Polityka Bezpieczeństwa Informacji

Spółdzielnia Mieszkaniowa Lokatorsko – Własnościowa w Raciążu

zwana dalej SMLW

RACIĄŻ 2018

Spis treści

Załączniki:

Załącznik nr 1 - Wykaz regulacji wewnętrznych i dokumentów stanowiących dokumenty powiązane z Polityką Bezpieczeństwa Informacji

Załącznik nr 2 - Wzór oświadczenia o stosowaniu się do zapisów Polityki bezpieczeństwa

Załącznik nr 3 - Słownik pojęć wykorzystywanych w regulacjach wewnętrznych związanych z Polityką bezpieczeństwa informacji

I. WSTĘP

§ 1
Cel Polityki

Polityka bezpieczeństwa informacji, zwana dalej „Polityką” ma na celu zapewnienie bezpieczeństwa informacji przetwarzanej w SMLW umożliwiającej działanie SMLW zgodne z jej misją, wymaganiami prawa, normami nadzorczymi, a także mająca na uwadze zobowiązania SMLW płynące z zawartych umów.

§ 2
Zaangażowanie organów SMLW

Zarząd SMLW oświadcza, że będzie podejmować wszelkie działania w celu zapewnienia bezpieczeństwa informacji w tym ochrony danych osobowych w SMLW, w tym także w zakresie przyjęcia, wdrożenia i nadzoru nad stosowaniem zasad niniejszej Polityki przez pracowników i inne osoby zatrudnione, a także podmioty trzecie świadczące usługi dla SMLW.

§ 3
Zakres Polityki

1. Niniejsza Polityka określa podstawowe zasady, normy i wymagania zgodności w zakresie bezpieczeństwa informacji przetwarzanej w SMLW, a także:
    1) polityki zarządzania incydentami naruszenia bezpieczeństwa informacji, w tym incydenty naruszenia bezpieczeństwa środowiska teleinformatycznego;
    2) polityki w zakresie zasad udostępniania informacji podmiotom zewnętrznym;
    3) polityki w zakresie zarządzania architekturą i jakością danych;
    4) polityki ochrony danych osobowych.
2. Niniejszy dokument został opracowany w oparciu o najlepsze praktyki z obszaru bezpieczeństwa informacji oraz w sposób niesprzeczny z wymaganiami norm PN-ISO/IEC 27001, PN-ISO/IEC 17799 (ISO/IEC 27002).

§ 4
Struktura i zakres regulacji wewnętrznych w zakresie bezpieczeństwa informacji

1. W przyszłości za dokumenty związane z niniejszą Polityką będą uznawane także wszystkie dokumenty niższych poziomów takie jak procedury, instrukcje, zasady i regulaminy zgodne z niniejszą Polityką.
2. W szczególności są to dokumenty bezpośrednio wymienione w Załączniku nr 1 do niniejszej Polityki, a także „Dokumentacja systemu zarządzania bezpieczeństwem informacji i systemów przetwarzania danych” powstała w wyniku stosowania regulacji wymienionych w Załączniku nr 1.

§ 5
Przeglądy Polityki

1. Niniejsza Polityka podlega przeglądom zarządczym i weryfikacji zgodnie z odpowiednimi regulacjami wewnętrznymi dotyczącymi przeglądów zarządczych w SMLW.

2. Przeglądy powinny być dokonywane co najmniej raz do roku lub też w trakcie roku w przypadku wystąpienia znaczących zmian, powinny obejmować weryfikację zasad i ewentualne dostosowanie Polityki do zmieniającego się profilu ryzyka SMLW, zmian środowiska organizacyjnego, warunków biznesowych, środowiska technicznego, a także w zakresie zachowania zgodności z przepisami prawa i normami nadzorczymi.
3. Wszelkie zmiany w niniejszej Polityce wymagają akceptacji Zarządu SMLW.

II. TERMINOLOGIA

§ 6
Definicje i terminologia

Podstawowe pojęcia stosowane w regulacjach wewnętrznych dotyczących bezpieczeństwa informacji i systemów teleinformatycznych w SMLW zostały zawarte w Załączniku nr 3 do niniejszej Polityki.

