Załącznik do zarządzenia Nr.209/2013 Burmistrza z dnia.20.06.2013 r.

Polityka Bezpieczeństwa Informacji – instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Łowiczu

Opracował Administrator Bezpieczeństwa Informacji

Spis treści

Wprowadzenie

Niniejszy dokument opisuje reguły dotyczące bezpieczeństwa danych osobowych zawartych w systemach informatycznych w Urzędzie Miejskim w Łowiczu. Opisane reguły określają granice dopuszczalnego zachowania wszystkich użytkowników systemów informatycznych wspomagających pracę Urzędu.
Dokument zwraca uwagę na konsekwencje, jakie mogą ponosić osoby przekraczające określone zasady i 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 i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim Łowicz", zwany dalej „Polityką bezpieczeństwa", wskazujący sposób postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych w systemach informatycznych, przeznaczony jest dla osób zatrudnionych przy przetwarzaniu tych danych.
Potrzeba jego opracowania wynika z ustawy z dnia 29 sierpnia 1997 o ochronie danych osobowych (tekst jednolity: Dz.U. z 2002r. Nr 101, poz. 926 z późń. zm.); §3 rozporządzenia Prezesa Rady Ministrów z dnia 25 lutego 1999 roku w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych (Dz.U. Nr 18 poz. 162) oraz §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).

Cele:

1. Zadaniem „Polityki Bezpieczeństwa Informacji" jest określenie trybu postępowania w przypadku, gdy:
   1) stwierdzono naruszenie zabezpieczenia systemu informatycznego,
   2) stanu urządzeń, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci informatycznej mogą wskazywać na naruszenie zabezpieczeń tych danych.

2. 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.

3. **Administrator Danych**, którym jest **Burmistrz Miasta Łowicz**, wyznacza **Administratora Bezpieczeństwa Informacji**, zwanego dalej "Administratorem Bezpieczeństwa Informacji" oraz osobę upoważnioną do zastępowania „Administratora Bezpieczeństwa Informacji".

4. Administrator Bezpieczeństwa Informacji realizuje zadania w zakresie ochrony danych, a w szczególności:

   1) ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach systemów informatycznych Urzędu,
   2) podejmowania stosownych działań zgodnie z niniejszą „Polityką bezpieczeństwa informacji" w przypadku wykrycia nieuprawnionego dostępu do wszelkich bazy danych lub naruszenia zabezpieczenia danych znajdujących się w systemie

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

5. „Polityka Bezpieczeństwa Informacji" obowiązuje wszystkich pracowników Urzędu Miejskiego w Łowiczu oraz osoby, które otrzymały stosowne zezwolenie do przetwarzania danych.

6. W przypadku nieobecności Administratora Bezpieczeństwa Informacji osoba zastępująca realizuje zadania Administratora Bezpieczeństwa Informacji a po jego powrocie składa relację z podejmowanych działań w czasie jego zastępstwa.

Rozdział 1. Zabezpieczenie danych osobowych.

1. **Administratorem Danych osobowych** zawartych i przetwarzanych w systemach informatycznych Urzędu Miejskiego w Łowiczu jest Burmistrz.

2. Administrator danych osobowych jest obowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w systemach informatycznych Urzędu, a w szczególności:

1) zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym,
2) zapobieganie przed zabraniem danych przez osobę nieuprawnioną,
3) zapobieganie przetwarzaniu danych z naruszeniem ustawy oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych.

3. Do zastosowanych środków technicznych należy:

1) przetwarzanie danych osobowych w wydzielonych pomieszczeniach położonych w strefie administracyjnej,
2) zabezpieczenie wejścia do pomieszczeń, o których mowa powyżej w pkt.1,
3) szczególne zabezpieczenie centrum przetwarzania danych (komputer centralny, serwerownia, archiwa) poprzez zastosowanie systemu kontroli dostępu,
4) wyposażenie pomieszczeń w szafy dające gwarancję bezpieczeństwa dokumentacji,
5) wszystkie pomieszczenia, w których dochodzi do wymiany informacji między petentem a urzędnikiem, a jednocześnie jest to pomieszczenie, w którym ma miejsce przetwarzanie danych osobowy muszą posiadać odpowiednie zabezpieczenia fizyczne uniemożliwiające nieautoryzowany wgląd w dane osobowe.

4. Do zastosowanych środków organizacyjnych należą przede wszystkim następujące zasady:

1) zapoznanie każdej osoby z przepisami dotyczącymi ochrony danych osobowych, przed dopuszczeniem jej do pracy przy przetwarzaniu danych osobowych,
2) przeszkolenie osób, o których mowa w pkt. 1), w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochroną danych osobowych,
3) kontrolowanie otwierania i zamykania pomieszczeń, w których są przetwarzane dane osobowe, polegające na otwarciu pomieszczenia przez pierwszą osobę,

która rozpoczyna pracę oraz zamknięciu pomieszczenia przez ostatnią wychodzącą osobę.

5. Niezależnie od niniejszych zasad opisanych w dokumencie „Polityka bezpieczeństwa w Urzędzie Miejskim w Łowiczu" w zakresie bezpieczeństwa mają zastosowanie wszelkie wewnętrzne regulaminy lub instrukcje dotyczące bezpieczeństwa ludzi i zasobów informacyjnych oraz indywidualne zakresy zadań osób zatrudnionych przy przetwarzaniu danych osobowych w określonym systemie.

6. Wykaz pomieszczeń, w których przetwarzane są dane osobowe oraz opis systemów informatycznych Urzędu Miejskim w Łowiczu i zawiera załącznik **nr 1 i nr 2** do niniejszego dokumentu.

