

Security Policy - Solutions de Repérage Emili Inc.

V1.4

Revision Date: 2023-11-30

Preamble

At Solutions de Repérage Emili Inc. (“Emili”), securing informational assets is of paramount importance. This Security Policy, revised in accordance with Canadian Law C-23, Quebec’s Law 25, and other applicable legislations, establishes mandatory standards for protecting the information and systems of the company.

Scope and Application

This Policy applies to all informational assets of Emili, its subsidiaries and associated companies, and is coherent with our Information Privacy Policy, Personal Information and Security Policy, and Data Erasure Policy.

Objectives

To protect all organizational informational assets against security incidents, including fraud, information leaks, and privacy breaches, aligning with current best practices and legislative framework.

Guiding Principles

- Categorization of informational assets and risk assessment.
- Protection and confidentiality of personal information, in accordance with our Personal Information and Security Policy.
- Availability, integrity, and management of document heritage of information.
- Securing and controlling user accesses, according to established security standards.

Classification of Informational Assets

Informational assets are evaluated and protected based on their level of confidentiality and integrity. This classification guides decision-making related to data management, exploitation, and security.

Roles and Responsibilities

- The CEO of Emili approves and supports the implementation of this Policy.
- The Information Security Officer (ISO) oversees the management and operation of information security.
- Asset owners are responsible for classifying and implementing appropriate security measures.
- Users must comply with regulatory and legal requirements and follow security policies and rules.

Training and Awareness

- Emili commits to educating and training its staff about threats and consequences of security breaches.
- An appropriate training program for different staff roles is established by the ISO.

Compliance

- Staff members must collaborate on any matters related to this Policy.
- Non-compliance with this Policy may result in disciplinary or legal actions.

Revision

- The Policy is reviewed annually to stay in line with legislative, technological evolutions, and our contractual obligations.