# POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH
# W
# ADMINISTRACJI MIESZKAŃ KOMUNALNYCH
# W LUBANIU

**SPIS TREŚCI**



*Podstawa prawna:*

1. *Rozporządzenie 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. z 2004 r. Nr 100, poz. 1024)*
2. *Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 i Nr 153, poz. 1271 oraz z 2004 r. Nr 25, poz. 219 i Nr 33, poz. 285).*

## ROZDZIAŁ I
## Postanowienia ogólne

**§ 1. 1**. Polityka bezpieczeństwa przetwarzania danych osobowych w Administracji Mieszkań Komunalnych w Lubaniu zwana dalej „Polityką bezpieczeństwa", określa podstawowe zasady dotyczące zapewnienia bezpieczeństwa w zakresie danych osobowych przetwarzanych w zbiorach danych:

1) tradycyjnych, w szczególności kartotekach, księgach, skorowidzach, aktach osobowych, wykazach, w zbiorach ewidencyjnych;
2) w systemach informatycznych, w szczególności deklaracje ZUS, ewidencje płacowe, informacje skarbowe, ewidencje statystyczne, plany organizacyjne.

2. Ilekroć w Polityce Bezpieczeństwa jest mowa o:
   1) *ustawie* – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych z dnia 29 sierpnia 1997r. (tekst jedn. Dz. U. z 2002 r. Nr 101, poz. 926 z poźn. zm.);
   2) *administrator bezpieczeństwa informatycznego (ABI)* – rozumie się pracownika odpowiedzialnego w Administracji Mieszkań Komunalnych w Lubaniu,
   3) *lokalny administrator danych osobowych* – rozumie się kierownika administracji
   4) *administrator sieci* – rozumie się osobę odpowiedzialną za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych, służących do przetwarzania danych osobowych;
   5) *nośniki danych osobowych* – dyskietki, płyty CD lub DVD, pamięć flash, dyski twarde, taśmy magnetyczne lub inne urządzenia/ materiały służące do przechowywania plików z danymi;
   6) *osoba upoważniona (użytkownik)* – osoba posiadająca upoważnienie wydane przez administratora danych osobowych ;
   7) *Pełnomocnik kierownika ds. Ochrony Danych Osobowych* – osoba powołana przez kierownika której zadaniem jest nadzorowanie i koordynowanie w jednostce zasad postępowania przy przetwarzaniu danych osobowych
   8) *dane osobowe* - w rozumieniu ustawy za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
   9) *przetwarzanie danych* - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;
   10) *zbiór danych* - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów;
   11) *system informatyczny* - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
   12) *identyfikator użytkownika (login*) - ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
   13) *hasło* - ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
   14) *uwierzytelnianie* — rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
   15) *poufności danych* — rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom.

**§ 2**. **1.** Kierownik Administracji Mieszkań Komunalnych w Lubaniu realizując politykę bezpieczeństwa dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia , aby dane te były: :

1) przetwarzane zgodnie z prawem;
2) zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane przetwarzaniu niezgodnemu z tymi celami;
3) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane;

4) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą..

**2**. Kierownik Administracji Mieszkań Komunalnych dąży do systematycznego unowocześniania stosowanych na terenie jednostki informatycznych, technicznych i organizacyjnych środków ochrony tych danych w celu zabezpieczenia danych osobowych przed ich udostępnianiem osobom nieupoważnionym, przetwarzaniem z naruszeniem przepisów o ochronie danych osobowych, nieautoryzowaną zmianą , uszkodzeniem lub zniszczeniem.

