ISO27001:2022
Information Security Policy

Company of reference	**APPLIED**
Scope of application	Companies within the Applied Group
Scope of the document	ISMS
Code	APPL-ISMS-PL-001
Full document name	APPL-ISMS-PL-001-Information Security Policy-v02
Document:	Information Security Policy
Version	No.2 dated 09/05/2025
Language	English
Approving Authority	Head of P & S Committee
Author	Cyber Security & Compliance Manager
Date of approval	09/05/2025
Data Classification	Public

REVIEW HISTORY **3**

1. INTRODUCTION **4**

2. DEFINITIONS **5**

3. PURPOSE **6**

4. SCOPE OF APPLICATION **7**

5. APPLIED GROUP SECURITY MANAGEMENT SYSTEM **8**

6. STRATEGIC SECURITY OBJECTIVES **9**

6.1 Business Strategy towards Current Regulations 9
6.2 technological innovation 9
6.3 Data Protection (Employees, Clients, Suppliers, third parties) 9
6.4 Applied's Objectives and Priorities 9
6.5 Systems and Technologies 9
6.6 Outsourcer and Suppliers 9
6.7 Human Resources 10
6.8 Ensuring Business Continuity 10

7. INFORMATION SECURITY MANAGEMENT SYSTEM OBJECTIVES **10**

7.1 Security Policies 10
7.2 User Responsibilities 11
7.3 Organisation of Security 11
7.4 Human resource security 12
7.5 Training and Continuous learning 12
7.6 Privacy 12
7.7 Data Classification & Protection Model 12
7.8 Asset management 13
7.9 Access control 13
7.10 Cryptography 13
7.11 Physical & environmental security 13
7.12 Operations security 13
7.13 Communications security 14
7.14 System acquisition, development and maintenance 14
7.15 Supplier relationships 14
7.16 Information security incident management 14
7.17 Business continuity management 14
7.18 Compliance 14
7.19 Climate Change 15

8. DUTIES AND RESPONSIBILITIES **15**

8.1 Steering Committee 16
8.2 Head of P & S Committee 16
8.3 Head of Staff 17
8.4 Cyber Security & Compliance Manager 18
8.5 ICT Manager / Service Manager 19

REVIEW HISTORY

Version	Date	Author	Comments
0.1	27/03/2024	Cyber Security & Compliance Manager	Document creation
0.1	02/05/2024	Head of P&S Committee	Document approval
0.2	15/04/2025	Cyber Security & Compliance Manager	Duties update, including detail of responsibilities and authority
0.2	09/05/2025	Head of P&S Committee	Document approval

1. INTRODUCTION

The set of organisational structures, policies, procedures, controls and technologies designed to protect IT resources and, more generally, the company's information assets is commonly understood as an Information Security Management System (ISMS).

The **ISO 27001:2022** standard *(now fully named ISO/IEC 27001:2022/Amd 1:2024, and which now introduces new action changes and requirements with regard to Climate Change)* is an international reference standard for Information Security, which sets out the requirements for establishing an Information Security Management System.

The term *Information Security* throughout this document refers to a set of measures designed to guarantee the three fundamental principles of security:

- **Confidentiality**: as the risk that access to information (meaning data or programmes) is granted or denied inappropriately;
- **Integrity**: as the risk that information is modified or deleted, accidentally or intentionally, by those who are not qualified to do so;
- **Availability**: as the risk that information is not available when needed.

Information protection must also follow the **7 Cyber levels**:

Level	Goal
Physical Security	Securing access to infrastructure and hardware
Network Security	Protecting network infrastructure and data flow
Perimeter Security	Controlling network access through routers and gateways
Endpoint Security	Protecting devices connected to the network
Application Security	Securing software and applications running on the network
Data Security	Securing data storage and transmission in the network
User Security	Raising user awareness of cyber security best practices

2. DEFINITIONS

Need To Know

The principle whereby users only access data that is strictly necessary for them to perform their duties (i.e. according to the tasks assigned to them by the company).

