INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SPÓŁDZIELNI MIESZKANIOWEJ „MISTRZEJOWICE –PÓŁNOC” W KRAKOWIE

Zatwierdzono uchwałą Zarządu nr 121/31/2018 z dnia 22.08.2018

Zarząd
1. Prezes Zarządu – Elżbieta Okine Tyrkiel 2. Zastępca Prezesa Zarządu - Piotr Rusek 3. Członek Zarządu – Piotr Podsiadło

I. Podstawa prawna.

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych- zwanej dalej RODO
- 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 służce do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024 z poźn. zm.)

II. Przepisy ogólne.

§ 1

1. Instrukcja zarządzania systemem informatycznym Spółdzielni Mieszkaniowej „Mistrzejowice Północ" w Krakowie, zwana dalej instrukcją, opisuje sposoby nadawania uprawnień użytkownikom, określa sposób pracy w systemie informatycznym, procedury zarządzania oraz czynności mające wpływ na zapewnienie bezpieczeństwa systemu informatycznego oraz danych w nim zgromadzonych w tym danych osobowych.
2. Niniejsza instrukcja realizuje "Politykę bezpieczeństwa przetwarzania danych osobowych" obowiązującą w Spółdzielni Mieszkaniowej „Mistrzejowice - Północ".

III. Definicje.

§2

Ilekroć w niniejszym dokumencie jest mowa:

- System Informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji narzędzi programowych zastosowanych w celu przetwarzania danych.
- Administratorze Danych - należy przez to rozumieć Spółdzielnię Mieszkaniową „Mistrzejowice - Północ" w imieniu której działa Zarząd.
- Administratorze Bezpieczeństwa Informacji - należy przez to rozumieć pracownika wyznaczonego do nadzorowania przestrzegania zasad opisanych w niniejszej instrukcji.
- Administratorze Systemu Informatycznego - należy przez to rozumieć osobę lub firmę zewnętrzną odpowiedzialną na podstawie umowy za funkcjonowanie systemu informatycznego Spółdzielni Mieszkaniowej „Mistrzejowice - Północ".
- Użytkowniku systemu - należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
- Sieci lokalnej - należy przez to rozumieć fizyczne i logiczne połączenie systemów

informatycznych w Spółdzielni Mieszkaniowej „Mistrzejowice - Północ” z wykorzystaniem urządzeń telekomunikacyjnych,

- Sieci Internet - należy przez to rozumieć publiczną sieć telekomunikacyjną w rozumieniu ustawy Prawo telekomunikacyjne (Dz. U. Z 2004 r., Nr 171, poz. 1800, z późn. zm.)

IV. Procedury nadawania i zmiany uprawnień do przetwarzania danych.

§3

1. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych musi zapoznać się z:
   - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych – zwanej dalej RODO
   - 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 służce do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024 z poźn. zm.)
   - Polityką bezpieczeństwa obowiązującą w Spółdzielni Mieszkaniowej „Mistrzejowice - Północ”.
   - Instrukcją w sprawie udzielania i udostępniania informacji w Spółdzielni Mieszkaniowej „Mistrzejowice - Północ”.
   - niniejszym dokumentem, oraz posiadać upoważnienie do przetwarzania danych osobowych.
2. Zapoznanie się z powyższymi informacjami pracownik potwierdza własnoręcznym podpisem na oświadczeniu, którego wzór stanowi załącznik nr 1.
3. Administrator Danych przyznaje uprawnienia w zakresie dostępu do systemu informatycznego na podstawie pisemnego upoważnienia (wniosku) określającego zakres uprawnień pracownika, którego wzór stanowi załącznik nr 2.
4. Przyznanie uprawnień w zakresie dostępu do systemu informatycznego zawierającego również dane osobowe polega na wprowadzeniu do systemu dla każdego użytkownika unikalnego identyfikatora, hasła oraz zakresu dostępnych danych i operacji i odbywa się po podpisaniu oświadczeń o których mowa w ust 2 i 3.
5. Hasło ustanowione podczas przyznawania uprawnień przez Administratora Systemu

Informatycznego należy zmienić na indywidualne podczas pierwszego logowania się w systemie.

