Zarządzenie Nr 748/14
Burmistrza Łobza
z dnia 25 lipca 2014 r

w sprawie ustalenia Polityki bezpieczeństwa i instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Miejskim w Łobzie.

Na podstawie art. 36 ust. 1 i 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.[1]) oraz § 3 ust. 1rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 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)

zarządza się, co następuje:

§ 1.

Ustala się „Politykę bezpieczeństwa i instrukcję zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Miejskim w Łobzie", zwaną dalej „Polityką bezpieczeństwa", która stanowi załącznik do niniejszego zarządzenia.

§ 2.

1. Zobowiązuje się kierowników wydziałów do zapoznania podległych pracowników z treścią niniejszego zarządzenia.
2. Zobowiązuje się pracowników Urzędu Miejskiego w Łobzie do stosowania zasad określonych w „Polityce bezpieczeństwa".

§ 3.

Wykonanie zarządzenia powierza się Administratorowi Bezpieczeństwa Informacji.

§ 4.

1. Traci moc zarządzenie Nr 201/07 Burmistrza Łobza z dnia 27 listopada 2007 r. w sprawie ustalenia Polityki bezpieczeństwa i instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Miejskim w Łobzie.
2. Zachowują moc upoważnienia wydane na podstawie zarządzenia, o którym mowa w ust. 1.

§ 5.

Zarządzenie wchodzi w życie z dniem podpisania.

Z up. BURMISTRZA
mgr Ireneusz Kabat
ZASTĘPCA BURMISTRZA

[1] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2002 r. Nr 153, poz. 1271, z 2004 r. Nr 25, poz. 219 i Nr 33, poz. 285, z 2006 r. Nr 104, poz. 708 i 711, z 2007 r. Nr 165, poz. 1170 i Nr 176, poz. 1238 oraz z 2010 r. Nr 41, poz. 233, Nr 182, poz. 1228 i Nr 229, poz. 1497 oraz z 2011 r. Nr 230, poz. 1371

Załącznik do
zarządzenia Nr 448/14
Burmistrza Łobza
z dnia 25 lipca 2014

Polityka bezpieczeństwa i instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych

w Urzędzie Miejskim w Łobzie

SPIS TREŚCI:

Załącznik nr 6 - Upoważnienie imienne do przeważania danych osobowych

Załącznik nr 7 - Raport z naruszenia bezpieczeństwa systemu informatycznego w Urzędzie

Załącznik nr 8 - Wykaz osób, które zostały zapoznane z Polityką Bezpieczeństwa.

Załącznik nr 9 - Oświadczenie

Załącznik nr 10 - Oświadczenie o zachowaniu w tajemnicy danych osobowych osób zatrudnionych przy przetwarzaniu danych osobowych dla pracowników Urzędu

Załącznik nr 11 - Oświadczenie o zachowaniu w tajemnicy danych osobowych osób zatrudnionych przy przetwarzaniu danych osobowych dla użytkowników nie będących pracownikami Urzędu

Załącznik nr 12 - Upoważnienie

Załącznik nr 13 - Ewidencja osób upoważnionych do przetwarzania danych osobowych w systemach informatycznych Urzędu Miejskiego w Łobzie

Załącznik nr 14 - Ewidencja oświadczeń o zachowaniu w tajemnicy danych osobowych osób zatrudnionych przy przetwarzaniu danych osobowych

Załącznik nr 15 - Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do ich przetwarzania

WPROWADZENIE

Polityka bezpieczeństwa, określa środki techniczne i organizacyjne zastosowane przez Administratora Danych dla zapewnienia ochrony danych osobowych oraz tryb postępowania w przypadku stwierdzenia naruszenia zabezpieczenia danych osobowych w systemie informatycznym lub kartotekach, albo w sytuacji powzięcia podejrzenia o takim naruszeniu.

Niniejszy dokument opisuje reguły dotyczące bezpieczeństwa danych osobowych w Urzędzie Miejskim w Łobzie (zwanym dalej Urzędem). Opisane reguły określają granice dopuszczalnego zachowania wszystkich użytkowników systemów informatycznych wspomagających pracę Urzędu. 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 i instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Miejskim w Łobzie", zwany dalej „Polityką bezpieczeństwa", wskazujący sposób postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych w systemach informatycznych, przeznaczony jest dla osób zatrudnionych przy przetwarzaniu tych danych.
Potrzeba jego opracowania wynika z § 3, 4 i 5 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).

Określenia i skróty użyte w „Polityce bezpieczeństwa":

1. **Administrator Danych Osobowych** – Burmistrz Łobza, zwany dalej **Administratorem Danych.**
2. **Administrator Bezpieczeństwa Informacji** - rozumie się przez to osobę wyznaczoną przez Administratora Danych nadzorującą przestrzeganie zasad ochrony przetwarzanych danych osobowych. Nadzór dotyczy przede wszystkim stosowanych środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczenia danych przed ich udostępnieniem osobom

nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t. j. Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.) oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Przeprowadza on także kontrole w zakresie określonym regulacjami wewnętrznymi obowiązującymi u Administratora Danych, zwany dalej **ABI**

3. **Administrator Systemów Informatycznych** - osoba wyznaczona przez Burmistrza Łobza, odpowiedzialna za sprawność i konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych w przetwarzanych zbiorach danych osobowych, zwany dalej **ASI.**
4. **Bezpieczeństwo systemu informatycznego** - wdrożenie przez Administratora Danych lub osobę przez niego uprawnioną środków organizacyjnych i technicznych w celu zabezpieczenia oraz ochrony danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz nieuprawnioną zmianą, utratą, uszkodzeniem lub zniszczeniem.
5. **Zbiór danych** - rozumie się przez to każdy posiadający strukturę zestaw o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
6. **Przetwarzanie danych osobowych** - wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie.
7. **Osoba upoważniona lub użytkownik systemu** - osoba posiadająca upoważnienie wydane przez Administratora Danych lub uprawnioną przez niego osobę i dopuszczona jako użytkownik do przetwarzania danych osobowych w systemie informatycznym danej komórki organizacyjnej w zakresie wskazanym w upoważnieniu, zwana dalej **użytkownikiem.**
8. **Przełożony użytkownika** - kierownik komórki organizacyjnej Urzędu Miejskiego w Łobzie, zwany dalej **przełożonym**.
9. **Osoba uprawniona** osoba posiadająca upoważnienie wydane przez Administratora do wykonywania w jego imieniu określonych czynności.
10. **Użytkownik uprzywilejowany** - osoba posiadająca najwyższy stopień uprawnień do zarządzania systemem informatycznym.
11. **Urząd** – Urząd Miejski w Łobzie.
12. **Systemy informatyczne Urzędu** zwane dalej systemami – zespoły współpracujących ze sobą urządzeń, programów, procedur gromadzenia i przetwarzania informacji, narzędzi programowych zastosowanych do przetwarzania danych wraz ze zgromadzonymi danymi oraz osobami upoważnionymi do pracy na tych systemach (w tym obsługa techniczna urządzeń).

13. **Kartoteka** - rozumie się przez to zewidencjonowany, usystematyzowany zbiór wykazów, skoroszytów, wydruków komputerowych i innej dokumentacji gromadzonej w formie papierowej, zawierający dane osobowe.
14. **Pomieszczenie** - rozumie się przez to budynki, pomieszczenia lub części pomieszczeń określone przez Administratora Danych tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego oraz gromadzone w kartotekach.

Postanowienia ogólne

1. „Polityka bezpieczeństwa" określa tryb postępowania w przypadku, gdy:
   1) stwierdzono naruszenie zabezpieczenia systemu informatycznego,
   2) stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci informatycznej mogą wskazywać na naruszenie zabezpieczeń tych danych.
2. „Polityka bezpieczeństwa" obowiązuje wszystkich pracowników Urzędu Miejskiego w Łobzie.
3. Wykonywanie postanowień tego dokumentu ma zapewnić właściwą reakcję, ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa systemów oraz zapewnić właściwy tryb działania w celu przywrócenia bezpieczeństwa danych przetwarzanych w systemach informatycznych Urzędu.
4. Administrator danych, którym jest Burmistrz Łobza, swoją decyzją wyznacza Administratora Bezpieczeństwa Informacji danych zawartych w systemach informatycznych Urzędu.
5. 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" w przypadku wykrycia nieuprawnionego dostępu do 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) Administrator Bezpieczeństwa Informacji prowadzi następujące ewidencje:

1) ewidencję baz danych w systemach informatycznych, w których przetwarzane są dane osobowe (załącznik nr 15 do niniejszego dokumentu),
2) ewidencję osób upoważnionych do przetwarzania danych osobowych w systemach informatycznych (załącznik nr 13 do niniejszego dokumentu),
3) ewidencje oświadczeń o zachowaniu w tajemnicy danych osobowych osób zatrudnionych przy przetwarzaniu danych osobowych (załącznik nr 14 do niniejszego dokumentu),

6. W celu zwiększenia efektywności ochrony danych osobowych dokonano połączenia różnych zabezpieczeń w sposób umożliwiający stworzenie kilku warstw ochronnych. Ochrona danych osobowych jest realizowana poprzez: zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz przez użytkowników.
7. Zastosowane zabezpieczenia mają służyć osiągnięciu poniższych celów i zapewnić:
   1) poufność danych - rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom,
   2) integralność danych - rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
   3) rozliczalność danych - rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie,
   4) integralność systemu - rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej.
8. Realizację zamierzeń określonych pkt. 6 i 7 powinny zagwarantować następujące założenia:
   1) wdrożenie procedur określających postępowanie osób dopuszczonych do przetwarzania danych osobowych oraz ich odpowiedzialność za ochronę tych danych,
   2) przeszkolenie użytkowników w zakresie bezpieczeństwa i ochrony danych osobowych,
   3) upoważnienie użytkowników do przetwarzania danych osobowych oraz przypisanie użytkownikom określonych atrybutów umożliwiających wykonywanie ustalonych operacji na różnych poziomach zbiorów danych osobowych - stosownie do indywidualnego zakresu upoważnienia, zgodnie z zakresem powierzonych obowiązków, które wyznaczają poziom uprawnień,
   4) podejmowanie niezbędnych działań w celu likwidacji słabych ogniw w systemie zabezpieczeń,
   5) okresowe sprawdzanie przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych osobowych,
   6) opracowanie procedur odtwarzania systemu w przypadku wystąpienia awarii.

7) śledzenie osiągnięć w dziedzinie zabezpieczania systemów informatycznych i w miarę możliwości organizacyjnych i techniczno-finansowych - wdrażanie nowych narzędzi i metod pracy oraz sposobów zarządzania systemem informatycznym, które będą służyły wzmocnieniu bezpieczeństwa danych osobowych.

9. Przez politykę bezpieczeństwa należy rozumieć określenie zadań, których realizacja jest niezbędna dla zapewnienia spójności wszystkich zabezpieczeń danych osobowych. Została ona sformułowana w kolejnych rozdziałach niniejszej Polityki bezpieczeństwa i Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Odzwierciedla ona podstawowe zasady bezpieczeństwa, a także zarządzania systemem informatycznym oraz kartotekami u Administratora Danych.