Risk

A risk is an event that could potentially have a negative impact on achieving business objectives. This is proportional to the loss value in the company's business framework and depends on the estimated frequency with which this loss could occur.

Segregation of Duty

The principle aims to divide activities in such a way as to avoid the simultaneous concentration of multiple critical activities under the same person or role.

ISMS (Information Security Management System)

The set of policies, procedures, guidelines, resources and associated activities managed by an organisation to protect its information assets. An ISMS is a systematic approach to establishing, implementing, conducting, monitoring, reviewing, maintaining and improving an organisation's information security to achieve its business objectives.

Information Security

Confidentiality, integrity and availability of information may be preserved; other relevant assets may also be involved, such as authenticity, accountability, non-repudiation and reliability.

Confidentiality

The right whereby information is not made available or disclosed to unauthorised individuals, entities or processes.

External Framework

The external framework in which the organisation seeks to achieve its objectives.

Internal Framework

Internal framework in which the organisation seeks to achieve its objectives.

Availability

The right to be available and accessible upon request by an authorised entity.

Integrity

The safeguarding of accuracy and completeness of assets.

Interested Party

A person or organisation that can influence or be influenced by a decision or activity.

Requirement

Whereby information is not made available or disclosed to unauthorised individuals, entities or processes.

3. PURPOSE

The purpose of this document is to establish the general and strategic direction to be pursued in order to prevent risks associated with information processing and to protect the information assets of the company and its legal entities.

Specifically, this information security policy has been defined by taking into account best practices in information security, as well as by focusing on the following standards:

- ISO/IEC 27001:2022/Amd 1:2024 Information Technology – Information Security Management Systems – Requirements;
- ISO 27002:2022 Information Technology – Code of Practice for Information Security Controls.

4. SCOPE OF APPLICATION

This document must be considered as a reference source on the topics in question by all the Applied Group entities and must be applied in each company in compliance with the central policy.

This policy applies to all users of the Applied Goup, including employees, external service provider personnel, and other types of collaborators. Group personnel will take measures to ensure compliance with this policy.

This policy cancels and replaces any previous procedures issued on this subject and is effective immediately.

5. APPLIED GROUP SECURITY MANAGEMENT SYSTEM

Applied has set itself a series of 'Strategic Security Objectives' aimed at ensuring that:

- Corporate security strategies are achieved
- Confidentiality, integrity and availability of information assets are maintained.

The Strategic Objectives are broken down into more detailed and technical ISMS Objectives, which are described in this document.

The ISMS Objectives, as per international standard ISO27001:2022, include all activities and controls that enable the creation and continuous monitoring of an information security management system. The output of the measurement procedures for the Strategic Objectives and ISMS Objectives results in a list of security measures that need to be implemented in order to pursue the aforementioned objectives.

In conclusion, in order to ensure adequate levels of security in relation to the above principles, the companies within the Applied Group aim to achieve the following objectives, divided into the two categories described below:

- ***Strategic Security Objectives***, aimed at achieving strategic business security objectives in compliance with the principles of confidentiality, integrity and availability of information assets.
- ***ISMS Objectives,*** aimed at the implementation, maintenance and continuous improvement of the management system, as well as instrumental to the achievement of the 'Strategic Security Objectives'.

6. STRATEGIC SECURITY OBJECTIVES

In order to ensure complete alignment between its business strategy and the protection of corporate information assets, Applied has defined specific Security Strategy objectives.

The Risk Management process ensures the management of risks that threaten the achievement of these objectives.

6.1 Business Strategy Towards Current Regulations

Ensuring compliance with specific regulations in force on security, privacy, confidentiality, personal data processing and protection, while also monitoring any changes to these regulations.

6.2 Technological Innovation

Ensuring adequate levels of information protection in line with the service's objectives, even when facing technological innovations and advances and related risks, including cyber risks, such as data loss and data breaches.

6.3 Data Protection (employees, clients, suppliers, third parties)

Ensuring system security, the integrity of archived documentation and service availability for employees and third parties. Safeguarding confidential client information from potential risks such as unauthorised access, data loss and data breaches. Ensuring compliance with the security clauses required by the client.