## ROZDZIAŁ II
## Wykaz zbiorów danych osobowych

**§ 3. 1 .** Dane osobowe gromadzone są w zbiorach:

1) Zbiór 1 – Ewidencja osób zatrudnionych przy przetwarzaniu danych osobowych;
2) Zbiór 2 – Kontrola wewnętrzna- wyniki, opracowania, protokóły, notatki,;
3) Zbiór 3 – Akta osobowe pracowników;
4) Zbiór 4 – Dokumentacja dotycząca polityki kadrowej –opiniowanie awansów, wyróżnień, odznaczeń, nagród, wnioski o odznaczenia, itp;
5) Zbiór 5 – Notatki służbowe oraz postępowanie dyscyplinarne;
6) Zbiór 6 – Zbiory informacji o pracownikach, oświadczenia na potrzeby ZFŚS;
7) Zbiór 7 – Ewidencja zwolnień lekarskich;
8) Zbiór 8 – Skierowania na badania okresowe, specjalistyczne;
9) Zbiór 9 – Ewidencja zasobów jednostki;
10) Zbiór 10 – Ewidencja urlopów, karty czasu pracy;
11) Zbiór 11 – Kartoteki wydanej odzieży ochronnej i środków ochrony indywidualnej;
12) Zbiór 12 – Rejestr delegacji służbowych;
13) Zbiór 13 – Ewidencja osób korzystających z funduszu socjalnego i dokumentacja;
14) Zbiór 14 – Listy płac pracowników;
15) Zbiór 15 – Kartoteki zarobkowe pracowników, nakazy komornicze;
16) Zbiór 16 – Deklaracje ubezpieczeniowe pracowników;
17) Zbiór 17 – Deklaracje i kartoteki ZUS pracowników;
18) Zbiór 18 – Deklaracje podatkowe pracowników;
19) Zbiór 19 – Spis najemców;
20) Zbiór 20 – kartoteki finansowe najemców;
21) Zbiór 21 – kartoteki osobowe najemców;
22) Zbiór 23 – Rejestr wypadków, ewidencja podejrzeń o chorobę zawodową, itp;
23) Zbiór 24 – Księga druków ścisłego zarachowania;
24) Zbiór 25 – Zbiór upoważnień;
25) Zbiór 26– Umowy zawierane z osobami fizycznymi;
26) Zbiór 27– Dokumenty archiwalne;

**§ 4.** Zbiory danych osobowych wymienione w § 3 ust.1 podlegają przetwarzaniu w sposób tradycyjny lub przy użyciu systemu informatycznego.

## ROZDZIAŁ III
## Wykaz budynków, pomieszczeń i stref do przetwarzania danych osobowych.

**§ 5. 1 .** Dane osobowe gromadzone i przetwarzane są w siedzibie jednostki, mieszczącej się w Lubaniu przy ulicy Brackiej 11.

**2.** Obszarami do przetwarzania danych osobowych z użyciem sprzętu komputerowego oraz sposobem ręcznym są :

1) Stanowisko głównej księgowej;
2) Stanowisko działu technicznego
3) Stanowisko działu ds. zasobów komunalnych we wspólnotach mieszkaniowych

4) Stanowisko działu ds. czynszów,opłat i kosztów
5) Stanowisko działu organizacyjnego
6) Stanowisko kierownika jednostki
7) archiwum jednostki.

## ROZDZIAŁ IV
## Opis zdarzeń naruszających ochronę danych osobowych

**§ 6.** Rodzaje zagrożeń naruszających ochronę danych osobowych:

**1**. Zagrożenia losowe:
1) zewnętrzne np. klęski żywiołowe, przerwy w zasilaniu – ich wystąpienie może prowadzić do utraty integralności danych lub ich zniszczenia lub uszkodzenia infrastruktury technicznej systemu: ciągłość zostaje naruszona , jednak nie dochodzi do naruszenia danych osobowych;
2) wewnętrzne np. niezamierzone pomyłki operatorów, awarie sprzętowe, błędy oprogramowania – w wyniku ich wystąpienia może dojść do zniszczenia danych, może nastąpić zakłócenie ciągłości pracy systemu i naruszenia poufności danych.

**2**. Zagrożenia zamierzone (świadome i celowe naruszenia poufności danych) – w wyniku ich wystąpienia zazwyczaj nie występuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy. W ramach tej kategorii zagrożeń wystąpić mogą:
)1 nieuprawniony dostęp do systemu z zewnątrz;
)2 nieuprawniony dostęp do systemu z wewnątrz;
)3 nieuprawnione przekazanie danych;
)4 bezpośrednie zagrożenie materialnych składników np. kradzież, zniszczenie.

**3**. Okoliczności zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe to w szczególności:
1) sytuacje losowe lub nieprzewidywalne oddziaływanie czynników zewnętrznych na zasoby systemu np. wybuch gazu, pożar, zalanie pomieszczeń, uszkodzenia wskutek prowadzonych prac remontowych;
2) niewłaściwe parametry środowiska np. nadmierna wilgotność, temperatura, wstrząsy, oddziaływania pola elektromagnetycznego, przeciążenia napięcia;;
3) awarie sprzętu lub oprogramowania, które są celowym działaniem na potrzeby naruszenia ochrony danych osobowych;
4) pojawienie się odpowiedniego komunikatu alarmowego od części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu ;
5) pogorszenie jakości danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub niepożądaną modyfikację w systemie;
6) naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie;
7) modyfikacja danych lub zmiana w strukturze danych bez odpowiedniego upoważnienia;
8) ujawnienie osobom nieuprawnionym danych osobowych lub objętych tajemnicą procedur ochrony ich przetwarzania;
9) podmienienie lub zniszczenie nośników z danymi osobowymi bez odpowiedniego upoważnienia lub skasowanie bądź skopiowanie w sposób niedozwolony danych osobowych;
10) rażące naruszenie obowiązków w zakresie przestrzegania procedur bezpieczeństwa informacji (niewylogowywanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce lub kserokopiarce, niewykonanie kopii zapasowych, prace na danych osobowych w celach prywatnych itp.);
11) nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych, znajdujących się na dyskach, płytach CD, kartach pamięci oraz wydrukach komputerowych w formie niezabezpieczonej (otwarte szafy, biurka, regały, archiwum).

