POLITYKA BEZPIECZEŃSTWA INFORMACJI W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH W SPÓŁDZIELNI MIESZKANIOWEJ „ŁABĘDY'' w Pyskowicach

§1

1. Niniejszy dokument opracowany został w oparciu o Ustawę z dnia 29 sierpnia 1997r. o ochronie danych osobowych, Rozporządzenie 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 , Rozporządzenie Parlamentu Europejskiego UE2016/679 z dnia 27.04.206r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, Kodeksy Cywilny, Ustawę o własności lokali i Statut SM „Łabędy" w Pyskowicach i ma na celu zapewnienie każdemu członkowi Spółdzielni, użytkownikowi lokalu należącego do spółdzielczych zasobów mieszkaniowych i jej pracownikom ochronę ich prywatności.
2. Polityka bezpieczeństwa określa zakres, zasady i tryb przetwarzania i udostępniania danych osobowych, sposób zabezpieczenia zbiorów danych osobowych będących w posiadaniu Spółdzielni, a także obowiązki administrowania danych osobowych oraz prawa osób, których dane Spółdzielnia przetwarza.

§2

Przez użyte w treści Polityki bezpieczeństwa sformułowania należy rozumieć:

1) Dane osobowe- wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania na ich podstawie osoby fizycznej.
2) Zbiór danych- każdy posiadający strukturę zestaw danych osobowych dostępny wg określonych kryteriów, w którym dane są oraz w którym dane te mogą być przetwarzane, a w szczególności: kartoteki, rejestry, skorowidz, księgi, systemy informatyczne, akta osobowe ,itp.
3) Jawny rejestr danych osobowych – rejestr danych przetwarzanych przez administratora danych, zawierający nazwę zbioru oraz informacje, o których mowa w art. 41 ust. 1 pkt 2-4a i 7.
4) Przetwarzanie danych –wszelkie operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,
5) System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur i narzędzi programowych zastosowanych w celu przetwarzania danych,
6) Usuwanie danych - zniszczenie danych osobowych, lub taka ich modyfikacja, która nie pozwala na ustalenie tożsamości osoby, której dane dotyczą,
7) Administrator danych osobowych - administratorem danych osobowych członków Spółdzielni, użytkowników lokali spółdzielczych zasobów i jej pracowników oraz osób współpracujących ze Spółdzielnią jest Spółdzielnia Mieszkaniowa „Łabędy'' w Pyskowicach, a w jej imieniu Zarząd Spółdzielni,
8) Inspektor ochrony danych osobowych – inspektorem ochrony danych osobowych członków Spółdzielni, użytkowników lokali spółdzielczych zasobów i jej pracowników oraz osób współpracujących ze Spółdzielnią jest Spółdzielnia Mieszkaniowa „Łabędy'' w Pyskowicach, a w jej imieniu Zarząd Spółdzielni,

§3

Głównym celem zabezpieczenia zbiorów danych osobowych członków Spółdzielni, jej pracowników i osób współpracujących oraz ich przetwarzania jest uniemożliwienie dostępu do zbioru danych osobom nieuprawnionym, bądź zbierania ich przez osoby nieuprawnione oraz zabezpieczenie danych przed ich uszkodzeniem lub zniszczeniem.
Polityka bezpieczeństwa służy ochronie przed niepowołanym dostępem do:
a) systemu informatycznego oraz informacji udostępnianych z jego wykorzystaniem;
b) informacji zgromadzonych, przetwarzanych w formie tradycyjnej.
Niniejsze opracowanie określa politykę bezpieczeństwa w zakresie przetwarzania danych osobowych przez pracowników Spółdzielni Mieszkaniowej a w szczególności Kierowników komórek organizacyjnych i pracowników samodzielnych oraz administratorów systemów informatycznych. Dane osobowe Spółdzielni Mieszkaniowej „Łabędy" w Pyskowicach są gromadzone, przechowywane, edytowane, archiwizowane w kartotekach, skorowidzach, księgach, wykazach, rejestrach oraz w innych zbiorach ewidencyjnych, jak również w systemach informacyjnych na elektronicznych nośnikach informacji. Polityka bezpieczeństwa

