*Załącznik nr 1*
*do Uchwały Zarządu*
*nr 69 z dnia 15.09.2016r.*

# INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W SPÓŁDZIELNI MIESZKANIOWEJ W LUBANIU

| Pieczęć firmowa: | Podpis Administratora Danych Osobowych (Zarząd Spółdzielni) | Data: |
|---|---|---|
| SPÓŁDZIELNIA MIESZKANIOWA<br>ul. B. Chrobrego 3, 59-800 Lubań<br>tel./fax 75-722-23-56<br>NIP 613-000-40-05 | | 15-09-2016 |

| Podpis Inspektora Bezpieczeństwa Informacji | Data: | Podpis Administratora Systemu Informatycznego | Data: |
|---|---|---|---|
| Bernat | 15-09-2016 | | 15-09-2016 |

SPIS TREŚCI

**WSTĘP**

Realizując postanowienia Ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tekst jedn. Dz. U. 2014r., poz. 1182 z późn. zm.) oraz wydane w oparciu o delegacje ustawą przepisy Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. (Dz. U. 2004r. Nr. 100 poz. 1024 z późn. zmianami) w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych jakim powinny odpowiadać urządzenia i systemy informacyjne służące do przetwarzania danych osobowych wprowadza się zestaw reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji informacji wrażliwej pozwalający na zapewnienie ochrony danych osobowych.

## 1. Definicje

Administrator Systemu Informatycznego (ASI) – może nim być informatyk zatrudniony na umowę o pracę, umowę -zlecenie lub zewnętrzna firma informatyczna.
Inspektor Bezpieczeństwa Informacji (IBI) - – wyznaczony przez Administratora Danych Osobowych, odpowiedzialny za organizację ochrony danych osobowych.

## 2. Poziom bezpieczeństwa

Poziom bezpieczeństwa systemów informatycznych przetwarzających dane osobowe określono jako wysoki.

## 3. Zabezpieczenia infrastruktury informatycznej i telekomunikacyjnej

Zabezpieczenia odnoszą się do:

1. technicznych środków zabezpieczenia komputerów przed skutkami awarii zasilania
    a. Zastosowano: UPS-y ochraniające serwer i komputery służace do bezpośredniego wprowadazania danych do bazy.
2. infrastruktury sieci informatycznej, w której użytkowane są komputery wykorzystywane do przetwarzania danych osobowych
    a. Komputery służące do przetwarzania danych osobowych są połączone z siecią publiczną poprzez router zabezpieczony firewall'em.
    b. Zbiory danych osobowych nie są przetwarzane na komputerach przenośnych.
    c. Zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej.
    d. Programy zainstalowane na komputerach obsługujących przetwarzanie danych osobowych są użytkowane z zachowaniem praw autorskich i posiadają licencje.
3. sprzętowych i programowych środków ochrony przed nieuprawnionym dostępem do danych osobowych, w tym środków zapewniających rozliczalność wykonywanych operacji
    a. Lokalizacja urządzeń komputerowych (komputerów typu PC, terminali, drukarek) uniemożliwia osobom niepowołanym (np. klientom, pracownikom innych działów,) dostęp do nich.
    b. Dostęp do systemu operacyjnego komputerów, w których przetwarzane są dane osobowe, zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora oraz hasła.

c. Zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych.

4. sprzętowych i programowych środków ochrony przed szkodliwym oprogramowaniem i nieuprawnionym dostępem do przetwarzanych danych
    a. Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity, inne – na wszystkich stanowiskach zainstalowany jest program antywirusowy "NOD32" firmy „Eset” z automatyczną aktualizacją baz wirusów.
    b. Użyto system Firewall do ochrony dostępu do sieci komputerowej.

## 4. Zabezpieczenia baz danych i oprogramowania przetwarzającego dane osobowe

Opis technicznych i programowych środków bezpieczeństwa zastosowanych w procedurach, aplikacjach i programach oraz innych narzędziach programowych wykorzystywanych do przetwarzania danych osobowych

1. Dostęp do zbioru danych osobowych (do bazy danych i do programu) wymaga uwierzytelnienia z wykorzystaniem identyfikatora oraz hasła.
2. Wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych.
3. Zastosowano mechanizm umożliwiający automatyczną rejestrację identyfikatora użytkownika i datę pierwszego wprowadzenia danych osobowych .
4. Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego.
5. Zastosowano system antywirusowy "NOD32" firmy „Eset” z automatyczną aktualizacją baz wirusów na stanowiskach, na których przetwarzane są dane osobowe.