**4.** Szczegółowe zasady postępowania w przypadku stwierdzenia naruszenia ochrony danych osobowych reguluje Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

## ROZDZIAŁ V
## Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzania danych osobowych

**§ 7. 1**. Formy zabezpieczeń pomieszczeń, w których przetwarzane są dane osobowe:
1) wszystkie pomieszczenia, w których przetwarzane są dane osobowe zamykane są na klucz, w przypadku opuszczenia przez ostatnia osobę upoważnioną do przetwarzania danych osobowych – także w godzinach pracy;
2) dane osobowe przechowywane w wersji tradycyjnej (papierowej) lub elektronicznej (pamięć flash, płyty CD, DVD, dyskietki, dyski) po zakończeniu pracy są przechowywane w zamykanych na klucz pokojach, a tam , gdzie jest to możliwe w szafach zamykanych, pancernych lub metalowych;
3) nieaktualne lub błędne wydruki zawierające dane osobowe niszczone są w niszczarkach;
4) pomieszczenia AMK, w którym są przetwarzane dane chroniony jest całodobowo przez wynajętą firmę ochroniarską.

**§ 8. 1**. Formy zabezpieczeń przed nieautoryzowanym dostępem do danych osobowych:
1) podłączenie urządzenia końcowego ( komputera, drukarki) do sieci komputerowej jednostki dokonywane jest przez administratora sieci;
2) udostępnianie użytkownikowi zasobów sieci zawierających dane osobowe przez administratora sieci następuje na podstawie upoważnienia do przetwarzania danych osobowych;
3) identyfikacja użytkownika w systemie następuje poprzez zastosowanie uwierzytelniania;
4) przydzielenie indywidualnego identyfikatora każdemu użytkownikowi;
5) udostępnianie kluczy do pomieszczeń , w których przetwarzane są dane osobowe tylko osobom upoważnionym;
6) ustawienie monitorów na stanowiskach pracy w sposób uniemożliwiający wgląd w dane osobowe.

**§ 9. 1**. Formy zabezpieczeń przed utratą danych osobowych w wyniku awarii:
1) odrębne zasilanie sprzętu komputerowego lub zastosowanie zasilaczy zapasowych UPS lub listew antyprzepięciowych;
2) ochrona przed utratą danych poprzez cykliczne wykonywanie kopii zapasowych;
3) zapewnienie właściwej temperatury i wilgotności w pomieszczeniach;
4) zastosowanie ochrony przeciwpożarowej.

**§ 10. 1**. Organizację ochrony danych osobowych realizuje się poprzez:
1) zapoznanie każdej osoby z przepisami dotyczącymi ochrony danych osobowych przed dopuszczeniem do pracy;
2) przeszkolenie osób w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem danych i programów;
3) kontrolowanie pomieszczeń budynku;
4) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;
5) wyznaczenie administratora bezpieczeństwa informacji.

Kierownik

……..

