POL Information Security 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

The purpose of this policy is to declare and communicate the Top Management's commitment to protecting the organisation's information assets. This document defines the framework for establishing, implementing, maintaining, and continuously improving the Information Security Management System (ISMS), in order to protect the confidentiality, integrity, and availability of information and to support the company's strategic objectives.

Table of Contents

Scope

This policy establishes the fundamental principles and guidelines for information security management at Aptus. Its purpose is to protect the organisation's information assets in order to ensure operational continuity, minimise risks, and ensure compliance with legal and contractual requirements. The provisions of this document apply to all personnel, processes, data, and technologies that fall within the scope of the Information Security Management System (ISMS).

Normative References

- **ISO/IEC 27001:2022**: Information security management systems — Requirements.
- **Regulation (EU) 2016/679 (GDPR)**: General Data Protection Regulation.

Terms and Definitions

- **Confidentiality**: The property that information is not made available or disclosed to unauthorised individuals, entities, or processes.
- **Integrity**: The property of safeguarding the accuracy and completeness of assets.
- **Availability**: The property of being accessible and usable on demand by an authorised entity.

Roles and Responsibilities

- **Top Management**: Bears ultimate responsibility for the effectiveness of the Information Security Management System, approving the relevant policy and ensuring the availability of the resources necessary for its maintenance and improvement.
- **ISMS Manager**: Ensures the definition, implementation, maintenance, and continuous improvement of the Information Security Management System in accordance with this policy and the reference standards.
- **HR Specialist**: Manages information security aspects throughout the personnel lifecycle, ensuring that employees read and accept company security policies upon hiring and upon updates.
- **VP of Compliance & Legal**: Oversees the identification and monitoring of legal, regulatory, and contractual requirements applicable to information security, ensuring their integration within the ISMS.
- **Compliance Specialist**: Supports the monitoring of company compliance with security requirements, internal policies, and reference standards, collaborating in risk management and audit activities.

Information Security Objectives

Aptus is committed to protecting its information assets to ensure business continuity, minimise damage, and maximise return on investment and business opportunities. The primary objective of the Information Security Management System (ISMS) is to ensure the confidentiality, integrity, and availability of processed information. Top Management periodically defines and reviews information security objectives, ensuring they are measurable, consistent with the business context, and aligned

with legal, regulatory, and contractual requirements. The definition and planning of these objectives are formalised in the document "PRO Objectives and Planning for their Achievement".

Aptus's strategic objectives include:

- Ensuring compliance with applicable laws and regulations, including those on personal data protection.
- Protecting customer information and trade secrets from unauthorised access, modification, or disclosure.
- Ensuring that services provided to customers are resilient and available in accordance with contractual terms.
- Promoting a security culture in which all personnel are aware of their responsibilities.
- Continuously improving the effectiveness of the ISMS through performance monitoring and risk analysis.

Responsibility for overseeing and achieving these objectives lies with Top Management, supported by the ISMS Manager.

Fundamental Principles of Information Security

Security Governance

Top Management approves this policy and all topic-specific policies, demonstrating its commitment to information security. The ISMS Manager is responsible for ensuring that all ISMS documentation, including this policy, is published, communicated to all personnel and relevant interested parties, and kept up to date.

The review of ISMS documentation is conducted at planned intervals and whenever significant changes occur, in accordance with the "PRO Management Review" and "PRO Change Management Procedure". The management of all documentation is described in the "PRO Documented Information Management Procedure".

The HR Specialist ensures that all personnel read and accept the information security policies upon hiring and upon significant updates.

Risk-Based Approach

Aptus adopts a risk management-based approach to information security. All control measures are implemented following a careful assessment of risks to information assets. The ISMS Manager oversees this process, which is formalised in the "PRO Risk Management Procedure", to ensure that risks are identified, analysed, and treated appropriately.

Roles and Responsibilities

Information security is a shared responsibility of all Aptus personnel. Top Management bears ultimate responsibility for the effectiveness of the ISMS. Specific roles and responsibilities relating to security are formally defined and assigned in the document "POL Policy on Roles and Responsibilities in Information Security" and integrated into company job descriptions.

Acceptable Use of Resources

All personnel are required to use information, IT systems, networks, and other associated resources exclusively for authorised business purposes and in compliance with applicable regulations and

internal guidelines. Use of company resources for unlawful activities or activities that could compromise the organisation's security is strictly prohibited. Detailed rules for acceptable use are defined in the "POL Operational Security Policy" and in the "Code of Conduct".

Protection of Information Assets

- **Information Classification**: All information assets must be classified based on their criticality, value, and sensitivity, as established in the "POL Information Classification and Labelling Policy". The protection measures applied must be proportionate to the classification level.
- **Workplace Security (Clear Desk and Clear Screen)**: Personnel must ensure that sensitive information, both in paper and digital format, is protected from unauthorised access. This includes the obligation to lock their workstation when unattended (clean screen) and to securely store documents and removable storage media at the end of the working day (clean desk).
- **Security of Off-Site Assets**: Company assets used outside Aptus's premises, including devices used for remote working, must be protected with adequate measures against theft, loss, damage, and unauthorised access. Each employee is responsible for the physical and logical protection of the devices entrusted to them and for the confidentiality of information processed remotely, as specified in the individual remote working agreement and in the "POL Operational Security Policy".

Reporting of Security Events

All personnel are obliged to promptly report any observed or suspected information security event, weakness, or incident. Reporting channels and procedures are defined in the "PRO Information Security Incident Management Procedure". The ISMS Manager ensures that the reporting process is known to all personnel.

Compliance

Aptus is committed to complying with all legal, regulatory, and contractual requirements applicable to information security. The VP of Compliance & Legal and the Compliance Specialist are responsible for identifying and monitoring these requirements, ensuring they are integrated into the ISMS.

Archiving and Updates

This policy is managed as documented information of the ISMS. It is reviewed at least annually, and whenever significant changes occur in the internal or external context, by the ISMS Manager and approved by Top Management to ensure its continued suitability, adequacy, and effectiveness.

Reference Documents

- PRO Objectives and Planning for their Achievement
- PRO Management Review
- PRO Change Management Procedure
- PRO Documented Information Management Procedure
- PRO Risk Management Procedure
- POL Policy on Roles and Responsibilities in Information Security
- POL Operational Security Policy

- Code of Conduct
- POL Information Classification and Labelling Policy
- PRO Information Security Incident Management Procedure