wprowadza regulacje w zakresie organizacji procesu przetwarzania i odnosi się swoja treścią informacji:
1) w formie papierowej- przetwarzanej w ramach systemu tradycyjnego;
2) w formie elektronicznej- przetwarzanych w ramach systemu informacyjnego.
Bezpośredni nadzór nad przetwarzaniem danych osobowych sprawują kierownicy komórek organizacyjnych w przypadku stanowisk samodzielnych pracownicy samodzielni.
Z zapisami w polityce bezpieczeństwa obowiązkowo są zapoznawani wszyscy użytkownicy systemów informatycznych i tradycyjnych. Do informacji przechowywanych w systemach informatycznych jak i dokumentów tradycyjnych mają dostęp jedynie upoważnieni pracownicy Spółdzielni Mieszkaniowej. Wszyscy pracownicy zobowiązani są do zachowania tych danych w tajemnicy. Każdy użytkownik systemu informatycznego zobowiązany jest zapamiętać swój identyfikator i hasło i nie udostępniać go innym osobom. Użytkownik systemu informatycznego powinien pamiętać o wylogowaniu się po zakończeniu korzystania z usług informatycznych.

§4

1.Spółdzielnia jako administrator danych osobowych przetwarza dane osobowe swoich członków dla realizacji celów statutowych w zakresie:
1) prowadzenia rejestru członków,
2) prowadzenia rejestru lokali, dla których zostały założone księgi wieczyste z adnotacja o ustanowionych hipotekach,
3) gromadzenia i przetwarzanie danych osobowych zawartych w indywidualnych aktach członków Spółdzielni,
4) sporządzania rejestrów niezbędnych do obliczania opłat za użytkowanie lokali,
5) sporządzania list niezbędnych do funkcjonowania organów samorządowych Spółdzielni,
6) sporządzania zestawień i analiz związanych z eksploatacja zasobów mieszkaniowych i lokali użytkowych,
7) prowadzenia korespondencji z właścicielami, użytkownikami lokali mieszkalnych i użytkowych,
8) wywieszania korespondencji z właścicielami, użytkownikami lokali mieszkalnych i użytkowych

2. Spółdzielnia jako administrator danych osobowych przetwarza dane osobowe swoich pracowników w zakresie określonym przepisami Kodeksu pracy, poprzez gromadzenie i przetwarzanie akt osobowych pracowników Spółdzielni.
3. W celu wypełnienia ustawowego obowiązku Spółdzielnia prowadzi Jawny rejestr zbiorów danych osobowych przetwarzanych w SM „Łabędy" w Pyskowicach

§5.

ADMINISTRACJA I ORGANIZACJA BEZPIECZEŃSTWA

1. Za bezpieczeństwo danych osobowych przetwarzanych w systemach przetwarzania danych osobowych odpowiada inspektor ochrony danych osobowych. Kierownicy komórek

organizacyjnych, pracownicy samodzielni obowiązani są zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, a w szczególności powinni zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą uszkodzeniem lub zniszczeniem. Inspektor wykonuje wszystkie prace niezbędne do efektywnego oraz bezpiecznego zarządzania systemami informatycznymi i tradycyjnymi. Szczegółowy zakres odpowiedzialności i obowiązków:

a) nadzoruje bezpieczeństwo systemów informatycznych tradycyjnych,

b) nadzoruje przestrzeganie przez wszystkich użytkowników stosowanie obowiązujących procedur

c) doradza użytkownikom w zakresie bezpieczeństwa,

d) zapewnia, aby pracownicy posiadający dostęp do systemu informatycznego posiadali nadane pisemne upoważnienie do przetwarzania danych osobowych,

e) prowadzi kontrole w zakresie bezpieczeństwa,

f) prowadzi ewidencje osób, którym nadano upoważnienie do przetwarzania danych osobowych,

g) przygotowuje wnioski pokontrolne dla administratora danych osobowych.