III ZADANIA I ODPOWIEDZIALNOŚĆ

§ 7
Nadzór

1. Zarząd SMLW nadzoruje bezpieczeństwo informacji, w tym funkcjonowanie obszarów technologii informacyjnej i obszaru bezpieczeństwa środowiska teleinformatycznego.
2. Sprawując swój nadzór szczególną uwagę poświęcają zagadnieniom:
   1) zarządzania bezpieczeństwem środowiska teleinformatycznego oraz ciągłością działania;
   2) procesowi tworzenia i aktualizacji strategii w obszarach technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego;
   3) zarządzania elektronicznymi kanałami dostępu;
   4) współpracy z zewnętrznymi dostawcami usług w zakresie środowiska teleinformatycznego i jego bezpieczeństwa;
   5) zapewnienia adekwatnej struktury organizacyjnej oraz zasobów kadrowych w obszarach technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego,
   6) zarządzania jakością danych o kluczowym znaczeniu dla SMLW;
   7) realizację procesów planowania, zgodnie z regulacjami wewnętrznymi w zakresie planowania strategicznego dotyczącego obszaru technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego;
   8) sporządzenie projektów odpowiednich planów strategicznych;
   9) wdrożeniu struktury organizacyjnej w zakresie bezpieczeństwa informacji, w tym obszaru technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego, zapewniającej zapobieganiu konfliktu interesów;
   10) zapewnienie odpowiedniej efektywności zarządzania ryzykiem bezpieczeństwa;
   11) przyjmowanie bieżących informacji o poziomie ryzyka, wynikach testów procedur planów i procedur awaryjnych, wynikach przeglądów zarządczych, a także wynikach kontroli wewnętrznej i audytu wewnętrznego, jak również audytów zewnętrznych;
   12) podejmowanie działań zmierzających do zmniejszenia ryzyka, w przypadkach jego nadmiernego wzrostu;

13) nadzór nad przestrzeganiem polityki bezpieczeństwa informacji w pracy SMLW;
14) promowanie i wymaganie postaw zgodnych z zasadami przyjętymi w SMLW, w tym reakcja na nieprawidłowości, w tym incydenty związane z bezpieczeństwem informacji.

§ 8
Administrator Systemów Informatycznych

1. Administrator Systemów Informatycznych (ASI) zapewnia efektywne działanie środowiska teleinformatycznego SMLW.
2. ASI powołuje Zarząd SMLW.
3. ASI w ramach swoich zadań:
   1) dba o poprawne i efektywne działanie administrowanych systemów;
   2) świadczy wsparcie techniczne dla użytkowników systemów, zapewniających sprawne i bezpieczne funkcjonowanie procesów SMLW;
   3) świadczy serwis i pomoc techniczną innym pracownikom SMLW w zakresie eksploatacji systemu informatycznego, w razie potrzeby zgłasza potrzebę zlecenia lub na podstawie posiadanych kompetencji zleca prace informatycznym firmom zewnętrznym oraz nadzoruje te prace;
   4) wykonuje lub nadzoruje procedury archiwizowania danych (sporządzania kopii awaryjnych);
   5) reaguje na incydenty naruszenia bezpieczeństwa informacji w zakresie wynikającym ze szczegółowych zadań;
   6) wprowadza prawa dostępu użytkowników do informacji i danych w systemach, zgodnie z przyznanymi przez uprawnione osoby poziomami dostępu do systemów dla tych użytkowników;
   7) dokonuje instalacji i uczestniczy w testowaniu nowych wersji oprogramowania w środowisku testowym oraz środowisku roboczym;
   8) monitoruje wykorzystanie kluczowych aktywów systemu, włączając w to procesory, pamięć główną, pamięć dyskową, drukarki i inne urządzenia wyjściowe oraz systemy komunikacyjne;
   9) uczestniczy w procesach zarządzania ciągłością działania;
   10) prowadzi dokumentację systemów i komponentów systemów zgodnie z regulacjami wewnętrznymi SMLW;
   11) sporządza zapotrzebowania na oprogramowanie, sprzęt i usługi związane z technicznymi aspektami ochrony systemu informatycznego;
   12) raportuje na temat bezpieczeństwa informacji, w tym bezpieczeństwa środowiska teleinformatycznego w ramach Systemu Informacji Zarządczej.
4. ASI nadzoruje działanie zewnętrznych dostawców usług w zakresie jakości i przestrzegania standardów bezpieczeństwa w zakresie czynności technicznych realizowanych w związku z wykonaniem umów.

§ 9
Zadania pracowników

Zadaniem pracowników (użytkowników informacji) jest:
1) przestrzeganie zasad Polityki;
2) przestrzeganie zasad zawartych w innych regulacjach wewnętrznych, na które wskazuje niniejsza Polityka, odpowiednio do zakresu swoich zadań i obowiązków;

3) w każdym przypadku bezpieczne i rozważne postępowanie z informacją, systemami, dokumentami i nośnikami informacji, w tym bezwzględne zachowanie tajemnicy;
4) zgłaszanie incydentów związanych z bezpieczeństwem informacji;
5) potwierdzenie zapoznania się z treścią Polityki oraz innych regulacji dotyczących bezpieczeństwa informacji w postaci odpowiedniego oświadczenia zawartego w Załączniku nr 1 do Polityki.

IV. ZAKRES OCHRONY I KLASYFIKACJA INFORMACJI

§ 10
Zakres ochrony informacji

SMLW chroni informacje podlegające ochronie z mocy prawa, a także istotne z uwagi na prawidłowość realizacji kluczowych procesów.