Ochrona zasobów danych Urzędu jako całości, przed ich nieuprawnionym użyciem lub zniszczeniem, jest jednym z podstawowych obowiązków każdego pracownika Urzędu. Obowiązkiem każdego pracownika Urzędu jest zachowanie tajemnicy służbowej, w tym ochrony danych osobowych gromadzonych i przetwarzanych przez Urząd. Obowiązek ten istnieje również po ustaniu zatrudnienia. Osoby zatrudnione przy przetwarzaniu danych (także poza systemami) są zobowiązane do szczególnej dbałości o zachowanie poufności, integralności i dostępności do danych gromadzonych w kartotekach, skorowidzach itp. oraz infrastruktury sprzętowo – programowej systemu.

Obszary przetwarzania danych

1. W celu zapewnienia bezpiecznych warunków przetwarzania danych w systemach Urzędu określa się obszary przetwarzania danych jako:
   a. obiekty, wydzielone pomieszczenia lub części pomieszczeń, w których przetwarzane są dane (także w postaci tradycyjnej – papierowej),
   b. części obiektów, w których znajdują się informatyczne urządzenia wyjścia (np. monitory, drukarki itp.).
2. Pomieszczenie określone jako obszar przetwarzania danych powinno spełniać następujące warunki:
   1) być wyposażone w zamek mechaniczny lub elektroniczny zamykany każdorazowo, gdy opuszczają je pracownicy zatrudnieni przy przetwarzaniu danych,
   2) jeżeli pomieszczenie znajduje się na parterze, lub istnieje możliwość podglądu z zewnątrz, ekrany monitorów umieszcza się w sposób uniemożliwiający taki podgląd,

3) monitory komputerów, na których wykonuje się przetwarzanie danych powinny być ustawione w sposób uniemożliwiający ich podgląd osobom nieuprawnionym.

3. Wydzielona część pomieszczenia określona jako obszar przetwarzania danych powinna spełniać następujące warunki:
   1) wyposażenie (meble) w tej części pomieszczenia muszą być tak ustawione, aby uniemożliwić lub istotnie utrudnić dostęp do tego obszaru osobom nieuprawnionym,
   2) monitory komputerów, na których dokonuje się przetwarzania danych powinny być ustawione w sposób uniemożliwiający ich podgląd osobom nieuprawnionym.
4. Obszary przetwarzania danych w obiektach i pomieszczeniach Urzędu nie mogą być dostępne dla osób nieuprawnionych.
5. Dopuszczalne odstępstwo stanowią pomieszczenia, w których przyjmowani są interesanci. Jeżeli pomieszczenia te wyposażone są jednocześnie w urządzenia z dostępem do systemów bazodanowych albo tradycyjne kartoteki, należy w nich stosować szczególne środki ostrożności, w tym:
   1) interesanci powinni wchodzić pojedynczo i pozostawać w pomieszczeniu tylko w obecności użytkownika systemu,
   2) kartoteki tradycyjne należy zabezpieczyć przed dostępem osób nieuprawnionych,
   3) nie należy pozostawiać dokumentów papierowych i nośników elektronicznych w miejscach umożliwiających ich wykorzystanie, przez osoby nieuprawnione,
   4) drukarki i urządzenia peryferyjne powinny być usytuowane tak, aby znajdowały się z dala od przestrzeni, po której poruszają się osoby nieuprawnione,

Rozdział 1

OPIS ZDARZEŃ NARUSZAJĄCYCH OCHRONĘ DANYCH OSOBOWYCH

1. **Podział zagrożeń:**
   1) zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych.
   2) zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych.
   3) zagrożenia zamierzone, świadome i celowe - najpoważniejsze zagrożenia,

naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na: nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu), nieuprawniony dostęp do systemu z jego wnętrza, nieuprawniony przekaz danych, pogorszenie jakości sprzętu i oprogramowania, bezpośrednie zagrożenie materialnych składników systemu.

2. **Przypadki zakwalifikowane, jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe to głównie:**

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

uporczywym nieautoryzowanym logowaniu, itp.,

11) ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki", itp.,

12) podmieniono lub zniszczono nośniki z danymi osobowymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane osobowe,

13) rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.).

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

Rozdział 2

ZABEZPIECZENIE DANYCH OSOBOWYCH

1. Administratorem danych osobowych zawartych i przetwarzanych w systemach informatycznych Urzędu Miejskiego w Łobzie jest Burmistrz Łobza.
2. Administrator danych osobowych jest obowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w systemach informatycznych Urzędu, a w szczególności:
   1) zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym,
   2) zapobiegać przed zabraniem danych przez osobę nieuprawnioną,
   3) zapobiegać przetwarzaniu danych z naruszeniem ustawy oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych.
3. Do zastosowanych środków technicznych należy:
   1) przetwarzanie danych osobowych w wydzielonych pomieszczeniach położonych w strefie administracyjnej,
   2) zabezpieczenie wejścia do pomieszczeń, o których mowa w pkt. 1,
   3) szczególne zabezpieczenie centrum przetwarzania danych (komputer centralny, serwerownia) poprzez zastosowanie systemu kontroli dostępu,
   4) wyposażenie pomieszczeń w szafy dające gwarancję bezpieczeństwa

dokumentacji.

5) zabezpieczenie wejść do pomieszczeń odpowiednimi zamkami,
6) zainstalowanie odpowiednich do zagrożeń systemów: alarmowych, monitoringu, telewizji przemysłowej, przeciwpożarowych, itp.

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 zakresie bezpieczeństwa mają zastosowanie wszelkie wewnętrzne regulaminy lub instrukcje dotyczące bezpieczeństwa ludzi i zasobów informacyjnych.
6. Stały dostęp do pomieszczeń, w których przetwarzane są dane osobowe, mają tylko użytkownicy.
7. Dostęp do pomieszczeń, w których przetwarzane są dane osobowe, osób innych, niż wymienione w pkt. 6, jest możliwy wyłącznie w obecności co najmniej jednego użytkownika lub za zgodą Administratora Danych.
8. Klucze do pomieszczeń przechowywane są w wyznaczonym pomieszczeniu.
9. Klucze wydawane są wyłącznie osobom do tego uprawnionym.
10. Klucze zapasowe do pomieszczeń, przechowywane są w specjalnej szafie i mogą być wydawane w sytuacjach awaryjnych.
11. Kartoteki należy przechowywać w przeznaczonych do tego szafach, do których dostęp mają wyłącznie użytkownicy.
12. Użytkownicy, o których mowa w pkt. 11, odpowiedzialni są za rzetelne prowadzenie kartotek, ich kompletność oraz ochronę.
13. Przebywanie użytkownika po godzinach pracy w pomieszczeniach, w których przetwarzane są dane osobowe jest dopuszczalne jedynie za zgodą Administratora Danych.
14. W trakcie prac technicznych wykonywanych przez osoby trzecie w pomieszczeniach, przetwarzanie danych osobowych jest zabronione.
15. Wykaz pomieszczeń, w których przetwarzane są dane osobowe, zawiera załącznik nr 1 do niniejszego dokumentu.

W celu ochrony przed utratą danych w Urzędzie Miejskim w Łobzie stosowane są następujące zabezpieczenia:

Sposoby zabezpieczeń

1) ochrona serwerów przed zanikiem zasilania poprzez stosowanie zasilaczy zapasowych UPS,
2) ochrona przed utratą zgromadzonych danych przez robienie kopii zapasowych na taśmach LTO, dyskach zewnętrznych oraz serwerze NAS, z których w przypadku awarii odtwarzane są dane,
3) ochrona przed awarią podsystemu dyskowego przez używanie macierzy RAID, uszkodzenie jakiegokolwiek z dysków nie spowoduje utraty danych,
4) Zabezpieczenia przed nieautoryzowanym dostępem do baz danych Urzędu:
   a. aby uzyskać dostęp do zasobów sieci, należy zwrócić się do ABI z odpowiednim wnioskiem, w którym podane będą dane nowego użytkownika oraz zasoby, jakie ma on mieć udostępnione.
   b. 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.
5) Zabezpieczenia przed nieautoryzowanym dostępem do baz danych Urzędu poprzez internet:
   a. 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.
   b. Firewall zapisuje do logu fakt zaistnienia wyjątkowych zdarzeń i śledzi ruch pakietów przechodzących przez nią. Oprócz filtra pakietów (firewall) zastosowano również system wykrywający obecność wirusów w poczcie

elektronicznej.

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

16. Postanowienia końcowe.

1) zabezpieczenie przed nieuprawnionym dostępem do danych, prowadzone jest przez ABI zgodnie z przyjętymi procedurami nadawania uprawnień do systemu informatycznego,
2) w pomieszczeniach, w których znajdują się serwery zamontowane są czujniki dymu,
3) w pomieszczeniach, w których znajdują się serwery zamontowana jest klimatyzacja, która zapewnia właściwą temperaturę i wilgotność powietrza dla sprzętu komputerowego,
4) w pobliżu wejścia do pomieszczenia z serwerami i innym urządzeniami znajduje się gaśnica, która okresowo jest napełniana i kontrolowana przez specjalistę,
5) aby dana osoba była zarejestrowana w systemie informatycznym, jako użytkownik muszą być spełnione następujące warunki:
    1) musi wykazać się znajomością ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.),
    2) musi wykazać się znajomością niniejszej „Polityki bezpieczeństwa" i uzyskać upoważnienie imienne do przetwarzania danych osobowych **(załącznik nr 5** do niniejszego dokumentu),
    3) podpisać oświadczenie o zachowaniu w tajemnicy danych osobowych osób zatrudnionych przy przetwarzaniu danych osobowych **(załącznik nr 10** do niniejszego dokumentu)

Odpowiedzialność za ochronę danych zawartych na komputerach przenośnych i innych przenośnych urządzeniach umożliwiających gromadzenie danych, spoczywa wyłącznie na dysponentach tych urządzeń; minimalnym wymaganym zabezpieczeniem każdego komputera PC w Urzędzie, jak również komputera przenośnego jest ograniczenie dostępu do tego komputera hasłem (hasło na BIOS, Windows, wygaszasz ekranu).

