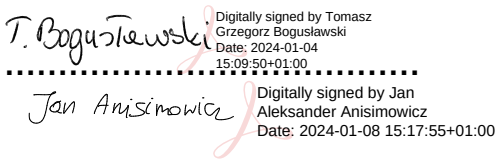
ZATWIERDZAM



Polityka Bezpieczeństwa Informacji

SEC_PBI

4.1

Historia wersji

Data	Wersja	Opis	Autor
14.04.2008	1.00	Wersja początkowa	Konrad Trubas
01.06.2008	1.01	Wersja polska. Dodano sygnatury dokumentów pochodnych.	Konrad Trubas
03.06.2008	1.02	Umocowano w polityce procedury DRP i kontrolne	Konrad Trubas
19.06.2008	1.03	Umocowanie procesu szkoleń	Konrad Trubas
05.10.2009	2.00	Zmiana systemu klasyfikacji danych	Konrad Trubas
11.04.2011	2.01	Aktualizacja	Konrad Trubas
10.05.2013	2.02	Przeniesienie zasad akceptowalnego użycia do osobnego dokumentu	Konrad Trubas
24.10.2013	2.03	Cybersecurity dodane	Konrad Trubas
18.06.2014	2.10	Zmiana struktury w zakresie elektronicznych metod ochrony danych	Konrad Trubas
16.12.2014	2.11	Przegląd procedur i dokumentacji po zmianie siedziby	Konrad Trubas
12.04.2018	3.01	Wersja zrewidowania pod katem ISO 27001 i GDPR	Konrad Trubas
17.08.2018	3.10	Poprawki edycyjne.	Konrad Trubas
25.02.2019	3.20	Poprawki edycyjne	Konrad Trubas
06.06.2019	3.30	Poprawki w związku z uwagami z audytu wewnętrznego	Konrad Trubas
21.03.2023	4.00	Zmiana struktury	Konrad Trubas
31.10.2023	4.1	Zmiana zakresu SZBI	Konrad Trubas

1. Deklaracja zarządu

Mając na względzie znaczenie ochrony bezpieczeństwa informacji dla celów spółki, Zarząd C&F S.A. ustanawia System Zarządzania Bezpieczeństwem Informacji (SZBI) oraz wprowadza niniejszą Politykę Bezpieczeństwa Informacji będąca dokumentem bazowym SZBI, jako deklarację swojego zaangażowania i wsparcia w proces zapewnienia bezpieczeństwa informacyjnego w firmie. Zarząd jest właścicielem SZBI i bezpośrednio nadzoruje przestrzeganie zasad określonych w niniejszej polityce praz politykach i innych dokumentach niższego rzędu. Zarząd potwierdza wiodącą rolę w procesie zapewnienia bezpieczeństwa informacji gwarantując właściwy poziom ochrony, między innymi poprzez zapewnienie niezbędnych i adekwatnych środków minimalizacji ryzyk w zakresie SZBI. Zapewnienie bezpieczeństwa informacji to zapewnienie poufności, integralności i dostępności przetwarzanych informacji i danych, w dowolny sposób i z wykorzystaniem dowolnych metod, adekwatnych do poziomu ryzyka, z zachowaniem zasad rozliczalności, wiarygodności i przejrzystości.
Określone w niniejszym dokumencie ramy postępowania z informacjami są celami całej organizacji rozumianej jako C&F S.A. oraz jej spółki zależne i powiązane, i przez to dotyczą wszystkich jej pracowników, współpracowników, zleceniobiorców i podwykonawców. Każdy z nich jest zobowiązany do dostosowania się do niniejszej polityki i spełnienia wszystkich wymogów określonej w niej i pochodnych dokumentach.

