SPÓŁDZIELNIA MIESZKANIOWA
LOKATORSKO-WŁASNOŚCIOWA
„WŁASNE MIESZKANIE"
05-870 Błonie, ul. Traugutta 1 a
tel. 725-35-45, 725-47-13

Załącznik nr 4

**INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM**
**służącym do przetwarzania danych osobowych**
w
Spółdzielni
Mieszkaniowej Lokatorsko – Własnościowej
„Własne Mieszkanie" w Błoniu
KRS 0000036028, REGON 000492150, NIP 529-001-46-21
z siedzibą w Błoniu, ul. Traugutta 1A,
05-870 Błonie

1. **Podstawa prawna**
Niniejsza **INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM** służącym do przetwarzania danych osobowych w Spółdzielni Mieszkaniowej Lokatorsko – Własnościowej „Własne Mieszkanie" w Błoniu, zwana dalej „Instrukcją", stanowi wykonanie obowiązku, o którym mowa w § 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. z 2004 r. Nr 100, poz. 1024).

2. **Zakres stosowania**
Instrukcja określa zasady zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych. Administrator Danych Osobowych może wyznaczyć pracownika lub inna osobę do wykonywania jego obowiązków w zakresie zarządzania Systemem Informatycznym.

3. **Rejestrowanie i wyrejestrowanie użytkownika – nadawanie uprawnień.**
Użytkownikiem Systemu Informatycznego, mającym dostęp do danych osobowych (osobą upoważnioną) może być osoba, której nadano upoważnienie do przetwarzania danych osobowych zgodnie ze wzorem stanowiącym załącznik nr 2 do Polityki Bezpieczeństwa Informacji.

4. **Sposób uwierzytelniania użytkownika i zasady korzystania z haseł.**

1) Każdorazowe uwierzytelnienie użytkownika w systemie informatycznym następuje po podaniu identyfikatora i hasła.

2) W Spółdzielni Mieszkaniowej Lokatorsko – Własnościowej „Własne Mieszkanie" w Błoniu obowiązują następujące zasady korzystania z haseł:

   a. Hasło składa się z co najmniej z 8 znaków.

   b. Hasło musi zawierać co najmniej jedną małą literę, jedną wielką literę, jedną cyfrę oraz znaki specjalne.

   c. Co 30 dni hasło musi zostać zmienione.

2) Nieupoważnieni pracownicy nie mogą wykonywać kopii baz (zbiorów) danych oraz zapisywać na informatycznych nośnikach danych osobowych, w szczególności dokonywać kopii zapasowej całych zbiorów danych.

3) Dane osobowe w postaci elektronicznej, za wyjątkiem kopii bezpieczeństwa, mogą być wynoszone poza obszar przetwarzania danych osobowych określony w Polityce Bezpieczeństwa tylko w przypadku zapisania ich na przeznaczonym do tego komputerze przenośnym i przez upoważnionych do tego pracowników lub współpracowników.

4) Wymienne elektroniczne nośniki informacji zawierające dane osobowe są przechowywane w pomieszczeniach stanowiących obszar przetwarzania danych osobowych.

5) Po zakończeniu pracy przez użytkowników Systemu Informatycznego wymienne elektroniczne nośniki informacji zawierające dane osobowe są przechowywane w zamykanych szafach biurowych lub kasetkach.

6) Urządzenia, dyski lub inne informatyczne nośniki zawierające dane osobowe, przeznaczone do likwidacji, są pozbawiane przez Administratora Danych zapisu tych danych, a w przypadku, gdy nie jest to możliwe, są uszkadzane w sposób uniemożliwiający ich odczytanie.

7) Urządzenia, dyski lub inne informatyczne nośniki zawierające dane osobowe przeznaczone do naprawy są pozbawiane przez administratora danych zapisu tych danych.

8) Fizycznej likwidacji zniszczonych lub niepotrzebnych informatycznych nośników danych z danymi osobowymi należy dokonywać w sposób uniemożliwiający odczyt danych osobowych.

9) Dopuszczalne jest zlecenie/powierzenie niszczenia wszelkich nośników danych osobowych wyspecjalizowanym podmiotom zewnętrznym. Podstawą przekazania danych do zniszczenia innemu podmiotowi powinna być w każdym przypadku umowa zawarta na piśmie.

10) Dostęp do wydruków z Systemu Informatycznego zawierających dane osobowe mają wyłącznie osoby do tego upoważnione.

11) Wydruki są przechowywane w miejscu uniemożliwiającym bezpośredni do nich dostęp osobom niepowołanym.

## 8. Procedura i sposób zabezpieczenia przed oprogramowaniem, którego celem jest nieuprawniony dostęp do zasobów systemu informatycznego.

1) Na wszystkich komputerach (w tym także komputerach przenośnych) oraz serwerach zostało zainstalowane oprogramowanie antywirusowe oraz oprogramowanie zapobiegające nieuprawnionemu dostępowi do Systemu Informatycznego.
2) W przypadku stwierdzenia wystąpienia wirusa Administrator Danych zobowiązany jest do podjęcia działań zmierzających do wykrycia źródła pojawienia się wirusa w Systemie Informatycznym, jego wyeliminowania, a jeśli jest to niemożliwe – do usunięcia zainfekowango pliku.
3) W przypadku stwierdzenia nieprawidłowości działania Systemu Informatycznego Administrator Danych zobowiązany jest do niezwłocznego podjęcia czynności, związanych z usunięciem awarii.