1. Zabrania się:
   1) zapisywania indywidualnych haseł dostępu,
   2) dokonywania samowolnych napraw sprzętu informatycznego oraz modyfikowania oprogramowania,
   3) samodzielnego zakupu sprzętu komputerowego lub oprogramowania,
   4) autoryzacji w systemie jako inny użytkownik,
   5) samodzielnego wgrywania oprogramowania,
   6) w celach innych niż służbowe, wynoszenia dokumentacji, w tym na nośnikach elektronicznych zawierającej dane, poza obszar jednostki organizacyjnej,
   7) wykorzystywania Internetu do celów innych niż służbowe oraz przeglądania stron o tematyce pornograficznej, nielegalnych stron z kodami aktywacyjnymi do programów lub programami łamiącymi zabezpieczenia programów przed nielegalnym kopiowaniem,
   8) korzystania z czatów internetowych, ściągania plików muzycznych oraz filmów, korzystania z sieci P2P.
2. Odwiedzanie stron internetowych jest monitorowane przez komórkę informatyki w wydziale Organizacyjno – Administracyjnym Urzędu.
3. Identyfikator i hasło osoby, która utraciła uprawnienia do korzystania z systemu należy bezzwłocznie unieważnić.
4. Identyfikator osoby, która utraciła uprawnienia i została wyrejestrowana z systemu nie może być przydzielony innej osobie.
5. Dostęp do poszczególnych elementów systemów bazodanowych powinien być realizowany tylko w zakresie określonym nadanymi uprawnieniami, po wydaniu upoważnienia użytkownikowi.
6. Dane wyeksportowane z systemu do komputera mogą znajdować się na tym komputerze tylko przez niezbędny do ich wykorzystania czas.
7. Po wykorzystaniu danych, określonych w ust. 6, należy je niezwłocznie usunąć.
8. Danych, określonych w ust. 6, nie można udostępniać osobom nieuprawnionym.

Rozdział 3

Procedury związane z zarządzaniem systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Miejskim w Łobzie

W celu nadania uprawnień do przetwarzania danych osobowych i rejestracji tych uprawnień w systemie informatycznym ma zastosowanie Procedura nadawania/cofania uprawnień do przetwarzania danych osobowych. Osobą odpowiedzialną za rejestrację

osoby upoważnionej do przetwarzania danych osobowych w ewidencji osób upoważnionych (*art. 39 ust. 1 ustawy o ochronie danych osobowych*) jest ABI. Osobą odpowiedzialną za rejestrację uprawnień użytkownika w systemach informatycznych jest ASI.

1. Każdy użytkownik dopuszczony do przetwarzania danych osobowych powinien posiadać stosowne upoważnienie.
2. Każdy użytkownik powinien posiadać indywidualny identyfikator umożliwiający logowanie do tych aplikacji, z którymi może pracować.
3. Identyfikator umożliwia wykonywanie czynności zgodnie z zakresem powierzonych obowiązków, które wyznaczają poziom uprawnień.
4. Postanowienia ust. 2 nie dotyczą użytkowników, którzy przetwarzają dane osobowe wyłącznie w kartotekach.

I. Procedura nadawania/cofania uprawnień do przetwarzania danych osobowych

1. Przełożony użytkownika będącego pracownikiem Urzędu Miejskiego w Łobzie wnioskuje na piśmie do administratora danych o upoważnienie imienne do przetwarzania danych osobowych dla siebie i swoich pracowników, wniosek stanowi załącznik nr 3 do niniejszego dokumentu. Załącznikiem do wniosku jest dokument uprawnień jednostkowych zawierający dokładny opis uprawnień użytkownika (załączniku nr 4 do niniejszego dokumentu) oraz podpisane przez użytkownika oświadczenia o zachowaniu w tajemnicy danych osobowych osób zatrudnionych przy przetwarzaniu danych osobowych (załącznik nr 10 do niniejszego dokumentu). Wniosek wraz z dokumentem uprawnień jednostkowych, oraz podpisane przez użytkownika oświadczenie o zachowaniu w tajemnicy danych osobowych osób zatrudnionych przy przetwarzaniu danych osobowych składa się do ABI.
2. W przypadku użytkowników nie będących pracownikami Urzędu Miejskiego w Łobzie, wniosek przygotowuje Kierownik Wydziału nadzorującego pracę. Wniosek stanowi załącznik nr 3 do niniejszego dokumentu. Załącznikiem do wniosku jest oświadczenie o zachowaniu w tajemnicy danych osobowych osób zatrudnionych przy przetwarzaniu danych osobowych (załącznik nr 11 do niniejszego dokumentu). Upoważnienie wygasa samoistnie po upływie okresu, na który zostało przydzielone.
3. ABI bada poprawność przesłanego dokumentu oraz:

   1) w przypadku uwag, przekazuje dokument kierownikowi do uzupełnienia (np.: gdy użytkownik nie został zapoznany z przepisami o ochronie danych osobowych). Na dokumencie podaje przyczynę odmowy zatwierdzenia dokumentu. Powtarza czynności do czasu uzyskania akceptacji dokumentu przez ABI;

2) w przypadku braku uwag ABI przygotowuje upoważnienie do przetwarzania danych osobowych dla użytkownika systemu. Upoważnienie przygotowane jest na piśmie w trzech egzemplarzach (upoważnienia stanowią załączniki nr 5 i 6 niniejszego dokumentu).

4. Administrator podpisuje upoważnienie do przetwarzania danych osobowych i przekazuje do ABI.
5. ABI rejestruje użytkownika oraz okres, na który upoważnienie zostało nadane w ewidencji osób upoważnionych.
6. Egzemplarz upoważnienia ABI niezwłocznie przekazuje ASI w celu rejestracji uprawnień użytkownika w systemach informatycznych.
7. ASI niezwłocznie dokonuje rejestracji uprawnień użytkownika systemu informatycznego, zgodnie z przekazanym upoważnieniem.
8. ASI przekazuje upoważnienie do ABI.
9. ABI dokonuje sprawdzenia nadanych użytkownikowi uprawnień.
10. ABI przechowuje egzemplarz upoważnienia.
11. Upoważnienie oraz oświadczenie o zachowaniu w tajemnicy danych osobowych do obsługi systemów informatycznych w zakresie przetwarzania danych jest załącznikiem do akt personalnych pracownika.
12. Ustanie stosunku pracy jest równoważne z cofnięciem uprawnień do przetwarzania danych osobowych.
13. Osoby dopuszczone do przetwarzania danych osobowych zobowiązane są do zachowania tajemnicy w zakresie tych danych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje również po ustaniu zatrudnienia.
14. ABI i ASI są jednocześnie użytkownikami uprzywilejowanymi.

W celu zarządzania metodami oraz środkami uwierzytelniania mają zastosowanie:

Procedura uwierzytelniania użytkownika w systemie informatycznym oraz Procedura rejestrowania /wyrejestrowania użytkownika z systemu informatycznego.

II. Procedura uwierzytelniania użytkownika w systemie informatycznym

1. Niepowtarzalny identyfikator oraz pierwsze hasło jest przydzielone użytkownikowi przez ASI po nadaniu uprawnień do przetwarzania danych osobowych.
2. Bezpośredni dostęp do danych użytkownik uzyskuje po podaniu identyfikatora i właściwego hasła.

III. Procedura rejestrowania/wyrejestrowania użytkownika z systemu informatycznego

1. Użytkownicy systemu informatycznego są niezwłocznie rejestrowani lub wyrejestrowywani przez ASI, gdy uzyskują lub tracą prawo dostępu do systemu, zgodnie z procedurą nadawania/cofania uprawnień do przetwarzania danych osobowych.
2. Identyfikator po wyrejestrowaniu użytkownika zostaje zablokowany przez ASI.
3. Ustanie stosunku pracy powoduje wyrejestrowanie użytkownika przez ASI. O fakcie ustania stosunku pracy ASI jest niezwłocznie informowany przez przełożonego.
4. Identyfikator po wyrejestrowaniu użytkownika nie jest przydzielany innej osobie.

IV. Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

A. Metody i środki uwierzytelniania.

1. W systemie informatycznym stosuje się uwierzytelniania dwustopniowe; na poziomie:
   a) dostępu do sieci lokalnej,
   b) dostępu do aplikacji.
2. Do uwierzytelnienia użytkownika w systemie na obu poziomach stosuje się hasła.
3. Hasło dostępu do sieci lokalnej składa się, co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry i znaki specjalne.
4. Hasło na poziomie dostępu do aplikacji składa się z 8 znaków, zawiera małe i wielkie litery oraz cyfry i znaki specjalne.
5. Hasło nie może być powtórnie użyte.
6. Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów.
7. Hasło nie może być ujawnione nawet po utracie przez nie ważności.
8. Zmiana hasła do systemu następuje nie rzadziej, niż co 30 dni oraz niezwłocznie w przypadku podejrzenia, że hasło mogło zostać ujawnione.

B. Procedury zarządzania środkami uwierzytelniania

1. Dla każdej osoby upoważnionej instalowany jest odrębny identyfikator i hasło, tak, aby bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym mogła mieć tylko ta osoba, która poda właściwy identyfikator i hasło.
2. System wymusi na użytkowniku zmianę swojego hasła, co 30 dni.
3. System zostanie wyłączony po trzykrotnej próbie nieudanego logowania się.

W celu rozpoczęcia, zawieszenia i zakończenia pracy w systemie informatycznym mają zastosowanie następujące procedury:

V. Procedura rozpoczęcia pracy

1. Przed przystąpieniem do pracy z systemem informatycznym lub kartotekami, użytkownik obowiązany jest dokonać sprawdzenia stanu urządzeń komputerowych oraz dokonać oględzin swojego stanowiska pracy, ze zwróceniem szczególnej uwagi, czy nie zaszły okoliczności wskazujące na naruszenie poufności danych osobowych.
2. W przypadku stwierdzenia bądź podejrzenia, iż miało miejsce naruszenie systemu, użytkownik obowiązany jest postępować zgodnie z zasadami określonymi w Polityce bezpieczeństwa.
3. W celu rozpoczęcia pracy w systemie informatycznym użytkownik obowiązany jest do podania hasła dostępu do systemu.
4. Podczas pierwszego uwierzytelniania w systemie użytkownik ma obowiązek zmiany hasła.
5. Hasło składa się co najmniej z 8 znaków. Hasło zawiera wielkie i małe litery oraz cyfry lub znaki specjalne.
   1) Użytkownik ma obowiązek zmieniać hasło nie rzadziej niż co 30 dni kalendarzowych.
   2) Zabrania się wpisywania hasła lub jego zmiany w obecności innych osób.
   3) Hasło nie może być zapisywane lub przechowywane w miejscu dostępnym dla osób nieuprawnionych.
   4) W przypadku zagubienia hasła użytkownik musi skontaktować się z ASI w celu uzyskania nowego hasła.

VI. Procedura zawieszenia/odwieszenia pracy w systemie informatycznym

1. Przy każdorazowym opuszczeniu stanowiska komputerowego, dopilnować, aby na ekranie nie były wyświetlane dane osobowe.
2. W celu zawieszenia pracy w systemie informatycznym służącym do przetwarzania danych osobowych użytkownik zobowiązany jest do wyrejestrowania się z systemu.
3. Przed opuszczaniem miejsca pracy na dłuższy czas użytkownik obowiązany jest poczekać, aż zaktywizuje się wygaszacz ekranu, który jest chroniony hasłem.
4. W celu ponownego uwierzytelnienia w systemie użytkownik odblokowuje pulpit i rozpoczyna pracę w systemie informatycznym zgodnie z procedurą rozpoczęcia pracy w systemie informatycznym.
5. Zabrania się pozostawiania stanowiska komputerowego z uruchomionym systemem bez kontroli pracującego na nim użytkownika.