6.4 Applied's Objectives And Priorities

Ensuring compliance with strategic objectives and business priorities, including those related to the protection of personal and confidential data.

6.5 Systems and Technologies

Ensuring the technology supporting operational activities is efficient in order to limit the impact on the Group's profitability, thereby preventing any misalignment between IT strategies and business strategies.

6.6 Outsourcer and Suppliers

Ensuring service level control provided by suppliers and compliance with security clauses defined in service level agreements (SLAs).

6.7 Human Resources

Ensuring the ability to recruit and retain sufficiently qualified and competent personnel in order to limit the likelihood of security incidents occurring due to errors or unauthorised access by service personnel.

6.8 Ensuring Business Continuity

Ensuring service continuity and availability in the event of disasters or malfunctions.

7. INFORMATION SECURITY MANAGEMENT SYSTEM OBJECTIVES

The general security requirements and principles are contextualised within the organisation through operational and regulatory objectives aimed at supporting the implementation and maintenance of the ISMS.

In accordance with the principles established within the ISO27001 standard, the ISMS must achieve the following main objectives:

- Security Policies
- User Responsibilities
- Security Organisation
- Human Resources Security
- Privacy
- Asset Management
- Access Control
- Cryptography
- Physical & Environmental Security
- Operations Security
- Communications Security
- System acquisition, development and maintenance
- Supplier relationships
- Information security incident management
- Business continuity management
- Compliance

The security domains listed above are described in detail below:

7.1 Security Policies

Providing guidelines and support for security issues in accordance with business requirements, laws and regulations. Detailed policies on specific topics are formalised, disclosed to the entire company and available within the ISMS document on the company SharePoint.

7.2 User Responsibilities

Ensuring that the Applied Group employees are fully aware of the central role that users themselves play in data protection and reporting suspicious circumstances. The training provided is aimed at disseminating "best practices". Please find below some rules shared in the "Fundamentals of Cyber Security" course, which is mandatory for all employees:

- ***Safeguard company devices properly*** (safeguard company devices and lock your computer screen when you leave your workstation).
- ***Use company resources correctly*** (do not remove, install, or modify any hardware or software components without prior authorization).
- ***Keep your workstation "clean"*** (pay attention to sheets, charts, notes, or any other paper documents from which personal or confidential information about Applied could be deduced, even indirectly).
- ***Protect the confidential part of your personal credentials*** (keep your passwords/PINs safe with the utmost care and do not disclose them to others. Be sure to change your password if you suspect a breach).
- ***Use the Internet correctly*** (do not download free software and do not send confidential company information unless expressly authorized to do so).
- ***Use email correctly*** (use company email only for work purposes and report any suspicious emails through the dedicated channel).
- ***File compression and encryption*** (7-zip is the compression and encryption tool recommended by Applied. It must be used to send personal data, while sending the password by other means).
- ***Report security incidents promptly*** (report any cases of security breaches or suspected breaches without delay)
- ***Pay attention to the Nature of the Information*** (use the labels implemented by Applied to distinguish the level of confidentiality of the information: Secret, Confidential, Restricted, Public).

7.3 Security Organisation

Establishing a Management Framework to launch and maintain the security management system with adequate allocation of resources and responsibilities, as well as ensuring the security of teleworking and the use of mobile devices.

7.4 Human Resources Security

Ensuring that management, personnel, partners, employees, and key suppliers understand their responsibilities, and fully comply with and fulfil their security responsibilities, as well as that Applied's interests are protected in the process of selecting, hiring, modifying, or terminating employment.

In the event of misconduct or violations of Information Security policies, employees will be subject to warnings/disciplinary measures in accordance with the relevant national collective labour agreement.

7.5 Training And Continuous Learning

Applied provides training on cyber security, data classification, and specific topics. Phishing campaigns and training sessions are planned with the aim of increasing awareness and sensitivity among all employees.