§ 11
Klasyfikacja informacji

1. Kryteriami klasyfikacji informacji jest wymagany poziom: poufności, integralności, dostępności, rozliczalności.
2. W przypadku konieczności stosowania wielu kryteriów rozstrzygające jest kryterium przyjmujące najwyższym poziom.
3. W celu identyfikacji poziomu istotności informacji i wymaganego poziomu ochrony, informacja klasyfikowana jest wg następujących kategorii:
   1) informacje wrażliwe – informacje chronione prawnie (kryterium poufności) lub chronione z powodu uznania za podlegające ochronie, np. w związku z istotną wagą informacji dla prawidłowej realizacji procesów krytycznych (kryterium integralności, dostępności);
   2) informacje niewrażliwe – informacje nie należące do informacji wrażliwych.

§ 12
Klauzule poufności informacji

1. W celu właściwej identyfikacji dokumentów i informacji wrażliwych wymagających spełnienia odpowiedniego kryterium poufności wprowadza się następujące klauzule dokumentów, a także informacji elektronicznej:
   1) „Do użytku służbowego” – stosowane w odniesieniu do informacji i dokumentów wrażliwych, które mogą być przetwarzane wyłącznie w SMLW przez upoważnionych pracowników i nie mogą być dystrybuowane poza Spółdzielnię bez odpowiedniego upoważnienia;
   2) „Poufne SMLW” – stosowane w odniesieniu do informacji i dokumentów, których nieautoryzowane ujawnienie lub modyfikacja może w bezpośredni sposób spowodować straty finansowe lub odpowiedzialność prawną SMLW, a których obieg jest ograniczony do konkretnie określonych osób.
2. Klauzule stosowane są w dokumentach, a także w treści informacji elektronicznej np. w nagłówkach wiadomości poczty elektronicznej.
3. Dokumenty i informacje nie zawierające klauzuli uznaje się za oznaczone co najmniej jako „Do użytku służbowego”.

IV. ZASADY ZAPEWNIENIA BEZPIECZEŃSTWA INFORMACJI I ŚRODOWISKA TELEINFORMATYCZNEGO

§ 13
Podstawowe zasady zapewnienia bezpieczeństwa informacji

1. Poprzez zapewnienie bezpieczeństwa informacji należy rozumieć działania oparte na systematycznym zarządzaniu ryzykiem, obejmujące wybór, wdrożenie i utrzymanie zabezpieczeń składających się z technicznych i organizacyjnych środków ochrony danych i infrastruktury teleinformatycznej.
2. W szczególności zapewnienie bezpieczeństwa obejmuje obszary:
   1) bezpieczeństwa organizacyjnego;
   2) bezpieczeństwa fizycznego i środowiskowego;
   3) bezpieczeństwa systemów i infrastruktury teleinformatycznej;
   4) zarządzania ciągłością działania;
   5) reagowania na incydenty bezpieczeństwa informacji;
   6) zarządzania jakością danych.

§ 14
Zarządzanie ryzykiem

1. W SMLW funkcjonuje sformalizowany system zarządzania bezpieczeństwem informacji, w tym bezpieczeństwem środowiska teleinformatycznego.
2. System obejmuje działania związane z identyfikacją, szacowaniem, kontrolą, przeciwdziałaniem, monitorowaniem i raportowaniem ryzyka bezpieczeństwa informacji, w tym bezpieczeństwa środowiska teleinformatycznego.
3. System zintegrowany jest z całościowym systemem zarządzania ryzykiem w SMLW, w tym analiza i ocena ryzyka realizowana jest zgodnie z metodyką dotyczącą zarządzania ryzykiem operacyjnym.
4. Na podstawie wyników analizy i oceny ryzyka:
   1) określany jest akceptowalny poziom ryzyka;
   2) podejmowane są lub weryfikowane działania zmierzające do postępowania z ryzykiem, zapewniające odpowiedni poziom bezpieczeństwa informacji, a także spełnienie wymagań wynikających z umów oraz przepisów prawnych.

§ 15
Bezpieczeństwo organizacyjne

1. SMLW zapewnia, aby struktura organizacyjna w obszarach technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego pozwalała na efektywną realizację celów SMLW, w tym poddaje ją cyklicznym przeglądom zarządczym.
2. W szczególności dokonując wewnętrznego podziału zadań w systemie zarządzania bezpieczeństwem środowiska teleinformatycznego rozdziela się:
   1) funkcję tworzenia lub modyfikowania systemów informatycznych od ich testowania (poza testami realizowanymi przez programistów w ramach wytwarzania oprogramowania), administracji i użytkowania;
   2) funkcję administrowania danym komponentem środowiska teleinformatycznego od projektowania związanych z nim mechanizmów kontrolnych w zakresie bezpieczeństwa;

3) funkcję administrowania danym systemem informatycznym od monitorowania działań jego administratorów;
4) funkcję audytu od pozostałych funkcji w obszarach technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego.