# Instrukcja bezpieczeństwa przetwarzania danych osobowych

**§ 1**. 1.**Nadawanie uprawnień do przetwarzania danych oraz ich rejestrowanie w systemie informatycznym.**

1) Do obsługi systemu informatycznego służącego do przetwarzania danych osobowych, może być dopuszczona wyłącznie osoba posiadająca upoważnienie do przetwarzania danych osobowych, wydane przez Administratora danych osobowych.
2) Upoważnienia do przetwarzania danych osobowych, o których mowa w punkcie 1.1. przechowywane są w teczkach akt osobowych pracowników oraz prowadzona jest ich ewidencja.
3) Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po :
   a) podaniu identyfikatora użytkownika i właściwego hasła w przypadku obsługi SIGID, THB, BIP, HOMEBANKING,
   b) podaniu właściwego hasła dostępu do stanowiska komputerowego w przypadku obsługi OFFICE, OPEN OFFICE
4) Dla każdego użytkownika systemu informatycznego, który przetwarza dane osobowe, Administrator Bezpieczeństwa Informacji ustala niepowtarzalny identyfikator i hasło początkowe.
5) Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego, nie powinien być przydzielany innej osobie.
6) W przypadku utraty przez daną osobę uprawnień do dostępu do danych osobowych w systemie informatycznym. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych, należy niezwłocznie wyrejestrować z systemu informatycznego, unieważnić jej hasło, oraz podjąć inne stosowne działania w celu zapobieżenia dalszemu dostępowi tej osoby do danych. Za realizację procedury rejestrowania i wyrejestrowywanie użytkowników w systemie informatycznym odpowiedzialny jest Administrator Bezpieczeństwa Informacji.

**§ 2. 1. Metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem.**

1) Dane osobowe przetwarzane są z użyciem dedykowanych serwerów, komputerów stacjonarnych.
2) Hasło użytkownika powinno mieć minimum 6znaków.
3) Hasło oprócz znaków małych i dużych liter winno zawierać ciąg znaków alfanumerycznych lub specjalnych;
4) Hasła wpisywane z klawiatury nie mogą pojawiać się na ekranie monitorów w formie jawnej;
5) Hasło nie może zawierać żadnych informacji, które można kojarzyć z użytkownikiem komputera np. osobiste dane użytkownika, tj. nazwisko, inicjały, imiona, marka lub nr rejestracyjny samochodu itp.;
6) Hasło nie może być zapisywane w miejscu dostępnym dla osób nieuprawnionych. Użytkownik nie może udostępnić swojego identyfikatora oraz hasła jak również dostępu do stanowiska roboczego po uwierzytelnieniu w systemie osobom nieuprawnionym ani żadnej osobie postronnej;
7) Hasło użytkownika, umożliwiające dostęp do systemu informatycznego, należy utrzymywać w tajemnicy, również po upływie jego ważności;
8) Raz użyty identyfikator nie może być przydzielony innemu użytkownikowi;
9) Hasła są zdeponowane w kasie pancernej w siedzibie kierownika jednostki.
10) W przypadku, gdy istnieje podejrzenie, że hasło mogła poznać osoba nieuprawniona, użytkownik zobowiązany jest do natychmiastowej zmiany hasła, lub w razie problemów powiadomić o tym fakcie Administratora Bezpieczeństwa Informacji.

**§ 3. 1. Procedury rozpoczęcia, zawieszenia i zakończenia pracy.**

1) Dane osobowe, których administratorem jest jednostka mogą być przetwarzane sposobem tradycyjnym lub z użyciem systemu informatycznego tylko na potrzeby realizowania zadań statutowych i organizacyjnych jednostki;
2) Rozpoczęcie pracy użytkownika w systemie informatycznym następuje po poprawnym uwierzytelnieniu (zalogowaniu się do systemu);
3) Rozpoczęcie pracy w aplikacji musi być przeprowadzone zgodnie z instrukcją zawartą w dokumentacji aplikacji;
4) Zakończenie pracy użytkownika następuje po poprawnym wylogowaniu się z systemu oraz poprzez uruchomienie odpowiedniej dla danego systemu opcji jego zamknięcia zgodnie z instrukcją zawartą w dokumentacji;
5) Niedopuszczalne jest zakończenie pracy w systemie bez wykonania pełnej i poprawnej operacji wylogowania z aplikacji i poprawnego zamknięcia systemu;
6) Monitory stanowisk komputerowych znajdujące się w pomieszczeniach, gdzie przebywają osoby, które nie posiadają upoważnień do przetwarzania danych osobowych, a na których przetwarzane są dane osobowe należy ustawić w taki sposób, aby uniemożliwić osobom postronnym wgląd w dane;
7) Użytkownik ma obowiązek wylogowania się w przypadku zakończenia pracy. Stanowisko komputerowe nie może pozostać z uruchomionym i dostępnym systemem bez nadzoru pracującego na nim pracownika;
8) Wydruki zawierające dane osobowe należy przechowywać w miejscu uniemożliwiającym ich odczytanie przez osoby postronne. Wydruki nieprzydatne należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.
9) Przebywanie osób nieuprawnionych w pomieszczeniach znajdujących się na obszarze, w którym są przetwarzane dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej do ich przetwarzania;
10) Pomieszczenia, w których przetwarzane są dane osobowe, należy zamykać, na czas nieobecności osób zatrudnionych, w sposób uniemożliwiający dostęp do nich osobom trzecim;
11) Użytkownik niezwłocznie powiadamia Administratora Bezpieczeństwa Informacji w przypadku podejrzenia fizycznej ingerencji w przetwarzane dane osobowe lub użytkowane narzędzia programowe lub sprzętowe. Wówczas, użytkownik jest zobowiązany do natychmiastowego wyłączenia sprzętu.