VII. Procedura zakończenia pracy w systemie informatycznym

1. W celu zakończenia pracy w systemie informatycznym użytkownik wyrejestrowuje się z programu służącego do obsługi danych osobowych.
2. Użytkownik zamyka system operacyjny i wyłącza komputer.

W celu zabezpieczenia danych i programów służących do przetwarzania danych osobowych ma zastosowanie poniższa procedura tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.

VIII. Procedura tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania:

1. Kopie zapasowe są tworzone codziennie przez ASI Urzędu Miejskiego w Łobzie po zakończeniu dnia pracy oraz automatycznie przez serwer NAS. Nośnikiem są taśma LTO oraz zewnętrzne dyski twarde. Kopie zapasowe dzienne są kopiami pełnymi.
2. Taśmy LTO z kopiami zapasowymi są przechowywane w pokoju nr 3 w pancernej metalowej szafie, zewnętrzne dyski twarde, przechowywane są w pokoju nr 4 w zamykanej szfie.
3. Kopie zapasowe są okresowo sprawdzane pod kątem ich dalszej przydatności.
4. Na koniec każdego miesiąca ABI tworzy kopię miesięczną .
5. Kopie miesięczne są przechowywane przez okres 5 lat.
6. Po okresie przechowywania kopie miesięczne podlegają komisyjnej likwidacji poprzez ich fizyczne zniszczenie. W komisji likwidacyjnej biorą udział ABI i ASI.

IX. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji oraz wydruków zawierających dane osobowe

A. Elektroniczne nośniki informacji

1. Dane osobowe w postaci elektronicznej przetwarzane w systemie informatycznym, zapisane na elektronicznych nośnikach danych, czy dyskach twardych nie mogą być wynoszone poza siedzibę Urzędu.
2. Po zakończeniu pracy przez użytkowników systemu elektroniczne nośniki informacji są przechowywane w zamykanych na klucz szafach biurowych lub szafach pancernych.
3. Dane osobowe w postaci elektronicznej, po ustaniu ich użyteczności należy usunąć z nośnika informacji w sposób uniemożliwiający ich ponowne odtworzenie.

4. W przypadku uszkodzenia lub zużycia nośnika elektronicznego zawierającego dane osobowe należy go fizycznie zniszczyć przez spalenie lub rozdrobnienie.
5. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
   1) likwidacji - pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
   2) przekazania podmiotowi nieuprawnionemu do przetwarzania danych - pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
   3) naprawy - pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

B. Kopie zapasowe

Kopie zapasowe zbioru danych osobowych są przechowywane w pokoju nr 3 w szafie pancernej.

C. Wydruki

1. Wszelkie wydruki zawierające dane osobowe przechowywane są w miejscu uniemożliwiającym ich odczyt przez osoby nieuprawnione, w zamkniętych szafach lub pomieszczeniach i po upływie czasu ich przydatności są niszczone przy użyciu niszczarek.
2. Wydruki, zawierające dane osobowe, należy zniszczyć przez pocięcie w niszczarce, po ich wykorzystaniu chyba, że z odrębnych przepisów wynika obowiązek ich przechowywania.
3. Wydruki zawierające dane sporządzane w oparciu o systemy Urzędu podlegają szczególnej ochronie, a w szczególności niedopuszczalne jest:

   1) pozostawianie wydruków zawierających dane, z możliwością dostępu do nich osób nieuprawnionych,
   2) wyrzucania nieudanych lub próbnych wydruków do kosza.

D. Dane wejściowe do systemu

Dane osobowe zapisane w formie papierowej inne niż wydruki z systemu (pisma, ankiety itp.) są przechowywane na podobnych zasadach, co wydruki.

X. Środki ochrony przed wirusami komputerowymi oraz oprogramowaniem, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

1. Nadzór nad instalowaniem nowego oprogramowania antywirusowego oraz nad bieżącą jego aktualizacją sprawuje ASI.
2. W celu zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego Urząd Miejskiego w Łobzie wykorzystuje:
    1) Oprogramowanie antywirusowe na serwerze.
    2) Oprogramowanie antywirusowe na stacjach roboczych.
3. Aktualizacja wyżej wymienionego oprogramowania jest automatyczna. Bazy wirusów są aktualizowane minimum raz dziennie.
4. Oprogramowanie zastosowane w systemach informatycznych automatycznie monitoruje występowanie wirusów w trakcie załączania lub wczytywania danych z zewnętrznych nośników informacji.
5. Kontrola antywirusowa jest przeprowadzana na wszystkich nośnikach magnetycznych i optycznych, służących zarówno do przetwarzania danych osobowych w systemie, jak i do celów instalacyjnych.
6. Użytkownik systemu importujący dane osobowe do systemu informatycznego z elektronicznego nośnika jest odpowiedzialny za sprawdzenie tych danych pod kątem możliwości występowania wirusów.
7. O każdorazowym wykryciu wirusa przez oprogramowanie antywirusowe użytkownik obowiązany jest niezwłocznie poinformować ASI.
8. Po usunięciu wirusa ASI sprawdza system informatyczny oraz przywraca go do pełnej funkcjonalności i sprawności.
9. Po dokonanej naprawie lub konserwacji należy przeprowadzić proces sprawdzenia pod kątem występowania wirusów.

XI. Ochrona przed nieautoryzowanym dostępem do sieci lokalnej

1. ASI jest odpowiedzialny za aktywowanie i poprawne konfigurowanie specjalistycznego oprogramowania monitorującego wymianę danych na styku:
    a) sieci lokalnej i sieci publicznej,
    b) stanowiska komputerowego użytkownika systemu i pozostałych urządzeń wchodzących w skład sieci lokalnej.

2. W celu zabezpieczenia systemu informatycznego przed nieautoryzowanym dostępem do sieci lokalnej, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego, Urząd Miejskiego w Łobzie wykorzystuje:

    1) Firewalla sprzętowego na styku sieci lokalnej i sieci publicznej, zaawansowane zabezpieczenie sieci przed niepowołanym dostępem; zawiera m.in. NAT (Network Address Translation),web filter, wykrywanie i zabezpieczenie przed atakami DoS (Denial of Service), alert przez e-mail, Anti-Virusa, Email filter, Applikation control, IPS (Intrusion Protection) system IPS wykrywa i blokuje intruzów przed uzyskaniem dostępu do chronionych zasobów.
    2) Oprogramowanie anty-virusowe, na stacjach roboczych.

3. Użytkownikowi systemu zabrania się dokonywania jakichkolwiek zmian konfiguracji w zainstalowanym oprogramowaniu monitorującym wymianę danych na styku tego stanowiska i sieci lokalnej.
4. Ochrona systemu informatycznego używanego w Urzędzie polega na:
    a) ochronie przez identyfikator,
    b) ochronie za pomocą hasła,
    c) przydzielaniu praw,
    d) ochronie katalogów,
    e) nadawaniu atrybutów.

XIII. Zasady i sposób odnotowywania w systemie informacji o udostępnieniu danych osobowych.

1. W systemie informatycznym odnotowywane są informacje o odbiorcach danych z tego systemu.
2. Odbiorcą danych jest każdy, komu udostępnia się dane osobowe, z wyłączeniem:
    a) osoby, której dane dotyczą,
    b) osoby użytkownika systemu lub innej osoby upoważnionej do przetwarzania danych osobowych w Urzędzie,
    c) przedstawiciela, o którym mowa w art. 31a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych,
    d) podmiotu, któremu powierzono przetwarzanie danych,
    e) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.
3. Odnotowanie obejmuje informacje o:

a) nazwie jednostki organizacyjnej lub imieniu i nazwisku osoby, której udostępniono dane,
b) zakresie udostępnianych danych,
c) dacie udostępnienia.

4. Odnotowanie informacji powinno nastąpić niezwłocznie po udostępnieniu danych.
5. Udostępnienie danych osobowych może nastąpić wyłącznie na pisemną prośbę odbiorcy danych.
6. Na żądanie osoby, której dane zostały udostępnione, informacje o udostępnieniu danych są zamieszczane w raporcie z systemu informatycznego, a raport przekazywany tej osobie.
7. Nadzór nad prawidłowością odnotowywania w systemie ww. informacji sprawuje ABI.

XIV. Procedury wykonywania przeglądów i konserwacji systemu

O przeprowadzanych przeglądach i konserwacjach systemu każdorazowo informowany jest ABI, który może nadzorować przebieg prac.

1. Systemy informatyczne oraz nośniki informacji służące do przetwarzania danych eksploatowane w Urzędzie Miejskim w Łobzie podlegają okresowym przeglądom i konserwacjom.
2. Do dokonywania przeglądów i konserwacji uprawniony jest ASI.
3. W przypadku stwierdzenia uszkodzenia urządzenia, dyski i inne informatyczne nośniki danych zawierające dane osobowe przed ich przekazaniem w celu naprawy innemu podmiotowi pozbawiane są zawartości.
4. W przypadku likwidacji urządzenia, dyski i inne informatyczne nośniki danych zawierające dane osobowe są uszkadzane w sposób uniemożliwiający odczytanie danych.
5. Naprawa wymienionych urządzeń zawierających dane osobowe, jeżeli nie można danych usunąć, wykonywana jest pod nadzorem ABI i/lub ASI.

A. Przeglądy i konserwacja urządzeń

1. Przeglądy i konserwacja urządzeń wchodzących w skład systemu informatycznego wykonywane są w terminach określonych przez producenta sprzętu.
2. Nieprawidłowości ujawnione w trakcie tych działań zostaną niezwłocznie usunięte, a ich przyczyny przeanalizowane i przekazane ABI.
3. Za terminowość przeprowadzenia przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada ASI.

B. Sprawdzanie poprawności działania programów i narzędzi programowych

1. Sprawdzanie poprawności działania programów i narzędzi programowych przeprowadza się w następujących przypadkach:
   a) zmiany wersji oprogramowania serwera plików;
   b) zmiany wersji oprogramowania stanowiska komputerowego użytkownika systemu;
   c) zmiany systemu operacyjnego serwera plików;
   d) zmiany systemu operacyjnego stanowiska komputerowego użytkownika systemu;
   e) wykonania zmian w projekcie systemu spowodowanych koniecznością naprawy, konserwacji lub modyfikacji systemu.
2. Przed dokonaniem zmian w systemie informatycznym należy dokonać przeglądu działania systemu w zmienionej konfiguracji w warunkach testowych na testowej bazie danych. Sprawdzenie powinno obejmować:
   a) poprawność logowania się do systemu w zależności od posiadanych uprawnień (zasymulować pracę wszystkich typów uprawnień użytkownika),
   b) poprawność działania wszystkich elementów aplikacji (menu, zestawienia, formularze, raporty).
3. Poprawność funkcjonowania systemu polega na symulacji działania wykonując następujące operacje:
   a) wprowadzania danych osobowych,
   b) edytowania danych osobowych,
   c) wyszukiwania danych osobowych,
   d) wydruku danych osobowych.
4. Przegląd zbiorów danych polega na:
   a) sprawdzeniu dostępu do zbiorów danych na poziomie użytkowników o różnych prawach dostępu,
   b) ocenie stanu zbiorów danych,
   c) sprawdzeniu ustawień dostępu dla poszczególnych użytkowników
5. W przypadku stwierdzenia nieprawidłowości w stanie zbiorów danych lub naruszenia praw dostępu, administrator systemu powiadamia o zaistniałym fakcie Administratora Bezpieczeństwa Informacji, a następnie podejmuje działania zmierzające do usunięcia nieprawidłowości i zidentyfikowania osoby, która doprowadziła do ich powstania.
6. Za prawidłowość przeprowadzenia przeglądów i konserwacji systemu odpowiada ASI.