3. SMLW zapewnia odpowiednią liczebność, jak i poziom wiedzy i kwalifikacji pracowników obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego tak, aby pozwalało to na bezpieczną i poprawną działalność.
4. SMLW przykłada szczególną uwagę do doboru pracowników zatrudnianych na stanowiskach dających dostęp do informacji o wysokim stopniu poufności.
5. Funkcjonująca w SMLW polityka kadrowa i inne regulacje dotyczące zarządzania kadrami uwzględnia zapewnianie, aby wszystkie osoby zatrudniane posiadały odpowiednią wiedzę na temat obowiązujących regulacji wewnętrznych dotyczących bezpieczeństwa informacji.
6. SMLW podejmuje systematyczne działania związane z edukacją i szkoleniem pracowników w zakresie zagrożeń i istniejących regulacji wewnętrznych odpowiednio do ich obowiązków.
7. SMLW zapewnia odpowiednią ciągłość działania związaną z obszarem technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego.

§ 16
Bezpieczeństwo fizyczne i środowiskowe

1. Stosowane w SMLW mechanizmy bezpieczeństwa fizycznego i środowiskowego są adekwatne do potrzeb i skali działalności SMLW w taki sposób, aby pozwalało to na bieżące funkcjonowanie kluczowych procesów oraz ich odtworzenie w przypadku wystąpienia sytuacji awaryjnej.
2. Wrażliwe środki przetwarzania informacji są umieszczane w obszarach bezpiecznych, chronionych fizyczną granicą przez odpowiednie bariery bezpieczeństwa oraz zabezpieczenia wejścia. Zapewnia się, aby były one chronione fizycznie przed nieuprawnionym dostępem fizycznym, uszkodzeniami lub zakłóceniami pracy.
3. Stosowana jest ochrona sprzętu (łącznie ze sprzętem wykorzystywanym poza siedzibą SMLW) niezbędna do redukowania ryzyka nieautoryzowanego dostępu do informacji i ochrony przed utratą lub uszkodzeniem. Ochrona obejmuje również odpowiednią lokalizację (miejsce instalacji), konserwację, zbywanie lub przekazanie sprzętu podmiotom zewnętrznym w sposób zapewniający bezpieczeństwo informacji.
4. Chroni się przed zagrożeniami instalacje wspomagające, takie jak zasilanie lub okablowanie sieciowe.

§ 17
Bezpieczeństwo systemów i infrastruktury teleinformatycznej

1. Stosowana jest zasada, że wszystkie komponenty środowiska teleinformatycznego (systemy, komponenty infrastruktury teleinformatycznej) powinny być zinwentaryzowane i udokumentowane oraz mają wyznaczonego właściciela odpowiedzialnego za właściwą ochronę i utrzymanie zabezpieczeń danego komponentu.
2. W zakresie zapewnienia bezpieczeństwa komponentów środowiska teleinformatycznego istotną rolę pełnią:
   1) właściciele systemów – osoby odpowiedzialne za zapewnienie prawidłowości działania i bezpieczeństwa systemu pod względem biznesowym (np. poprzez właściwe zdefiniowanie procedur korzystania z systemu, udział w procesie

zarządzania ciągłością jego działania, udział w procesie zarządzania uprawnieniami), nadzór nad działaniami użytkowników systemu, udział w procesie podejmowania decyzji w zakresie rozwoju tych systemów;
   2) ASI – jako właściciel komponentów infrastruktury teleinformatycznej.
3. Stosowane są następujące mechanizmy bezpieczeństwa:
   1) pozyskiwanie, rozwój i utrzymanie systemów zapewniających bezpieczeństwo systemów, oddzielanie środowiska testowego i eksploatacyjnego;
   2) planowanie, zarządzanie pojemnością i wydajnością systemów;
   3) rozdzielanie obowiązków zapobiegające celowej, nieumyślnej modyfikacji lub niewłaściwego użycia systemów;
   4) regulacje wewnętrzne w zakresie eksploatacji komponentów;
   5) zarządzanie zmianami w środowisku teleinformatycznym;
   6) świadczenie pomocy technicznej użytkownikom systemów;
   7) zarządzanie ryzykiem usług dostarczanych przez podmioty trzecie;
   8) ochrona przed złośliwym oprogramowaniem;
   9) stosowanie zabezpieczeń kryptograficznych;
   10) stosowanie regularnego dokonywania i testowania kopii zapasowych;
   11) zapewnianie bezpieczeństwa sieci teleinformatycznych;
   12) zapewnianie bezpieczeństwa nośników informacji;
   13) zapewnianie bezpieczeństwa wymiany informacji;
   14) zapewnianie bezpieczeństwa elektronicznych kanałów dostępu;
   15) kontrola dostępu i nadawanie uprawnień;
   16) zarządzanie oprogramowaniem użytkownika końcowego.
4. Sposób inwentaryzacji, dokumentowania komponentów infrastruktury środowiska teleinformatycznego, a także realizacji mechanizmów bezpieczeństwa uregulowany jest w pozostałych regulacjach wewnętrznych powiązanych z Polityką bezpieczeństwa informacji.