**§ 4. 1. Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi do ich przetwarzania.**

1) Zbiory danych osobowych w systemie informatycznym są zabezpieczane przed utratą lub uszkodzeniem za pomocą:
   a) urządzeń zabezpieczających przed awarią zasilania lub zakłóceniami w sieci zasilającej,
   b) sporządzanie kopii zapasowych ( kopie pełne).
2) Pełne kopie zapasowe zbiorów danych tworzone są cyklicznie.
3) W szczególnych sytuacjach, np. przed aktualizacją lub zmianą oprogramowania lub systemu należy wykonać bezwzględnie pełną kopię zapasową systemu;
4) Kopie zapasowe zbiorów danych należy okresowo sprawdzać pod kątem ich przydatności do odtworzenia w przypadku awarii systemu. Za przeprowadzenie tych czynności odpowiada Administrator Bezpieczeństwa Informacji;
5) Nośniki danych po ustaniu ich użyteczności należy pozbawić danych lub zniszczyć w sposób uniemożliwiający odczyt danych.

**§ 5. 1.Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych**

1) Okresowe kopie zapasowe wykonywane są na płytach CD lub innych elektronicznych nośnikach informacji. Kopie zapasowe przechowuje się w sposób uniemożliwiający nieuprawnione przejęcie, modyfikacje, uszkodzenie lub zniszczenie.
2) Dostęp do nośników z kopiami zapasowymi systemu oraz kopiami danych osobowych, ma wyłącznie Administrator Bezpieczeństwa Informacji .

3) Kopie przechowuje się przez okres 1 roku. Kopie zapasowe należy bezzwłocznie usuwać po ustaniu ich użyteczności.
4) Usunięcie danych z systemu powinno zostać zrealizowane przy pomocy oprogramowania przeznaczonego do bezpiecznego usuwania danych z nośnika informacji.
5) W przypadku kopii zapasowych sporządzanych indywidualnie przez użytkownika odpowiedzialnością za ich zniszczenie obarczony jest użytkownik.
6) W przypadku nośników informacji, przez ich zniszczenie rozumie się ich trwałe i nieodwracalne zniszczenie fizyczne do stanu nie dającego możliwości ich rekonstrukcji i odzyskania danych.

**§ 6. 1.Sposób zabezpieczenia systemu informatycznego przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego**

1) W związku z istnieniem zagrożenia dla zbiorów danych osobowych, ze strony wirusów komputerowych, których celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego, konieczna jest ochrona sieci komputerowej i stanowisk komputerowych.

2) Wirusy komputerowe mogą pojawić się systemach jednostki poprzez: Internet, nośniki informacji takie jak: dyskietki, płyty CD, dyski przenośne, itp.

3) Przeciwdziałanie zagrożeniom ze strony wirusów komputerowych realizowane jest następująco:
   a) Komputer z dostępem do Internetu musi być zabezpieczony za pomocą oprogramowania antywirusowego.
   b) Zainstalowany program antywirusowy powinien być tak skonfigurowany, by co najmniej raz w tygodniu dokonywał aktualizacji bazy wirusów oraz dokonywał automatycznie sprawdzenie komputera pod kątem obecności wirusów komputerowych.
   c) Elektroniczne nośniki informacji takie jak dyskietki, dyski przenośne, należy każdorazowo sprawdzać programem antywirusowym przed użyciem, po zainstalowaniu ich w systemie. Czynność powyższą realizuje użytkownik systemu. W przypadku problemów ze sprawdzeniem zewnętrznego nośnika danych użytkownik jest zobowiązany zwrócić się z tym do Administratora Bezpieczeństwa Informacji.
   d) Komputery i systemy pracujące muszą mieć zainstalowany program antywirusowy a w przypadku komputerów z dostępem do Internetu, również posiadać oprogramowanie i mechanizmy zabezpieczające przed nieautoryzowanym dostępem z sieci (firewall).
   e) W przypadku, gdy użytkownik stanowiska komputerowego zauważy komunikat oprogramowania zabezpieczającego system wskazujący na zaistnienie zagrożenia lub rozpozna tego typu zagrożenie, zobowiązany jest zaprzestać jakichkolwiek czynności w systemie i niezwłocznie skontaktować się z Administratorem Bezpieczeństwa Informacji.
   f) Przy korzystaniu z poczty elektronicznej należy zwrócić szczególną uwagę na otrzymywane załączniki dołączane do treści wiadomości. Zabrania się otwierania załączników i wiadomości poczty elektronicznej od „niezaufanych" nadawców.
   g) Zabrania się użytkownikom komputerów, wyłączania, blokowania odinstalowywania programów zabezpieczających komputer (skaner antywirusowy, firewall) przed oprogramowaniem złośliwym oraz nieautoryzowanym dostępem.