h) prowadzi wykaz podmiotów, którym udostępniono dane osobowe,

i) prowadzi wykaz podmiotów, którym powierzono dane osobowe do przetwarzania,

j) prowadzi wykaz zbioru danych osobowych

3. Osobowy upoważnione do przetwarzania danych osobowych maja obowiązek:

- przetwarzać je zgodnie z przepisami,
- nie udostępniać ich oraz uniemożliwić dostęp do nich osobom nieupoważnionym,
- zabezpieczać je przed zniszczeniem

4. Użytkownik systemu informatycznego wykonuje wszystkie prace niezbędne do efektywnej oraz bezpiecznej pracy na stanowisku pracy również z wykorzystaniem stacji bezpieczeństwa w szczególność do przestrzegania procedur dostępu do systemu i ochrony danych osobowych.

INSPEKTOR OCHRONY DANYCH

Inspektor ochrony danych pełni jeszcze ważniejszą rolę w systemie ochrony danych aniżeli dotychczas funkcjonujący ABI. Inspektor ochrony danych, tak jak dotychczas ABI, podlegać będzie bezpośrednio Zarządowi. Inspektor zobowiązany jest m.in. do:

- informowania administratora oraz pracowników o obowiązkach spoczywających na nich na mocy Rozporządzenia oraz innych przepisów,
- monitorowania przestrzegania Rozporządzenia oraz innych przepisów Unii i państw członkowskich oraz polityk administratora lub procesora,
- szkolenia personelu uczestniczącego w operacjach przetwarzania
- przeprowadzania systematycznych audytów,
- udzielania wskazówek administratorowi w przedmiocie wdrożenia odpowiednich i skutecznych środków technicznych jak również organizacyjnych mających zabezpieczyć dane osobowe oraz jak wykazać przestrzeganie prawa przez administratora lub podmiotu przetwarzającego dane w szczególności jeżeli chodzi o

identyfikowanie ryzyka związanego z przetwarzaniem, o jego ocenę pod katem źródła, charakteru, prawdopodobieństwa i wagi zagrożenia oraz o najlepsze praktyki pozwalające zminimalizować to ryzyko,

- udzielania na żądanie zaleceń co do oceny skutków oraz monitorowanie ich wykonania w przypadku, gdy administrator danych przed rozpoczęciem przetwarzania zobowiązany jest do przeprowadzenia oceny skutków planowanych operacji przetwarzania dla ochrony danych.

UDOSTĘPNIENIE POSIADANYCH DANYCH W ZBIORACH DANYCH OSOBOWYCH

1. Dostęp do rejestru członków mają wszyscy członkowie Spółdzielni i ich współmałżonkowie oraz wierzyciele członka Art. 30 Prawa spółdzielczego.
2. Dostęp do rejestru danych określonych w § 4 p.1 ppkt 2÷8 mają pracownicy biura Spółdzielni, którzy uzyskali pisemne upoważnienie wydane przez zarząd Spółdzielni oraz członkowie Spółdzielni pełniący funkcje w organach Spółdzielni w zakresie związanym z pełnioną funkcją.
3. Każdy z pracowników Spółdzielni podpisuje oświadczenie o przestrzeganiu przepisów w zakresie ochrony danych osobowych i nie wykorzystywaniu danych w innych celach niż są one niezbędne do wykonania czynności zgodnie z poleceniem lub zakresem obowiązków służbowych i pełnionych funkcji.
4. Każdy, kto uzyskał dostęp do zbioru danych osobowych zgodnie z § 5 p.1 zobowiązany jest do założenia oświadczenia o zachowaniu ich w tajemnicy, które jest przechowywanie w Spółdzielni.
5. Członkowie Rady Nadzorczej oraz pracownicy podpisują oświadczenie o zapoznaniu się z przepisami o ochronie danych osobowych i zachowaniu w tajemnicy danych osobowych, które uzyskali w związku z pełnioną funkcją w Radzie Nadzorczej i zatrudnieni w Spółdzielni.