6. Pracownik ma prawo do wykonywania tylko tych czynności, do których został upoważniony.
7. Pracownik ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu.
8. W systemie informatycznym stosuje się uwierzytelnianie dwustopniowe na poziomie dostępu do systemu operacyjnego i sieci lokalnej oraz dostępu do aplikacji.
9. Odebranie uprawnień pracownikowi następuje na pisemny wniosek bezpośredniego przełożonego pracownika z podaniem daty oraz przyczyny odebrania uprawnień.
10. Bezpośredni przełożony zobowiązany jest pisemnie informować Administratora Danych o każdej zmianie dotyczącej pracowników mającej wpływ na zakres posiadanych uprawnień w systemie informatycznym.
11. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych niezwłocznie blokuje w systemie informatycznym oraz unieważnia hasło Administrator Systemu Informatycznego.
12. Administrator Systemu Informatycznego zobowiązany jest do prowadzenia i ochrony rejestru użytkowników i ich uprawnień w systemie informatycznym. Wzór rejestru stanowi załącznik nr 3.
13. Administrator Systemu Informatycznego zobowiązany jest do prowadzenia i ochrony rejestru nośników elektronicznych zawierających dane osobowe. Wzór rejestru stanowi załącznik nr 4.

V. Zasady posługiwania się hasłami.

§4

1. Bezpośredni dostęp do systemu informatycznego może mieć miejsce wyłącznie po podaniu identyfikatora osoby i właściwego hasła.
2. Dla każdego użytkownika Systemu informatycznego ustalony jest odrębny Identyfikator i hasło.
3. Identyfikator użytkownika nie może być zmieniany bez wyraźnej przyczyny, a po wyrejestrowaniu użytkownika z systemu informatycznego nie może zostać przydzielany innej osobie.
4. Hasło użytkownika powinno być zmieniane co najmniej raz w miesiącu.
5. Pracownicy są odpowiedzialni za zachowanie poufności swoich identyfikatorów i haseł.
6. Hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności.
7. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego

poznanie. W sytuacji, kiedy zachodzi podejrzenie, ze ktoś poznał hasło w sposób nieuprawniony, pracownik zobowiązany jest do natychmiastowej zmiany hasła i poinformowania o zaistniałym fakcie Administratora Bezpieczeństwa Informacji .

8. Przy wyborze hasła obowiązują następujące zasady:

- minimalna długość hasła - 8 znaków,
- zakazuje się stosowania haseł, które Użytkownik stosował uprzednio, swojego identyfikatora w jakiejkolwiek formie, swojego imienia, drugiego imienia, nazwiska, przezwiska, pseudonimu w jakiejkolwiek formie, imion (w szczegó1ności imion osób z najbliższej rodziny), ogó1nie dostępnych informacji o użytkowniku (numer telefonu, numer rejestracyjny samochodu, numeru PESEL, itp.)
- Należy stosować: hasła zwierające kombinacje liter i cyfr,
- Zmiany hasła nie wolno zlecać innym osobom.
- Zabrania się używania Identyfikatora lub hasła drugiej osoby.

VI. Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie.

§5

1. Pracownik po przyjściu do pracy uruchamia stację roboczą.
2. Przed uruchomieniem stacji roboczej pracownik jest zobowiązany do sprawdzenia czy nie zostały podłączone do stacji roboczej żadne niezidentyfikowane urządzenia.
3. Rozpoczęcie pracy w systemie komputerowym wymaga zalogowania się do systemu przy użyciu indywidualnego identyfikatora oraz hasła dostępu.
4. Przed opuszczeniem stanowiska pracy należy zablokować stację roboczą w taki sposób aby niemożliwe było uzyskanie doń dostępu przez osobę nieuprawnioną lub wylogować się z oprogramowania i systemu operacyjnego.
5. W trakcie pracy przy każdorazowym opuszczeniu stanowiska komputerowego należy dopilnować, aby na ekranie nie były wyświetlane dane osobowe.
6. Przed wyłączeniem komputera należy bezwzględnie zakończyć prace uruchomionych programów, wylogować się z systemu operacyjnego i wykonać zamknięcie systemu.
7. Niedopuszczalne jest wyłączanie komputera przed zamknięciem oprogramowania systemu operacyjnego.