7. W celu ochrony przed utratą danych w Urzędzie Miejskim w Łowiczu stosowane są następujące zabezpieczenia:

   1) odrębne zasilanie sprzętu komputerowego;
   2) ochronę serwerów przed zanikiem zasilania poprzez stosowanie zasilaczy zapasowych UPS;
   3) ochronę przed utratą zgromadzonych danych przez robienie kopii zapasowych na taśmach magnetycznych, z których w przypadku awarii odtwarzane są dane i system operacyjny;
   4) ochronę przed awarią podsystemu dyskowego przez używanie macierzy dyskowych. Uszkodzenie jakiegokolwiek z dysków zestawu nie spowoduje utraty danych, a nawet zatrzymania pracy systemu (zastosowanie elementów hotswap i hot spare);
   5) Zabezpieczenia przed nieautoryzowanym dostępem do baz danych Urzędu – w systemie informatycznym Urzędu zastosowano podwójną autoryzację użytkownika. Pierwszej autoryzacji należy dokonać w momencie uzyskania dostępu do serwera Urzędu, podając login użytkownika i hasło. Drugiej autoryzacji należy dokonać uruchamiając program użytkowy, podając login użytkownika i hasło. Dostęp do wybranej bazy danych Urzędu uzyskuje się dopiero po poprawnym podwójnym zalogowaniu się do systemu informatycznego Urzędu.
   6) Zabezpieczenia przed nieautoryzowanym dostępem do baz danych Urzędu poprzez Internet - w zakresie dostępu z sieci wewnętrznej Urzędu do sieci rozległej Internet zastosowano środki ochrony przed podsłuchiwaniem, penetrowaniem i atakiem z zewnątrz. Zastosowano firewall, który ma za zadanie uwierzytelnianie źródła przychodzących wiadomości oraz filtrowanie pakietów w oparciu o adres IP, numer portu i inne parametry. Ściana ogniowa składa się z bezpiecznego systemu operacyjnego i filtra pakietów. Ruch pakietów, który firewall przepuszcza jest określony przez administratora. Firewall zapisuje do logu fakt zaistnienia wyjątkowych zdarzeń i śledzi ruch pakietów przechodzących przez nią. Dostęp do sieci jest ustalony indywidualnie dla każdego użytkownika na podstawie wniosku.
   7) Oprócz filtra pakietów (firewall) zastosowano również system wykrywający obecność złośliwego kodu w poczcie elektronicznej z zastosowaniem programów antywirusowych i antyspyware'owych itp. W efekcie zapewnione jest: zabezpieczenie sieci przed atakiem z zewnątrz poprzez blokowanie wybranych portów, filtrowanie pakietów i blokowanie niektórych usług, objęcie ochroną antywirusową wszystkich danych pobieranych z Internetu na stacjach lokalnych, zapisywanie logów połączeń użytkowników z siecią Internet.
   8) Dodatkowo do pomieszczeń w których następuje przetwarzanie danych osobowych mają dostęp tylko uprawnione osoby bezpośrednio związane z nadzorem nad serwerami lub aplikacjami.

9) Zabezpieczenie przed nieuprawnionym dostępem do danych, prowadzone jest przez Administratora Bezpieczeństwa zgodnie z przyjętymi procedurami nadawania uprawnień do systemu informatycznego. Hasło do zalogowania się do systemów przetwarzających dane osobowe powinno składać się z minimum 8 znaków (duże i małe litery, znaki specjalne i cyfry). Musi być zmieniane nie rzadziej niż raz na 30 dni, przy czym nowe hasło nie może być takie samo jak hasła poprzednie.
10) W pomieszczeniach w których znajdują się serwery zamontowane są czujniki dymu, w pomieszczeniach w których znajdują się serwery powinna być zamontowana klimatyzacja, która zapewnia właściwą temperaturę i wilgotność powietrza dla sprzętu komputerowego.
11) W pobliżu wejścia do pomieszczenia z serwerami i innym urządzeniami znajduje się gaśnica, która okresowo jest napełniana i kontrolowana przez specjalistę.
12) Większość urządzeń w serwerowni umieszczona jest w szafach serwerowych i sieciowych.

8. Podłączenie danego użytkownika do sieci komputerowej dokonuje Administrator Bezpieczeństwa Informacji aby uzyskać dostęp do zasobów sieci, należy zwrócić się do Administratora Bezpieczeństwa z odpowiednim upoważnieniem, w którym podane będą dane nowego użytkownika oraz zasoby jakie ma on mieć udostępnione (zał. nr 6).

9. Osoby mające dostęp do danych powinny posiadać zaświadczenie o przebytym szkoleniu z zakresu ustawy o ochronie danych osobowych.

10. Dodatkowe zasady ochrony danych osobowy przeznaczonych wyłącznie dla Administrator Bezpieczeństwa Informacji oraz osób bezpośrednio związanych z działaniem środowiska informatycznego zawiera załącznik **nr 7** „Polityka bezpieczeństwa informacji w zakresie dostępu do systemów oraz projekt sieci" opracowany w ramach realizacji projektu „E-Urząd w Łowiczu".

Rozdział 2. Kontrola przestrzegania zasad zabezpieczenia danych osobowych.

1. Administrator Danych i wyznaczony Administrator Bezpieczeństwa Informacji sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych wynikających z ustawy o ochronie danych osobowych oraz zasad ustanowionych w niniejszym dokumencie.

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

3. Na podstawie zgromadzonych materiałów, o których mowa w pkt. 2, Administrator Bezpieczeństwa Informacji sporządza roczne sprawozdanie i przedstawia Administratorowi Danych.

Rozdział 3. Opis zdarzeń naruszających ochronę danych osobowych.

1 Podział zagrożeń:

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

2 Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe obejmują w szczególności:

1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.,
2) niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,
3) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru,
4) pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,
5) naruszenie jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
6) naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,
7) próba lub modyfikacja danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
8) nastąpiła niedopuszczalna manipulacja danymi osobowymi w systemie,
9) ujawnienie osobom nieupoważnionym danych osobowych lub objętych tajemnicą procedur ochrony przetwarzania albo innych strzeżonych elementów systemu zabezpieczeń,
10) praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych - np. praca przy komputerze lub w sieci osoby, która nie jest

formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.,
11) ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki", itp.,
12) podmieniono lub zniszczono nośniki z danymi osobowymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane osobowe,
13) rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, próba instalacji niedozwolonego oprogramowania itp.).

3 Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, dyskietkach w formie niezabezpieczonej. Inne niedopuszczalne zachowania a mogące mieć miejsce ze względu na błędne przyzwyczajenia to: widoczne karteczki z hasłami, ekrany monitorów zwrócone w stronę klientów, dokumenty leżące na biurku, które mogą zostać zabrane przez osobę niepowołaną, dokumenty zawierające istotne informacje wyrzucone do śmietnika itp.

Rozdział 4. Postępowanie w przypadku naruszenia ochrony danych osobowych.

1 W przypadku stwierdzenia naruszenia:

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

każda osoba zatrudniona przy przetwarzaniu danych osobowych jest obowiązana niezwłocznie powiadomić o tym fakcie Administratora Bezpieczeństwa Informacji.

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

3 Do czasu przybycia na miejsce naruszenia ochrony danych osobowych Administratora Bezpieczeństwa Informacji lub upoważnionej przez niego osoby, należy:

1) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców,
2) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
3) zaniechać - o ile to możliwe - dalszych planowanych przedsięwzięć, które wiążą się

z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,
4) podjąć inne działania przewidziane i określone w instrukcjach technicznych i technologicznych stosownie do objawów i komunikatów towarzyszących naruszeniu,
5) podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej,
6) zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku,
7) udokumentować wstępnie zaistniałe naruszenie,
8) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora Bezpieczeństwa Informacji lub osoby upoważnionej.