§6.

1. Dane osobowe członków Spółdzielni i jej pracowników są przechowywane i przetwarzane w pomieszczeniach Spółdzielni.
2. Bezpieczeństwo danych osobowych zapewniane jest przez pracowników, których zakres obowiązków jest z nimi związany.
3. Pomieszczenia, w których są gromadzone, przechowywane i przetwarzane dane osobowe są zamykane na czas nieobecności w nich osób zatrudnionych.
4. Osoby niezatrudnione mogą przebywać w pomieszczeniach spółdzielni, w których są przechowywane dane osobowe tylko w obecności osób zatrudnionych lub członków Zarządu Spółdzielni.

§7.

1. Zarząd Spółdzielni może udostępnić dane osobowe członków Spółdzielni Walnemu Zgromadzeniu i Radzie Nadzorczej jedynie w przypadku, gdy w sprawie danego członka toczy się postępowanie wewnątrzspółdzielcze w trybie określonym postanowieniami

Statutu Spółdzielni, gdy związane jest ono z potrzebą dotyczącą eksploatacji i zarządzania zasobami Spółdzielni lub prowadzoną działalnością gospodarczą.

2. Dane osobowe członka Spółdzielni mogą być udostępnione organom samorządowym Spółdzielni rozpatrującym jego sprawę w postępowaniu wewnątrzspółdzielczym tylko w zakresie mogącym mieć znaczenie dla danej sprawy.
3. Zarząd Spółdzielni jest zobowiązany do poinformowania członków samorządowych Spółdzielni rozpatrującym sprawę członka Spółdzielni w postępowaniu wewnątrzspółdzielczym lub posługującym się danymi osobowymi w sprawach związanych z wypełnianiem swoich funkcji – o przepisach dotyczących ochrony danych osobowych.
4. Udostępnianie danych osobowych przetwarzanych przez Spółdzielnie może nastąpić podmiotom lub osobom uprawnionym do ich otrzymania na mocy przepisów prawa.
5. Dane osobowe z wyłączeniem danych osobowych, o których mowa w art.27 ust.1 Ustawy o ochronie danych osobowych mogą być udostępnione w celach innych niż włączenie do zbioru, innym osobom i podmiotom niż wymienione w ust.4 na pisemnie umotywowany wniosek, jeżeli w sposób wiarygodny uzasadnią potrzebę posiadania tych danych, a ich udostępnienie nie narusza praw i wolności osób, których dane dotyczą.
6. Spółdzielnia może odmówić udostępnienia danych osobowych swoich członków i pracowników w przypadkach określonych Ustawą o ochronie danych osobowych art.30.
7. Umieszczenie nazwiska członka Spółdzielni lub użytkownika mieszkania na liście lokatorów lub przy instalacji domofonowej jest możliwe po wyrażeniu pisemnej zgody osoby, której dotyczą dane.

§8.

OCHRONA DANYCH OSOBOWYCH PRZETWARZANYCH W SYSTEMIE INFORMATYCZNYM

1. System komputerowy SM „Łabędy" w Pyskowicach zainstalowany jest na zestawach komputerowych przypisanych do poszczególnych działów zgodnie z zatwierdzoną strukturą organizacyjną Spółdzielni.
2. Dostęp do komputerów lub jego części posiadają poszczególni pracownicy, którzy wykonują czynności z wykorzystaniem oprogramowania oraz danych i zbiorów wchodzących w skład oprogramowania. W skład oprogramowania wchodzi systemowe oprogramowanie firmy M. Informatyka Sp. z o.o. Sp. K. i firmy „PIK" oraz oprogramowanie narzędziowe zakupione razem z komputerami.
3. Każdy pracownik posiada odrębny identyfikator i hasło pozwalające na użytkowanie wybranego zakresu oprogramowania w ramach którego przetwarza dane, które jest odnotowane w teczce osobowej pracownika.
4. Konserwację, modyfikację oraz uaktualnienie oprogramowania wykonują przedstawiciele autora oprogramowania firmy M. Informatyka Sp. z o.o. Sp. K.
5. Funkcję inspektora ochrony danych osobowych w SM „Łabędy" w Pyskowicach pełni Zarząd.

