Information Security Policy

DOCUMENT CLASSIFICATION	Public
DOCUMENT REF	ISMS-DOC-05-4
VERSION	v1.2 final
DATED	27 October 2025
DOCUMENT AUTHOR	Project Manager
DOCUMENT OWNER	IS Officer

Revision history

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES
V1.0 Final	12 Apr 24	Duarte Damas	Development Base version
V1.1 Final	21 Jun 24	Duarte Damas	Items added: 2.3; 2.4; 2.5; 2.6
V1.2 Final	27 Oct 25	Project Manager	Updates: (i) Section 2.6 – Objectives 3 and 9 have been revised to be more generic, in line with the remaining objectives. The associated KPI values have been moved exclusively to the KPI file; (ii) Document reclassification from "Protected" to "Public" following publication on the institutional website.

Distribution

NAME	TITLE
Teams / Sharepoint	

Approval

NAME	POSITION	APPROVEMENT METHOD	DATE	VERSION APPROVED
Joaquim Francisco	Partner	e-mail	13 Set 2024	V1.1
Joaquim Francisco	Partner	e-mail	03.10.2025	V1.1 final
Joaquim Francisco	Partner	e-mail	24.11.2025	V1.2 final

Contents

Tables

1 Introduction

This document defines the information security policy of **AMT Consulting**.

As a modern, forward-looking business, **AMT Consulting** recognises at senior levels the need to ensure that its business operates smoothly and without interruption for the benefit of its customers, shareholders and other stakeholders.

In order to provide such a level of continuous operation, **AMT Consulting** has implemented an Information Security Management System (ISMS) in line with the International Standard for Information Security, ISO/IEC 27001. This standard defines the requirements for an ISMS based on internationally recognised best practice.

The operation of the ISMS has many benefits for the business, including:

- Protection of revenue streams and company profitability
- Ensuring the supply of services to customers
- Maintenance and enhancement of shareholder value
- Compliance with legal and regulatory requirements

AMT Consulting has decided to maintain full certification to ISO/IEC 27001 in order that the effective adoption of information security best practice may be validated by an independent third party, a Registered Certification Body (RCB).

In accordance with ISO/IEC 27001, reference controls detailed in Annex A of the standard should be adopted where appropriate by **AMT Consulting.** These are reviewed on a regular basis in the light of the outcome from risk assessments and in line with information security risk treatment plans. Details of which Annex A controls have been implemented, and which have been excluded are defined in *Statement of Applicability_(SoA) (ISMS-FORM-06-2).*

In addition, enhanced and additional controls from the following codes of practice / Regulations were adopted and implemented where appropriate:

- ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements
- ISO/IEC 27002:2022 - Information security, cybersecurity and privacy protection - Information security controls
- ISO/IEC 27005:2022 - Information security, cybersecurity and privacy protection - Guidance on managing information security risks
- Portuguese Law 58/2019 (ensures national implementation Regulation (EU) 2016/679)

The adoption of these references provide additional assurance to our customers and help further with our compliance with international data protection legislation.

2 Information security policy

2.1 Purpose

This policy establishes the framework for managing and protecting the organization's information assets, ensuring compliance with legal, regulatory, and contractual requirements, and supporting **AMT Consulting**'s Information Security Management System (ISMS).

2.2 Scope

The Information Security Policy applies to all individuals at **AMT Consulting**, including employees, contractors, and third-party associates. It governs the use and protection of all information assets covering digital systems, networks, software applications, and physical documents, regardless of format or medium.

The policy comprehensively covers all activities and processes related to handling information assets, whether on-site, remotely, or via personal devices for official purposes, including operational procedures, data processing, communication activities, and interactions with the organization's information systems.

The broad scope ensures that all information security activities, from daily operations to strategic decisions, are consistently and securely managed, reflecting the organization's commitment to protecting its information assets from threats and vulnerabilities.