## 5. Procedura korzystania z Internetu

1. Użytkownik zobowiązany jest do korzystania z Internetu wyłącznie w celach służbowych.
2. Zabrania się zgrywania na dysk twardy komputera oraz uruchamia jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą Inspektora Bezpieczeństwa Informacji i tylko w uzasadnionych przypadkach.
3. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie ściągnięte z Internetu i przez niego zainstalowane.
4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hakerskim, pornograficznym, lub innym zakazanym przez prawo.
5. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.
6. Należy korzystać wyłącznie z przeglądarek posiadających odpowiednie opcje zabezpieczeń.

7. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka, protokół https).

## 6. Procedura korzystania z poczty elektronicznej

1. Przesyłanie informacji poza organizację może odbywać się tylko przez osoby do tego upoważnione.
2. W przypadku przesyłania informacji wrażliwych wewnątrz organizacji bądź wszelkich danych osobowych poza organizację należy wykorzystywać mechanizmy kryptograficzne (pakowanie i zabezpieczanie hasłem wysyłanych plików lub podpis elektroniczny)
3. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
4. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.
5. Nie należy otwierać załączników (plików) w korespondencji elektronicznej nadesłanej przez nieznanego nadawcę lub podejrzanych załączników nadanych przez znanego nadawcę.
6. Użytkownicy nie powinni rozsyłać za pośrednictwem poczty elektronicznej informacji o zagrożeniach dla systemu informatycznego, tzw. „łańcuszków szczęścia" itp.
7. Użytkownicy nie powinni rozsyłać wiadomości zawierających załączniki o dużym rozmiarze dla większej liczby adresatów - określenie krytycznych rozmiarów przesyłek i krytycznej liczby adresatów jest uzależnione od wydajności systemu poczty elektronicznej
8. Użytkownicy powinni okresowo kasować niepotrzebne wiadomości pocztowe.

## 7. Procedura nadawania uprawnień do przetwarzania danych osobowych.

Procedura opisuje zasady: przyznawania, modyfikacji i usuwania uprawnień użytkownika do przetwarzania zbiorów w systemie informatycznym lub w wersji papierowej. Celem procedury jest minimalizacja ryzyka nieuprawnionego dostępu do danych osobowych i utraty ich poufności przez osoby nieupoważnione.

### *7.1. Zarządzanie uprawnieniami użytkowników*

1. Przyznanie, zmiana lub usunięcie uprawnień użytkownika do przetwarzania danych osobowych w systemie informatycznym lub w zbiorze papierowym realizowane jest na zlecenie przełożonego. Zlecenie przekazywane jest Inspektorowi Bezpieczeństwa Informacji.
2. W przypadku zlecenia nadania bądź zmiany uprawnień (np. z powodu zatrudnienia osoby lub zmiany stanowiska pracy), IBI zobowiązany jest do sprawdzenia, czy użytkownik:
    a. Odbył szkolenie z zakresu przestrzegania zasad bezpieczeństwa danych osobowych,
    b. Podpisał oświadczenie o zachowaniu poufności,

c. Będzie przetwarzał dane osobowe w zakresie i celu określonym w polityce bezpieczeństwa i instrukcji zarządzania.

3. Po akceptacji zlecenia, IBI przekazuje go bezpośrednio Informatykowi (ASI) celem nadania identyfikatora oraz uprawnień użytkownika w systemie informatycznym.
4. Usunięcie uprawnień użytkownikowi polega na wyrejestrowaniu go z systemu przez Informatyka (ASI) na zlecenie IBI.
5. Identyfikator użytkownika po wyrejestrowaniu z systemu informatycznego nie może być przydzielony innej osobie.
6. IBI odpowiada za przechowywanie i aktualizację wszystkich Upoważnień.
7. IBI opowiada za prowadzenie rejestru osób upoważnionych do przetwarzania danych osobowych.