§ 18
Zarządzanie ciągłością działania

1. W celu zapewnienia ciągłości działania środowiska teleinformatycznego SMLW stosuje proces zarządzania ciągłością działania tak, aby zminimalizować wpływ utraty i odtwarzania komponentów środowiska teleinformatycznego wynikającego z katastrof naturalnych, wypadków, awarii urządzeń oraz celowego działania.
2. Odpowiedni poziom ciągłości działania w zakresie środowiska teleinformatycznego uzyskiwany jest poprzez stosowanie kombinacji zabezpieczeń prewencyjnych i środków służących do odtwarzania komponentów środowiska teleinformatycznego.
3. W ramach procesu zarządzania ciągłością działania:
   1) określa się krytyczne procesy biznesowe i integruje wymagania bezpieczeństwa informacji odnoszące się do ciągłości działania z wymaganiami ciągłości działania związanymi z innymi aspektami działalności SMLW;
   2) dokonuje się analizy wpływu na biznes konsekwencji wynikających z katastrof, awarii, utraty usług oraz ich dostępności;
   3) opracowuje się i wdraża plany awaryjne, aby zapewnić możliwość przywrócenia procesów biznesowych w wymaganym czasie.

§ 19
Reagowanie na incydenty bezpieczeństwa informacji

1. SMLW wdraża i stosuje regulacje wewnętrzne dotyczące zgłaszania i reagowania na zidentyfikowane incydenty bezpieczeństwa informacji, w tym incydenty naruszenia bezpieczeństwa środowiska teleinformatycznego.
2. Obowiązkiem wszystkich pracowników jest stosowanie zasad w zakresie zgłaszania incydentów.
3. Podmioty trzecie, podczas przetwarzania informacji SMLW, są zobowiązane stosownymi zapisami w umowach do informowania SMLW o incydentach bezpieczeństwa informacji po swojej stronie, niezwłocznie po ich wykryciu.
4. Informacje dotyczące stwierdzonych incydentów wraz z opisem ich przyczyny i podjętymi działaniami korygującymi są rejestrowane w celu dalszej analizy.
5. SMLW podejmuje działania zmierzające do ustalenia przyczyn i usunięcia skutków incydentów bezpieczeństwa.
6. Informacje dotyczące incydentów są uwzględniane w procesie analizy ryzyka, w tym raportowane jako zdarzenia ryzyka operacyjnego.

V. ZARZĄDZANIE ARCHITEKTURĄ I JAKOŚCIĄ DANYCH

§ 20
Zarządzanie architekturą i jakością danych

1. Zarządzając bezpieczeństwem środowiska teleinformatycznego SMLW zarządza architekturą i jakością przetwarzanych danych.
2. W ramach zarządzania architekturą danych SMLW inwentaryzuje grupy danych, identyfikuje źródła danych oraz określa w jakich jednostkach i komórkach organizacyjnych są one przetwarzane, wyznaczane są również osoby odpowiedzialne za jakość przetwarzanych danych.

§ 21
Proces zarządzania jakością danych

1. W ramach procesu zarządzania jakością danych dokonywane są:
   1) okresowe oceny i monitoring jakości danych;
   2) identyfikacja przyczyn błędów występujących w danych;
   3) bieżące monitorowanie i raportowanie jakości danych;
   4) czyszczenie danych.
2. Okresowe oceny i monitoring jakości danych dokonywane są poprzez stosowanie mechanizmów kontroli wewnętrznej, a także zarządzania ryzykiem operacyjnym.
3. W zakresie oceny jakości danych identyfikuje się błędy w danych stwierdzone w czasie kontroli wewnętrznej lub w zarejestrowanych incydentach ryzyka operacyjnego oraz ocenia się ich wpływ na działalność SMLW, w tym przekroczenie ustalonego progu jakości danych.
4. Szczególne obszary oceny kontroli będącej elementem oceny jakości danych dotyczą:
   1) ryzyka błędów ręcznego wprowadzania danych do systemów;
   2) ryzyka błędów wymiany danych pomiędzy systemami wewnętrznymi i zewnętrznymi.
5. W przypadku stwierdzenia danych błędnych, ustala się przyczyny stwierdzonych błędów, np. związane z niewłaściwymi procedurami przetwarzania danych oraz z niską

skutecznością mechanizmów kontrolnych funkcjonujących w zakresie zapewniania jakości danych.

6. W uzasadnionych przypadkach, o ile wyniki oceny jakości danych wykazały liczne błędy i istnieją odpowiednie mechanizmy techniczne, stosowane jest czyszczenie danych, tzn. automatyczna weryfikacja i korekty posiadanych danych. Mechanizmy te stosowane są w ostrożny sposób, tak aby czyszczenie danych realizowane z błędnymi założeniami lub formułami korekty nie powodowało zaburzenia poprawności danych.
7. Wyniki oceny jakości danych sprawozdaje się poprzez zawarcie informacji o jakości danych (np. błędach wykrytych w czasie kontroli wewnętrznej), w postaci wykazania stwierdzonych błędów oraz ich przyczyn w sprawozdawczości zarządczej dotyczącej wyników kontroli dla Zarządu SMLW.