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

4 Administrator Bezpieczeństwa Informacji dokumentuje zaistniały przypadek naruszenia oraz sporządza raport wg wzoru stanowiącego załącznik **nr 3**, który powinien zawierać w szczególności:
   1) wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpytanych w związku z naruszeniem,
   2) określenie czasu i miejsca naruszenia i powiadomienia,
   3) określenie okoliczności towarzyszących i rodzaju naruszenia,
   4) wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania,
   5) wstępną ocenę przyczyn wystąpienia naruszenia,
   6) ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.

5. Raport, o którym mowa w pkt. 4, Administrator Bezpieczeństwa Informacji niezwłocznie przekazuje Administratorowi Danych, a w przypadku jego nieobecności osobie uprawnionej.

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

7. Zaistniałe naruszenie może stać się przedmiotem szczegółowej, zespołowej analizy prowadzonej przez Administrator Danych, Administratora Bezpieczeństwa Informacji, Pełnomocnika ds. Ochrony Informacji Niejawnych.

8. Analiza, o której mowa w pkt. 7, powinna zawierać wszechstronną ocenę zaistniałego naruszenia, wskazanie odpowiedzialnych, wnioski co do ewentualnych przedsięwzięć proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.

Rozdział 5. Monitorowanie zabezpieczeń

1. Prawo do monitorowania systemu zabezpieczeń posiadają, zgodnie z zakresem czynności:
   1) Administrator Danych,
   2) Administrator Bezpieczeństwa Informacji,
   3) osoby bezpośrednio związanych z działaniem środowiska informatycznego.

2. W ramach kontroli należy zwracać szczególna uwagę na:
   1) okresowe sprawdzanie kopii bezpieczeństwa pod względem przydatności do możliwości odtwarzania danych,
   2) kontrola ewidencji nośników magnetycznych,
   3) kontrola właściwej częstotliwości zmiany haseł.

Rozdział 6. Szkolenia

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

Rozdział 7. Niszczenie wydruków i zapisów na nośnikach magnetycznych

1. Nośniki magnetyczne przekazywane na zewnątrz powinny być pozbawione zapisów zawierających dane osobowe,
2. Niszczenie poprzednich zapisów powinno odbywać się poprzez wymazywanie informacji (z użyciem odpowiedniego oprogramowania) oraz formatowanie nośnika. Operacje te wykonywane są przez osoby wskazane przez Administratora Bezpieczeństwa Informacji.
3. Poprawność przygotowania nośnika magnetycznego powinna być sprawdzona przez Administratora Bezpieczeństwa Informacji,
4. Uszkodzone nośniki magnetyczne przed ich wyrzuceniem należy fizycznie zniszczyć poprzez przecięcie, przełamanie itp.
5. Wydruki po wykorzystaniu należy zniszczyć w mechanicznej niszczarce do papieru.

Rozdział 8. Archiwizacja danych

1. Dane systemów kopiowane są w systemie tygodniowym. Nośniki z kopiami bezpieczeństwa przechowywane są w miejscach bezpiecznych (kasa Urzędu, kancelaria tajna itp.).

2. Kopie awaryjne danych zapisywanych w programach wykonywane są codziennie.
3. Odpowiedzialnym za wykonywanie kopii danych i kopii awaryjnych jest Administrator Bezpieczeństwa Informacji.
4. Na koniec danego miesiąca wykonywane są kopie bezpieczeństwa z całego programu przetwarzającego dane. Nośniki z kopiami bezpieczeństwa przechowywane są w miejscach bezpiecznych (kasa Urzędu, kancelaria tajna itp.).
5. Kopie awaryjne przechowywane są w kasie pancernej, szafie metalowej w wyznaczonym pomieszczeniu lub instytucji, z którą podpisano stosowne porozumienie.
6. Dyskietki, na których zapisywane są kopie bezpieczeństwa są każdorazowo wymazywane i formatowane, w taki sposób, by nie można było odtworzyć ich zawartości.
7. Płyty CD, DVD na których przechowuje się kopie awaryjne niszczy się w sposób mechaniczny, tak by nie można było użyć ich ponownie.
8. Administrator Bezpieczeństwa Informacji odpowiedzialny jest za dokonywanie wymiany kopii awaryjnych na aktualne.
9. Administrator Bezpieczeństwa Informacji dokonuje okresowej weryfikacji kopii bezpieczeństwa pod kątem ich przydatności.

Rozdział 9. Postanowienia końcowe

1 Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, podlega odpowiedzialności na podstawie odrębnych przepisów.

2 Administrator Bezpieczeństwa zobowiązany jest prowadzić ewidencję osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych wg wzoru stanowiącego załącznik **nr 5** do niniejszego dokumentu.

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

4 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.

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

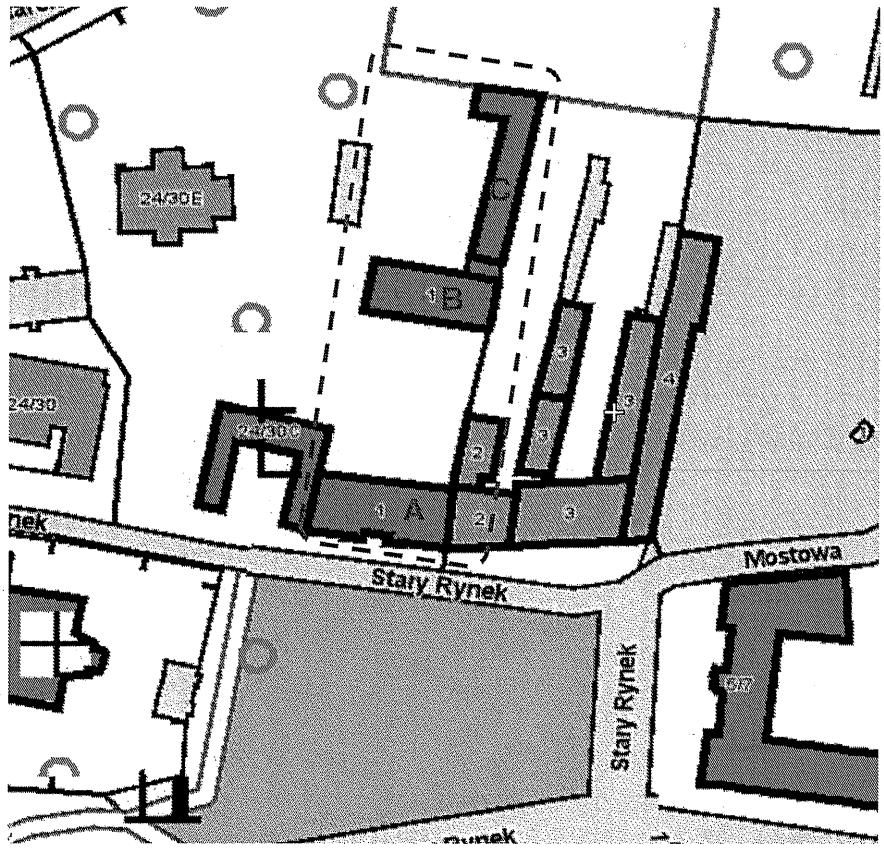
6 W sprawach nie uregulowanych niniejszym dokumentem mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych Dz.U. z 2002 r. Nr 101, poz. 926, rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100,