**§ 7. Udostępnianie danych osobowych i sposób odnotowania informacji o udostępnionych danych**

7.1.Udostępnienie danych instytucjom może odbywać się wyłącznie na pisemny uzasadniony wniosek lub zgodnie z przepisami prawa.

**§ 8. Wykonywanie przeglądów i konserwacji systemu oraz nośników informacji służących do przetwarzania danych**

1) Przeglądy i konserwacje systemu oraz zbiorów danych wykonuje Administrator Bezpieczeństwa Informacji na bieżąco.
2) Administrator Bezpieczeństwa Informacji okresowo sprawdza możliwość odtworzenia danych z kopii zapasowej.

3) Umowy dotyczące instalacji i konserwacji sprzętu należy zawierać z podmiotami, których kompetencje nie budzą wątpliwości, co do wykonania usługi oraz których wiarygodność finansowa zostały sprawdzone na rynku.
4) Naprawy sprzętu należy zlecać podmiotom, których kompetencje nie budzą wątpliwości, co do wykonania usługi. Naprawa sprzętu, na którym mogą znajdować się dane osobowe powinna odbywać się pod nadzorem osób użytkujących sprzęt oraz Administratora Bezpieczeństwa Informacji w miejscu jego użytkowania.
5) W przypadku konieczności naprawy poza miejscem użytkowania, sprzęt komputerowy, przed oddaniem do serwisu, powinien być odpowiednio przygotowany. Dane należy zarchiwizować na nośniki informacji, a dyski twarde, bezwzględnie, wymontować na czas naprawy.
6) Zmiana konfiguracji sprzętu komputerowego, na którym znajdują się dane osobowe lub zmiana jego lokalizacji, może być dokonana tylko za wiedzą i zgodą Administratora Bezpieczeństwa Informacji.

**§ 9. Ustalenia końcowe**

Osobom korzystającym z systemu informatycznego, w którym przetwarzane są dane osobowe w jednostce zabrania się:

1) ujawniania loginu i hasła współpracownikom i osobom z zewnątrz,
2) pozostawiania haseł w miejscach widocznych dla innych osób,
3) udostępniania stanowisk pracy wraz z danymi osobowymi osobom nieuprawnionym,
4) udostępniania osobom nieuprawnionym programów komputerowych zainstalowanych w systemie,
5) używania oprogramowania w innym zakresie niż pozwala na to umowa licencyjna,
6) przenoszenia programów komputerowych, dysków twardych z jednego stanowiska na inne,
7) kopiowania danych na nośniki informacji, kopiowania na inne systemy celem wynoszenia ich poza jednostkę,
8) samowolnego instalowania i używania jakichkolwiek programów komputerowych w tym również programów do użytku prywatnego; programy komputerowe instalowane są za zgodą Administratora Bezpieczeństwa Informacji,
9) używania nośników danych udostępnionych przez osoby postronne,
10) przesyłania dokumentów i danych z wykorzystaniem konta pocztowego prywatnego (niesłużbowego),
11) otwierania załączników i wiadomości poczty elektronicznej od nieznanych i „niezaufanych" nadawców,
12) używania nośników danych niesprawdzonych, niewiadomego pochodzenia lub niezwiązanych z wykonywaną pracą; w przypadku konieczności użycia niesprawdzonych przenośnych nośników danych, należy zgłosić te nośniki, w celu sprawdzenia - przeskanowania programem antywirusowym, Administratorowi Bezpieczeństwa Informacji,
13) tworzenia kopii zapasowych niechronionych hasłem i/lub bez odpowiednich zabezpieczeń miejsca ich przechowywania.