VI. UDOSTĘPNIANIE I PUBLIKOWANIE INFORMACJI

§ 22
Udostępnianie informacji wrażliwych podmiotom zewnętrznym

1. Udostępnianie informacji wrażliwych osobom i organom zewnętrznym jest możliwe wyłącznie zgodnie z przepisami prawa.
2. Udostępnianie informacji wrażliwych osobom i organom zewnętrznym za każdym razem wymaga akceptacji Zarządu SMLW i jest odpowiednio dokumentowane.

§ 23
Publikowanie lub udostępnianie informacji niewrażliwych

1. Z uwagi na zagrożenie ryzykiem utraty reputacji, a także możliwość zwiększenia poziomu innych rodzajów ryzyka należy dochować jak największej ostrożności i staranności związanej z publikowaniem lub udostępnianiem informacji niewrażliwych podmiotom zewnętrznym – pomimo, że istnieje pewność, że informacja taka nie jest objęta ochroną prawa.
2. Szczególną uwagę należy zwrócić na informacje publikowane w sieci Internet, w tym w tzw. mediach społecznościowych.
3. Publikowanie lub udostępnianie informacji niewrażliwych podmiotom zewnętrznym jest możliwe wyłącznie z zachowaniem zasad prawa, przepisów wewnętrznych i za każdym razem wymaga:
   1) weryfikacji treści udostępnianej informacji pod kątem poprawności i zagrożenia dla reputacji SMLW przez odpowiedniego dla sprawy pracownika;
   2) akceptacji czynności opublikowania lub udostępnienia - przed opublikowaniem lub udostępnieniem informacji – przez Zarząd SMLW.

VI. KONSEKWENCJE NARUSZANIA ZASAD

§ 24
Obowiązki pracowników

1. Pracownicy przetwarzający informacje wrażliwe zobowiązani są do ścisłego przestrzegania przepisów prawa oraz przepisów wewnętrznych SMLW oraz do nie

rozpowszechniania wiadomości stanowiących tajemnicę przedsiębiorstwa lub objętych ochroną danych osobowych oraz innych rodzajów tajemnicy.
2. Zarząd SMLW podkreśla, że obowiązek ochrony tajemnicy przedsiębiorstwa oraz tajemnicy zawodowej nie wygasa po ustaniu stosunku pracy.

§ 25

Konsekwencje związane z naruszaniem postanowień
„Polityki bezpieczeństwa informacji"

Pracownicy SMLW mogą podlegać konsekwencjom dyscyplinarnym i prawnym za nieprzestrzeganie postanowień niniejszej Polityki Bezpieczeństwa Informacji, a także innych regulacji szczegółowo określających zasady zachowania bezpieczeństwa informacji, które wskazuje niniejsza Polityka.

VII. DYSTRYBUCJA POLITYKI

§ 26

1. Z treścią niniejszego dokumentu, jak i innych regulacji składających się na Politykę bezpieczeństwa informacji są zapoznani wszyscy pracownicy SMLW, odpowiednio do ich zakresów obowiązków.
2. Niniejszy dokument może być przedstawiany wszystkim innym podmiotom, w tym organom władzy i administracji publicznej, w celu prezentacji zasad ochrony informacji i środowiska teleinformatycznego obowiązujących w SMLW.

Załącznik nr 1 - Wykaz regulacji wewnętrznych i dokumentów stanowiących dokumenty powiązane z Polityką Bezpieczeństwa Informacji

Nazwa regulacji / dokumentu	**Uwagi**
Polityka bezpieczeństwa informacji SMLW	
Instrukcja zarządzania systemami informatycznymi w SMLW	
1) Instrukcja użytkowania systemów informatycznych	
2) Instrukcja ochrony danych osobowych	
3) Instrukcja ochrony tajemnicy	
Dokumentacja systemu zarządzania bezpieczeństwem informacji i systemów przetwarzania danych	Dokumentacja powstająca na skutek realizacji regulacji wewnętrznych wymienionych w niniejszym załączniku
Instrukcja zarządzania ciągłością działania	

Załącznik nr 2 - Wzór oświadczenia o stosowaniu się do Polityki bezpieczeństwa informacji

...., data.....
imię i nazwisko miejscowość

.....
komórka organizacyjna - stanowisko

OŚWIADCZENIE

Niniejszym oświadczam, iż znana mi jest treść dokumentu „Polityka Bezpieczeństwa Informacji" oraz innych wymienionych w niej regulacji wewnętrznych przyjętych w instrukcji użytkowania systemów informatycznych w Spółdzielni Mieszkaniowej Lokatorsko – Własnościowej w Raciążu.
Jednocześnie oświadczam, że będę się stosować do zawartych w wyżej wymienionych dokumentach zasad i procedur.

