

BART Sp. z o.o. | POLITYKA BEZPIECZEŃSTWA INFORMACJI I OCHRONY DANYCH OSOBOWYCH

1. Cel i zakres Polityki

Celem niniejszej Polityki Bezpieczeństwa Informacji jest zapewnienie ochrony informacji przetwarzanych w BART Sp. z o.o., ich poufności, integralności i dostępności oraz określenie ram dla tworzenia, wdrażania i doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji (SZBI). Główny cel SZBI, to zapewnienie bezpieczeństwa przetwarzanych informacji oraz ciągłości świadczonych usług z poszanowaniem wymagań prawnych obowiązujących w tym zakresie.

Przetwarzane w BART Sp. z o.o. informacje podlegają nadzorowi i ochronie zgodnie z przepisami prawa i procedurami wewnętrznymi, adekwatnie do zidentyfikowanych zagrożeń.

Informacja jest kluczowym zasobem BART Sp. z o.o., szczególnie w obszarach projektowania, przygotowania inwestycji i realizacji projektów w zakresie generalnego wykonawstwa, czy „projektuj i wybuduj” na rynku budownictwa przemysłowego i obiektów Cleanroom. Nasze zaangażowanie w ochronę informacji jest kluczem do osiągnięcia zakładanych celów, w tym utrzymania zaufania naszych Klientów, partnerów i innych interesariuszy. Mamy świadomość kluczowej roli bezpieczeństwa informacji dla wartości i wizerunku Spółki.

Dokument obejmuje wszystkich pracowników, współpracowników, dostawców oraz inne osoby mające dostęp do informacji firmy, niezależnie od formy ich przetwarzania (papierowej, elektronicznej, ustnej).

2. Cele bezpieczeństwa informacji

Cele BART Sp. z o.o. w zakresie bezpieczeństwa informacji obejmują:

- 1) Ochronę informacji przed nieautoryzowanym dostępem, ujawnieniem, utratą, modyfikacją lub zniszczeniem.
- 2) Zapewnienie ciągłości działania procesów kluczowych dla organizacji.
- 3) Ograniczenie ryzyka związanego z naruszeniem bezpieczeństwa informacji.
- 4) Zapewnienie zgodności z obowiązującymi przepisami prawa, w tym z przepisami o ochronie danych osobowych. Spełnienie wymagań prawnych i kontraktowych.
- 5) Podnoszenie świadomości pracowników w zakresie bezpieczeństwa informacji.
- 6) Stałe doskonalenie systemu zarządzania bezpieczeństwem informacji.
- 7) Budowanie zaufania do marki BART i BT Cleanroom Engineering.

3. Podstawowe pojęcia

Stosowane definicje (zgodne ze słownikiem pojęć ISO/IEC 27001):

- 1) Informacja – każdy zasób danych mający wartość dla firmy, niezależnie od formy jej przetwarzania.
- 2) Bezpieczeństwo informacji – zapewnienie poufności, integralności i dostępności informacji.
- 3) Incydent bezpieczeństwa – każde zdarzenie, które może prowadzić do naruszenia bezpieczeństwa informacji
- 4) Uprawniony dostęp – dostęp do informacji mają tylko osoby przeszkolone i upoważnione.
- 5) Minimalizacja uprawnień – dostęp ograniczony jest do niezbędnych danych.
- 6) Świadomość zbiorowa – wszyscy pracownicy są świadomi konieczności ochrony informacji.
- 7) Odpowiedzialność indywidualna – każdy odpowiada za bezpieczeństwo informacji w swoim zakresie.
- 8) Gotowość systemu – systemy muszą być przygotowane na zagrożenia.
- 9) Ewolucja – mechanizmy bezpieczeństwa są stale doskonalone.
- 10) Ochrona poufności - zabezpieczenie informacji przed dostępem do niej osób nieuprawnionych.

- 11) Ochrona integralności - zabezpieczenie informacji przed wprowadzeniem przypadkowych lub celowych zmian powodujących jej zafałszowanie.
- 12) ochrona dostępności - zabezpieczenie informacji przed jej zniszczeniem, jak również zapewnienie takiego działania systemu informatycznego, aby dane były dostępne dla osób upoważnionych do dostępu do nich, a także do ich przetwarzania.