2.3 Responsability

The Information Security Policy must be implemented by all **AMT Consulting** departments and business units, in conjunction with IT. The Information Security Policies define the control objectives as they must be applied to all **AMT Consulting** departments.

Top management is committed to satisfying applicable information security requirements and continually improving the Information Security Management System.

Additionally, **AMT Consulting** Management is primarily responsible for the implementation and control of the Information Security Management System (ISMS), including Oversight, Alignment, Approvement, Review and Continual Improvement of Policies. Top Management must also ensure that authorities and responsibilities are assigned for information management functions and compliance with applicable legal obligations, as well as representing the commitment to Information Security.

Employees, including top management and all members of the Information Security Management organizational structure, are responsible for maintaining behaviour consistent with the "Information Security Policy." This includes following all guidelines and procedures for secure handling of information and Data Protection.

Additionally, **AMT Consulting employees are responsible** for **reporting** any suspected policy violations, security incidents, or potential breaches promptly, to the appropriate authority within the organization; **maintain vigilance** and **adopt security best practices** in daily operations. This includes safeguarding credentials and organization assets, using strong passwords, and being cautious with email attachments and links.

Non-compliance with information security rules will be treated as a violation of internal policies and will result in corrective actions as per internal Disciplinary Process and/or applicable laws and regulations.

2.4 Guidelines for Information Security Management

In line to our commitment to robust information security, **AMT Consulting** has implemented an Information Security Management System (ISMS) aligned with the ISO/IEC 27001:2022 standard.

2.4.1 Information Security Definition

Information Security involves protecting the **confidentiality, integrity,** and **availability** of all forms or format of information, including digital data, paper-based documents, and tacit knowledge. It ensures data is safeguarded from unauthorized access, use, disclosure, alteration, or destruction, thereby ensuring the safeguarding of its value, reliability, and accessibility. The scope includes all processes and practices that maintain the safety and confidentiality of an organization's information assets.

2.4.2 Risk Management

Risk Management is the process of identifying, assessing, and controlling threats to an organization’s information assets.

Therefore **AMT Consulting** has established a security governance model that includes the definition of security roles and responsibilities, as well as methodologies for managing and evaluating security risks. This involves identifying, controlling, and eliminating various threats to information. Additionally, **AMT Consulting** has set security requirements for third-party management, aligning with business and customer needs and relevant regulations.

2.4.3 Information security requirements

A clear definition of the requirements for information security within **AMT Consulting** has been agreed upon and is maintained with the internal business to ensure all ISMS activities focus on fulfilling those requirements. Statutory, regulatory, and contractual requirements have also been documented and incorporated into the planning process.

For **AMT Consulting**, an Information Security Management System fundamental principle is that business needs drive the implemented controls. The company regularly communicates these controls to all staff through team meetings and briefing documents.

2.4.4 Security Incidents Management

Security Incident Management within **AMT Consulting** involves defining responsibilities and procedures for managing security incidents. This includes prevention, detection, recording, communication, treatment, and investigation of incidents and vulnerabilities that could compromise information security, personal data protection, or business continuity. A single point of contact is identified for all incident reports. The process ensures incidents are recorded and includes continuous improvement and periodic reviews.

2.4.5 Human Resources Security Management

Human Resources Security at **AMT Consulting** involves that all employees understand and fulfil their information security responsibilities according to their roles. Key measures include, **Wide Dissemination of Information Security Policy** to all employees, contractors, and relevant parties; **Regular Training and Awareness Sessions** to reinforce the importance of information security and individual responsibilities; **Protective Controls During Employment Changes** to protect the interests of both **AMT Consulting** and its employees during processes of starting, changing, or terminating functions.

2.5 Principles Guiding Information Security Activities

The information managed by **AMT Consulting**, including its support processes, systems, applications, and networks, are valuable assets. The loss of **confidentiality, integrity,** and **availability** may lead to a loss of credibility in the services provided by **AMT Consulting**. Therefore, **AMT Consulting** is committed to upholding a robust set of principles that form the bedrock of our Information Security Policy. These principles are integral to our dedication to safeguarding the confidentiality, integrity, and availability of our information assets.

