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (tekst jednolity - Dz. U. z 2000, Nr 80, póz. 904, ze zmianami) za niezgodne z prawem korzystanie, rozpowszechnianie, utrwalanie, uzyskiwanie lub zwielokrotnianie Oprogramowania.

_____

Podpis pracownika

Załącznik nr 4 do

Instrukcji zarządzania oprogramowaniem

(WZÓR)

Rejestr porozumień z pracownikami Urzędu Miejskiego w Wyrzysku

L.p	Nazwisko i imię	Data	Podpis
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			
16.			
17.			
18.			
19.			
20.			
21.			
22.			
23.			
24.			
25.			
26.			
27.			
28.			
29.			
30.			
31.			
32.			
33.			
34.			
35.			
36.			
37.			

Uzasadnienie

uzasadnienie
do zarządzenia nr 0050.142.2012 z dnia 30 listopada 2012 r. w sprawie ochrony danych osobowych w Urzędzie Miejskim w Wyrzysku.

Wydany akt prawny opisuje reguły dotyczące bezpieczeństwa danych osobowych zawartych w systemach informatycznych w Urzędzie Miejskim w Wyrzysku. Opisane reguły określają granice dopuszczalnego zachowania wszystkich użytkowników systemów informatycznych wspomagających pracę Urzędu Miejskiego. 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 Urzędzie Miejskim w Wyrzysku", zwanym 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 i §4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. 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). 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 sieci informatycznej mogą wskazywać lub sugerować naruszenie zabezpieczeń tych danych,

Polityka bezpieczeństwa obowiązuje wszystkich pracowników Urzędu Miejskim w Wyrzysku. 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 Urzędu Miejskiego.

Niniejszy dokument jest zgodny z następującymi aktami prawnymi:

1) ustawą z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.),
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 18 poz. 162).

Polityka bezpieczeństwa została oparta również na zapisach Polskiej Normy PN-ISO/IEC 17799, PN-I-02000 oraz PN-I-13335-1 określających praktyczne zasady zarządzania bezpieczeństwem informacji w obszarze technik informatycznych, która jako cel polityki bezpieczeństwa wskazuje „zapewnienie kierunków działania i wsparcie kierownictwa dla bezpieczeństwa informacji". W zaleceniach dotyczących dokumentu określającego politykę bezpieczeństwa informacji wskazuje się tam, że dokument polityki bezpieczeństwa powinien być zatwierdzony przez kierownictwo, opublikowany i udostępniony w odpowiedni sposób wszystkim pracownikom.