### *7.2. Zarządzanie uprawnieniami administratorów*

1. Administratora Systemów Informatycznych powołuje Zarząd Spółdzielni Mieszkaniowej.
2. Każdy Administrator systemu zobowiązany jest do bieżącej pracy na koncie roboczym. Użycie tzw. konta „root" dopuszczalne jest jedynie w sytuacjach awaryjnych lub podczas poważnych zmian wprowadzanych w administrowanym systemie.
3. Hasło „root” znane jest tylko administratorowi odpowiedzialnemu za dany system.
4. W przypadkach awaryjnych (np. nieobecność administratora) hasło może być przekazane decyzją członka Zarządu Spółdzielni osobie zastępującej administratora.
5. Po ustaniu sytuacji awaryjnej, Administrator jest zobowiązany do zmiany hasła.

## 8. Metody i środki uwierzytelnienia

Celem procedury jest zapewnienie, że do systemów informatycznych przetwarzających dane osobowe mają dostęp jedynie osoby do tego upoważnione.

### *8.1. Ogólne zasady postępowania z hasłami*

1. ASI informuje użytkownika o nadaniu pierwszego hasła do systemu.
2. Użytkownik systemu zobowiązany jest do niezwłocznej zmiany tego hasła.
3. Użytkownik systemu w trakcie pracy w aplikacji może zmienić swoje hasło.
4. Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów.
5. Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności
6. Zabronione jest zapisywanie haseł w sposób jawny oraz przekazywanie ich innym osobom.

### *8.2. Hasła do programów przetwarzających dane osobowe*

1. Hasło dostępu do systemu informatycznego przetwarzającego dane osobowe składa się co najmniej z 8 znaków.
2. Hasło składa się z dużych i małych liter oraz z cyfr lub znaków specjalnych.

3. Zmiana hasła odbywa się nie rzadziej niż raz na 1 miesiąc.

### *8.3. Hasła administratora*

1. Hasło administratora składa się co najmniej z 8 znaków.
2. Hasło składa się z dużych i małych liter oraz z cyfr lub znaków specjalnych.
3. Administrator systemu zobowiązany jest zmieniać swoje hasło nie rzadziej niż raz na 1 miesiąc.
4. W przypadku utraty uprawnień przez osobę administrującą systemem należy niezwłocznie zmienić hasła, do których miała dostęp.

## 9. Procedura rozpoczęcia, zawieszenia i zakończenia pracy

Celem procedury jest zabezpieczenie danych osobowych przed nieuprawnionym dostępem i utratą poufności w sytuacji, gdy użytkownik rozpoczyna, przerywa lub kończy pracę w systemie informatycznym przetwarzającym dane osobowe.

1. Użytkownik rozpoczyna pracę z systemem informatycznym przetwarzającym dane osobowe z użyciem identyfikatora i hasła.
2. Użytkownik jest zobowiązany do powiadomienia IBI o próbach logowania się do systemu osoby nieupoważnionej, jeśli system to sygnalizuje.
3. W przypadku, gdy użytkownik podczas próby zalogowania się zablokuje system, zobowiązany jest powiadomić o tym ASI, który odpowiada za odblokowanie systemu użytkownikowi.
4. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np. klientom, pracownikom innych działów) wgląd do danych wyświetlanych na monitorach komputerowych – tzw. Polityka czystego ekranu.
5. Po zakończeniu pracy, użytkownik zobowiązany jest:
   a) wylogować się z systemu informatycznego oraz wyłączyć sprzęt komputerowy,
   b) zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki magnetyczne i optyczne, na których znajdują się dane osobowe.

## 10. Procedura tworzenia kopii zapasowych

1. Kopie zapasowe danych znajdujących się w folderach „Moje dokumenty” na komputerach poszczególnych użytkowników są automatycznie wykonywane z częstotliwością raz na dzień na dysku serwera w oddzielnym dla każdego użytkownika wolumenie.
2. Kopie wszystkich danych z dysku serwera, w tym bazy danych SQL programu Comarch Optima z nakładką Aquila, przetwarzających dane osobowe, wykonywane są codziennie na osobnym dla każdego roboczego dnia tygodnia dysku zewnętrznym podłączanym bezpośrednio do serwera w pomieszczeniu serwerowni; za sporządzanie tych kopii odpowiedzialny jest Inspektor Bezpieczeństwa Informacji.
3. Dyski zewnętrzne z kopiami przechowywane są kasetce pancernej zamykanej na zamek szyfrowy, w pomieszczeniu innym niż serwerownia.
4. Dostęp do kopii mają: Inspektor Bezpieczeństwa Informacji, Administrator Systemu Informatycznego, z-ca Prezesa ds. technicznych Spółdzielni Mieszkaniowej.