2. Cele i inicjatywy bezpieczeństwa informacji

Niniejsza polityka została ustanowiona w celu zapewnienia, że podejmowane są działania na rzecz rzeczywistego wsparcia osiągania przez organizację celów biznesowych, w szczególności :

- Dane powierzone nam przez klientów oraz własne, w tym dane osobowe, są chronione w sposób oczekiwany i adekwatny do ich wartości;
- Rozwiązania i usługi dostarczane klientom nie generują nieznanych i nieakceptowalnych ryzyk
- Podejmowane działania pozostają w zgodzie z przepisami prawnymi w zakresie bezpieczeństwa informacyjnego w szczególności odnośnie ochrony danych osobowych
- Wiedza i specyficzne zdolności wypracowane przez lata działalności firmy pozostają chronione
- Zdefiniowane zostały ramy mechanizmów pozwalających na ciągłe mierzenie i doskonalenie procesów związanych z zapewnieniem bezpieczeństwa informacyjnego w organizacji

Co osiągane jest poprzez następujące cele bezpieczeństwa informacyjnego:

1. Zgodność z prawem, regulacjami oraz wymaganiami kontraktowymi (compliance), ochrona zasobów informacyjnych, a w szczególności ochrona praw własności, informacji kontraktowych oraz wizerunku Spółki,
2. Uzyskanie i utrzymanie odpowiednio wysokiego poziomu bezpieczeństwa zasobów rozumiane jako zapewnienie poufności, integralności i dostępności zasobów oraz zapewnienie rozliczalności podejmowanych działań pracowników, współpracowników, jak i dostawców,
3. Zapewnienie ciągłości działania procesów biznesowych i właściwej reakcji na incydenty bezpieczeństwa,
4. Zapewnienie odpowiedniego poziomu wiedzy dotyczącej bezpieczeństwa informacji wśród pracowników i współpracowników oraz ciągła edukacja i budowanie szerokiej świadomości bezpieczeństwa informacji.

3. System Zarządzania Bezpieczeństwem Informacji (SZBI)

Aby zapewnić realizację celów SZBI bazuje na następujących założeniach:
1. Dopasowanie do kontekstu Spółki - SZBI musi być dopasowany do kontekstu zewnętrznego i wewnętrznego Spółki, z uwzględnieniem prowadzonych operacji, jak i ich skali;
2. Skuteczność SZBI - SZBI musi zapewnić wysoki współczynnik skuteczności zgodności i bezpieczeństwa w powiązaniu do ustalonego poziomu akceptowalnego ryzyka;
3. Efektywność SZBI - SZBI musi zapewnić wysoki stosunek skuteczności osiąganych rezultatów do kosztów jego wdrożenia i utrzymania;
4. Łatwość stosowania i zwinność - SZBI musi opierać się na minimalnych wymaganiach formalnych, bezpieczeństwo musi być scalone z istniejącymi procesami organizacyjnymi, a zmiany systemu muszą być dopasowane do dynamicznych warunków rynkowych.
5. SZBI jest referencyjny względem normy ISO27001:2022
6. SZBI opiera się na podejściu procesowym i cyklu Deminga (PDCA - Plan, Do, Check, Act). Podejście to składa się z następujących działań:

6.1. przygotowania i wdrożenia,
6.2. funkcjonowania i utrzymywania,
6.3. zarządzania ciągłością działania,
6.4. zmian i ciągłego doskonalenia.

7. W ramach SZBI kluczowym elementem jest proces zarządzania ryzykiem.
8. Sposób funkcjonowania SZBI regulują odrębne dokumenty bezpieczeństwa informacji.

4. Inicjatywy bezpieczeństwa Informacyjnego

Określone cele bezpieczeństwa informacyjnego w ramach SZBI realizowane są po przez następujące inicjatywy:

1. Zapewnienie stałego przywództwa i wsparcia dla rozwoju i doskonaleniu SZBI,
2. Właściwe struktury i procesy SZBI oparte na zintegrowanym podejściu GRC (governance, risk, compliance), wpisane w wewnętrzny ład organizacyjny Spółki,
3. Właściwe udokumentowanie SZBI, wynikające z wymogów zewnętrznych i potrzeb wewnętrznych,
4. Bieżące zarządzanie ryzykiem, w celu posiadania adekwatnych informacji do podejmowana świadomych decyzji zarządczych oraz dążenie ograniczenia ryzyka do akceptowalnych poziomów, przy zachowaniu równowagi koszty / korzyści,
5. Właściwą ochronę informacji, w szczególności informacji prawnie chronionych oraz praw autorskich i majątkowych,
6. Zapewnienie odpowiedniego poziomu poufności, dostępności i integralności informacji w systemach informacyjnych, jak i niezawodności systemów informatycznych,
7. Stałe podnoszenie świadomości i zaangażowania pracowników w budowanie kultury i standardów bezpieczeństwa informacji,
8. Okresowe monitorowanie, przeglądy oraz audyty SZBI.