poz. 1024) oraz rozporządzenie Ministra Sprawiedliwości z dnia 28 kwietnia 2004r. w sprawie sposobu technicznego przygotowania systemów i sieci do przekazywania informacji – do gromadzenia wykazów połączeń telefonicznych i innych przekazów informacji oraz sposobów zabezpieczenia danych informatycznych (Dz. U. Nr 100, poz. 1023).

7 Niniejsza „Polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Łowiczu" wchodzi w życie z dniem jej podpisania przez Burmistrza.

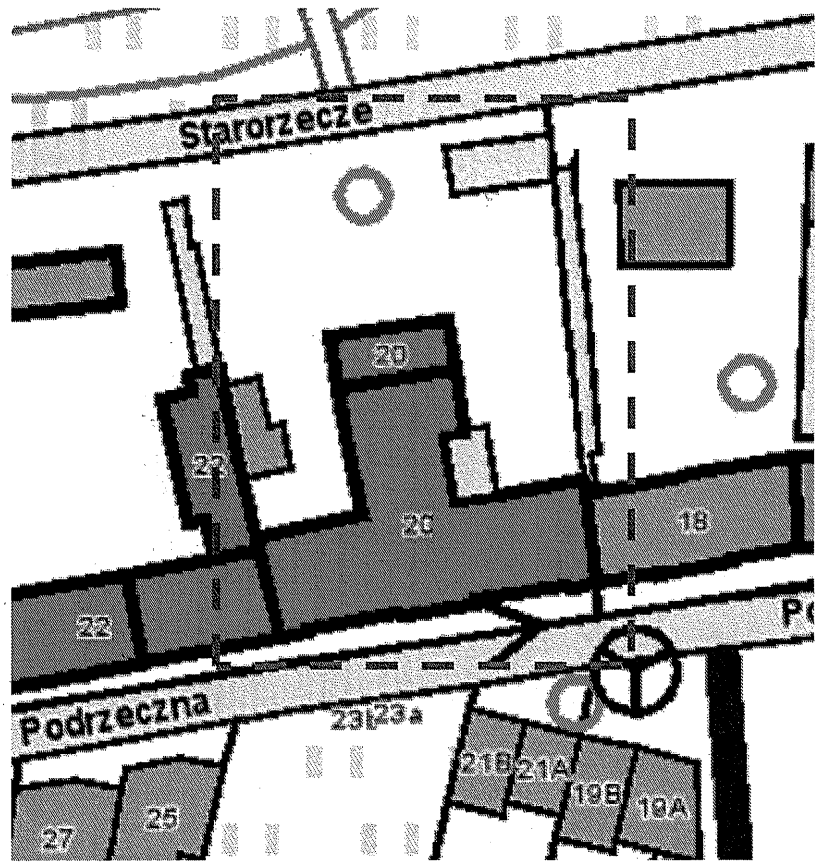
***Załącznik nr 1.* Granice obszarów oraz wykaz pomieszczeń z uwzględnieniem wydziałów, w których przetwarzane są dane osobowe.**

Dane osobowe są przetwarzane w trzech odrębnych budynkach położonych w Łowiczu odpowiednio dwa przy ul. Stary Rynek 1 oraz trzeci przy ulicy Podrzecznej 20. Pierwszy budynek to dwupiętrowy Ratusz (współrzędne geograficzne 52°6'29,5"N 19°56'42"E) dodatkowo dla rozróżnienia przyjmuję się oznaczenie tego budynku jako **A**. Za nim w odległości ok. 35 metrów znajduję się drugi budynek w kształcie znaku „⌋" – w którym ze względu na budowę wyróżnia się dwie części **B** (budynek jednopiętrowy) i **C** (budynek parterowy) patrz rysunek 1 poniżej. Przed głównym wejściem do budynku Ratusza (budynek A) znajduje się duży plac parkingowy zaś za budynkiem C drugi plac parkingowy z wjazdem od ulicy Starorzecze.



Rys.1 Położenie budynku Ratusza pl. Stary Rynek 1 –mapę pobrano z http://geoportal.gov.pl

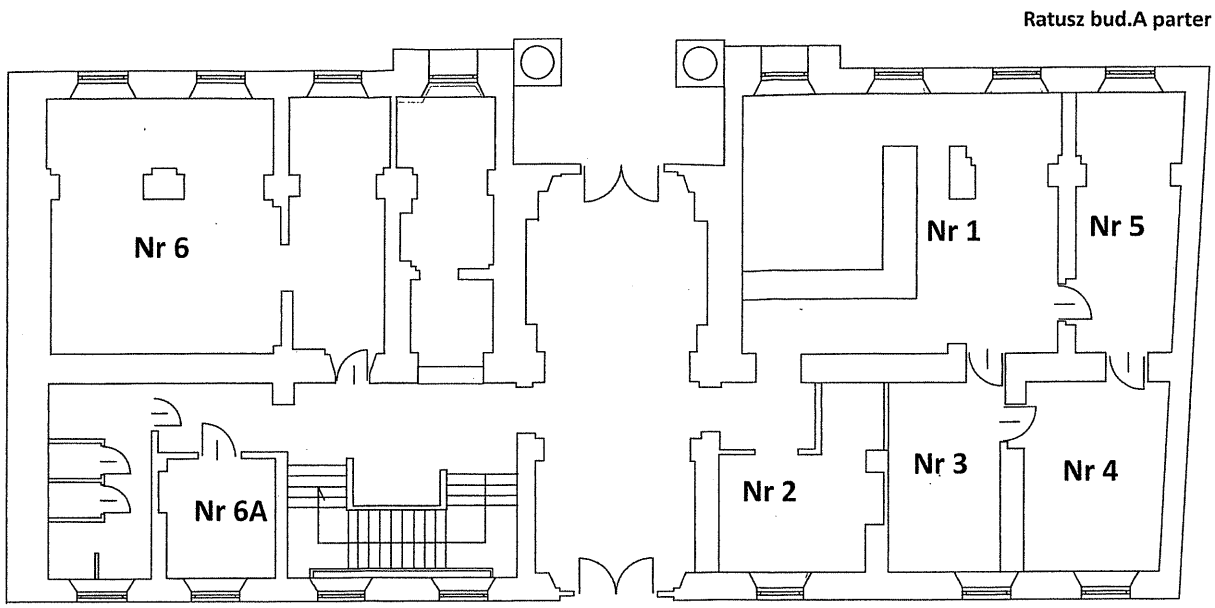
Budynek trzeci położony jest przy ulicy Podrzecznej 20 (współrzędne geograficzne 52°6'29,47"N 19°56'21"E) z czego tylko część pomieszczeń zajmuje Urząd Stanu Cywilnego a w pozostałych mieści się Łowicki Ośrodek Kultury (rysunek 2 poniżej).