VII. Procedury tworzenia kopii zapasowych.

§6

1. Za systematyczne przygotowanie kopii zapasowych odpowiada Administrator Systemu Informatycznego nadzorowany bezpośrednio przez Administratora

Bezpieczeństwa Informacji.

2. Kopie bezpieczeństwa wykonywane są na bieżąco.
3. Kopie bezpieczeństwa wykonywane są na twardych dyskach serwera.
4. Zachowuje się minimum 20 kopii bezpieczeństwa z poprzednich dni.
5. Wszystkie dane archiwizowane powinny zawierać informację o dokonanej dacie zapisu oraz Identyfikator osoby dokonującej archiwizacji.

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

§7

1. Elektroniczne nośniki informacji.
   a. Dane osobowe w postaci elektronicznej - za wyjątkiem kopii zapasowych - zapisane, płytach CD/DVD, dyskach twardych oraz na zewnętrznych nośnikach informacji nie mogą opuścić obszaru przetwarzania danych osobowych.
   b. Elektroniczne nośniki informacji są przechowywane w pokojach stanowiących obszar przetwarzania danych osobowych, w zamkniętych szafach lub metalowych kasetach.
   c. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a następnie uszkadza się w sposób mechaniczny.
   d. Elektroniczne nośniki informacji, zawierające dane osobowe, nie mogą zostać przekazane innemu podmiotowi nieuprawnionemu do dostępu do tych danych, nawet po uprzednim usunięciu danych z nośnika.
   e. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem Administratora Bezpieczeństwa Informacji.
   f. Zabrania się wynoszenia jakichkolwiek nośników zawierających dane osobowe z miejsca pracy.

2. Kopie zapasowe.
   a. Kopie zapasowe są przechowywane w serwerowni siedziby spółdzielni, winny być zabezpieczone przed dostępem osób nieupoważnionych, a także przed uszkodzeniem lub kradzieżą.
   b. Dostęp do danych opisanych w punkcie a ma Administrator Systemu Informatycznego oraz Administrator Bezpieczeństwa Informacji.
   c. Kopie które są już nieprzydatne należy zniszczyć fizycznie lub stosując wymazywanie poprzez wielokrotny zapis nieistotnych informacji w obszarze

zajmowanym przez dane kasowane (tzw. nadpisywanie plików).

XI. Sposób zabezpieczenia systemu informatycznego przed wirusami, szkodliwym oprogramowaniem, nieuprawnionym dostępem oraz awarią zasilania,

§8

1. System informatyczny jest zabezpieczony przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawionego dostępu oraz przed działaniami inicjowanymi z sieci zewnętrznej. Zabezpieczenie obejmuje m.in.:

a) w przypadku stacji roboczych:
   a. zabezpieczenie programem antywirusowym;
   b. zabezpieczenie programem typu „firewall”;
   c. szyfrowanie nośników danych;
   d. zabezpieczenie sieci radiowej uwierzytelnieniem kluczem WPA-2;
   e. zabezpieczenie przed skutkami awarii zasilania w postaci urządzenia typu UPS,
b) w przypadku sieci wewnętrznej:
   a. zabezpieczenie programem antywirusowym;
   b. zabezpieczenie programem typu „firewall”;
c) w przypadku skrzynek e-mailowych
   a. zabezpieczenie programem antywirusowym;
   b. zabezpieczenie programem antyspamowym;
   c. szyfrowanie danych.