7.6 Privacy

Ensuring that Applied has proper processes' and procedures' management and periodic updates to guarantee personal data protection within the company. This applies in particular to employee, collaborator, supplier, and client data.

The Group companies keep a Processing Register (by using the *Utopia* platform), where the processing operations carried out are updated, both with regard to the Register as Data Controllers and as Data Processors for their clients. Please refer to the policy ***"APPL-GDPR-PL-001-Group Data Protection Management-v01"*** for a full explanation of the principles on which the defined model and key processes are based.

7.7 Data Classification & Protection Model

Ensuring that Applied personnel know how to appropriately classify the information they handle and apply the most adequate security measures at each identified level (Secret, Confidential, Restricted, and Public).

7.8 Asset Management

Identifying the Group's resources, defining appropriate responsibilities for protection, developing security controls proportionate to the importance of the asset, and preventing unauthorized disclosure, modification, removal, or destruction of information stored on media.

This also includes security measures relating to mobile devices' management (implementation of MAM – Mobile Application Management found in all company applications accessed through an Applied account on the device, whether company or personal, Android and iOS).

7.9 Access Control

Restricting access to information and systems in accordance with the principle of least privilege, ensuring access for authorised users and preventing unauthorised access to systems and services, making users responsible for safeguarding their authentication information (username, password, any tokens or secure codes) and preventing unauthorised access to systems and applications.

7.10 Cryptography

Ensuring the correct and effective use of encryption to protect the confidentiality, authenticity and/or integrity of information.

7.11 Physical & Environmental Security

Preventing unauthorised physical access, damage and interference with information and information processing systems, as well as other facilities, and preventing unauthorised access, loss, damage, theft or compromise of company assets and disruption of operations.

7.12 Operations Security

Ensuring the correct and secure operation of information processing systems, the protection against malware and data loss, and preventing the exploitation of technical vulnerabilities by wrongdoers.

Ensuring adequate controls to record events and provide evidence, ensuring the integrity of operating systems and minimising the impact of control activities on the systems themselves.

7.13 Communications Security

Ensuring the protection of information in telecommunications networks and maintaining the security of information transferred either internally or to external organisations.

7.14 System Acquisition, Development And Maintenance

Ensuring that information security and data protection are an integral part of the information systems lifecycle, starting from the design, testing and implementation of systems and/or services.

7.15 Supplier Relationships

Ensuring the protection of assets accessible by key suppliers, maintaining the agreed level of information security, and providing services in line with established agreements.

7.16 Information Security Incident Management

Ensuring a consistent and effective approach to security incident management (e.g., detection, containment, and resolution), and ensuring communication and sharing of security events and vulnerabilities.

7.17 Business Continuity Management

Implementing controls for crisis management, business continuity and disaster recovery, ensuring that information security continuity is incorporated into business continuity management systems, as well as ensuring that the availability of facilities supporting the processing is guaranteed by means of several systems.

7.18 Compliance

Preventing breaches of legal, statutory, regulatory or contractual requirements relating to security and ensuring that security is implemented and managed in accordance with applicable policies and procedures.

7.19 Climate Change

The issue of climate change is highly relevant today and also impacts information security management systems. Applied has determined that climate change is a significant issue and it has implemented specific measures (reported in the document "***APPL-ISMS-LG-ISMS Manual-v01***").

8. DUTIES AND RESPONSIBILITIES

Information security management must be an integral part of business objectives and must involve the necessary resources at every organisational level. It is essential that information security is supported, both visibly and practically, by senior management.