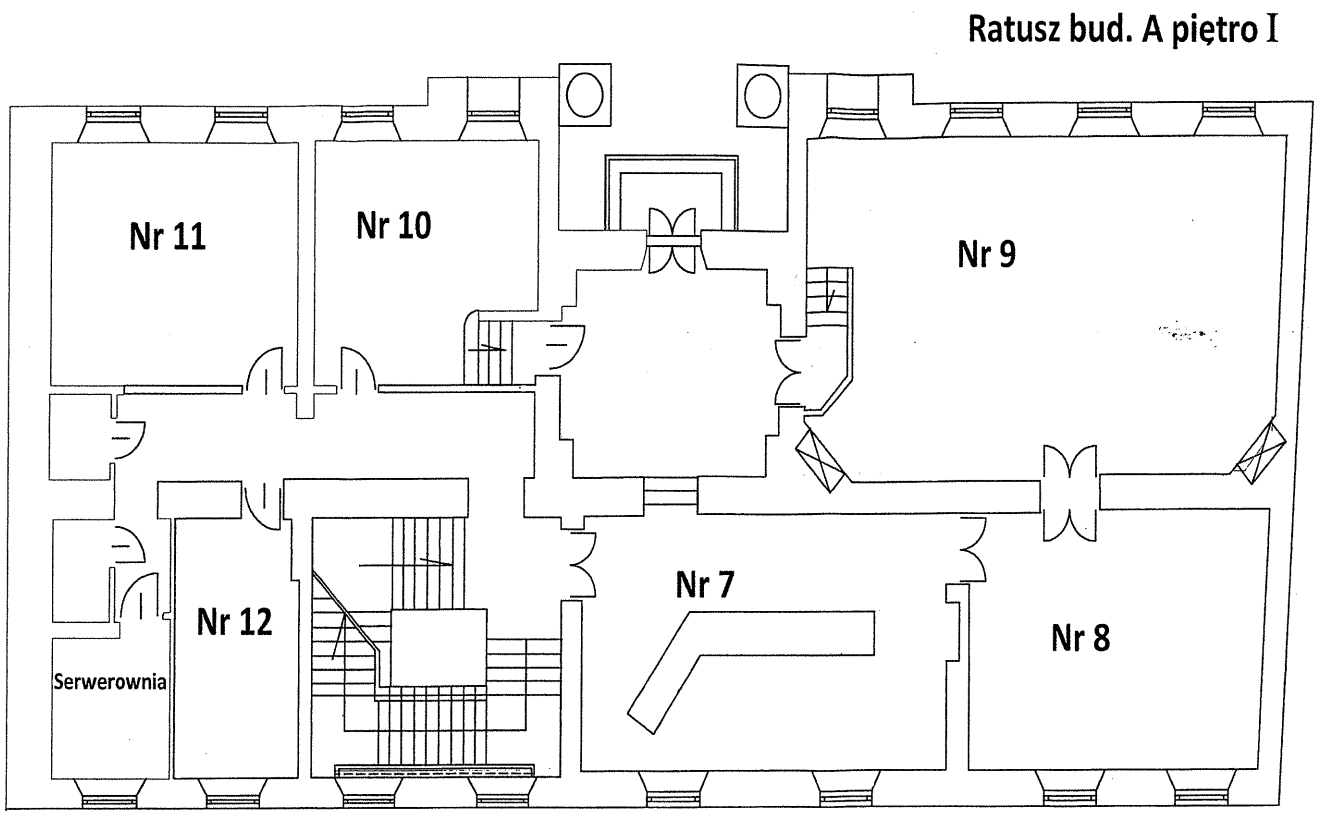
Rys.2 Położenie budynku USC ul Podrzeczna 20 – mapę pobrano z http://geoportal.gov.pl

Wykaz pomieszczeń w których przetwarzane są dane osobowe w Urzędzie Miejskim w Łowiczu.