5. Odpowiedzialności i role

1. Za bezpieczeństwo informacji odpowiedzialny jest każdy pracownik i współpracownik C&F S.A.
2. W procesie zarządzania bezpieczeństwem informacji kluczową rolę odgrywają dostawcy oraz poddostawcy w ramach świadczonych usług związanych z procesami łańcucha dostaw.
3. Każdy pracownik, współpracownik oraz dostawca odpowiada on za przestrzeganie zasad bezpieczeństwa wynikających z przyjętych rozwiązań SZBI.
4. Za nadzór oraz przestrzeganie regulacji i zasad SZBI, w tym utrzymanie i doskonalenie odpowiada delegowany przez Zarząd Spółki Pełnomocnik ds. Bezpieczeństwa Informacji (Information Security Officer).
5. Każda z osób wymieniona w p.1-4 dokłada należytej staranności, aby czynności wykonywane w ramach jej roli były niepowątpiewalne, udokumentowane i po ich wykonaniu należycie udowodnione.

6. Zakres stosowania

1. Niniejszy dokument Polityki Bezpieczeństwa Informacji jest dokumentem nadrzędnym nad wszystkimi dokumentami dotyczącymi bezpieczeństwa informacji w Spółce.
2. Zasady określone w niniejszym dokumencie oraz całym SZBI mają zastosowanie do następujących procesów i obszarów działalności:
   2.1. Usługi wytwarzania i utrzymania oprogramowania
   2.2. Usługi konsultingu i analityki zarządzania danymi
   w tym informacji w postaci dokumentów papierowych, elektronicznych i innych, przetwarzanych w systemach i sieciach komputerowych, papierowych i komunikacyjnych będących własnością lub jedynie administrowanych przez Spółkę, w jej siedzibie głównej.
3. Do zapoznania się z właściwymi dokumentami niższego rzędu, stosowania zasad określonych zobowiązani są wszyscy pracownicy w rozumieniu przepisów Kodeksów Pracy, wszystkie osoby współpracujące i inne mające dostęp do informacji podlegającej ochronie.
4. Zasady niniejszej polityki są obligatoryjne w odpowiednim zakresie dla partnerów, dostawców, klientów i kooperantów Spółki, z zastrzeżeniem zasady proporcjonalności, pracowników zaś obligują do zarządzania ryzykiem strony trzeciej.

7. Utrzymanie i aktualizacja

1. Pełnomocnik ds. Bezpieczeństwa Informacji podlega i raportuje bezpośrednio do Dyrektora Operacyjnego.
2. Pełnomocnik ds. Bezpieczeństwa Informacji jest odpowiedzialny, w szczególności za osiągnięcie i utrzymanie odpowiedniego poziomu bezpieczeństwa, przeprowadzanie wspólnie z właścicielami procesów oraz informacji analizy ryzyka, opracowanie i aktualizacja dokumentacji SZBI, budowanie kultury bezpieczeństwa informacji poprzez programy edukacyjne, szkolenia, działania świadomościowe oraz promocyjne, także za nadzór nad realizacją i oceną skuteczności zabezpieczeń oraz monitorowanie skuteczności SZBI.
3. Polityka Bezpieczeństwa Informacji będzie weryfikowana i dostosowana w celu zapewnienia odpowiedniego poziomu bezpieczeństwa wraz ze zmieniającymi się wymaganiami kontekstu wewnętrznego i zewnętrznego, w tym wymaganiami biznesowymi.
4. Niniejszy dokument będzie aktualizowany w przypadku zmiany przepisów związanych z bezpieczeństwem informacji, m.in. celem zapewnienia zgodności z odnośnymi aktami zewnętrznymi prawa i regulatorów.