§9

1. Na każdym stanowisku komputerowym musi być zainstalowane oprogramowanie antywirusowe z włączoną ochroną: antywirusową i antyspyware.
2. Każdy email wpływający na konta pocztowe spółdzielni musi być sprawdzony pod kątem występowania wirusów przez oprogramowanie antywirusowe.
3. Definicje wzorcowe wirusów aktualizowane są nie rzadziej niż 1 raz dziennie.
4. Bezwzględnie zabrania się używania nośników niewiadomego pochodzenia.
5. Bezwzględnie zabrania się pobierania z sieci Internet plików niewiadomego pochodzenia.
6. System Informatyczny jest automatycznie skanowany z częstotliwością zalecaną przez producenta programów – nie rzadziej niż 1 raz w miesiącu.
7. Aktualizacja bazy wirusów odbywa się poprzez automatyczne pobieranie bazy wirusów przez program antywirusowy.

8. W przypadku wykrycia wirusa należy:
   a) uruchomić program antywirusowy i skontrolować użytkowany system;
   b) usunąć wirusa z systemu przy wykorzystaniu programu antywirusowego
   c) powiadomić o zaistniałej sytuacji Administratora Danych.

   Jeżeli operacja usunięcia wirusa się nie powiedzie, należy:
   a) zakończyć pracę w systemie komputerowym;
   b) odłączyć zainfekowany komputer od sieci;
   c) powiadomić o zaistniałej sytuacji Administratora Danych.
9. Urządzenia i nośniki zawierające Dane osobowe przekazywane poza obszar, w którym są one przetwarzane, zabezpiecza się w sposób zapewniający poufność i integralność danych. Przekazywanie, o którym mowa powyżej winno odbywać się jedynie wyjątkowo i jedynie na wyraźne polecenie Administratora Danych. Rejestr nośników elektronicznych zawierających dane osobowe oraz szczegółowy regulamin użytkowania komputerów przenośnych stanowi załącznik nr 5.

X. Poczta elektroniczna.

§10

1. Pracownicy mogą korzystać z poczty elektronicznej w celach służbowych oraz w celach prywatnych w zakresie ograniczonym swoimi obowiązkami.
2. Administrator może mieć dostęp do treści wiadomości elektronicznych, wykorzystywanych przez pracowników, znajdujących się w Systemie informatycznym Administratora.
3. Zabronione jest otwieranie wiadomości e-mail pochodzących od nieznanego nadawcy bądź z podejrzanym tytułem (tzw. *phishing e-mail*). W szczególności zabronione jest jakiekolwiek otwieranie linków bądź pobieranie plików zapisanych w komunikacji zewnętrznej od nieznanego nadawcy.

XI. Procedury wykonywania przeglądów i konserwacji systemu.

§11

1. Przeglądy i konserwacja urządzeń.
   - Przeglądy i konserwacja urządzeń wchodzących w skład systemu informatycznego powinny być wykonywane w terminach określonych przez producenta sprzętu.
   - Nieprawidłowości ujawnione w trakcie tych działań powinny być niezwłocznie usunięte, a ich przyczyny przeanalizowane. O fakcie ujawnienia

nieprawidłowości należy zawiadomić Administratora Bezpieczeństwa Informacji.

2. Przeglądy programów i narzędzi programowych.
   - Konserwacja baz danych osobowych przeprowadzana jest zgodnie z zaleceniami twórców poszczególnych programów.
   - Administrator Systemu Informatycznego zobowiązany jest uaktywnić mechanizm zliczania nieudanych prób dostępu do systemu oraz ustawić blokady konta użytkownika po wykryciu trzech nieudanych prób, we wszystkich systemach posiadających taką funkcję.
3. Rejestracja działań konserwacyjnych, awarii oraz napraw.
   - Administrator Bezpieczeństwa Informacji prowadzi "Dziennik systemu Informatycznego Spółdzielni ". Wzór i zakres informacji rejestrowanych w dzienniku określony jest w załączniku nr 6.
   - Wpisów do dziennika może dokonywać Administrator Danych, Administrator Bezpieczeństwa Informacji lub Administrator Systemu Informatycznego.