By adhering to these guiding tenets, we ensure a consistent and effective approach to information security, aligning our practices with industry best standards and regulatory requirements. Each principle has been carefully selected to address the diverse aspects of information security, from protecting personal and sensitive data to establishing a resilient and transparent security infrastructure. Below are the key principles that **AMT Consulting** faithfully follows to maintain the highest standards of information security:

- **Confidentiality:** Ensuring information is accessible only to those authorized to have access.
- **Integrity**: Maintaining the accuracy and completeness of data and preventing unauthorized modification.
- **Availability**: Guaranteeing that authorized users have access to information and associated assets when required.
- **Authentication and Identification**: Accurately identifying and authenticating users and entities to ensure that only authorized entities and users can access information systems.
- **Non-Repudiation:** Establishing mechanisms to prevent denial of involvement in transactions or activities, providing proof of the integrity and origin of data.
- **Accountability and Auditing**: Holding individuals and systems accountable for their actions, with regular audits for compliance and security.
- **Privacy:** Protecting personal and sensitive data in compliance with privacy laws and best practices.
- **Principle of Least Privilege and Separation of Duties**: Granting only the minimum levels of access necessary for individuals to perform their functions based on their identity and role, distributing tasks and privileges among multiple roles to prevent conflicts of interest and fraud.
- **Principle of Open Security**: Avoiding reliance on secrecy of design or implementation for security, and ensuring robust, visible security measures.
- **Principle of Defense in Depth**: Implementing multiple layers of security controls to protect against a variety of threats.
- **Principle of Fail Safe**: Designing systems to maintain security posture in the event of failure or compromise.
- **Principle of Zero Trust**: *"Never trust, always verify"* by implementing continuous access verification and minimizing trust zones.

2.6 Information Securities Objectives

Information security objectives are essential for protecting sensitive data, ensuring compliance with regulations, managing risks, and preventing security incidents. **AMT Consulting**'s Information security objectives are based on a clear understanding of business requirements, informed by the management review process, during which the views of relevant interested parties are obtained. These objectives are documented for an agreed period, along with details on how they will be achieved. They are evaluated and monitored as part of management reviews to ensure they remain valid. Any required

amendments will be managed through the change management process. The following objectives have been carefully formulated to address various aspects of our information security framework:

- **Objective 1** – Effective Implementation of ISO27001 and obtain certification
- **Objective 2** – Maintain shareholder confidence by Communicate and report on the information security and ISO 27001 activities and results
- **Objective 3** – provide high-quality customer service and minimize system downtime
- **Objective 4** –Maintain and enhance the information security system to minimise loss of revenue
- **Objective 5** - Manage IT equipment and software to plan for future needs and avoid resource shortages
- **Objective 6** - Increase in Employee Information Security Awareness
- **Objective 7** - Compliance with Legal and Regulatory Requirements
- **Objective 8** - Improvement in Risk Management Effectiveness
- **Objective 9** - efficiently mitigate any information security incidents.

2.7 Continual improvement of the ISMS

At **AMT Consulting**, we understand that the landscape of information security is ever-evolving, with new challenges and threats emerging constantly. Therefore, we are committed to a philosophy of continual improvement in our Information Security Management System (ISMS).