Ponadto zabrania się:

1) wyrzucania dokumentów zawierających dane osobowe bez uprzedniego ich trwałego zniszczenia,
2) pozostawiania dokumentów, kopii dokumentów zawierających dane osobowe w drukarkach, kserokopiarkach,
3) pozostawiania kluczy w drzwiach, szafach, biurkach, zostawiania otwartych pomieszczeń, w których przetwarza się dane osobowe,
4) pozostawiania bez nadzoru osób trzecich przebywających w pomieszczeniach jednostki, w których przetwarzane są dane osobowe,
5) pozostawiania dokumentów na biurku po zakończonej pracy, pozostawiania otwartych dokumentów na ekranie monitora bez blokady konsoli,
6) ignorowania nieznanych osób z zewnątrz poruszających się w obszarze przetwarzania danych osobowych,
7) przekazywania informacji będącymi danymi osobowymi osobom nieupoważnionym,
8) ignorowania zapisów Polityki Bezpieczeństwa jednostki.

9.1. Konieczne jest:

1) posługiwanie się własnym loginem i hasłem w celu uzyskania dostępu do systemów informatycznych,
2) tworzenia haseł trudnych do odgadnięcia dla innych,
3) traktowanie konta pocztowego jednostki jako narzędzia pracy i wykorzystywanie go jedynie w celach służbowych,
4) nie przerywanie procesu skanowania przez program antywirusowy na komputerze,
5) wykonywanie kopii zapasowych danych przetwarzanych na stanowisku komputerowym,
6) zabezpieczenie sprzętu komputerowego przed kradzieżą lub nieuprawnionym dostępem do danych.

9.2. Wszelkie przypadki naruszenia niniejszej Instrukcji należy zgłaszać Administratorowi Bezpieczeństwa Informacji lub bezpośredniemu przełożonemu.

9.3. Dane kontaktowe

- Administrator Bezpieczeństwa Informacji – sekretariat jednostki, nr telefonu : (75)7222658, e-mail : amkluban@op.pl.
- Pełnomocnik kierownika ds. Ochrony Danych Osobowych – sekretariat jednostki, nr telefonu : (75)7222658, e-mail : amkluban@op.pl.

## § 10. Zalecenia w zakresie przetwarzania danych osobowych sposobem tradycyjnym

1) Miejscem tworzenia, uzupełniania, przechowywania dokumentacji dotyczącej przetwarzania danych osobowych sposobem tradycyjnym są pomieszczenia w jednostce.
2) Osoby prowadzące dokumentację zobowiązane są do zachowania tajemnicy służbowej.
3) Dokumentacji, o której mowa w punkcie 1.1. nie można wynosić poza teren jednostki bez zgody przełożonego.
4) Dokumentację, o której mowa w punkcie 1.1. archiwizuje się zgodnie z Instrukcją kancelaryjną.
5) Osoby prowadzące dokumentację zobowiązane są do niezwłocznego poinformowania Pełnomocnika kierownika ds. przetwarzania danych osobowych o podejrzeniu dostępu do dokumentacji przez osoby nieupoważnione.

## § 11. Obowiązki Administratora Danych

1. Administrator danych zobowiązany jest do zapewnienia, aby dane osobowe były:

a) przetwarzane zgodnie z prawem,
b) zbierane dla oznaczonych, zgodnych z prawem celów,
c) merytorycznie poprawne i adekwatne w stosunku do celów.

2. Wyznacza osobę, zwaną dalej Administratorem Bezpieczeństwa Informacji, odpowiedzialnym za bezpieczeństwo danych osobowych w systemie informatycznym, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe, oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń.
3. Opracowuje instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych, przeznaczoną dla osób zatrudnionych przy przetwarzaniu tych danych.
4. Określa budynki, pomieszczenia lub części pomieszczeń, tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego.
5. Opracowuje instrukcję, określającą sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji.
6. Prowadzi ewidencję osób uprawnionych do przetwarzania danych osobowych w poszczególnych systemach.
7. Organizuje szkolenia mające na celu zaznajomienie każdej osoby przetwarzającej dane osobowe z przepisami dotyczącymi ich ochrony.

8. Odpowiada za to by zakres czynności osoby zatrudnionej przy przetwarzania danych osobowych określał odpowiedzialność tej osoby za:

a) ochronę danych przed niepowołanym dostępem,
b) nieuzasadnioną modyfikację lub zniszczenie danych,
c) nielegalne ujawnienie danych.
w stopniu odpowiednim do zadań realizowanych w procesie przetwarzania danych osobowych.