.....
podpis

Załącznik nr 3
Słownik pojęć wykorzystywanych w regulacjach wewnętrznych związanych z Polityką bezpieczeństwa informacji

§ 1
Ogólne definicje związane z bezpieczeństwem informacji

1) **bezpieczeństwo informacji** – zachowanie poufności, integralności i dostępności informacji; w ramach bezpieczeństwa informacji mogą być uwzględniane również inne właściwości, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność;
2) **dane** – zapisy w formie elektronicznej lub papierowej będące reprezentacją informacji;
3) **dostępność danych** – właściwość danych polegająca na tym, że są one dostępne i mogą być wykorzystywane na żądanie uprawnionej jednostki;
4) **incydent naruszenia bezpieczeństwa środowiska teleinformatycznego** – pojedyncze niepożądane lub niespodziewane zdarzenie bezpieczeństwa środowiska teleinformatycznego (tj. wystąpienie stanu komponentu środowiska teleinformatycznego wskazującego na potencjalne naruszenie jego bezpieczeństwa, błąd mechanizmu kontrolnego lub uprzednio nieznaną sytuację, która może być istotna z perspektywy bezpieczeństwa) lub seria takich zdarzeń, w przypadku których występuje znaczne prawdopodobieństwo zakłócenia działalności lub naruszenia bezpieczeństwa informacji;
5) **incydent naruszenia bezpieczeństwa informacji** - pojedyncze niepożądane lub niespodziewane zdarzenie bezpieczeństwa informacji (tj. wystąpienie stanu wskazującego na potencjalne naruszenie bezpieczeństwa, błąd mechanizmu kontrolnego lub uprzednio nieznaną sytuację, która może być istotna z perspektywy bezpieczeństwa informacji) lub seria takich zdarzeń, w przypadku których występuje znaczne prawdopodobieństwo zakłócenia działalności lub naruszenia bezpieczeństwa informacji, w tym incydent naruszenia bezpieczeństwa środowiska teleinformatycznego;
6) **integralność danych** – właściwość danych stanowiąca o ich dokładności i kompletności;
7) **informacja** – treści wszelkiego rodzaju przechowywane na dowolnym nośniku informacji. Informacja może być wyrażona za pomocą mowy, pisma, obrazu, rysunku, znaku, kodu, dźwięku lub w jakikolwiek inny sposób;
8) **kluczowe procesy** – wskazane przez SMLW procesy w obrębie jej działalności, które warunkują realizację strategii SMLW (w tym strategii biznesowej i zarządzania ryzykiem);
9) **krytyczne procesy** – wskazane przez SMLW procesy w obrębie jej działalności, w przypadku których szybkie odzyskanie sprawności działania może mieć istotne znaczenie z punktu widzenia ciągłości działania;
10) **logowanie** – proces uwierzytelniania użytkownika w systemie przetwarzania informacji;
11) **podatność** – słabość zasobu lub mechanizmu kontrolnego, która może być wykorzystana przez zagrożenie;
12) **postępowanie z ryzykiem** – metody obejmujące akceptację ryzyka, ograniczanie, transfer lub unikanie ryzyka;
13) **poufność danych** – właściwość danych polegająca na tym, że pozostają one niedostępne lub niejawne dla nieuprawnionych osób, procesów lub innych podmiotów;

14) **rozliczalność danych** - zachowanie dowodów o podjętych czynnościach względem przetwarzanej informacji;
15) **system zarządzania bezpieczeństwem środowiska teleinformatycznego** – zbiór zasad i mechanizmów odnoszących się do procesów mających na celu zapewnienie odpowiedniego poziomu bezpieczeństwa środowiska teleinformatycznego;
16) **tworzenie lub modyfikowanie systemów informatycznych** – modyfikacje kodów źródłowych systemu;
17) **uwierzytelnianie** – proces pozwalający na jednoznaczną identyfikację użytkownika w systemie przetwarzania informacji;
18) **zabezpieczenie danych w systemie informatycznym przetwarzającym dane osobowe** – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem (Ustawa o ochronie danych osobowych);
19) **zagrożenie** – potencjalna przyczyna niepożądanego incydentu, który może spowodować szkodę dla systemu lub organizacji.