C. Konserwacja oprogramowania

1. Konserwację oprogramowania przeprowadza się po zgłoszeniu przez użytkownika systemu potrzeby wprowadzenia zmian pozwalających utrzymać funkcjonalność systemu w dynamicznie zmieniającym się środowisku pracy.
2. Przed dokonaniem zmian w systemie informatycznym należy dokonać przeglądu działania systemu w zmienionej konfiguracji w warunkach testowych na testowej bazie danych na podobnych zasadach jak ma to miejsce w przypadku przeglądu oprogramowania.
3. Konserwację przeprowadza ASI.

Rozdział 4

KONTROLA PRZESTRZEGANIA ZASAD ZABEZPIECZENIA DANYCH OSOBOWYCH

1. Administrator danych lub osoba przez niego wyznaczona, którą jest ABI sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych wynikających z ustawy o ochronie danych osobowych oraz zasad ustanowionych w niniejszym dokumencie.
2. W przypadku nieobecności Administratora Bezpieczeństwa Informacji, osobę zastępującą wyznacza Administrator Danych.
3. Administrator Bezpieczeństwa Informacji lub osoba przez niego upoważniona dokonuje okresowych kontroli i oceny funkcjonowania mechanizmów zabezpieczeń oraz przestrzegania zasad postępowania w przypadku naruszenia ochrony danych osobowych.
4. Administrator Bezpieczeństwa dokonuje rocznych ocen stanu bezpieczeństwa danych osobowych.

Rozdział 5

POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Przed przystąpieniem do pracy użytkownik obowiązany jest dokonać sprawdzenia stanu urządzeń komputerowych oraz oględzin swojego stanowiska pracy, ze zwróceniem szczególnej uwagi, czy nie zaszły okoliczności wskazujące na naruszenie lub próby naruszenia ochrony danych osobowych.
2. 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.)
3. każda osoba zatrudniona przy przetwarzaniu danych osobowych jest obowiązana niezwłocznie powiadomić o tym fakcie ABI.
4. W razie niemożliwości zawiadomienia ABI, należy powiadomić bezpośredniego przełożonego.
5. Postanowienia ust. 3 i 4 mają zastosowanie zarówno w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych gromadzonych w systemie informatycznym, jak i w kartotekach.
6. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych ABI:
    1) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców,
    2) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
    3) zaniechać - o ile to możliwe - dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,
    4) podjąć inne działania przewidziane i określone w instrukcjach technicznych i technologicznych stosownie do objawów i komunikatów towarzyszących naruszeniu,

5) podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej,
6) zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku,
7) udokumentować wstępnie zaistniałe naruszenie,
8) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia ABI.
9) Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych, ABI:

7. zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy Urzędu,
8. może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
9. rozważa celowość i potrzebę powiadamia o zaistniałym naruszeniu Administratora danych,
10. nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba, ze specjalistami spoza Urzędu,
11. ABI dokumentuje zaistniały przypadek naruszenia oraz sporządza raport wg wzoru stanowiącego załącznik **nr 7**, 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 ust. 5, ABI niezwłocznie przekazuje Administratorowi Danych (Burmistrzowi), a w przypadku jego nieobecności osobie uprawnionej.
6. Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu ABI zasięga niezbędnych opinii i proponuje postępowanie naprawcze, a w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych.
7. Zaistniałe naruszenie może stać się przedmiotem szczegółowej, zespołowej analizy

prowadzonej przez Kierownictwo Urzędu, Administratora Bezpieczeństwa Informacji, Pełnomocnika ds. Ochrony Informacji Niejawnych.

8. Analiza, o której mowa w ust. 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 6

MONITOROWANIE ZABEZPIECZEŃ

1. Prawo do monitorowania systemu zabezpieczeń posiadają, zgodnie z zakresem czynności:
   a) Administrator Danych,
   b) Administrator Bezpieczeństwa Informacji.
2. W ramach kontroli należy zwracać szczególną uwagę na:
   a) okresowe sprawdzanie kopii bezpieczeństwa pod względem przydatności do możliwości odtwarzania danych,
   b) kontrolę ewidencji nośników magnetycznych,
   c) kontrolę właściwej częstotliwości zmiany haseł.

Rozdział 7

SZKOLENIA

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

Rozdział 8

Inne uregulowania związane z przetwarzaniem danych osobowych w Urzędzie Miejskim w Łobzie

Przetwarzanie danych osobowych w zbiorach doraźnych

1. Dostęp do danych osobowych powinien odbywać się poprzez aplikację edytora tekstu lub, gdy zachodzi potrzeba zapisania danych w innym formacie np. w postaci pliku arkusza kalkulacyjnego, można tego dokonać w doraźnym zbiorze danych osobowych pod warunkiem, że zapisane dane będą należycie chronione, tj.:
   a) uniemożliwi się dostęp do danych osobom nieuprawnionym,
   b) uniemożliwi się zmiany danych, a tym samym zafałszowanie informacji pochodzących z systemu,
   c) zabezpieczy się bezpośredni dostęp do danych hasłem;
2. Doraźny zbiór danych osobowych należy usunąć z nośnika danych, na którym został utworzony lub zniszczyć nośnik.
3. Zawiadamiać ABI w przypadku podejrzenia lub stwierdzenia dostępu do zbioru osób nieuprawnionych.
4. Przetwarzać dane w pokojach stanowiących obszar przetwarzania danych osobowych w systemie informatycznym Urzędu.

Ogólne zasady i odpowiedzialność przy instalacji oprogramowania

Na wszystkich komputerach w Urzędzie dopuszcza się instalację tylko legalnego, licencjonowanego oprogramowania.

I. Wprowadza się następujące zasady korzystania z oprogramowania:

1. Oryginalne dokumenty licencyjne oraz nośniki każdego oprogramowania przechowywane są w Wydziale Administracyjno – Organizacyjnym w zamkniętej szafie. Nośniki oprogramowania nie mogą znajdować się w żadnym innym miejscu, a szczególnie nie mogą być kopiowane, wypożyczane lub w żaden sposób przekazywane osobom trzecim. Dotyczy to również kodów aktywacyjnych produktów.
2. Zabrania się użytkownikom wykonywania kopii oprogramowania.

3. Wszyscy pracownicy zobowiązani są do pracy na legalnym oprogramowaniu oraz otrzymują wyraźny zakaz instalacji i użytkowania oprogramowania pochodzącego ze źródeł innych niż komórka Informatyki.
4. Konieczne zakupy oprogramowania powinny być konsultowane z ASI.
5. 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. Zabrania się korzystania z jakiegokolwiek oprogramowania, do którego Urząd nie jest uprawniony.

II. Instalowanie oprogramowania testowego i bezpłatnego dopuszcza się pod warunkiem:

1. Do instalacji i modyfikacji oprogramowania na stacjach roboczych uprawniony jest wyłącznie ASI.
2. Na stacjach roboczych może być instalowane tylko oprogramowanie, na które Urząd posiada licencję.
3. Oprogramowanie testowe może być instalowane wyłącznie na wydzielonych stacjach roboczych.
4. Przed dopuszczeniem do zainstalowania oprogramowania testowego lub bezpłatnego Administrator Bezpieczeństwa Informacji sprawdza i nadzoruje legalność procesu instalacji oprogramowania
5. W szczególnych przypadkach dopuszcza się instalowanie na stacji roboczej oprogramowania testowego, wyłącznie za pisemną zgodą ASI.
6. Oprogramowanie testowe, określone w ust. 5 odinstalowuje się bezzwłocznie po zakończeniu testowania.
7. użytkownik prowadzący, test oprogramowania, określonego w ust. 5, informuje ASI o stwierdzonych nieprawidłowościach.

Zasady wyposażania i eksploatacji stacji roboczych

1. Zasadność zakupu sprzętu komputerowego oraz oprogramowania podlega ocenie i akceptacji przez ASI.
2. ASI nadzoruje proces zakupu sprzętu komputerowego oraz oprogramowania.
3. Instalacja sprzętu komputerowego na stanowiskach pracy wykonywana jest przez ASI.
4. Przeniesienia sprzętu do innych pomieszczeń wykonywane będą przez ASI na wniosek Kierownika Wydziału. Zabrania się samodzielnego przenoszenia sprzętu przez innych pracowników.

Rozdział 10

POSTANOWIENIA KOŃCOWE

1. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie dyscyplinarne.
2. ABI zobowiązany jest prowadzić ewidencję osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych wg wzoru stanowiącego załącznik nr 8 do niniejszego dokumentu.
3. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, w szczególności przez osobę, która wobec naruszenia zabezpieczenia systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym ABI.
4. Orzeczona kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia administratora bezpieczeństwa informacji nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
5. W sprawach nie uregulowanych niniejszym dokumentem mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.), rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024) oraz rozporządzenie Ministra Sprawiedliwości z dnia 28 kwietnia 2004 r. w sprawie sposobu technicznego przygotowania systemów i sieci do przekazywania informacji – do gromadzenia wykazów połączeń telefonicznych i innych przekazów informacji oraz sposobów zabezpieczenia danych informatycznych (Dz. U. Nr 100, poz. 1023).

Załącznik nr 1 do „Polityki bezpieczeństwa"

1. Przetwarzanie danych osobowych z użyciem stacjonarnego sprzętu komputerowego i kartotek odbywa się wyłącznie w obszarze przetwarzania danych, w pomieszczeniach Administratora Danych.

2. Pomieszczenia określone w punkcie 1 niniejszego załącznika znajdują się przy ul. Niepodległości 13, 73 - 150 Łobez w budynku Urzędu Miejskiego w Łobzie.

3. W pomieszczeniach Administratora Danych przetwarzanie danych jest zabronione, jeśli nie są zapewnione warunki ochrony danych osobowych określone w niniejszej Polityce.