**§ 12. Obowiązki Administratora Bezpieczeństwa Informacji**

1. Nadzór na przestrzeganiem instrukcji określającej sposób zarządzania systemem informatycznym.
2. Nadzór nad właściwym zabezpieczeniem sprzętu oraz pomieszczeń, w których przetwarzane są dane osobowe.
3. Nadzór nad wykorzystywanym w jednostce oprogramowaniem.
4. Przeciwdziałanie dostępowi osób niepowołanych do systemu, w których przetwarzane są dane osobowe.
5. Podejmowanie odpowiednich działań w celu właściwego zabezpieczenia danych.
6. Badanie ewentualnych naruszeń w systemie zabezpieczeń danych osobowych.
7. Podejmowanie decyzji o instalowaniu nowych urządzeń oraz oprogramowania wykorzystywanego do przetwarzania danych osobowych.
8. Nadzór na naprawami, konserwacją oraz likwidacją urządzeń komputerowych zawierających dane osobowe.
9. Definiowanie użytkowników i haseł dostępu.
10. Aktualizowanie oprogramowania antywirusowego i innego, chyba że aktualizacje te wykonywane są automatycznie.
11. Nadzór nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności.
12. Wdrożenie szkoleń z zakresu przepisów dotyczących ochrony danych osobowych oraz środków technicznych i organizacyjnych przy przetwarzaniu danych w systemach informatycznych.
13. Sporządzanie raportów z naruszenia bezpieczeństwa systemu informatycznego.

**Załącznik Nr 2** do „Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Administracji Mieszkań Komunalnych w Lubaniu

## ANEKS nr .....

do przydziału czynności Pani/u ....., zatrudnionej/emu na stanowisku .....

*Na podstawie Rozporządzenie 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. z 2004 r. Nr 100, poz. 1024) oraz Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 i Nr 153, poz. 1271 oraz z 2004 r. Nr 25, poz. 219 i Nr 33, poz. 285).*

rozszerzam Pani zakres obowiązków o dodatkowe zadania i czynności, jak niżej:

1. Ochrona danych osobowych w systemie informatycznym i ręcznym, a w szczególności przeciwdziałanie dostępowi osób niepowołanych oraz przeciwdziałanie w przypadku wykrycia naruszeń zabezpieczeń systemu zgodnie z ustawą o ochronie danych osobowych (Dz. U. z 1997 r., poz. 883).
2. Przestrzeganie zasad określonych w instrukcji określającej sposób zarządzania systemem informatycznym i ręcznym.
3. Przestrzeganie zasad określonych w instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych.
4. Przestrzeganie zachowania tajemnicy również po ustaniu zatrudnienia.
5. W szczególności przetwarzanie danych osobowych w następujących zbiorach:

Zbiór nr 1- Ewidencja osób zatrudnionych przy przetwarzaniu danych osobowych

Zbiór nr 2 - Kontrola wewnętrzna - wyniki, opracowania, raporty, notatki

Zbiór nr 4 - Dokumentacja dotycząca polityki kadrowej: opiniowanie awansów, wyróżnień, odznaczeń - nagrody i kary, itp.

Zbiór nr 5 - .....

Zbiór nr 7 - .....

Przyjęłam do wiadomości i stosowania:

.....
podpis kierownika

.....
podpis pracownika

……, dnia .....

**Załącznik Nr 3** do „Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Administracji Mieszkań Komunalnych w Lubaniu

**UPOWAŻNIENIE nr .....**

z dnia .....

Na podstawie ustaw *Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 i Nr 153, poz. 1271 oraz z 2004 r. Nr 25, poz. 219 i Nr 33, poz. 285).*

upoważniam Panią ..... zatrudnioną w ….. w ……. na
stanowisku ..... do obsługi systemu ręcznego i informatycznego zbiorów
Nr .....( wypisać zbiory)

Administrator danych / Kierownik

….....

---

**Załącznik Nr 4** do „Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Administracji Mieszkań Komunalnych w Lubaniu

.....
*imię i nazwisko*

.....
*stanowisko*

OŚWIADCZENIE

Oświadczam, że zapoznałem(łam) się z przepisami prawa dotyczącymi ochrony danych osobowych, a w szczególności z ustawą z 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U z 2002 r.,Nr 101 poz. 926 ze zm.) oraz Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. *sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024)* i zobowiązuję się do ich przestrzegania.

Oświadczam ponadto, że zapoznałem(łam) się z wewnętrzną Instrukcją określającą sposób zarządzania systemem informatycznym i ręcznym, służącym przetwarzaniu danych osobowych i instrukcją postępowania w sytuacji naruszenia ochrony danych osobowych.

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

*Otrzymałem(łam) dnia:*

.....
(*podpis pracownika)*