§ 2

Definicje dotyczące systemów i infrastruktury przetwarzania informacji

1) **cloud computing** („przetwarzanie w chmurze") – model świadczenia usług zapewniający niezależny od lokalizacji, dogodny dostęp sieciowy „na żądanie" do współdzielonej puli konfigurowalnych zasobów obliczeniowych (np. serwerów, pamięci masowych, aplikacji lub usług), które mogą być dynamicznie dostarczane lub zwalniane przy minimalnych nakładach pracy zarządczej i minimalnym udziale dostawcy usług;
2) **infrastruktura teleinformatyczna** – zespół urządzeń i łączy transmisyjnych obejmujący w szczególności platformy sprzętowe (w tym: serwery, macierze, stacje robocze), sieć teleinformatyczną (w tym: routery, przełączniki, zapory sieciowe oraz inne urządzenia sieciowe), oprogramowanie systemowe (w tym systemy operacyjne i systemy zarządzania bazami danych) oraz inne elementy umożliwiające bezawaryjną i bezpieczną pracę w/w zasobów (w tym zasilacze UPS, generatory prądotwórcze, urządzenia klimatyzacyjne), także te wykorzystywane w ośrodkach zapasowych;
3) **nośnik informacji** – medium magnetyczne, optyczne lub papierowe, na którym zapisuje się i przechowuje informacje;
4) **przetwarzanie danych** - jakiekolwiek operacje wykonywane na danych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie;
5) **system informatyczny** – aplikacja komputerowa lub zbiór powiązanych aplikacji komputerowych, którego celem jest przetwarzanie danych;
6) **system informatyczny przetwarzający dane osobowe** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych (Ustawa o ochronie danych osobowych);
7) **środowisko teleinformatyczne** – infrastruktura teleinformatyczna SMLW wraz z wykorzystującymi ją systemami informatycznymi oraz eksploatowane w SMLW systemy informatyczne wspierające jego działalność, oparte na infrastrukturze teleinformatycznej zapewnianej przez podmioty zewnętrzne;
8) **szyfrowanie (kryptografia)** – proces polegający na takim przetworzeniu informacji wrażliwych, aby nie mogły być one odczytane przez osoby nieupoważnione;
9) **uwierzytelnianie** – proces pozwalający na jednoznaczną identyfikację użytkownika w systemie informatycznym;

10) **wirtualizacja serwerów** – technika pozwalająca na jednoczesne funkcjonowanie wielu serwerów logicznych na danej platformie sprzętowej.

§ 3

Definicje i terminy dotyczące organizacji i ról w zakresie zapewnienia bezpieczeństwa informacji

1) **administrator danych –** Spółdzielnia Mieszkaniowa Lokatorsko – Własnościowa w Raciążu;
2) **administrator systemu informatycznego (ASI)** – osoba lub osoby wyznaczane przez Zarząd SMLW, odpowiedzialne z prawidłowy stan i działanie środowiska teleinformatycznego od strony technicznej, realizuje zadania obszaru technologii informacyjnej;
3) **obszar bezpieczeństwa środowiska teleinformatycznego** – obszar działalności SMLW mający na celu zapewnienie, że ryzyko dotyczące bezpieczeństwa środowiska teleinformatycznego SMLW jest odpowiednio zarządzane;
4) **obszar biznesowy** – obszar działalności SMLW, którego funkcjonowanie jest wspierane przez środowisko teleinformatyczne, w tym np. działalność operacyjna, zarządzanie ryzykiem, rachunkowość, finanse itp.;
5) **obszar technologii informacyjnej** – obszar działalności SMLW mający na celu zapewnienie właściwego wsparcia funkcjonowania SMLW przez środowisko teleinformatyczne;
6) **właściciel systemu** - osoba odpowiedzialna za zapewnienie prawidłowości działania i bezpieczeństwa systemu pod względem biznesowym, nadzór nad działaniami użytkowników systemu, udział w procesie podejmowania decyzji w zakresie rozwoju tych systemów;
7) **właściciel danych** - komórki organizacyjne lub funkcje odpowiadające za jakość danych i nadzór nad nimi.

§ 4

Pojęcia dotyczące klasyfikacji informacji (zasobów) ze względu na ich znaczenie dla SMLW

1) **informacje wrażliwe** – informacje przetwarzane w SMLW, chronione prawnie lub chronione z powodu uznania za wymagające ochrony, np. w związku z istotną wagą informacji dla prawidłowej realizacji procesów kluczowych. Informacje wrażliwe mają jasno określone reguły dostępu i odpowiednio do wymagań podlegają ochronie w zakresie poufności, integralności i dostępności;
2) **informacje niewrażliwe** – informacje nie należące do informacji wrażliwych, podlegają ochronie w zakresie integralności i dostępności w stopniu wynikającym z potrzeby ochrony interesów SMLW;
3) **system informatyczny wysokiej istotności** – system przetwarzający informacje wrażliwe, w tym prawnie chronione lub istotne dla prawidłowej realizacji kluczowych procesów;
4) **wrażliwe dane płatnicze** – dane, które w przypadku wejścia w ich posiadanie przez osoby nieuprawnione mogą być wykorzystane w celu dokonania nadużycia, w tym dane umożliwiające zainicjowanie transakcji płatniczej, dane wykorzystywane do uwierzytelnienia, dane wykorzystywane do zamawiania przez klientów instrumentów płatniczych lub narzędzi uwierzytelniających.