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

POKÓJ NR 1 – parter- OBSŁUGA programów "CEIDG - centralna ewidencja informacji o działalności gospodarczej"	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	**Imię i nazwisko:** **- Jan Cecholnyk**

POKÓJ NR 2 – parter- "Ewidencja skarg i wniosków", „oświadczenia o stanie majątkowym radnych"	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	**Imię i nazwisko:** **- Aneta Konstanta-Dajnowska** **- Alicja Tuligłowicz**

POKÓJ NR 3 – parter- OBSŁUGA programów "Płatnik", „Wf-Gang" – Kadry-płace,	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	**Imię i nazwisko:** **- Romualda Bajerowicz**

POKÓJ NR 4 – parter- Serwerownia OBSŁUGA wszystkich programów znajdujących się w Urzędzie.	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	**Imię i nazwisko:** **- Grzegorz Lew**

POKÓJ NR 5,– parter- OBSŁUGA programów iNet- Powiat Łobeski ewidencja gruntów, Rejestr zezwoleń na wycięcie drzew	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	**Imię i nazwisko:** **- Marian Koziotyński** **- Piotr Dynowski**

POKÓJ NR 6,7,8 – parter- OBSŁUGA programów „Opłaty za usuwanie odpadów', Odpady komunalne, iNet- Powiat Łobeski ewidencja gruntów, Rejestr wydanych decyzji o warunkach zabudowy i zagospodarowania tren"	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	**Imię i nazwisko:** **- Ewa Ciechański** **- Agnieszka Kielar** **- Kamila Bryczkowska** **- Małgorzata Muszyńska-Rudzka** **- Małgorzata Różańska**

POKÓJ NR 10 - 11 – parter - OBSŁUGA programów „Ewidencja Gruntów", "Dzierżawy, Wieczyste użytkowanie", „iNet- Powiat Łobeski ewidencja gruntów" Ewidencja miejscowości, ulic i adresów	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	**Imię i nazwisko:** **- Katarzyna Danylczak** **- Krystyna Rusak** **- Irena Libiszewska**

POKÓJ NR 9 – parter - OBSŁUGA programu „Czynsze" , dodatki mieszkaniowe, ewidencja właścicieli lokali mieszkalnych i użytkowych	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	**Imię i nazwisko:** **- Grażyna Wawżoła** **- Mariola Kawczak** **- Konrad Stelmaszyński**

POKÓJ NR 15 – parter - Rejestr zamówień publicznych	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	**Imię i nazwisko:** **- Arkadiusz Kogut**

POKÓJ NR 17 – parter - OBSŁUGA programów „Stypendia" Stypendia i zasiłki szkolne, Przewozy szkolne, "SIO", Alkohole (Zezwolenia na sprzedaż napojów alkoholowych),	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	**Imię i nazwisko:** **- Piotr Blumensztajn** **- Anna Wróbel**

POKÓJ NR 18 – parter - Akta osób podejrzanych o nadużywanie alkoholu	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	**Imię i nazwisko:** **- Piotr Blumensztajn**

POKÓJ NR 19 – parter - Osoby wykonujące nieodpłatnie kontrolowaną pracę na cele społeczne	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	**Imię i nazwisko:** **- Agnieszka Michna**

POKÓJ NR 24 – I piętro - OBSŁUGA programu „SIDAS" dziennik korespondencyjny, Ewidencja Interesantów	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	**Imię i nazwisko:** **- Magdalena Chmura**

POKÓJ NR 26 – I piętro - Oświadczenia majątkowe	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	**Imię i nazwisko:** **- Monika Jarzębska**

POKÓJ NR 30 – I piętro - OBSŁUGA programu „PB_USC" Komputerowy system rejestracji stanu cywilnego	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	**Imię i nazwisko:** **- Magdalena Kowalec** **- Joanna Kardaś**

POKÓJ NR 31 – I piętro - Ochotnicza straż pożarna, Zarządzanie kryzysowe	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	**Imię i nazwisko:** **- Zbigniew Gromek**

POKÓJ NR 34 – I piętro - OBSŁUGA programu „SWDO" System wymiany dowodów osobistych	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	**Imię i nazwisko:** **- Kamila Deuter** **- Joanna Kardaś** **- Magdalena Kowalec**

POKÓJ NR 35 – I piętro - OBSŁUGA programu „Ewidencja ludności" Komputerowa ewidencja ludności i rejestr wyborców, Obronność	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Imię i nazwisko: - Joanna Kardaś - Kamila Deuter - Magdalena Kowalec

POKÓJ NR 39 – I piętro - OBSŁUGA programów " Internet Banking"	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Imię i nazwisko: - Olga Radziwanowska

POKÓJ NR 39 – I piętro - OBSŁUGA programów „Wf-gang Kadry -Płace", „Płatnik", „E-Pfron", " Internet Banking"	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Imię i nazwisko: - Anna Post - Kamila Rokosz

POKÓJ NR 40 – I piętro - OBSŁUGA programów „FK", „Internet Banking",	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Imię i nazwisko: - Henryka Markowska - Ewa Skonieczka -Aleksandra Dembicka

POKÓJ NR 41 – I piętro - OBSŁUGA programu „Podatki", „Środki Transportu", "Dopłaty Paliwowe" ,iNet- Powiat Łobeski ewidencja gruntów „	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	Imię i nazwisko: - Małgorzata Mosiądz - Lucyna Frymus

POKÓJ NR 42 – I piętro - OBSŁUGA programów „Podatki”, "Dzierżawy, Wieczyste użytkowanie", "Opłaty za usuwanie odpadów", "Opłaty", "Kasa", "alkohole", „tytuły wykonawcze”, Opłata skarbowa.	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	**Imię i nazwisko:** **- Jolanta Jaremko** **- Elżbieta Skwara** **- Iwona Żyła**
POKÓJ NR 43 Kasa – I piętro - OBSŁUGA programów „Czynsze”, "Kasa"	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	**Imię i nazwisko:** **- Elżbieta Marcinów**

POKÓJ NR 52 – II piętro - Mandaty karne, Postępowanie mandatowe w sprawach o wykroczenie	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	**Imię i nazwisko:** **- Jerzy Ratajski** **- Leszek Bryczkowski**

Strych - ARCHIWUM ZAKŁADOWE	
Osoby edytujące dane, mające wgląd do danych osobowych i ich edycji	**Imię i nazwisko:** **- Aneta Konstanta-Dajnowska**

Osoby mające prawo wglądu do danych osobowych w kartotekach z uwagi na wykonywane zakresy czynności	
Administrator Danych	**Imię i nazwisko:** **- Ryszard Sola**
Zastępca Burmistrz	**Imię i nazwisko:** **- Ireneusz Kabat**
Sekretarz Gminy	**Imię i nazwisko:** **- Monika Jarzębska**
Skarbnik Gminy	**Imię i nazwisko:** **- Olga Radziwanowska**
Administrator Bezpieczeństwa Informacji	**Imię i nazwisko:** **- Grzegorz Lew**
Radca Prawny	**Imię i nazwisko:** **- Bogdan Skólmowski**
Kierownik Wydziału Spraw Obywatelskich	**Imię i nazwisko:** **- Zbigniew Gromek**
Kierownik Wydziału Infrastruktury Komunalnej i Ochrony Środowiska	**Imię i nazwisko:** **- Ewa Ciechańska**
Kierownik Wydziału Rolnictwa i Gospodarki Nieruchomościami	**Imię i nazwisko:** **- Mieczysław Fojna**
Kierownik Wydziału Inwestycji i Rozwoju Lokalnego	**Imię i nazwisko:** **- Witold Mazur**
Kierownik Wydziału Spraw Społecznych Promocji i Zdrowia	**Imię i nazwisko:** **- Mirosława Turbak**
Kierownik Biura Rady	**Imię i nazwisko:** **- Alicja Tuligłowicz**
Kierownik Wydziału Sportu Turystyki i Wypoczynku	**Imię i nazwisko:** **- Zdzisław Urbański**
Komendant Straży Miejskie	**Imię i nazwisko:** **- Jerzy Ratajski**

Uwaga!

1. Obsługa techniczna urzędu, (sprzątaczki, pracownicy gospodarczy podpisują oświadczenie , którego wzór stanowi załącznik nr 9 do „Polityki bezpieczeństwa".
2. Osoby odbywające staż, praktykę mają wgląd do danych osobowych oraz do systemu informatycznego na podstawie upoważnienia (**zał. nr 12**) nadanego przez Administratora oraz oświadczenia (**zał. nr 9**).

<u>Załącznik nr 2 do „ Polityki bezpieczeństwa"</u> - Opis struktur zbiorów danych oraz sposób przepływu danych pomiędzy poszczególnymi systemami.

Opis struktur zbiorów danych

Szczegółowy opis struktury zbiorów danych osobowych określonych w załączniku nr 15 wraz ze wskazaniem poszczególnych pól informacyjnych i powiązań między nimi znajduje się w dokumentacji technicznej znajdującej się w pokoju nr 4, Urzędu Miejskiego w Łobzie.

Programem wykorzystywanym do przetwarzania danych osobowych jest system SIDAS, to kompleksowy, wielomodułowy system wspomagający pracę jednostek administracji samorządowej w zakresie zarządzania dokumentacją, procesami i informacją, oprogramowanie i usługi, dostępne przez przeglądarkę internetową. Aplikacja oferuje szeroki zakres możliwości rejestrowania

a. daty wprowadzenia danych,
b. identyfikatora użytkownika,
c. źródła danych,

Zakres przetwarzanych danych osobowych uzależniony jest od informacji jakie zostaną zamieszczone w korespondencji przychodzącej do Urzędu Miejskiego w Łobzie.

Programem wykorzystywanym do przetwarzania danych osobowych w Urzędzie jest między innymi pakiet biurowy Office.

Dane osobowe przetwarzane są w aplikacjach:

a. Edytor tekstów,
b. Arkusz kalkulacyjny,
c. Program pocztowy.

Aplikacje pakietu Office oferują szeroki zakres możliwości rejestrowania:

a. daty wprowadzenia danych,
b. identyfikatora użytkownika,
c. źródła danych,

Aplikacją wykorzystywaną do przetwarzania danych jest m.in. program pocztowy. Program pocztowy pozwala na różne możliwości przepływu danych pomiędzy aplikacjami, od bezpośredniego udostępnienia danych bezpośrednio z modułu „Kontakty" poprzez dowolny eksport wybranych pól informacyjnych do plików w standardowych formatach pozwalających na import danych do dowolnych aplikacji obsługujących te formaty.
Zakres przetwarzanych danych osobowych uzależniony jest od informacji jakie zamieści nadawca wiadomości. Informacje te znajdują się zarówno w treści wiadomości, jak i w załącznikach do listu elektronicznego stanowiącego np. pliki: doc, rtf, pdf, jpg. itp. oraz informacje przesyłane automatycznie z listem, które mogą być rejestrowane w module „Kontakty".

Sposób przepływu danych pomiędzy poszczególnymi systemami informatycznymi w sieci lokalnej Urzędu Miejskiego w Łobzie

System Kadry i Płace „WF-gang" - Z systemu Wf-Gang istnieje możliwość wyeksportowania danych do pliku o formacie ustalonym przez twórców programu PŁATNIK. Plik ten jest importowany przez system PŁATNIK, który służy do rozliczeń pracowników z ZUS. Transmisja danych do ZUS odbywa się przez teletransmisję, drogą jaką określił ZUS. Z systemu Wf-Gang istnieje możliwość wyeksportowania danych do pliku o formacie określonym przez bank. Plik ten jest importowany do systemu Internet- banking w celu automatycznego przygotowania przelewów płacowych dla pracowników urzędu. Z systemu Wf- gang istnieje również możliwość złożenia poprzez moduł e-deklaracje elektronicznej deklaracji Pit w formacie pliku XML podpisanego bezpiecznym podpisem kwalifikowanym do Urzędów skarbowych odpowiednich dla pracowników.