## 9. Procedura usuwania awarii sprzętu lub oprogramowania.

1) W przypadku wystąpienia awarii Systemu Informatycznego pracownik lub współpracownik, który ją stwierdził zobowiązany jest do zgłoszenia faktu wystąpienia awarii Administratorowi Danych.
2) Administrator Danych zobowiązany jest do niezwłocznego podjęcia czynności zmierzających do usunięcia awarii np. poprzez wezwanie serwisu.
3) W przypadku stwierdzenia uszkodzenia danych zgromadzonych w Systemie, Administrator Danych, zobowiązany jest do otworzenia danych z ostatniej posiadanej kopii bezpieczeństwa (backup).
4) W przypadku gdy usunięcie awarii wymaga przekazania sprzętu komputerowego na zewnątrz, przed przekazaniem tego sprzętu Administrator Danych zobowiązany jest do usunięcia z dysków twardych wszystkich danych, po ich uprzednim skopiowaniu na inny nośnik. Jeśli z przyczyn technicznych jest to niemożliwe, Administrator Danych zobowiązany jest uzyskać od serwisanta protokół przyjęcia danych i zobowiązanie do zachowania ich poufności.

## 10. Sposób realizacji wymogu zapisania w systemie informatycznym informacji o odbiorcach danych.

1) Aktualnie dane osobowe nie są udostępniane innym podmiotom, niż wynika to z przepisów prawa.
2) W przypadku udostępniania danych osobowych w Systemie Informatycznym możliwe jest sporządzenie i wydrukowanie raportu, zawierającym następujące informacje:
   - identyfikatora osoby, której dane dotyczą;
   - odbiorcy danych;
   - zakresu udostępnienia danych osobowych;
   - daty operacji udostępnienia.

## 11. Sposób i czas przechowywania nośników informacji, w tym kopii informatycznych oraz wydruków.

1) Dokumenty papierowe zawierające dane osobowe przechowywane są wyłącznie w specjalnie do tego celu przeznaczonych segregatorach, w szafach zamykanych na klucz.
2) Nieupoważnieni pracownicy nie mogą wykonywać kopii baz danych oraz zapisywać - na informatycznych nośnikach danych - danych osobowych, w szczególności dokonywać kopii zapasowej całych zbiorów danych.
3) Fizycznej likwidacji zniszczonych lub niepotrzebnych informatycznych nośników danych z danymi osobowymi należy dokonywać w sposób uniemożliwiający odczyt danych osobowych.
4) Dopuszczalne jest zlecenie/powierzenie niszczenia wszelkich nośników danych osobowych wyspecjalizowanym podmiotom zewnętrznym. Podstawą przekazania danych

do zniszczenia innemu podmiotowi powinna być w każdym przypadku umowa zawarta na piśmie.

## 12. Procedury wykonywania przeglądów i konserwacji systemu informatycznego oraz informatycznych nośników danych.

1) Przegląd i konserwacja Systemu Informatycznego oraz informatycznych nośników danych zawierających dane osobowe dokonywane są poprzez:

   a. sprawdzanie zgodności danych z dokumentami;
   b. analizę zgłaszanych uwag użytkowników.

2) Przeglądu i konserwacji Systemu Informatycznego dokonuje Administrator Danych. Dopuszczalne jest zlecenie/powierzenie przeglądów i konserwacji zbiorów danych wyspecjalizowanym podmiotom zewnętrznym na podstawie pisemnych umów.
3) Przekazywane na zewnątrz informatyczne nośniki danych (komputery, dyski, laptopy), dla celów naprawy czy konserwacji, nie zawierają baz (zbiorów) danych osobowych.

## 13. Rozpowszechnianie i zarządzanie dokumentem.

1) Za zarządzanie Instrukcją, w tym jej rozpowszechnianie, aktualizację, utrzymywanie spójności z innymi dokumentami, jest odpowiedzialny Administrator Danych.
2) Z treścią niniejszego dokumentu powinny być zapoznane wszystkie osoby upoważnione do przetwarzania danych osobowych.

Członek Zarządu
Wojciech Mańkowski

PREZES ZARZĄDU
Karol Czerwiec

30.05.2022

**Oświadczam, że zapoznałem/zapoznałam się z INSTRUKCJĄ ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM służącym do przetwarzania danych osobowych**

| L.p. | Imię | Nazwisko | Podpis |
|---|---|---|---|
| 1 | Adam | Bukowski | |
| 2 | Karol | Czernic | |
| 3 | | | |
| 4 | | | |
| 5 | | | |
| 6 | | | |
| 7 | | | |
| 8 | | | |
| 9 | | | |
| 10 | | | |
| 11 | | | |
| 12 | | | |
| 13 | | | |
| 14 | | | |
| 15 | | | |
| 16 | | | |
| 17 | | | |
| 18 | | | |
| 19 | | | |
| 20 | | | |
| 21 | | | |
| 22 | | | |
| 23 | | | |
| 24 | | | |
| 25 | | | |
| 26 | | | |
| 27 | | | |
| 28 | | | |
| 29 | | | |
| 30 | | | |

| | | | |
|---|---|---|---|
| 31 | | | |
| 32 | | | |
| 33 | | | |
| 34 | | | |
| 35 | | | |
| 36 | | | |
| 37 | | | |
| 38 | | | |
| 39 | | | |
| 40 | | | |
| 41 | | | |
| 42 | | | |
| 43 | | | |
| 44 | | | |
| 45 | | | |
| 46 | | | |
| 47 | | | |
| 48 | | | |
| 49 | | | |
| 50 | | | |
| 51 | | | |
| 52 | | | |
| 53 | | | |
| 54 | | | |
| 55 | | | |
| 56 | | | |
| 57 | | | |
| 58 | | | |
| 59 | | | |
| 60 | | | |
| 61 | | | |
| 62 | | | |
| 63 | | | |