4. Zakres działań w związku z realizacją celów

Cele SZBI są realizowane poprzez:

- 1) zdefiniowanie odpowiedzialności w obszarze bezpieczeństwa informacji,
- 2) zabezpieczenie wykorzystywanych aktywów informacyjnych oraz systemów informatycznych poprzez wdrożenie odpowiednich mechanizmów mających na celu minimalizację zagrożeń i zapewnienie ochrony przed nieupoważnionym dostępem, fizycznym zniszczeniem, działalnością szkodliwego oprogramowania oraz utratą poufności, integralności i dostępności informacji,
- 3) określenie ścieżek komunikacji oraz zasad postępowania w sytuacjach awaryjnych i wystąpienia incydentu w obszarze bezpieczeństwa informacji,
- 4) podnoszenie świadomości, wiedzy i zaangażowania pracowników w zakresie bezpieczeństwa informacji,
- 5) zapewnienie zgodności realizowanych działań z obowiązującymi przepisami prawa, w tym RODO, regulacjami wewnętrznymi oraz umowami i wymaganiami kontraktowymi dotyczącymi ochrony informacji.
- 6) opracowanie klasyfikacji oraz zasad postępowania z informacją,
- 7) systematyczne zarządzanie ryzykiem bezpieczeństwa informacji zgodnie z ustaloną i przyjętą metodyką i planem postępowania z ryzykiem.

5. Zakres odpowiedzialności

- 1) **Prezes Zarządu BART Sp. z o.o.** (PZ) odpowiada za ustanowienie, zatwierdzenie i okresowy przegląd niniejszej Polityki oraz zapewnienie zasobów do jej realizacji. **Prezes Zarządu BART Sp. z o.o.**, jako Administrator Danych Osobowych (ADO) wyznacza **Pełnomocnika ds. Systemu Zarządzania Jakości ISO i Koordynatora Bezpieczeństwa Informacji (PZ)**, oraz **Administratorsa Systemu Informatycznego (ASI)**.
- 2) **Koordynator Bezpieczeństwa Informacji** jest odpowiedzialny za wdrożenie, monitorowanie i doskonalenie SZBI, sprawuje nadzór w imieniu Prezesa nad przestrzeganiem obowiązujących zasad bezpieczeństwa informacji i danych osobowych.
- 3) **Administratorsa Systemu Informatycznego (ASI)** dba o bezpieczeństwo i utrzymanie ciągłości działania sieci teleinformatycznych oraz systemów i oprogramowania używanego w Spółce. Zapewnia gotowość systemu i proponuje jego ewolucję.
- 4) **Kierownicy działów** są zobowiązani do wdrażania zasad bezpieczeństwa informacji w podległych im obszarach. Przydzielają dostęp podległym pracownikom według zasady minimalizacji uprawnień.
- 5) **Wszyscy pracownicy** zobowiązani są do przestrzegania zasad określonych w niniejszej Polityce i ponosi odpowiedzialność indywidualną oraz do zgłaszania wszelkich incydentów bezpieczeństwa.

6. Zasady ogólne bezpieczeństwa informacji

- 1) Wszystkie informacje przetwarzane w BART Sp. z o.o. stanowią aktywa firmy i podlegają ochronie stosownie do ich wartości, wrażliwości i znaczenia dla działalności.
- 2) Informacje muszą być chronione przed nieuprawnionym dostępem, modyfikacją, utratą lub zniszczeniem.
- 3) Dostęp do informacji przyznawany jest wyłącznie osobom uprawnionym, w zakresie niezbędnym do wykonywania obowiązków służbowych.
- 4) Każdy pracownik jest odpowiedzialny za bezpieczeństwo informacji, z którymi pracuje.
- 5) Informacje klasyfikowane są zgodnie z przyjętym *Systemem Klasyfikacji Informacji*.
- 6) Informacje osobowe i poufne muszą być przetwarzane zgodnie z zasadami ochrony danych osobowych (RODO).
- 7) Systemy informatyczne podlegają zabezpieczeniom fizycznym, logicznym i organizacyjnym odpowiednim do poziomu ryzyka.
- 8) Wszelkie incydenty bezpieczeństwa informacji powinny być niezwłocznie zgłaszane Koordynatorowi Bezpieczeństwa Informacji.
- 9) Pracownicy są zobowiązani do przestrzegania zasad bezpieczeństwa określonych w procedurach, instrukcjach oraz w umowach o zachowaniu poufności.