## 11. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji i wydruków

Procedura określa sposób postępowania z nośnikami danych osobowych takimi jak: twarde dyski, płyty CD/DVD/BR, pendrive, telefonami komórkowymi, pamięciami typu „flash", kartami pamięci na których znajdują się dane osobowe, celem zabezpieczenia ich przez niszczeniem, kradzieżą, dostępem osób nieupoważnionych.

### *11.1. Zabezpieczenie elektronicznych nośników informacji*

1. Nośniki danych są przechowywane w sposób uniemożliwiający dostęp do nich osób nieupoważnionych, jak również zabezpieczający je przed zagrożeniami środowiskowymi (zalanie, pożar, wpływ pól elektromagnetycznych).
2. Zabrania się wynoszenia poza obszar organizacji wymiennych nośników informacji a w szczególności twardych dysków z zapisanymi danymi osobowymi bez zgody ADO.
3. W sytuacji przekazywania nośników z danymi osobowymi poza obszar organizacji należy stosować następujące zasady bezpieczeństwa:
    a. adresat powinien zostać powiadomiony o przesyłce,
    b. nadawca powinien posiadać kopię przesyłanych danych,
    c. przy przesyłaniu metodami elektronicznej transmisji danych, przed wysłaniem powinny one zostać zaszyfrowane, a hasło podane adresatowi inną drogą,
    d. przy przesyłaniu środkami tradycyjnymi należy stosować bezpieczne koperty depozytowe,
    e. przesyłkę należy przesyłać przez kuriera,
    f. adresat powinien powiadomić nadawcę o otrzymaniu przesyłki.
4. Użytkownicy są zobowiązani do niezwłocznego i trwałego usuwania/kasowania danych osobowych z nośników informacji po ustaniu powodu ich przechowywania (chyba, że z powodu odrębnych przepisów należy je zachować na dłużej).
5. Podlegające likwidacji uszkodzone lub przestarzałe nośniki, a w szczególności twarde dyski z danymi osobowymi są niszczone w sposób fizyczny, a fakt ich zniszczenia zostaje potwierdzony protokołem.
6. Nośniki informacji zamontowane w sprzęcie IT, a w szczególności twarde dyski z danymi osobowymi powinny być wymontowane lub wyczyszczone specjalistycznym oprogramowaniem, zanim zostaną przekazane poza obszar organizacji (np. sprzedaż lub darowizna komputerów stacjonarnych / laptopów).

### *11.2. Zabezpieczenie kopii zapasowych*

Zabezpieczenie kopii zapasowych opisane jest w procedurach tworzenia kopii zapasowych.

### *11.3. Zabezpieczenie dokumentów i wydruków*

1. Dokumenty i wydruki zawierające dane osobowe przechowuje się w pomieszczeniach zabezpieczonych fizycznie zgodnie z zasadami określonymi w Polityce bezpieczeństwa.
2. Za bezpieczeństwo dokumentów i wydruków odpowiedzialne są osoby je przetwarzające oraz kierownicy właściwych jednostek lub komórek organizacyjnych, a w szczególności odpowiadają za:

a) Zamykanie dokumentów na klucz w szafach, biurkach, sejfach podczas nieobecności w pomieszczeniach lub po zakończeniu pracy (tzw. Polityka czystego biurka).
b) Niszczenie dokumentów i tymczasowych wydruków w niszczarkach niezwłocznie po ustaniu celu ich przetwarzania.
c) Nie pozostawianie wydruków i ksero na urządzeniach lub w ich okolicy bez nadzoru.

