

POL Management System Policy

Company Name	Aptus
Effective Date	10/07/2024

Version History

Version	Date	Description	Author	Approved by
1	10/07/2024	-- N/D --	Enrico Lucia	Lorenzo De Mattei

Purpose

Aptus promotes productive/service delivery policies that balance the needs of economic development and value creation inherent to its business activities, with the requirements of environmental protection, social responsibility, and information and data security. It is also committed to complying with applicable regulations, encouraging the spread of a culture of respect for legal principles.

Table of Contents

- Scope
- Normative References
- Terms and Definitions
- Roles and Responsibilities
- Management System Commitment and Objectives
- Archiving and Updates
- Reference Documents

Scope

This policy defines the direction, commitment, and principles that guide the Information Security Management System (ISMS) of Aptus.AI. Its purpose is to protect the company's information assets, in line with the mission of Aptus.AI, the requirements of interested parties, and international standards. This document applies to all processes, activities, technological and human resources that fall within the scope of the ISMS.

Normative References

- **ISO/IEC 27001:2022:** Specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system.
- **Regulation (EU) 2016/679 (GDPR):** General regulation on data protection that strengthens and unifies the protection of personal data for all individuals within the European Union.

Terms and Definitions

- **Availability:** The property of being accessible and usable on demand by an authorised entity.
- **Integrity:** The property of safeguarding the accuracy and completeness of assets.
- **Confidentiality:** The property that information is not made available or disclosed to unauthorised individuals, entities, or processes.
- **Information Security Management System (ISMS):** A systematic approach to managing sensitive company information so that it remains secure. It includes people, processes, and IT systems applying a risk management process.

Roles and Responsibilities

- **Top Management (Board):** Defines, supports, and reviews the information security policy, ensuring alignment with strategic objectives and promoting the continuous improvement of the ISMS.
- **ISMS Manager:** Plans, organises, and monitors activities for the continuous improvement of the Management System, prepares documentation, maintains its updates, and oversees its communication within the organisation.

Management System Commitment and Objectives

The Top Management (Board) of Aptus.AI establishes, implements, and maintains this Information Security Policy in order to define the direction, commitment, and principles that guide the Information Security Management System (ISMS).

Top Management (Board) is committed to ensuring that this policy is:

- **Appropriate to the context of Aptus.AI:** The policy is aligned with the company's mission and vision, which consist of revolutionising regulatory compliance management through Artificial Intelligence solutions (RegTech). It takes into account internal and external factors, interested parties and their requirements, as documented in the "Context Analysis", to adequately protect critical information assets, including customer data, proprietary algorithms, and processed regulatory information.
- **Objective-oriented:** The policy establishes the commitment to define and pursue measurable objectives for information security, focused on safeguarding the confidentiality, integrity, and availability of company assets. It provides the framework for defining these objectives, which are planned and monitored in accordance with the "PRO Objectives and Planning for their Achievement" procedure.
- **Compliant with applicable requirements:** Aptus.AI is committed to meeting all legal, regulatory (including GDPR), and contractual requirements relating to information security, a fundamental aspect of its business model.

- **Focused on continuous improvement:** Top Management (Board) is committed to the continuous improvement of ISMS effectiveness. This commitment is realised through constant performance monitoring, the execution of internal audits, and the conduct of periodic reviews, as defined in the "PRO Management Review" procedure.

Top Management (Board) also ensures that the Information Security Policy:

- Is maintained and made available as documented information, in accordance with the "PRO Documented Information Management Procedure".
- Is communicated to all Aptus.AI personnel and collaborators through appropriate internal channels, such as the company wiki on Notion and periodic training sessions, to ensure its understanding and application. The ISMS Manager is tasked with overseeing this communication.
- Is made available to relevant external interested parties, such as customers and partners, in an appropriate and controlled manner, to demonstrate Aptus.AI's commitment to security and transparency.

Archiving and Updates

This document is managed as controlled documented information. It is reviewed at least annually and updated whenever significant changes occur in the organisational, regulatory, or technological context, subject to Top Management approval.

Reference Documents

- Context Analysis
- PRO Objectives and Planning for their Achievement
- PRO Management Review
- PRO Documented Information Management Procedure