XII. Połączenie do sieci Internet.

§12

Połączenie do sieci Internet jest realizowane poprzez sieć lokalną SM „Mistrzejowice- Północ" z zastosowaniem zaawansowanych metod ochrony za pomocą urządzenia „Fire Wall".

XIII. Polityka bezpieczeństwa.

§13

1. Dane osobowe przetwarzane są w pomieszczeniach budynku administracji spółdzielni oś. Bohaterów Września 26 w Krakowie.
2. Spółdzielnia przetwarza dane osobowe członków spółdzielni, właścicieli i najemców lokali w celu realizacji zadań statutowych.
3. Dla każdej osoby, której Dane osobowe są przetwarzane w Systemie informatycznym system zapewnia odnotowanie:
   a. daty pierwszego wprowadzenia danych do Systemu informatycznego;
   b. identyfikatora Użytkownika wprowadzającego Dane osobowe do systemu;
   c. informacji o odbiorcach, którym Dane osobowe zostały udostępnione.
4. Przetwarzanie danych w Spółdzielni odbywa się przy użyciu programu Zarządzania Obiegiem Dokumentów – Zakładu Usług Informatycznych „Mieszczanin", przy użyciu następujących modułów programu:
   a. Zarządzanie obiegiem dokumentów,

b. System łatwej obsługi nieruchomości,
c. Techniczna obsługa nieruchomości,
d. Nieruchomości, członkowie , wkłady,
e. Finanse i księgowość,
f. Kadry i płace,
g. Fakturowanie sprzedaży
h. Kasa.
i. Środki trwałe

5. Przetwarzanie i przeglądnie danych przy użyciu programu „Mieszczanin" przez uprawnionych pracowników odbywa się po uprzednim zalogowaniu do systemu przy pomocy identyfikatora i hasła.
6. Dane dotyczące rozliczeń pomiędzy użytkownikami mieszkań a spółdzielnią są publikowane na stronie internetowej spółdzielni. Użytkownicy lokali mają dostęp do swoich danych na podstawie indywidualnych kodów dostępu wygenerowanych przez Firmę „Mieszczanin".
7. Transmisja danych realizowana jest przez program Centrala firmy „Mieszczanin" za pomocą protokołu FTP. Dane przesyłane są do siedziby firmy „Mieszczanin" .

XIV. Środki bezpieczeństwa.

§14

W Spółdzielni Mieszkaniowej „Mistrzejowice Północ" stosuje się środki bezpieczeństwa na poziomie wysokim poprzez :

1. Zastosowanie zabezpieczeń logicznych i fizycznych.
2. Kontrolę przepływu informacji pomiędzy systemem informatycznym spółdzielni a siecią publiczną.
3. Przestrzeganie zasad niniejszej instrukcji.

Niniejsza Instrukcja Zarządzania Systemem Informatycznym została zatwierdzona przez zarząd spółdzielni w dniu 22 sierpnia 2018 uchwałą nr 121/31/2018./2018 i obowiązuje od dnia podjęcia uchwały.
Z dniem 23 sierpnia 2018 traci moc dotychczasowa obowiązująca Polityka Bezpieczeństwa oraz Instrukcja zarządzania Systemem Informatycznym w Spółdzielni Mieszkaniowej Mistrzejowice – Północ w Krakowie" z dnia 21.12.2011 roku uchwalona uchwałą nr 295/49/2011.

