POLITYKA BEZPIECZEŃSTWA INFORMACJI

dla serwisu https://swit.elk.pl/

1. Wprowadzenie

1.1. Polityka Bezpieczeństwa Informacji (dalej: „PBI") określa kompleksowe zasady ochrony informacji, w tym danych osobowych, przetwarzanych przez Administratora Danych w ramach działalności prowadzonej z wykorzystaniem serwisu internetowego https://swit.elk.pl/ (dalej: „Serwis").

1.2. Dokument stanowi nadrzędny akt wewnętrzny w systemie zarządzania bezpieczeństwem informacji i obejmuje wszystkie procesy, systemy, zasoby techniczne oraz osoby uczestniczące w przetwarzaniu informacji.

2. Cel Polityki

Celem PBI jest:

- zapewnienie poufności, integralności i dostępności informacji,
- spełnienie wymagań RODO, ustawy o ochronie danych osobowych oraz przepisów sektorowych,
- minimalizacja ryzyka utraty, nieuprawnionego ujawnienia lub zniszczenia informacji,
- ujednolicenie zasad postępowania z informacją w całej organizacji.

3. Zakres obowiązywania

3.1. Polityka obowiązuje: - pracowników, współpracowników i osoby działające na rzecz Administratora, - użytkowników systemów informatycznych, - podmioty przetwarzające dane na podstawie umów powierzenia.

3.2. Polityka ma zastosowanie do wszystkich informacji niezależnie od ich postaci (papierowej, elektronicznej, ustnej).

4. Podstawa prawna

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO),
- ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych,
- ustawa o świadczeniu usług drogą elektroniczną,
- Kodeks pracy (w zakresie obowiązków pracowniczych),
- wytyczne Prezesa UODO,
- normy ISO/IEC 27001 i 27002 (dobre praktyki).

5. Definicje i skróty

- **Informacja** – każda treść posiadająca wartość dla Administratora.
- **Dane osobowe** – informacje o osobie fizycznej możliwej do zidentyfikowania.
- **Zasób informacyjny** – informacja wraz z nośnikiem i systemem przetwarzania.
- **System informatyczny** – środki techniczne i programowe służące do przetwarzania informacji.
- **Naruszenie bezpieczeństwa informacji** – każde zdarzenie naruszające poufność, integralność lub dostępność.

6. Klasyfikacja informacji

6.1. W Spółdzielni Mieszkaniowej „ŚWIT" w Ełku wprowadza się formalną klasyfikację informacji, mającą na celu określenie poziomu ochrony oraz zasad postępowania z informacją.

6.2. Informacje klasyfikuje się do następujących kategorii:

6.2.1. **Informacje publiczne** – informacje przeznaczone do publicznego udostępniania, w szczególności publikowane na stronie internetowej Spółdzielni lub przekazywane na podstawie przepisów prawa.

6.2.2. **Informacje wewnętrzne** – informacje przeznaczone wyłącznie do użytku wewnętrznego Spółdzielni, których ujawnienie osobom nieupoważnionym mogłoby utrudnić jej funkcjonowanie.
6.2.3. **Informacje chronione** – informacje, których ujawnienie mogłoby narazić Spółdzielnię na szkodę organizacyjną, finansową lub wizerunkową.
6.2.4. **Dane osobowe** – informacje dotyczące członków Spółdzielni, mieszkańców, kontrahentów, pracowników i innych osób fizycznych, podlegające szczególnej ochronie zgodnie z RODO.
6.3. Każda kategoria informacji podlega adekwatnym środkom ochrony technicznej i organizacyjnej.