System Districtus - Opłaty za usuwanie odpadów' - istnieje możliwość przepływu danych osobowych z systemu Ewidencja ludności - Districtus. Jest możliwość tylko odczytu tych danych, czyli ruch jest jednokierunkowy. Istnieje mechanizm sprawdzający przy wybraniu konkretnej osoby czy dane osobowe nie uległy zmianie. System w przypadku zauważenia zmian zadaje pytanie czy zaktualizować dane. Wybór należy do użytkownika systemu z uprawnieniami do zapisu w danym systemie. Istnieje również możliwość przepływu danych pomiędzy system Kasa – Districtus, jest to ruch dwukierunkowy (do odczytu i do zapisu)dotyczący naliczeń i wpłat należności konkretnego płatnika.

System Podatki- Districtus- istnieje możliwość przepływu danych osobowych z systemu Ewidencja ludności - Districtus. Jest możliwość tylko odczytu tych danych, czyli ruch jest jednokierunkowy. Istnieje mechanizm sprawdzający przy wybraniu konkretnej osoby czy dane osobowe nie uległy zmianie. System w przypadku zauważenia zmian zadaje pytanie czy zaktualizować dane. Wybór należy do użytkownika systemu z uprawnieniami do zapisu w danym systemie. Istnieje mechanizm importu danych z powiatowej ewidencji gruntów i budynków w formacie SWDE – chodzi tutaj o dane nieruchomości należących do podatnika. Dane te są zapisywane na kontach podatników. . Istnieje również możliwość przepływu danych pomiędzy system Kasa – Districtus, jest to ruch dwukierunkowy (do odczytu i do zapisu)dotyczący naliczeń i wpłat należności konkretnego płatnika.

System Środki Transportu - Districtus- istnieje możliwość przepływu danych

osobowych z systemu Ewidencja ludności - Districtus. Jest możliwość tylko odczytu tych danych, czyli ruch jest jednokierunkowy. Istnieje mechanizm sprawdzający przy wybraniu konkretnej osoby czy dane osobowe nie uległy zmianie. System w przypadku zauważenia zmian zadaje pytanie czy zaktualizować dane. Wybór należy do użytkownika systemu z uprawnieniami do zapisu w danym systemie.

System Dopłaty paliwowe dla rolników – Districtus - istnieje możliwość przepływu danych osobowych z systemu Ewidencja ludności - Districtus. Jest możliwość tylko odczytu tych danych, czyli ruch jest jednokierunkowy. Istnieje mechanizm sprawdzający przy wybraniu konkretnej osoby czy dane osobowe nie uległy zmianie. System w przypadku zauważenia zmian zadaje pytanie czy zaktualizować dane. Wybór należy do użytkownika systemu z uprawnieniami do zapisu w danym systemie. Istnieje również możliwość przepływu danych pomiędzy system Kasa – Districtus, jest to ruch dwukierunkowy (do odczytu i do zapisu) dotyczący wypłat należności konkretnego płatnika. Z systemu Dopłaty paliwowe dla rolników istnieje możliwość wyeksportowania danych do pliku o formacie określonym przez bank. Plik ten jest importowany do systemu Internet- banking w celu automatycznego przygotowania przelewów dopłat dla rolników.

System Dzierżawy i wieczyste – Districtus - istnieje możliwość przepływu danych osobowych z systemu Ewidencja ludności - Districtus. Jest możliwość tylko odczytu tych danych, czyli ruch jest jednokierunkowy. Istnieje mechanizm sprawdzający przy wybraniu konkretnej osoby czy dane osobowe nie uległy zmianie. System w przypadku zauważenia zmian zadaje pytanie czy zaktualizować dane. Wybór należy do użytkownika systemu z uprawnieniami do zapisu w danym systemie. Istnieje również możliwość przepływu danych pomiędzy system Kasa – Districtus, jest to ruch dwukierunkowy (do odczytu i do zapisu) dotyczący naliczeń i wpłat należności konkretnego płatnika.

System Kasa - Districtus- istnieje możliwość przepływu danych osobowych z systemu Ewidencja ludności - Districtus. Jest możliwość tylko odczytu tych danych, czyli ruch jest jednokierunkowy. Istnieje mechanizm sprawdzający przy wybraniu konkretnej osoby czy dane osobowe nie uległy zmianie. System w przypadku zauważenia zmian zadaje pytanie czy zaktualizować dane. Wybór należy do użytkownika systemu z uprawnieniami do zapisu w danym systemie. W systemie Kasa – Districtus, istnieje również możliwość przepływu danych, ruch dwukierunkowy (do odczytu i do zapisu) pomiędzy systemami dziedzinowymi.

System Ewidencja Ludności – Districtus istnieje możliwość wyeksportowania danych do pliku o formacie ustalonym przez MSW , zmian w ewidencji ludności do TBD oraz CBD , istnieje możliwość wydania całej bazy ewidencji ludności.
Program Ewidencja Ludności wraz z danymi jest tzw. Lokalnym Bankiem Danych (LBD) i stanowi najniższe ogniwo w hierarchii systemów informatycznych PESEL (Powszechny Elektroniczny System Ewidencji Ludności). W związku z tym warunkiem jego prawidłowej pracy jest ciągła wymiana informacji z systemami nadrzędnymi, a mianowicie: Terenowym Bankiem Danych (TBD), Centralnym Bankiem Danych (CBD) zlokalizowanym w Rządowym Centrum Informatycznym (RCI) w Warszawie. Użytkownik systemu Ewidencja Ludności jest zobowiązany do okresowego (najczęściej raz w tygodniu) przesyłania zmian w LBD do nadrzędnego banku danych (TBD lub CBD).
Program umożliwia pełną, automatyczną wymianę danych z systemami nadrzędnymi, począwszy od kontroli poprawności wysyłanych danych poprzez eksport, kopiowanie na dyskietki, wczytanie odpowiedzi i jej analizę, na wydruku błędów skończywszy.

Przepływ danych pomiędzy system elektronicznego zarządzania dokumentacja SIDAS, a pozostałymi systemami.

Przepływ danych między systemem Sidas a pozostałymi systemami elektronicznymi nie odbywa się. Obieg dokumentów odbywa się za pomocą nośników papierowych odbieranych przez merytorycznych pracowników w sekretariacie urzędu. Dokumenty skanowane są w sekretariacie i wprowadzane do systemu Sidas oraz dekretowane. Każdy pracownik merytoryczny pracuje na systemie Sidas tylko w zakresie powierzonych mu spraw, które to otrzymuje po dekretacji zgodnie z założonym kontem w systemie Sidas. Pracownik merytoryczny pracujący na systemie Sidas nie ma wglądu w sprawy pozostałych pracowników. Sekretariat z racji wykonywanych zdań mogą poprzez wyszukiwarkę uzyskać informację o składanych wnioskach i wysyłanej korespondencji gminnej.

Przepływ danych pomiędzy systemami, które nie zostały wymienione

Przepływ danych pomiędzy pozostałymi systemami nie odbywa się, lub nie występuje w wersji elektronicznej. Przepływ danych jeżeli występuje to tylko na nośnikach papierowych.

Załącznik nr 3 do „Polityki bezpieczeństwa"

Łobez, dnia .....

W N I O S E K

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 r. 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** .....

.....

data, podpis wnioskującego

Załącznik nr 4 do „Polityki bezpieczeństwa"

DOKUMENT UPRAWNIEŃ JEDNOSTKOWYCH

IMIĘ I NAZWISKO.....

Lp	Nazwa bazy danych	Rodzaj uprawnień(1)	Uwagi

(1)Skróty stosowane do określenia uprawnień
Z – pełne prawa do zarządzania bazą danych
W – pełne prawa do edycji danych (w tym drukowania, archiwizowania, usuwania)
N – prawo do zakładania nowych kont
M – prawo do dodawania i modyfikacji danych
P – prawo do przeglądania danych na ekranie
D – prawo do drukowania danych
A – prawo do wykonywania kopii archiwalnych
Uwaga: w przypadku praw ograniczonych do określonej części bazy danych należy ograniczenie to podać w polu Uwagi

.....

Kierownik komórki organizacyjnej

Załącznik nr 5 do „Polityki bezpieczeństwa"

Łobez, dnia .....

UPOWAŻNIENIE IMIENNE NR...../.....

DO PRZETWARZANIA DANYCH OSOBOWYCH

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

upoważniam Panią/Pana .....

pracownika Wydziału.....Urzędu Miejskiego w Łobzie do wykonywania czynności związanych z przetwarzaniem danych osobowych w zakresie:.

.....

.....

.....

.....

.....

i nadaję identyfikator:

.....

ze szczególnym uwzględnieniem zadań zawartych w rozporządzeniu 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)

Wyżej wymieniona osoba została przeszkolona i zrozumiała treści ochrony danych osobowych i dopuszczona jest do ich przetwarzania jedynie w zakresie określonym w Ustawie z dnia 29.08.1997r, o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) i wydanych do niej przepisach wykonawczych

Upoważnienie niniejsze nie upoważnia do udzielania dalszych upoważnień jest ważne w terminie od ..... do ....., wygasa z dniem ustania stosunku pracy, a ponadto może być w każdym czasie zmienione lub odwołane.

Wymieniona osoba została wpisana do ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych Urzędu Miejskiego w Łobzie

Z dniem podpisania niniejszego upoważnienia traci moc upoważnienie udzielone Pani/Panu Nr ...../.....

.....

Administrator Danych Osobowych

Załącznik nr 6 do „Polityki bezpieczeństwa"

Łobez, dnia .....

UPOWAŻNIENIE IMIENNE NR...../.....

DO PRZETWARZANIA DANYCH OSOBOWYCH

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

upoważniam Panią/Pana.....

pracownika .....

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

.....

.....

.....

.....

.....

ze szczególnym uwzględnieniem zadań zawartych w rozporządzeniu 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)

Upoważnienie nie upoważnia do udzielania dalszych upoważnień i jest ważne w terminie od ..... do .....

.....

Administrator Danych Osobowych

Załącznik nr 7 do „Polityki bezpieczeństwa"

R a p o r t
z naruszenia bezpieczeństwa systemu informatycznego w Urzędzie Miejskim w Łobzie

1. Data: ..... Godzina:.....
(dd.mm.rrrr) *(00:00)*

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

.....
(Imię, nazwisko, stanowisko służbowe, nazwa użytkownika (jeśli występuje))

3. Lokalizacja zdarzenia:

.....
(np. nr pokoju, nazwa pomieszczenia)

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

.....

.....

5. Podjęte działania:

.....
.....

6. Przyczyny wystąpienia zdarzenia:

.....
.....

7. Postępowanie wyjaśniające:

.....
.....