Załącznik nr 1

DO
INSTRUKCJI ZARZĄDZANIA
SYSTEMEM INFORMATYCZNYM
SPÓŁDZIELNI MIESZKANIOWEJ
“MISTRZEJOWICE –PÓŁNOC”
W KRAKOWIE

Oświadczam, ze zapoznałem się z przepisami dotyczącymi ochrony danych osobowych i zobowiązuję się do przestrzegania:

1. Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych- zwanej dalej RODO
2. Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Z 2004 r. nr 100, poz. 1024).
3. Polityki bezpieczeństwa przetwarzania danych osobowych w Spółdzielni Mieszkaniowej „Mistrzejowice- Północ” w Krakowie.
4. Instrukcją w sprawie udzielania i udostępniania informacji w Spółdzielni Mieszkaniowej „Mistrzejowice- Północ” w Krakowie.
5. Instrukcji zarządzania systemem informatycznym Spółdzielni Mieszkaniowej „Mistrzejowice- Północ ”w Krakowie.

Jednocześnie w czasie wykonywania swoich obowiązków służbowych zobowiązuje się do:

1. Zapewnienia ochrony danych osobowych przetwarzanych w zbiorach Spółdzielni Mieszkaniowej „Mistrzejowice- Północ” w Krakowie, zabezpieczenia przed udostępnianiem osobom trzecim i nieuprawnionym, zabraniem, uszkodzeniem oraz nieuzasadnioną modyfikacją lub zniszczeniem,
2. Zachowaniem w tajemnicy, także po ustaniu stosunku pracy, wszelkie informacje dotyczące funkcjonowania systemów lub urządzeń służących do przetwarzania danych osobowych oraz haseł dostępu do tych zbiorów.

Kraków dn…….. ……..

podpis pracownika

Załącznik nr 2
DO
INSTRUKCJI ZARZĄDZANIA
SYSTEMEM INFORMATYCZNYM
SPÓŁDZIELNI MIESZKANIOWEJ
“MISTRZEJOWICE –PÓŁNOC”
W KRAKOWIE

WNIOSEK O NADANIE UPRAWNIEŃ DO SYSTEMU INFORMATYCZNEGO W SPÓŁDZIELNI MIESZKANIOWEJ „MISTRZEJOWICE- PÓŁNOC” w KRAKOWIE

Rodzaj zmiany w systemie informatycznym: / niepotrzebne skreślić/.

1. Nowy użytkownik.
2. Modyfikacja uprawnień.
3. Odebranie uprawnień.

Imię i nazwisko użytkownika:	
Opis zakresu uprawnień Użytkownika w systemie Informatycznym:	

Data wystawienia: ……..

……..

Podpis Administratora Danych

Załącznik nr 3
DO
INSTRUKCJI ZARZĄDZANIA
SYSTEMEM INFORMATYCZNYM
SPÓŁDZIELNI MIESZKANIOWEJ
“MISTRZEJOWICE –PÓŁNOC”
W KRAKOWIE

REJESTR UŻYTKOWNIKÓW I ICH UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM W SPÓŁDZIELNI MIESZKANIOWEJ „MISTRZEJOWICE- PÓŁNOC” w KRAKOWIE

Lp.	Nazwisko i Imię (identyfikator)	System, moduł, zbiór danych osobowych	Data nadania upoważnienia	Data ustania uprawnień.
1				
2				

Data wystawienia: ……..

……..

Podpis Administratora Systemu Informatycznego

Załącznik nr 4

DO
INSTRUKCJI ZARZĄDZANIA
SYSTEMEM INFORMATYCZNYM
SPÓŁDZIELNI MIESZKANIOWEJ
“MISTRZEJOWICE –PÓŁNOC”
W KRAKOWIE

REJESTR NOŚNIKÓW ELEKTRONICZNYCH ZAWIERAJĄCYCH DANE OSOBOWE W SPÓŁDZIELNI MIESZKANIOWEJ „MISTRZEJOWICE- PÓŁNOC” w KRAKOWIE

l.p	Nazwa/oznaczenie nośnika	data włączenia nośnika do systemu	Opis nośnika	Miejsce przechowywania nośnika	Upoważniony pracownik do pracy z nośnikiem	Dodatkowe uwagi
1.	Komputer DELL Insprion 15	24 maja 2018 r	laptop	Pomieszczenie nr 1, szafa pancerna	Pani XYZ	nośnik w naprawie
2.						
3.						