7. Umowy o poufności

- 1) Informacje powierzone w ramach umów o poufności, które firma BART Sp. z o.o. zawiera z Klientami podlegają procedurom określonym w tych umowach, a zaangażowane osoby dokładają wszelkich starań aby zapewnić odpowiedni poziom bezpieczeństwa informacji powierzonej przez klientów i partnerów oraz wytwarzanej w organizacji w toku realizacji usług projektowych i budowlanych dotyczących tych umów.
- 2) Jednocześnie firma BART Sp. z o.o. przy braku klauzuli zakazującej informowania o uczestnictwie firmy w danym projekcie i procesie budowlanym zastrzega sobie prawo o poinformowaniu rynku o zakresie wykonywanych w tym projekcie prac po jego ukończeniu, z wyłączeniem danych określonych jako niejawne.

8. Dokumentacja SZBI

- 1) Polityka SZBI.
- 2) System Klasyfikacji Informacji.
- 3) Polityka Czystego Biurka.
- 4) Procedury i instrukcje bezpieczeństwa, w tym Procedury i instrukcje z Księgi Jakości PN EN ISO 9001:2015:
 - a. Procedura nr P/P3/01/PZJ - Nadzór nad udokumentowaną informacją (data wydania 25.09.2024).
 - b. INSTRUKCJA I: 02/KIZ/O1 - NADZÓR NAD SPRZĘTEM KOMPUTEROWYM (data wydania: 8.02.2018).
- 5) Instrukcja Administratora Systemu Informatycznego (ASI) dla BART Sp. z o.o. - określająca sposób zarządzania systemem informatycznym, służącym do przetwarzania danych, w tym danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji przygotowana przez firmę informatyczną, której BART Sp. z o.o. powierzył nadzór nad infrastrukturą IT, i która pełni rolę ASI.
- 6) Dokumentacja operacyjna: plan postępowania z ryzykiem, analizy ryzyka, rejestry incydentów.

9. Zarządzanie ryzykiem

BART Sp. z o.o. stosuje podejście oparte na analizie ryzyka w celu identyfikacji, oceny i ograniczania zagrożeń dla bezpieczeństwa informacji.

Ocena ryzyka jest przeprowadzana okresowo lub po każdej istotnej zmianie w strukturze organizacyjnej, technologicznej lub procesowej; oraz w momencie wystąpienia incydentu bezpieczeństwa.

Wyniki analizy ryzyka stanowią podstawę do opracowania *Planu postępowania z ryzykiem* oraz do określenia środków kontrolnych.

10. Szkolenia i świadomość pracowników

Firma zapewnia szkolenia z zakresu bezpieczeństwa informacji oraz prowadzi działania zwiększające świadomość personelu w tym zakresie. W tym rozpoznawania zagrożeń i reagowania na incydenty.

Każdy nowy pracownik jest zapoznawany z zasadami bezpieczeństwa informacji przed rozpoczęciem pracy.

11. Przegląd i doskonalenie polityki

Polityka Bezpieczeństwa Informacji jest przeglądana w przypadku zmian prawnych, organizacyjnych lub technologicznych, które mogą wpływać na bezpieczeństwo informacji.

Zarząd BART Sp. z o.o. deklaruje swoje pełne zaangażowanie w realizację i ciągłe doskonalenie Systemu Zarządzania Bezpieczeństwem Informacji. Zapewnia stosowanie odpowiednich i proporcjonalnych środków technicznych, operacyjnych i organizacyjnych, które mitygują ryzyko bezpieczeństwa informacji.

12. Zatwierdzenie

Niniejsza Polityka wchodzi w życie z dniem jej podpisania przez Zarząd BART Sp. z o.o.
Stanowi dokument nadrzędny w zakresie bezpieczeństwa informacji w firmie i jest dostępna dla wszystkich pracowników.

Zatwierdził: Zarząd BART Sp. z o.o.

Data wejścia w życie: 20.05.2024 r.

PREZES ZARZĄDU
BART Sp. z o.o.
Podpis: 
mgr inż. Roman Burgiel