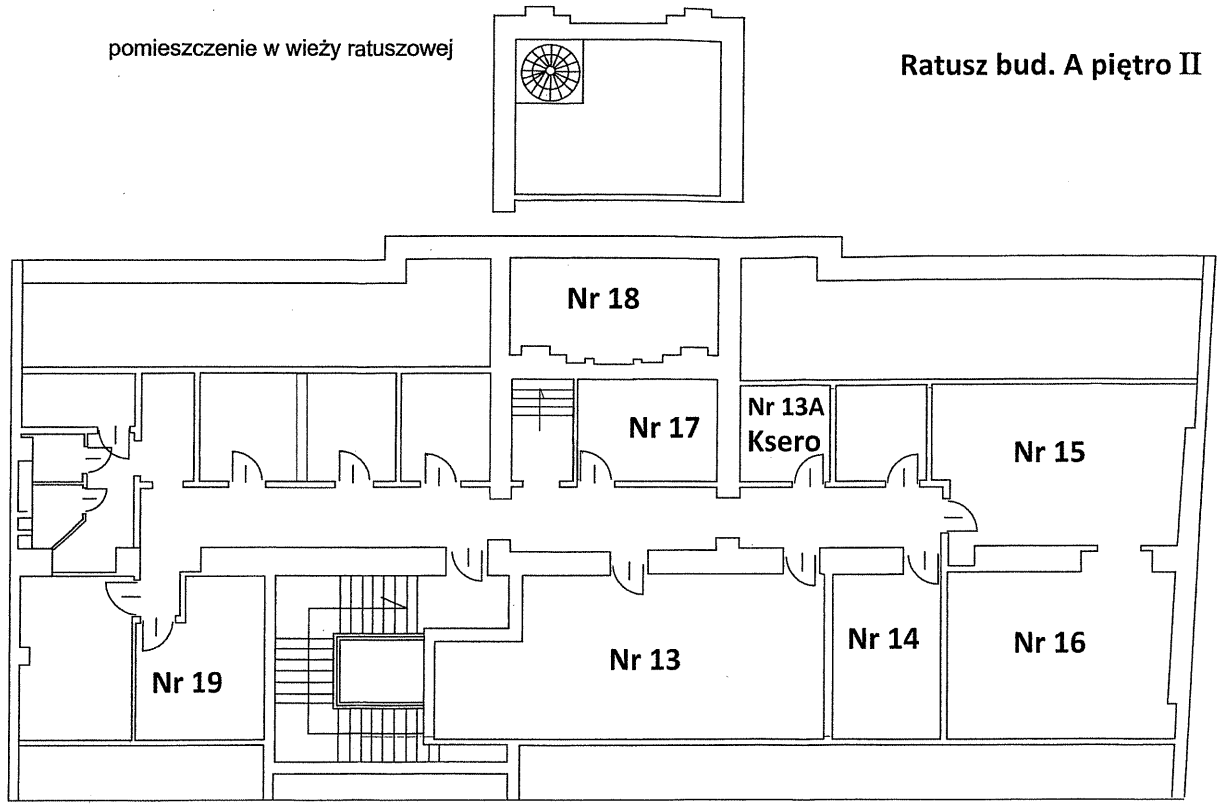
Lp.	Wydział	Budynek	Oznaczenie pomieszczenia
1	Wydział Finansowy	Stary Rynek 1, Ratusz - bud.A	Pok. Nr 1-5
2	Wydział Promocji, Kultury, Sportu i Turystyki	Stary Rynek 1, Ratusz - bud.A	Pok. Nr 6 (podwójne wejście –przez PTTK)
3	Wydział Spraw Społecznych	Stary Rynek 1, Ratusz - bud.A	Pok. Nr 6a
4	Sekretariat	Stary Rynek 1, Ratusz - bud.A	Pok. Nr 7
5	Burmistrz Miasta	Stary Rynek 1, Ratusz - bud.A	Pok. Nr 8
6	Sala konferencyjna	Stary Rynek 1, Ratusz - bud.A	Pok. Nr 9
7	Z-ca Burmistrza	Stary Rynek 1, Ratusz - bud.A	Pok. Nr. 10 (2 wejścia)
8	Biuro Rady	Stary Rynek 1, Ratusz - bud.A	Pok. Nr 11
9	Biuro Rady - Przewodniczący	Stary Rynek 1,Ratusz - bud.A	Pok. Nr. 12
10	Serwerownia	Stary Rynek 1,Ratusz - bud.A	Serwerownia
11	Wydział Organizacyjny	Stary Rynek 1, Ratusz - bud.A	Pok. Nr 13, 13A(Ksero)
12	Zespół Radców Prawnych	Stary Rynek 1, Ratusz - bud.A	Pok. Nr 14
13	Wydział finansowy	Stary Rynek 1, Ratusz - bud.A	Pok. Nr 15
14	Skarbnik Miasta	Stary Rynek 1, Ratusz - bud.A	Pok. Nr 16
15	Sekretarz Miasta	Stary Rynek 1, Ratusz - bud.A	Pok. Nr 17
16	Wydział do Spraw Pozyskiwania Środków Zewnętrznych	Stary Rynek 1, Ratusz - bud.A	Pok. Nr 18



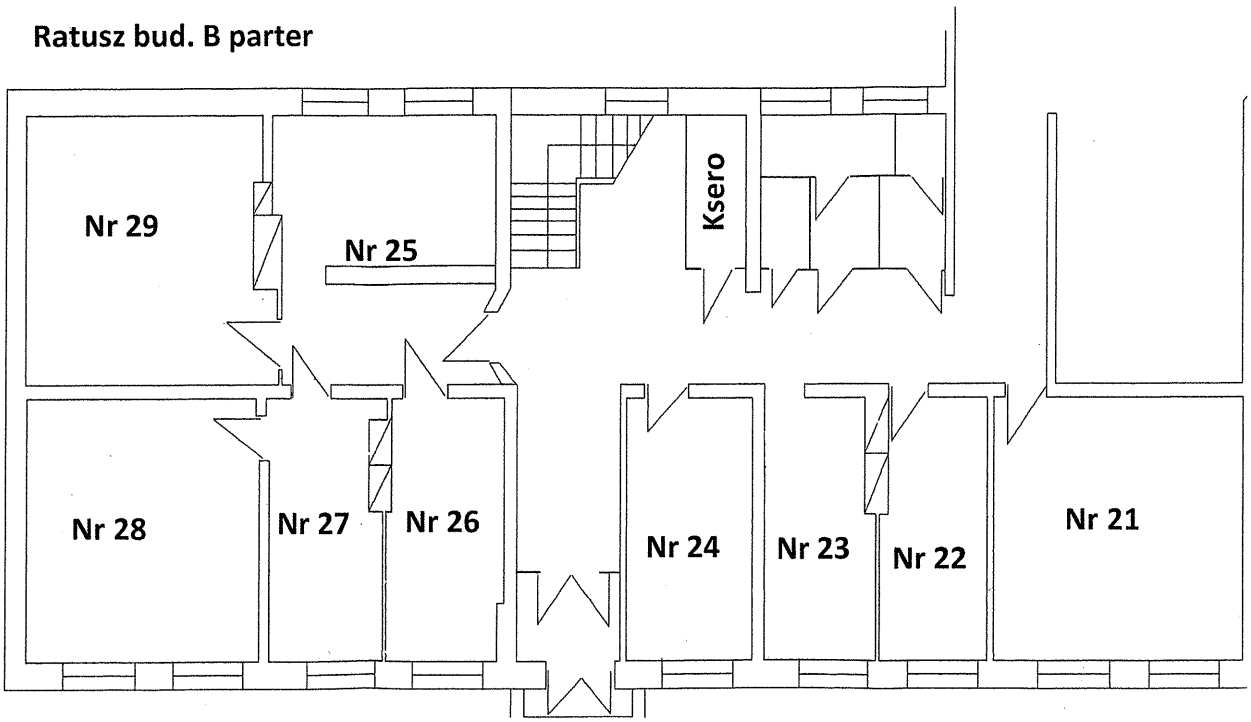
Rys. 3 Ratusz budynek A parter pokoje od nr 1 do 6A