Wpisane dane są przykładowe.

Data wystawienia: ……..

……..

Podpis Administratora Systemu Informatycznego

Załącznik nr 5

DO
INSTRUKCJI ZARZĄDZANIA
SYSTEMEM INFORMATYCZNYM
SPÓŁDZIELNI MIESZKANIOWEJ
"MISTRZEJOWICE –PÓŁNOC"
W KRAKOWIE

REGULAMIIN UŻYTKOWANIA KOMPUTERÓW PRZENOŚNYCH W SPÓŁDZIELNI MIESZKANIOWEJ „MISTRZEJOWICE- PÓŁNOC" W KRAKOWIE

1. Każdy pracownik użytkujący komputer przenośny musi zapoznać się z treścią Regulaminu oraz zobowiązać się do jego przestrzegania.
2. Każdy pracownik ma obowiązek należytego zabezpieczenia komputera przenośnego przed kradzieżą/zagubieniem/zniszczeniem/zhackowaniem.
   2.1. Komputer winien być transportowany w odpowiednim etui (teczka, torba, plecak) zabezpieczającym przed zniszczeniem komputera w trakcie transportowania.
   2.2. Pracownik nie może korzystać z komputera poza swoim stałym miejscem pobytu oraz miejscem pracy (ewentualnie: miejscem świadczenia pracy jeśli nie znajduje się ono w siedzibie Administratora); wykluczone jest korzystanie (transportowanie) komputera do restauracji, kawiarni, na spotkania towarzyskie i zawodowe (niewymagające korzystania z komputera) itp.
   2.3. W przypadku pozostawienia komputera w miejscu stałego pobytu, pracownik winien zadbać o to by nie miały do niego dostępu osoby nieuprawnione.
   2.4. Pracownik przed wyniesieniem komputera z siedziby Administratora winien dokonać kopii zapasowej systemu. Kopia winna być przechowywana w innym, niż komputer miejscu.
3. W przypadku stwierdzenia przez pracownika, że doszło do kradzieży/zagubienia/zniszczenia/zhackowania komputera zobowiązany jest on do natychmiastowego powiadomienia o tym fakcie Administratora, przekazując mu wszystkie informacje w tym zakresie.
4. Komputer przenośny może być wykorzystywany poza siedzibą

Administratora Danych, tylko i wyłącznie w celach służbowych oraz tylko i wyłącznie na podstawie zgody Administratora Danych.

5. Każdy pracownik musi zabezpieczyć komputer przenośny hasłem. Hasło musi zawierać co najmniej 8 znaków (w tym co najmniej: jedną małą literę, jedną wielką, jedną cyfrę i jeden znak specjalny).

Zapoznałam/em się z treścią Regulaminu użytkowania komputerów przenośnych i zobowiązuję się do przestrzegania w/w zasad.

_____

Data i *podpis pracownika*

Data przyjęcia regulaminu: ……..

……..

Podpis Administratora Danych

Załącznik nr 6

DO
INSTRUKCJI ZARZĄDZANIA
SYSTEMEM INFORMATYCZNYM
SPÓŁDZIELNI MIESZKANIOWEJ
“MISTRZEJOWICE –PÓŁNOC”
W KRAKOWIE

DZIENNIK SYSTEMU INFORMATYCZNEGO SPÓŁDZIELNI MIESZKANIOWEJ „MISTRZEJOWICE- PÓŁNOC” w KRAKOWIE.

Dziennik zawiera opisy wszystkich zdarzeń istotnych dla działania systemu informatycznego a w szczególności:

1. Opis awarii, przyczynę, szkody wynikłe na skutek awarii, sposób usunięcia awarii, opis systemu po awarii, wnioski.
2. Konserwację systemu – opis podjętych działań, wnioski.

Lp.	Data i godzina zdarzenia	Opis zdarzenia	Podjęte działania	Wnioski i Podpis.
1				
2				

……..

Podpis Administratora Systemu Informatycznego