There are specific aspects of the management system in which senior management shows both leadership and commitment. These include, but are not limited to:

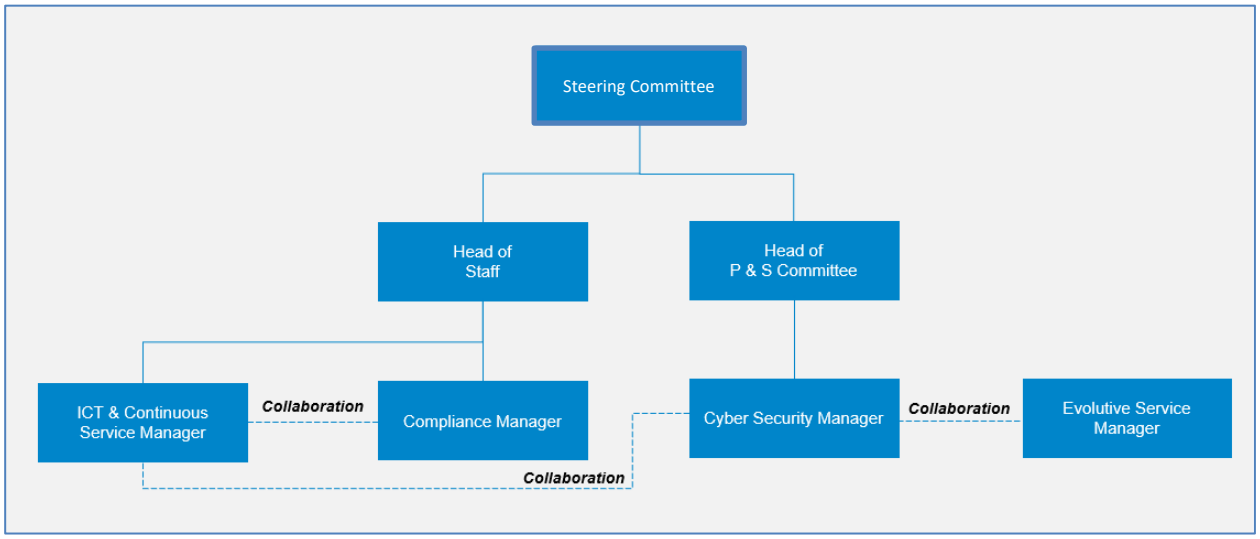
- Taking accountability for the effectiveness of the ISMS.
- Ensuring that policies and objectives are established and are compatible with the context and strategic direction of the organisation.
- Ensuring that ISMS integration is incorporated into business processes.
- Promoting the use of the risk-based approach and strategy.
- Ensuring that adequate resources are available.
- Ensuring that the ISMS achieves its intended results.
- Involving, directing and supporting people to contribute to the effectiveness of the ISMS.

The Applied Group has identified **the organisational model for information security management** described below. The responsibilities and authorities for each role within the Information Security Management System are detailed.

Within the Information Security Management System (ISMS), each corporate role must be clearly defined in terms of responsibilities and authority, as required by the ISO27001 standard.

- ***Responsibility***: refers to the obligation assigned to a person or function to perform certain tasks, ensure that security objectives are met, and ensure compliance with ISMS requirements. Responsibility also implies the duty to report on actions taken.

- ***Authority***: constitutes the right conferred upon a person or function to make decisions, approve activities and resources, issue instructions or take action within the scope of the ISMS.



8.1 Steering Committee

Responsibilities

- Defining the strategic vision for information security.
- Ensuring that information security is integrated into business processes.
- Taking note of management reviews.

Authority

- Allocating resources for the implementation and maintenance of the ISMS in a continuous improvement perspective.

8.2 Head of P & S Committee

Responsibilities

- Assessing and approving suggestions made by the Cyber Security & Compliance Manager.
- Ensuring the economic and strategic oversight of information security.

- Verifying that the suggested choices are compatible with business objectives as well as sustainable in terms of resources.
- Actively participating in management reviews.
- Approving the Information Security Policy and other documents belonging to the ISMS documentation.

Authority

- Approving:
  - Information Security Budget
  - Key documents (policy, risk assessment, disaster recovery)
  - Strategic initiatives for security and compliance
- Withholding or postponing the implementation of non-priority measures.

8.3 Head of Staff

Responsibilities

- Ensuring that HR/procurement/legal/physical security and other processes in the STAFF area are aligned with security policies.
- Coordinating the inclusion of security controls in suppliers' contracts and in recruitment processes.
- Coordinating any emergencies (unavailability of buildings, people, strategic suppliers and systems).