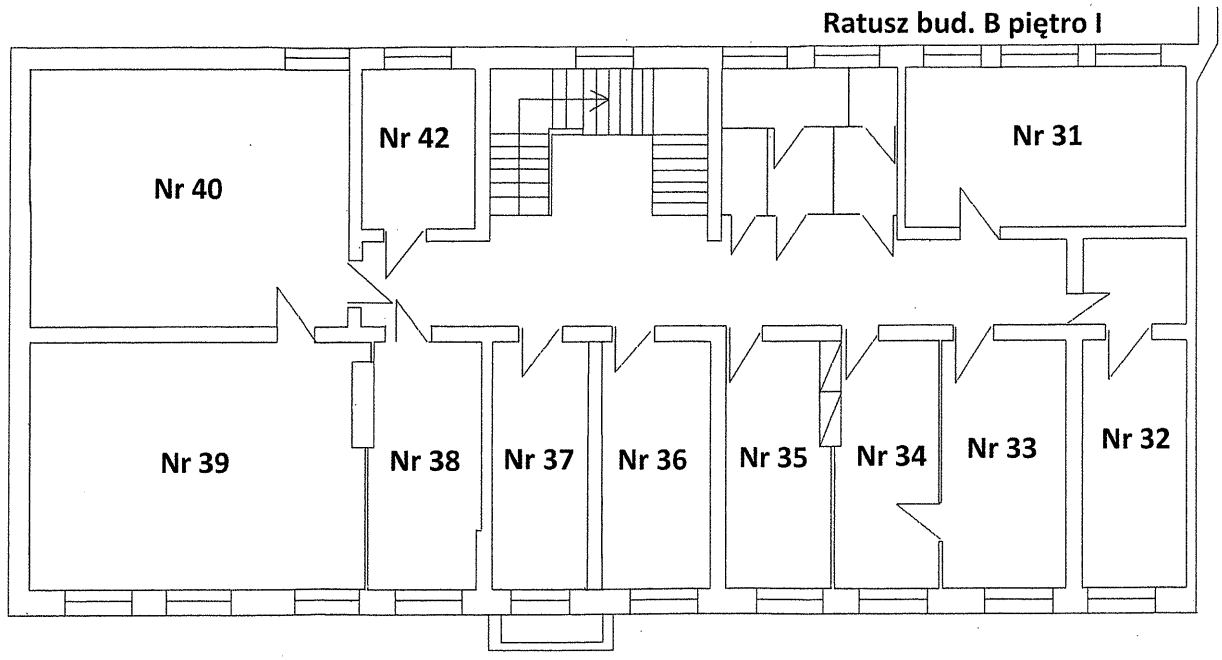
Rys. 4 Ratusz budynek A piętro I pokoje od nr 7 do 12



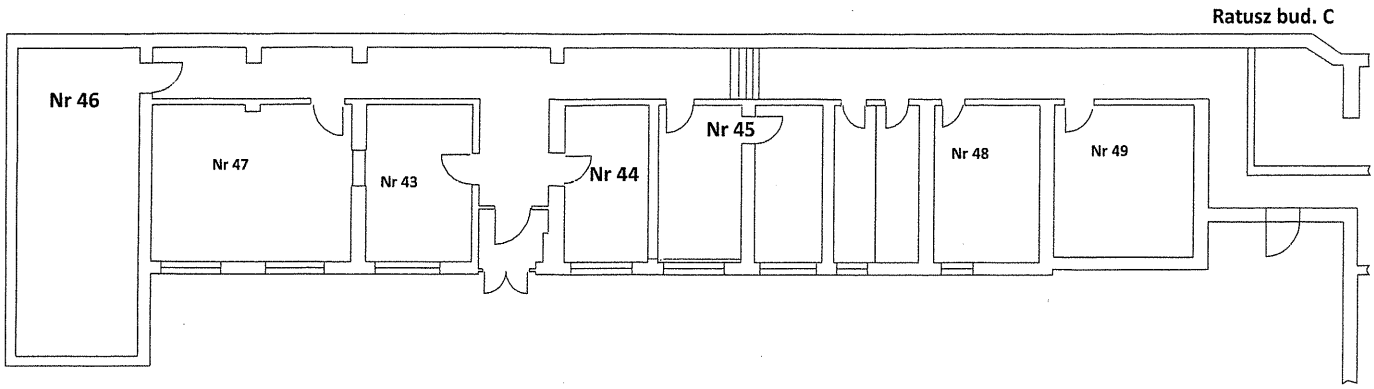
Rys. 5 Ratusz budynek A piętro II pokoje od nr 13 do 20B



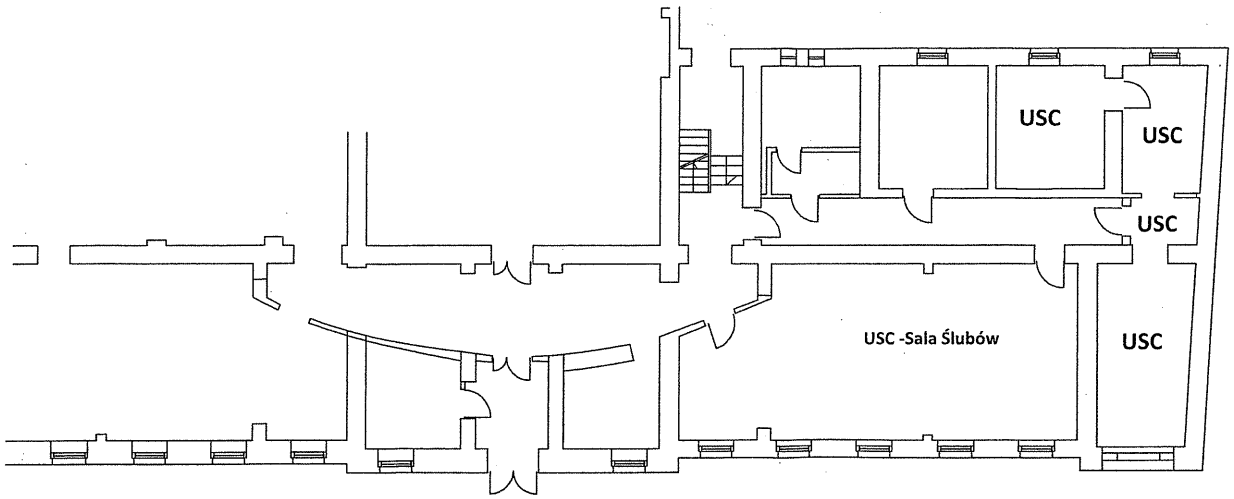
Rys. 6 Ratusz budynek B parter pokoje od nr 21 do 29