6. Pracownik zatrudniony przy przetwarzaniu danych osobowych w systemie informatycznym obowiązany jest niezwłocznie powiadomić inspektora bezpieczeństwa, gdy:
   1) stwierdzi naruszenie zabezpieczeń informatycznych,
   2) stan urządzeń, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakości komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszanie zabezpieczeń tych danych.
7. Inspektor ochrony danych osobowych po potwierdzeniu naruszenia systemu informatycznego ma obowiązek :
   1) zabezpieczyć ślady pozwalające na określenie przyczyn naruszenia systemu informatycznego,
   2) przeanalizować i określić skutki naruszenia informatycznego,
   3) określić czynniki, które spowodowały naruszenie systemu informatycznego,
   4) dokonać niezbędnych korekt w systemie informatycznym polegających na zabezpieczeniu systemu przed ponownym jego naruszeniem,
   5) powiadomić organa ścigania, jeżeli skutki noszą znamiona przestępstwa oraz gdy sposób naruszenia i skutki mogą być powtórzone w innym miejscu lub przyszłości.
8. Prowadzony jest rejestr pracowników – użytkowników systemu informatycznego oraz mających dostęp do danych osobowych zawierający :
   -imię i nazwisko pracownika,
   -stanowisko,
   -zakres, w jakim pracownik został dopuszczony do przetwarzania danych osobowych,
   -datę wydania upoważnienia,
   -indywidualny identyfikator pracownika.
9. System informatyczny powinien zapewnić odnotowanie :
   1) daty wprowadzenia i modyfikacji danych osobowych,
   2) identyfikatora użytkownika systemu wprowadzającego dane,
   3) informację, kiedy i w jakim zakresie dane zostały wygenerowane przez system.
10. Sposób przechowywania i dystrybucje wygenerowanych danych określa Zarząd Spółdzielni.
11. W pomieszczeniu biurowym Spółdzielni, osoby niezatrudnione mogą przebywać jedynie w obecności osoby zatrudnionej i za zgodą Zarządu Spółdzielni.
12. Pomieszczenia, w których są przechowywane lub przetwarzane dane osobowe muszą być zamykane na czas nieobecności osób w nich zatrudnionych w taki sposób, aby uniemożliwić dostęp do nich osób nieuprawnionych.
13. Wprowadzający oraz przetwarzający dane wykonują kopie awaryjne danych w okresach tygodniowych, miesięcznych i rocznych, które są przechowywane w pomieszczeniach archiwum Spółdzielni.
14. Kopie awaryjne należy :
   1) okresowo sprawdzić pod kątem ich dalszej przydatności do odtworzenia danych w przypadku awarii systemu,
   2) bezzwłocznie usuwać po ustaniu ich użyteczności,

3) kopie przeznaczone do archiwizowania po odpowiednim oznakowaniu złożyć do archiwum Spółdzielni.

§9.

1. Osoba, której dane przetwarzane są przez Spółdzielnie ma prawo :
   1) do informacji o:
      -sposobie i zakresie przetwarzania danych osobowych,
      -treści danych,
      -sposobie udostępniania danych oraz odbiorcami lub kategorii odbiorców danych.
   2) żądania uzupełnienia, uaktualnienia i sprostowania danych osobowych.
2. Informacji, o których mowa w ust. 1 Zarząd Spółdzielni jest zobowiązany udzielić w terminie 30 dni od otrzymania wniosku.