AMT Consulting policy regarding continual improvement is to:

- Continually improve the effectiveness of the ISMS
- Enhance current processes to bring them into line with good practice as defined within ISO/IEC 27001 and related standards
- Achieve ISO/IEC 27001 certification and maintain it on an on-going basis
- Increase the level of proactivity (and the stakeholder perception of proactivity) with regard to information security
- Implementing both internal and external audits. Internal audits, conducted periodically to ensure that our ISMS is functioning as intended and to identify areas for improvement. External audits, conducted by independent parties, provide an objective assessment of our compliance with standards such as ISO/IEC 27001 and relevant legal requirements.
- Review relevant metrics on an annual basis to assess whether it is appropriate to change them, based on collected historical data
- Obtain ideas for improvement via regular meetings and other forms of communication with interested parties
- Review ideas for improvement at regular management meetings in order to prioritise and assess timescales and benefits

- Regularly update our risk assessment and risk management processes to ensure that they accurately reflect the current threat landscape and the organization's risk appetite.
- Continuously update our training programs and awareness initiatives to ensure that all employees are equipped with the latest knowledge and skills to contribute effectively to our ISMS.

By ingraining continual improvement into the core of our ISMS, we ensure that our information security measures remain effective, relevant, and aligned with both our organizational objectives and the evolving nature of cyber threats.

2.8 Information security policy areas

AMT Consulting defines policy in a wide variety of information security-related areas which are described in detail in a comprehensive set of policy documentation that accompanies this overarching information security policy. These policies are designed to work in harmony with this overarching policy and contribute to the comprehensive Information Security Management System of **AMT Consulting**. These include, but are not limited to the set of policies showed in the table bellow.

Each of these policies is defined and agreed by one or more people with competence in the relevant area and, once formally approved, is communicated to an appropriate audience, both within and external to, the organization.

The table below shows the individual policies within the documentation set and summarises each policy's content and the target audience of interested parties.

POLICY TITLE	AREAS ADDRESSED	TARGET AUDIENCE
Internet Access Policy	Business use of the Internet, personal use of the Internet, Internet account management, security and monitoring and prohibited uses of the Internet service.	Users of the Internet service
Cloud Computing Policy	Due diligence, signup, setup, management and removal of cloud computing services.	Employees involved in the procurement and management of cloud services
Mobile Device Policy	Care and security of mobile devices such as laptops, tablets and smartphones, whether provided by the organization for business use.	Users of company-provided mobile devices
BYOD Policy	Bring Your Own Device (BYOD) considerations where personnel wish to make use of their own mobile devices to access corporate information.	Users of personal devices for restricted business use
Teleworking Policy	Information security considerations in establishing and running a teleworking site and arrangement e.g. physical security, insurance and equipment	Management and employees involved in

POLICY TITLE	AREAS ADDRESSED	TARGET AUDIENCE
		setting up and maintaining a teleworking site
Access Control Policy	User registration and deregistration, provision of access rights, external access, access reviews, password policy, user responsibilities and system and application access control.	Employees involved in setting up and managing access control
Dynamic Access Control Policy	Applicability and use of dynamic access controls available in specific environments.	Asset owners and ICT team
Cryptographic Policy	Risk assessment, technique selection, deployment, testing and review of cryptography, and key management	Employees involved in setting up and managing the use of cryptographic technology and techniques
Physical Security Policy	Secure areas, paper and equipment security and equipment lifecycle management	All employees
Anti-Malware Policy	Firewalls, anti-virus, spam filtering, software installation and scanning, vulnerability management, user awareness training, threat monitoring and alerts, technical reviews and malware incident management.	Employees responsible for protecting the organization's infrastructure from malware
Backup Policy	Backup cycles, cloud backups, off-site storage, documentation, recovery testing and protection of storage media	Employees responsible for designing and implementing backup regimes
Logging and Monitoring Policy	Settings for event collection. protection and review	Employees responsible for protecting the organization's infrastructure from attacks
Software Policy	Purchasing software, software registration, installation and removal, in-house software development and use of software in the cloud.	All employees
Technical Vulnerability Management Policy	Vulnerability definition, sources of information, patches and updates, vulnerability assessment, hardening, awareness training and vulnerability disclosure.	Employees responsible for protecting the organization's infrastructure from malware
Network Security Policy	Network security design, including network segregation, perimeter security, wireless networks and remote access; network security management, including roles and responsibilities, logging and monitoring and changes.	Employees responsible for designing, implementing and managing networks
Electronic Messaging Policy	Sending and receiving electronic messages, monitoring of electronic messaging facilities and use of email.	Users of electronic messaging facilities
Online Collaboration Policy	Use of collaboration tools for communication, sharing and video conferencing.	Users of online collaboration tools