Rys. 7 Ratusz budynek B piętro I pokoje od nr 31 do 42



Rys. 8 Ratusz budynek C



Rys. 9 USC - ul. Podrzeczna 20

17	Wydział Spraw Społecznych	Stary Rynek 1, Ratusz - bud.A	Pok. Nr 19
18	Wydział Spraw Lokalowych i Działalności Gospodarczej	Stary Rynek 1, Budynek **B**	Pok. Nr 21-22
19	Samodzielne stanowisko do Spraw Informatyki	Stary Rynek 1, Budynek **B**	Pok. Nr 23
20	Samodzielne stanowisko do Spraw Kontroli / Audytor Wewnętrzny	Stary Rynek 1, Budynek **B**	Pok. Nr 24
21	Wydział Spraw Obywatelskich	Stary Rynek 1, Budynek **B**	Pok. Nr 25-29
22	Wydział Gospodarki Gruntami, Planowania Przestrzennego i Rolnictwa	Stary Rynek 1, Budynek **B**	Pok. Nr 31
23	Wydział Spraw Obywatelskich	Stary Rynek 1, Budynek **B**	Pok. Nr 32
24	Wydział Gospodarki Gruntami, Planowania Przestrzennego i Rolnictwa	Stary Rynek 1, Budynek **B**	Pok. Nr 33 -36
25	Wydział Gospodarki Gruntami, Planowania Przestrzennego i Rolnictwa	Stary Rynek 1, Budynek **B**	Pok. Nr 37
26	Wydział Inwestycji i Remontów	Stary Rynek 1, Budynek **B**	Pok. Nr 38 - 40
27	Wydział Gospodarki Gruntami, Planowania Przestrzennego i Rolnictwa	Stary Rynek 1, Budynek **B**	Pok. Nr 42
28	Wydział Spraw Komunalnych i Reagowania Kryzysowego	Stary Rynek 1, Budynek **C**	Pok. Nr 43-44
29	Miejski Zespół Reagowania Kryzysowego	Stary Rynek 1, Budynek **C**	Pok. Nr 45
30	Wydział Spraw Komunalnych i Reagowania Kryzysowego	Stary Rynek 1, Budynek **C**	Pok. Nr 46
31	Archiwum	Stary Rynek 1, Budynek **C**	Pok. Nr 46
32	USC	Ul. Podrzeczna 20	USC (Patrz. Rys 9.)

Poniżej schematy poszczególnych budynków wraz ze wskazaniem poszczególnych pomieszczeń, w których przetwarzane są dane osobowe.

Załącznik nr 2. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.

Do przetwarzania zbiorów danych osobowych w systemie informatycznym Urzędu Miejskiego w Łowiczu stosowane są pakiety biurowe (Ms Office 2010) lub specjalizowane programy (aplikacje) do których zaliczamy:

1) **Zbiór danych personalny pracowników** – przetwarzany przez program **PŁATNIK** – pełny opis systemu zawiera *załącznik 2a* – pobrany ze strony dostawcy oprogramowania.
2) **Zbiór danych osobowych ELUD, EDG, KOS** – przetwarzany przez system OTAGO – (wykaz poniżej) - pełny opis systemu, zawiera *załącznik 2b.*

Lp.	Nazwa podsystemu	Opis
1.	ADMIN	Administrowanie systemem OTAGO
2.	DOCZ	Obsługa dopłat czynszowych
3.	E-URZĄD	Elektroniczny Urząd
4.	ELUD	Ewidencja ludności
5.	FKJB	Obsługa finansowo-księgowa jednostki budżetowej
6.	FKORG	Obsługa finansowo-księgowa organu
7.	FKPLAN	NW (brak danych osobowych)
8.	GEOD	Obsługa Zasobu Geodezyjnego
9.	ENIER-BL	Ewidencja nieruchomości - budynki, lokale
10.	ENIER-G	Ewidencja nieruchomości - grunty
11.	IMPORTGEOD	NW (brak danych osobowych)
12.	GRU	Obsługa generalnego rejestru umów wraz z omówieniem umów dochodowych waloryzowanych.
13.	INSO	Informator użytkownika systemu
14.	KADRY	Obsługa kadr
15.	KASA	Obsługa kasy dochodowej i wydatkowej
16.	KOALA	Obsługa koncesji
17.	KOS	Obsługa kartotek systemu
18.	KSOD	Kompleksowy System Obiegu Dokumentów
19.	LOK	Obsługa lokali komunalnych ?
20.	NWPOJ	Naliczanie i windykacja podatku od środków transportowych
21.	OPGRU	Podsystem opłat gruntowych
22.	PLBUD	Obsługa planowania budżetu oraz plan budżetu
23.	PŁACE	Płace
24.	PNIER	Naliczanie podatku od nieruchomości
25.	PPW	Przekształcenie użytkowana wieczystego w prawo własności oraz windykacja
26.	PROL	Naliczanie podatku rolnego, leśnego i od nieruchomości
27.	ST	Gospodarka środkami trwałymi
28.	STP	Obsługa stypendiów i zapomóg szkolnych
29.	WIND	(NW)
30.	WNIER	Windykacja podatku od nieruchomości
31.	WOGRU	Windykacja opłat za wieczyste użytkowanie gruntów
32.	WPBUD	Obsługa wpływów budżetowych.
33.	WPF	Wieloletnia prognoza finansowa (NW)

34.	WPPW	Windykacja PPW (NW)
35.	WROL	Windykacja podatku rolnego, leśnego i od nieruchomości
36.	WYBORY	Obsługa wyborów
37.	WYBUD	Obsługa wydatków budżetowych

3) **Zbiór danych osobowych** – przetwarzany przez system **RADIX** – opis danych zawiera *załącznik 2c*. (Uwaga! W związku z wprowadzeniem systemu Eurząd firmy Otago system RADIX będzie pełni rolę systemu archiwalnego)

Lp.	Nazwa podsystemu	Opis
1.	ELUD+	Ewidencja ludności
2.	KADRY	Obsługa kadr
3.	POST	Podatek od środków transportu
4.	NDM	Dodatki mieszkaniowe
5.	EGW	Ewidencja dzierżaw wieczystych
6.	EPOD	Ewidencja działalności gospodarczej
7.	POGRON	Naliczanie podatku rolnego, leśnego i od nieruchomości
8.	WIP	Windykacja Podatkowa

4) **Zbiór danych osobowych** – przetwarzany przez program **EWOPIS** w połączeniu z programem **EWMAPA.**
5) **Zbiór danych osobowych** – przetwarzany przez program **ESS**. (4 HSCO)