7. Role i odpowiedzialności

7.1. **Zarząd Spółdzielni Mieszkaniowej „ŚWIT" w Ełku**: - odpowiada za ustanowienie, wdrożenie i utrzymanie Polityki Bezpieczeństwa Informacji, - zapewnia środki organizacyjne i finansowe niezbędne do realizacji PBI, - podejmuje decyzje w sprawach strategicznych dotyczących bezpieczeństwa informacji.
7.2. **Administrator Danych Osobowych**: - odpowiada za zgodność przetwarzania danych osobowych z przepisami prawa, - określa cele i sposoby przetwarzania danych, - nadzoruje stosowanie środków bezpieczeństwa.
7.3. **Inspektor Ochrony Danych (IOD)**: - monitoruje przestrzeganie RODO oraz niniejszej Polityki, - prowadzi szkolenia i działania informacyjne, - doradza Zarządowi i pracownikom, - uczestniczy w obsłudze incydentów i naruszeń.
7.4. **Pracownicy i współpracownicy**: - przetwarzają informacje wyłącznie w zakresie posiadanych upoważnień, - zobowiązani są do zachowania poufności informacji, - są zobowiązani do niezwłocznego zgłaszania incydentów bezpieczeństwa.

8. Zarządzanie ryzykiem

8.1. Administrator prowadzi cykliczną analizę ryzyka dla zasobów informacyjnych.
8.2. Ryzyko oceniane jest pod kątem prawdopodobieństwa i skutków.
8.3. Dla ryzyk istotnych wdraża się środki redukujące.

9. Bezpieczeństwo organizacyjne

9.1. Upoważnienia do przetwarzania danych nadawane są pisemnie.
9.2. Prowadzona jest ewidencja osób upoważnionych.
9.3. Szkolenia z bezpieczeństwa informacji odbywają się okresowo.

10. Bezpieczeństwo fizyczne

10.1. Dostęp do pomieszczeń, w których przetwarzane są dane, jest kontrolowany.
10.2. Dokumentacja papierowa przechowywana jest w zamykanych szafach.

11. Bezpieczeństwo teleinformatyczne

11.1. Spółdzielnia stosuje środki techniczne zapewniające ochronę systemów teleinformatycznych przed nieuprawnionym dostępem, utratą danych oraz zakłóceniami działania.
11.2. W szczególności stosuje się:

- zabezpieczenia sieciowe typu firewall,
- szyfrowanie transmisji danych (SSL/TLS),
- mechanizmy uwierzytelniania użytkowników,
- oprogramowanie antywirusowe i antymalware,
- regularne aktualizacje systemów i aplikacji.

11.3. Dostęp do systemów informatycznych Spółdzielni:

- odbywa się na podstawie indywidualnych kont użytkowników,
- jest rejestrowany i podlega okresowej analizie,
- jest ograniczony do zakresu obowiązków służbowych.

11.4. Zabrania się instalowania nieautoryzowanego oprogramowania oraz podłączania niezatwierdzonych urządzeń.

12. Zarządzanie hasłami i dostępami

12.1. Hasła muszą spełniać wymagania złożoności.

12.2. Zabrania się udostępniania haseł osobom trzecim.

13. Kopie zapasowe i odtwarzanie

13.1. Wykonywane są regularne kopie zapasowe.

13.2. Testuje się procedury odtwarzania danych.

14. Praca zdalna i urządzenia mobilne

14.1. Praca zdalna wymaga zabezpieczonych połączeń.

14.2. Urządzenia mobilne muszą być zabezpieczone hasłem.

15. Zarządzanie incydentami

15.1. Incydenty zgłasza się niezwłocznie do IOD.

15.2. Prowadzi się rejestr incydentów.

16. Naruszenia danych osobowych

16.1. Naruszenia są analizowane pod kątem ryzyka.

16.2. Zgłoszenia do UODO dokonywane są w terminach ustawowych.

17. Podmioty przetwarzające

17.1. Dane powierzane są wyłącznie na podstawie umów.

17.2. Podmioty przetwarzające podlegają kontroli.

18. Audyty i kontrola

18.1. Przeprowadzane są audyty wewnętrzne.

18.2. Wyniki audytów są dokumentowane.

19. Odpowiedzialność i sankcje

19.1. Naruszenie PBI może skutkować odpowiedzialnością służbową.

20. Postanowienia końcowe

20.1. Polityka podlega corocznemu przeglądowi.

20.2. Wchodzi w życie z dniem zatwierdzenia.