.....
data, podpis Administratora
Bezpieczeństwa Informacji

Załącznik nr 8 do „Polityki bezpieczeństwa"

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

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

Nazwisko i Imię	Komórka organizacyjna	Data, podpis

Załącznik nr 9 do „Polityki bezpieczeństwa"

.....
/imię i nazwisko pracownika/

.....

.....
/adres zamieszkania/

OŚWIADCZENIE

1. Stwierdzam własnoręcznym podpisem, że znana jest mi treść przepisów :
   a) o ochronie tajemnic prawnie chronionych stanowiących tajemnicę służbową wynikającą z Kodeksu Pracy,
   b) o ochronie danych osobowych wynikająca z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.)
   c) o odpowiedzialności karnej za naruszenie ochrony danych osobowych.

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

.....
... (podpis pracownika)

Załącznik nr 10 do „Polityki bezpieczeństwa"

OŚWIADCZENIE nr ...../.....

Ja niżej podpisany(a) zobowiązuję się do zachowania w tajemnicy danych osobowych, do których mam/ będę miał(a) dostęp w związku z wykonywaniem przeze mnie zadań służbowych i obowiązków pracowniczych w Urzędzie Miejskim w Łobzie, **zarówno w trakcie obecnie wiążącego mnie stosunku pracy, jak i po ustaniu zatrudnienia.**

Zobowiązuję się przestrzegać regulaminów, instrukcji i procedur obowiązujących w Urzędzie Miejskim w Łobzie, wiążących się z ochroną danych osobowych, a w szczególności nie będę bez upoważnienia służbowego wykorzystywał (a) danych osobowych ze zbiorów Urzędu Miejskiego w Łobzie.

Stwierdzam, że jest mi znana definicja danych osobowych w rozumieniu art. 6 Ustawy z dnia 29.08.1997r, o ochronie danych osobowych (tekst jednolity Dz. U z roku 2002 nr 101, poz. 926 z późn. zm.) oraz zostałem (am) zaznajomiony (a) z przepisami o ochronie danych osobowych.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane za naruszenie obowiązków pracowniczych w rozumieniu Kodeksu Pracy.

.....

data i podpis

Załącznik nr 11 do „Polityki bezpieczeństwa"

OŚWIADCZENIE ...../.....

Ja niżej podpisany(a) zobowiązuję się do zachowania w tajemnicy danych osobowych, do których mam/ będę miał(a) dostęp w związku z wykonywaniem umowy zawartej z Urzędem Miejskim w Łobzie, zarówno w trakcie trwania umowy jak i po jej "wygaśnięciu lub rozwiązaniu".

Zobowiązuję się do ścisłego przestrzegania warunków ww. umowy, które wiążą się z ochroną danych osobowych, a w szczególności nie będę bez upoważnienia służbowego wykorzystywał (a) danych osobowych ze zbiorów w Urzędu Miejskiego w Łobzie w celach nie związanych z wykonywaniem tej umowy.

Stwierdzam, że jest mi znana definicja danych osobowych w rozumieniu art. 6 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) oraz zostałem (am) zaznajomiony (a) z przepisami o ochronie danych osobowych.

Przyjmuję do wiążącej wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami oznacza naruszenie warunków umowy zawartej z Urzędem Miejskim w Łobzie.

.....

data i podpis

Załącznik nr 12 do „Polityki bezpieczeństwa"

.....
/miejscowość, data/

U P O W A Ż N I E N I E Nr.....

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

U p o w a ż n i a m

.....
/imię i nazwisko/

zatrudnionego na stanowisku .....

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

w.....
/nazwa jednostki organizacyjnej/

Upoważnienie jest ważne w terminie od ..... do .....

.....
Administrator Danych

Załącznik nr 13 do „Polityki bezpieczeństwa"

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH W SYSTEMACH INFORMATYCZNYCH URZĘDU MIEJSKIEGO W ŁOBZIE						
Lp.	**Imię i nazwisko**	**Numer upoważnienia**	**Nazwa zbioru**	**Login/ identyfikator**	**Okres dostępu**	**Zakres upoważnienia**
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						
10.						

Zakres upoważnienia:
Z – pełne prawa do zarządzania bazą danych
W – pełne prawa do edycji danych (w tym drukowania, archiwizowania, usuwania)
N – prawo do zakładania nowych kont
M – prawo do dodawania i modyfikacji danych
P – prawo do przeglądania danych na ekranie
D – prawo do drukowania danych
A – prawo do wykonywania kopii archiwalnych

Załącznik nr 14 do „Polityki bezpieczeństwa"

EWIDENCJA OŚWIADCZEŃ O ZACHOWANIU W TAJEMNICY DANYCH OSOBOWYCH OSÓB ZATRUDNIONYCH PRZY PRZETWARZANIU DANYCH OSOBOWYCH				
Lp.	**Imię i nazwisko**	**Numer oświadczenia**	**Data podpisania oświadczenia**	**Podpis ABI**
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				

Załącznik nr 15 do „Polityki bezpieczeństwa"

WYKAZ ZBIORÓW DANYCH OSOBOWYCH WRAZ ZE WSKAZANIEM PROGRAMÓW ZASTOSOWANYCH DO ICH PRZETWARZANIA

w Urzędzie Miejskim w Łobzie

Lp.	*Zbiór danych*	*Programy zastosowane do przetwarzania*	*Lokalizacja zbioru*	*Miejsce przetwarzania danych*
1	Ewidencja Działalności Gospodarczej	CEIDG - centralna ewidencja informacji o działalności	parter - pok. 1	parter - pok. 1,
2	Ewidencja skarg i wniosków	rejestr papierowy	parter - pok. 2	parter - pok. 2,
3	oświadczenia o stanie majątkowym radnych	rejestr papierowy	parter - pok. 2	parter - pok. 2,
4	Obsługa dokumentów ubezpieczeniowych i wymiany informacji z ZUS	Płatnik	parter - pok. 4	parter - pok. 3 I piętro - pok.39 I piętro - pok.26
5	Kadry - płace	Wf-Gang	parter - pok. 4	parter - pok. 3 I piętro - pok.39
6	Powiat Łobeski ewidencja gruntów	iNet	STAROSTWO POWIATOWE Wydział Geodezji i Kartografii, ul. Głowackiego 4 73-	parter - pok. 5,6,7,8,10,11 I piętro - pok.41
7	Rejestr wydanych decyzji o warunkach zabudowy i zagospodarowania tren	rejestr papierowy	parter - pok. 8	parter - pok. 8
8	Rejestr zezwoleń na wycięcie drzew	rejestr papierowy	parter - pok. 5	parter - pok. 5

9	Opłaty za usuwanie odpadów'	Districtus - Opłaty za usuwanie odpadów'	parter - pok. 4	parter - pok. 6,7,8 I piętro - pok.42
10	Dzierżawy	Sigid -Dzierżawy	parter - pok. 4	parter - pok. 10,11 I piętro -pok. 42
11	Wieczyste użytkowanie	Sigid - Wieczyste użytkowanie	parter - pok. 4	parter - pok. 10,11 I piętro -pok. 42
12	Gospodarka terenami	GEO – ewidencja gruntów	parter - pok. 4	parter - pok. 10,11 I piętro -pok. 42
13	Dodatki mieszkaniowe	Czynsze –VS-system	parter - pok. 4	parter - pok. 9 I piętro -pok. 43
14	Ewidencja właścicieli lokali mieszkalnych i użytkowych	Czynsze –VS-system	parter - pok. 4	parter - pok.9 I piętro -pok. 43
15	Rejestr zamówień publicznych	rejestr papierowy	parter - pok.15	parter - pok.15
16	Stypendia i zasiłki szkolne	Stypendia - Tensoft	parter - pok.17	parter - pok.17
17	System informacji oświatowej	SIO	parter - pok.17	parter - pok.17
18	Zezwolenia na sprzedaż napojów alkoholowych	Alkohole - Districtus	parter - pok. 4	parter - pok.17 I piętro -pok. 42, 43
19	Akta osób podejrzanych o nadużywanie alkoholu	rejestr papierowy	parter - pok.18	parter - pok.18
20	Osoby wykonujące nieodpłatnie kontrolowaną pracę na cele społeczne	rejestr papierowy	parter - pok.19	parter - pok.19
21	Dziennik korespondencyjny	SIDAS - EZD	parter - pok. 4	I piętro –pok. 24
22	Ewidencja Interesantów	SIDAS - EZD	parter - pok. 4	I piętro –pok. 24
23	Elektroniczne zarządzanie dokumentacją	SIDAS - EZD	parter - pok. 4	Budynek Urzędu
24	Oświadczenia majątkowe	rejestr papierowy	I piętro –pok. 26	I piętro –pok. 26

25	Komputerowy system rejestracji stanu cywilnego	PB_USC-Technika	I piętro –pok. 30	I piętro –pok. 30
26	Ochotnicza straż pożarna	rejestr papierowy	I piętro –pok. 32	I piętro –pok. 32
27	Zarządzanie kryzysowe	rejestr papierowy	I piętro –pok. 32	I piętro –pok. 32
28	System wymiany dowodów osobistych	SWDO	I piętro –pok. 34	I piętro –pok. 34
29	Komputerowa ewidencja ludności i rejestr wyborców	Ewidencja ludności - Districtus	parter - pok. 4	I piętro –pok. 34,35
30	Obronność	Ewidencja ludności - Districtus	parter - pok. 4	I piętro –pok. 34,35
31	Elektroniczne przelewy	Internet Banking	Bank Spółdzielczy w Goleniowie ul. Konstytucji 3-go Maja 20 72-100 Goleniów	I piętro –pok. 23,25,26,38,39,40
32	Państwowy Fundusz Rehabilitacji Osób Niepełnosprawnych	E-Pfron	Państwowy Fundusz Rehabilitacji Osób Niepełnosprawnych Al. Jana Pawła II 13, 00-828 Warszawa	I piętro –pok. 39
33	System finansowo-księgowy	FK- Districtus	parter - pok. 4	I piętro –pok. 38,40
34	Podatki	Podatki- Districtus	parter - pok. 4	I piętro –pok. 41,42
35	Środki Transportu	Środki Transportu - Districtus	parter - pok. 4	I piętro –pok. 41,42
36	Dopłaty paliwowe dla rolników	Dopłaty paliwowe dla rolników - Districtus	parter - pok. 4	I piętro –pok. 41
37	Dzierżawy i wieczyste użytkowanie oraz inne opłaty	Dzierżawy i wieczyste - Districtus	parter - pok. 4	parter - pok. 10, 11 I piętro –pok. 42
38	Kasa	Kasa - Districtus	parter - pok. 4	I piętro –pok. 42,43
39	Tytuły wykonawcze	rejestr papierowy	I piętro –pok. 42	I piętro –pok. 42
40	Opłata skarbowa	Dzierżawy i wieczyste - Districtus	parter - pok. 4	I piętro –pok. 42
41	Postępowanie mandatowe w sprawach	rejestr papierowy	II piętro –pok. 52	II piętro –pok. 52

	o wykroczenie			
42	Archiwum zakładowe	rejestr papierowy	strych	strych