§10.

1. Wgląd do indywidualnej teczki członka może mieć tylko członek, którego teczka dotyczy, Zarząd oraz osoby zatrudnione przy przetwarzaniu danych mające upoważnienie Zarządu Spółdzielni.
2. W przypadku, gdy w sprawie danego członka toczy się postępowanie wewnątrzspółdzielcze, dane zawarte w jego indywidualnej teczce mogą być udostępnione organowi samorządowemu rozpatrującemu sprawę, ale tylko w zakresie danych mogących mieć znaczenie dla sprawy.
3. Wgląd do rejestru lokali, dla których zostały założone księgi wieczyste wraz z adnotacją o ustanowionych hipotekach, mogą mieć tylko osoby upoważnione przez Zarząd.
4. Wgląd do danych gromadzonych dla zapewnienia prawidłowego wymiaru opłat za używanie lokalu mogą mieć tylko osoby zatrudnione przy przetwarzaniu danych osobowych, mające upoważnienie Zarządu Spółdzielni oraz upoważniony przedstawiciel podmiotu, któremu Spółdzielnia zleca wykonanie określonych rozliczeń.
5. Wgląd do danych osób zatrudnionych w Spółdzielni mogą mieć tylko osoby, których dane te dotyczą, Zarząd Spółdzielni oraz osoby zatrudnione przy przetwarzaniu danych, mające upoważnienie Zarządu Spółdzielni. Udostępnienie tych danych innym osobom lub podmiotom jest możliwe tylko wtedy, gdy obowiązek taki wynika z przepisów prawa.

§11.

POLITYKA ANTYWIRUSOWA

W zakresie ochrony antywirusowej wprowadza się następujące zalecenia:
a) nie należy używać oprogramowania na stacjach roboczych innego niż zaleca administrator systemu,
b) zabrania się instalowania oprogramowania typu freeware czy shareware,
c) regularnie uaktualniać bazę wirusów zainstalowanego oprogramowania antywirusowego,

d) przed użyciem nośnika danych sprawdzić czy nie jest zainfekowany wirusem komputerowym,

§12.

INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Instrukcja jest przeznaczona dla osób zatrudnionych przy przetwarzaniu danych osobowych.

2. Za naruszenie ochrony danych osobowych uznaje się przypadki, gdy:

1) stwierdzono naruszenie zabezpieczenia systemu informatycznego lub naruszenie zabezpieczenia zbioru danych osobowych zebranych i przetwarzanych w innej formie,
2) stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń tych danych.

3. Każdy pracownik Jednostki, który stwierdzi lub podejrzewa naruszenie ochrony danych osobowych w systemie informatycznym (lub przetwarzanych w inny sposób) zobowiązany jest do niezwłocznego poinformowania o tym administratora tego systemu informatycznego lub w przypadku jego nieobecności inspektora ochrony danych.

4. Dane osobowe zostają ujawnione, gdy stają się znane w całości lub części pozwalającej na określenie osobom nieuprawnionym tożsamości osoby, której dane dotyczą.

5. W stosunku do danych, które zostały zagubione, pozostawione bez nadzoru poza obszarem bezpieczeństwa należy przeprowadzić postępowanie wyjaśniające, czy dane osobowe należy uznać za ujawnione.

6. Inspektor ochrony danych osobowych, który stwierdził lub uzyskał informację wskazującą na naruszenie ochrony tej bazy danych zobowiązany jest do niezwłocznego:

1) zapisania wszelkich informacji i okoliczności związanych z danym zdarzeniem, a w szczególności dokładnego czasu uzyskania informacji o naruszeniu ochrony danych osobowych lub samodzielnym wykryciu tego faktu,
2) jeżeli zasoby systemu na to pozwalają, wygenerowania i wydrukowania wszystkich dokumentów i raportów, które mogą pomóc w ustaleniu wszelkich okoliczności zdarzenia, opatrzenia ich datą i podpisania,
3) przystąpienia do zidentyfikowania rodzaju zaistniałego zdarzenia, w tym do określenia skali zniszczeń, metody dostępu osoby niepowołanej do danych itp.
4) podjęcia odpowiednich kroków w celu powstrzymania lub ograniczenia dostępu osoby niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów naruszenia ochrony danych, w tym m.in.
   a) fizycznego odłączenia urządzeń i segmentów sieci które mogły umożliwić dostęp do bazy danych osobie niepowołanej,
   b) wylogowania użytkownika podejrzanego o naruszenie ochrony danych,

c) zmianę hasła na konto administratora i użytkownika poprzez którego uzyskano nielegalny dostęp w celu uniknięcia ponownej próby uzyskania takiego dostępu.

5) szczegółowej analizy stanu systemu informatycznego w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych,

6) przywrócenia normalnego działania systemu, przy czym, jeżeli nastąpiło uszkodzenie bazy danych, odtworzenia jej z ostatniej kopii awaryjnej z zachowaniem wszelkich środków ostrożności mających na celu uniknięcie ponownego uzyskania dostępu przez osobę nieupoważnioną, tą samą drogą.

7. Po przywróceniu normalnego stanu bazy danych osobowych należy przeprowadzić szczegółową analizę w celu określenia przyczyn naruszenia ochrony danych osobowych lub podejrzenia takiego naruszenia, oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.

8. Jeżeli przyczyną zdarzenia był błąd użytkownika systemu informatycznego, należy przeprowadzić szkolenie wszystkich osób biorących udział w przetwarzaniu danych.

9. Jeżeli przyczyną zdarzenia była infekcja wirusem należy ustalić źródło jego pochodzenia i wykonać zabezpieczenia antywirusowe i organizacyjne wykluczające powtórzenie się podobnego zdarzenia w przyszłości.

10. Jeżeli przyczyną zdarzenia było zaniedbanie ze strony użytkownika systemu należy wyciągnąć konsekwencje dyscyplinarne wynikające z kodeksu pracy oraz ustawy o ochronie danych osobowych.

11. Inspektor ochrony danych osobowych, w której nastąpiło naruszenie ochrony danych osobowych przygotowuje szczegółowy raport o przyczynach, przebiegu i wnioskach ze zdarzenia.

§13.

Niniejszy dokument stanowiący Politykę bezpieczeństwa Spółdzielni zatwierdzono Uchwałą Zarządu Nr. 21/2018 z dnia 23.05.2018

Postanowienia Polityki bezpieczeństwa obowiązują od dnia jego uchwalenia i odnoszą się do danych wytworzonych i przetwarzanych w Spółdzielni Mieszkaniowej „Łabędy" w Pyskowicach przed jego uchwaleniem.

Uchwała Nr 21/2018

Zarządu Spółdzielni Mieszkaniowej „Łabędy"

w Pyskowicach z dnia 23.05.2018 roku.

w sprawie: zatwierdzenia Polityki Bezpieczeństwa Informacji w zakresie przetwarzania danych osobowych w Spółdzielni Mieszkaniowej „Łabędy" w Pyskowicach

Na podstawie art. 48 ustawy z dnia 16 września 1982 Prawo spółdzielcze oraz § 78 ust.1 Statutu Spółdzielni Mieszkaniowej „Łabędy" w Pyskowicach,

Zarząd Spółdzielni Mieszkaniowej „Łabędy" w Pyskowicach postanawia :

§ 1

1. Zatwierdzić Politykę Bezpieczeństwa Informacji w zakresie przetwarzania danych osobowych w Spółdzielni Mieszkaniowej „Łabędy" w Pyskowicach.

§ 2

Uchwała wchodzi w życie z dniem podjęcia.

ZARZĄD SPÓŁDZIELNI MIESZKANIOWEJ
"ŁABĘDY"
W PYSKOWICACH