# 12. Procedura zabezpieczenia systemu informatycznego, w tym przed wirusami komputerowymi

## *12.1. Ochrona antywirusowa*

Celem procedury jest zabezpieczenie systemów informatycznych przed szkodliwym oprogramowaniem (np. typu robaki, wirusy, konie trojańskie, rootkity) oraz nieautoryzowanym dostępem do systemów przetwarzających dane osobowe

1. Za zaplanowanie i zapewnienie ochrony antywirusowej odpowiada ASI, w tym za zapewnienie odpowiedniej ilości licencji dla użytkowników.
2. Użytkownicy zobowiązani są do skanowania plików przychodzących programem antywirusowym, chyba że program antywirusowy robi to automatycznie.
3. ASI zapewnia stałą aktywność programu antywirusowego, tzn. program antywirusowy musi być aktywny podczas pracy systemu informatycznego przetwarzającego dane osobowe.
4. Aktualizacja definicji wirusów odbywa się automatycznie przez system.
5. W przypadku stwierdzenia pojawienia się wirusa, każdy użytkownik winien powiadomić ASI.

## *12.2. Ochrona przed nieautoryzowanym dostępem do sieci lokalnej*

Stosowane zabezpieczenia mają na celu zabezpieczenie systemów informatycznych przed nieautoryzowanym dostępem do sieci lokalnej np. przez programy szpiegujące, hackerów.

1. Za zaplanowanie, konfigurowanie, aktywowanie specjalistycznego oprogramowania monitorującego wymianę danych na styku sieci lokalnej i sieci rozległej odpowiada ASI.
2. Stosowany jest sprzętowy i programowy Firewall na serwerze i stacjach roboczych.
3. Zastosowano mechanizmy kontroli dostępu do sieci przy użyci techniki NAT.
4. W Spółdzielni Mieszkaniowej nie jest wykorzystywana sieć bezprzewodową (Wi-Fi).

# 13. Procedura wykonywania przeglądów i konserwacji

Celem procedury jest zapewnienie ciągłości działania systemów informatycznych przetwarzających dane osobowe oraz zabezpieczenie danych osobowych przed ich nieuprawnionym udostępnieniem.

## *13.1. Przeglądy i konserwacje systemu informatycznego i aplikacji*

1. ASI odpowiada za bezawaryjną pracę systemu IT, w szczególności: stacji roboczych, aplikacji serwerowych, baz danych, poczty email.

2. Przegląd i konserwacja systemu informatycznego powinny być wykonywane w terminach określonych przez producentów systemu lub zgodnie z harmonogramem ASI, jednak nie rzadziej niż raz w miesiącu.
3. Za terminowość przeprowadzenia przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada ASI.
4. ASI odpowiada za optymalizację zasobów serwerowych, wielkości pamięci i dysków.
5. ASI odpowiada za sprawdzanie poprawności działania systemu IT, w szczególności: stacji roboczych, serwerów, drukarek, baz danych, poczty email.
6. ASI odpowiada za identyfikację i przyjmowanie zgłoszeń o nieprawidłowościach w działaniu systemu informatycznego oraz oprogramowania celem ich niezwłocznego usunięcia.
7. Wszelkie prace konserwacyjne i naprawcze sprzętu komputerowego oraz uaktualnienia systemu informatycznego, wykonywane przez podmiot zewnętrzny, powinny odbywać się na zasadach określonych w szczegółowej umowie z uwzględnieniem klauzuli dotyczącej ochrony danych.
8. Czynności konserwacyjne i naprawcze wykonywane doraźnie przez osoby nie posiadające upoważnień do przetwarzania danych (np. specjalistów z firm zewnętrznych), muszą być wykonywane pod nadzorem osób upoważnionych.
9. Przed przekazaniem uszkodzonego sprzętu komputerowego z danymi osobowymi do naprawy poza teren organizacji, należy:
    a. wymontować nośniki z danymi osobowymi,
    b. trwale usunąć dane osobowe z użyciem specjalistycznego oprogramowania,
    c. nadzorować proces naprawy przez osobę upoważnioną przez administratora systemu, gdy nie ma możliwości usunięcia danych z nośnika.

## *13.2. Aktualizacje oprogramowania*

1. ASI odpowiada za aktualizację oprogramowania zgodnie z zaleceniami producentów co do bezpieczeństwa i stabilności nowych wersji (np. aktualizacje, service pack-i, łatki).
2. ASI odpowiada za zapewnienie licencjonowanego oprogramowania do przetwarzania danych osobowych.