Authority

- Amending or updating HR/procurement/legal/physical security processes and other processes in the STAFF area to align them with ISMS requirements.
- Authorising the emergency event to be managed in coordination with other key figures (IT Manager, Cyber Security & Compliance Manager, HR Manager, depending on the event).

8.4 Cyber Security & Compliance Manager

Responsibilities

- Designing, implementing and updating the ISMS.
- Drafting and keeping the ISMS documentation (policies, operating procedures, guidelines and models), including:
    - ISMS Policies
    - Risk Assessment & Risk Treatment
    - Security Controls
    - Audit programme
    - Business continuity policy and plan
    - Disaster recovery plan
- Coordinating security incident management.
- Monitoring regulatory compliance (e.g. ISO 27001, GDPR, NIS2).
- Conducting the BIA (Business Impact Analysis) annually.
- Developing and monitoring the information security management programme.
- Ensuring that all security controls are implemented and effective.
- Training and raising awareness among employees on information security.
- Performing internal audits to verify ISMS compliance.
- Ensuring that appropriate control measures are implemented.
- Preparing audit reports and following up on corrective actions.
- Coordinating and implementing the ISMS, ensuring that the organisation complies with information security requirements and regulatory compliance (e.g. GDPR, ISO 27001).
- Identifying and managing information security risks.
- Developing and implementing policies and procedures to ensure data and IT resources security.
- Issuing information security policies, including guidelines for protecting company data and managing IT risks.
- Issuing operating procedures for security and business continuity management, ensuring that all employees comply with the required security standards.
- Coordinating the implementation of security solutions, such as firewalls, antivirus software, encryption and access management, to protect company systems.
- Manage the disaster recovery plan, defining specific procedures for restoring operations in the event of significant disruptions.

- Monitoring security incidents and managing their responses, ensuring that they are documented and analysed to prevent future events.
- Continuously analysing relevant regulations (National, European, International).
- Managing the Compliance Office in relation to all matters concerning the GDPR with various stakeholders (employees, clients, suppliers, partners).

Authority

- Launching ISMS projects and defining risk treatment plans.
- Suggesting security measures and recovery plans.
- Requesting the temporary suspension of activities or systems in the event of serious breaches.
- Reporting non-compliance and areas for improvement to Management.
- Providing recommendations for corrective and preventive actions.
- Implementing policy changes based on audit findings, security incidents or regulatory developments.
- Making operational decisions for information security management and in relation to GDPR.
- Coordinating security incident recovery and response, in collaboration with the IT team and other business functions.
- Conducting periodic audits to verify compliance with security policies and ISMS performance.

8.5 ICT Manager (supported by the Service Manager if necessary)

Responsibilities

- Executing the technical controls outlined in the risk treatment plan
- Managing:
    - Access control
    - Backup and restore
    - Patch management
    - Monitoring and alerting systems
- Collaborating on the definition and implementation of the Disaster Recovery Plan.
- Ensuring the operational continuity of critical IT infrastructures.
- Collaborating on periodic backup and DR testing.
- Ensuring the operational continuity of critical IT infrastructure.

- Collaborating on periodic backup and DR testing.
- Working with the Cyber Security & Compliance Manager to implement security solutions.
- Ensuring through continuous monitoring that all activities within their areas of responsibility promptly meet the requirements of technology policies and procedures with regard to the implementation and operational management of protective countermeasures.
- Administrating and managing the technology, information and company data underlying multiple technical operations (related to hardware, software and networks in physical or virtual environments)
- Managing the technological resources lifecycle.
- Managing wireless and wired network operations.
- Managing security against potential data breaches (for example by using firewalls, antivirus and antispam software).
- Managing mobile connectivity.
- Managing the maintenance of all elements that constitute the IT infrastructure.

Authority

- Making urgent technical changes to ensure security or restore services.
- Defining IT recovery priorities based on the DR plan.
- Isolating compromised systems to contain incidents.
- Taking operational actions to ensure IT system security and implement technical controls.