POLICY TITLE	AREAS ADDRESSED	TARGET AUDIENCE
Secure Development Policy	Business requirements specification, system design, development and testing and outsourced software development.	Employees responsible for designing, managing and writing code for bespoke software developments
Information Security Policy for Supplier Relationships	Due diligence, supplier agreements, monitoring and review of services, changes, disputes and end of contract.	Employees involved in setting up and managing supplier relationships
Availability Management Policy	Availability requirements and design, monitoring and reporting, non-availability, testing availability plans and managing changes.	Employees responsible for designing systems and managing service delivery
IP and Copyright Compliance Policy	Protection of intellectual property, the law, penalties and software license compliance.	All employees
Records Retention and Protection Policy	Retention period for specific record types, use of cryptography, media selection, record retrieval, destruction and review.	Employees responsible for creation and management of records
Privacy and Personal Data Protection Policy	Applicable data protection legislation, definitions and requirements.	Employees responsible for designing and managing systems using personal data
Clear Desk and Clear Screen Policy	Security of information shown on screens, printed out and held on removable media.	All employees
Social Media Policy	Guidelines for how social media should be used when representing the organization and when discussing issues relevant to the organization.	All employees
HR Security Policy	Recruitment, employment contracts, policy compliance, disciplinary process, termination	All employees
Acceptable Use Policy	Employee commitment to organizational information security policies.	All employees
Asset Management Policy	This document sets out the rules for how assets must be managed from an information security perspective.	All employees
Configuration Management Policy	The secure configuration of hardware, software, services and networks.	Employees responsible for designing systems and managing service delivery
Information Deletion Policy	The deletion of information stored in information systems, devices or in any other storage media, when no longer required.	Employees responsible for designing and managing systems using personal data
Data Masking Policy	The use of data masking techniques such as anonymization and pseudonymization to protect personally identifiable information (PII).	Employees responsible for designing and managing systems using personal data
Data Leakage Prevention Policy	The configuration of relevant software tools to detect and prevent leakage of data.	Employees responsible for designing systems and managing service delivery

POLICY TITLE	AREAS ADDRESSED	TARGET AUDIENCE
Monitoring Policy	The monitoring of the ICT environment to detect anomalous activity.	Employees responsible for designing systems and managing service delivery
Web Filtering Policy	Restricting access to Internet sites that are deemed inappropriate.	Employees responsible for designing systems and managing service delivery
Secure Coding Policy	The principles that will be used when developing secure code.	Employees responsible for designing, managing and writing code for bespoke software developments
Threat Intelligence Policy	The collection and use of threat intelligence at the strategic, tactical and operational levels.	Employees responsible for protecting the organization's infrastructure from attacks
Whistleblowing Policy	The raising of issues about information security within the organization.	All employees and other interested parties

Table 1: Set of policy documents

2.9 Application of information security policy

The policy statements made in this document and in the set of supporting policies listed in Table 1 have been reviewed and approved by top management of **AMT Consulting** and must be complied with. Failure by an employee to comply with these policies may result in disciplinary action being taken in accordance with the organization's *Employee Disciplinary Process (ISMS-DOC-A06-4-1).*

Questions regarding any **AMT Consulting** policy should be addressed in the first instance to the employee's immediate line manager.

3 Areas of the standard addressed

The following areas of the ISO/IEC 27001 standard are addressed by this document:

- 5 Leadership
  - 5.1 Leadership and commitment
  - 5.2 Policy
- A.5 Organizational controls
  - A.5.1 Policies for information security

4 Review frequency

This document is reviewed as part of an annual exercise which also covers key documents such as the risk assessment and training plan.