M-Cube Group

Global Information Security Policy

DOCUMENT CLASSIFICATION	Public
DOCUMENT REF	ISMS-PLS-05
APPROVED BY	CEO

Revision history

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES
1	27/03/2022	Alexandre Lienard	First release
2	31/12/2023	Andrea Ceiner	Document classification changed from “internal” to “public” to be made available from website to the public like all other Group level main policies (whistleblowing, privacy, etc…)

MCUBE	**Global Information Security Policy**

Index

Sommario

1 Context

As a future-oriented modern business, M-CUBE recognizes at senior levels the need to ensure that its business operates flawlessly and without interruption for the advantage of its customers, shareholders, and other interested parties.

To provide such a level of continuous operation, M-CUBE has implemented an Information Security Management System (ISMS) in line with the International Standard for Information Security, ISO/IEC 27001:2022. 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 goods and services to customers
- Maintenance and enhancement of shareholder value
- Compliance with legal and regulatory requirements.

A clear definition of the requirements for information security within M-CUBE will be agreed and maintained with the internal business and cloud service customers so that all ISMS activity is focussed on the fulfilment of those requirements. Statutory, regulatory, and contractual requirements will also be documented and input to the planning process. Specific requirements about the security of new or changed systems or services will be captured as part of the design stage of each project.

It is a fundamental principle of the M-CUBE Information Security Management System that the controls implemented are driven by business needs and this will be regularly communicated to all staff through team meetings and briefing documents.

2 Introduction

2.1 The organization is defined by M-CUBE Italy and its existing subsidiaries and future ones.

2.2 Information is an asset that the organization has a duty and responsibility to protect. The availability of complete and accurate information is essential to the organization functioning in an efficient manner and to providing products and services to clients.

2.3 The organization is aware that the confidentiality, the integrity, and the availability of the assets are a real stake for the business. It is why the organization has developed an Information Security Management System (ISMS) to protect its assets.

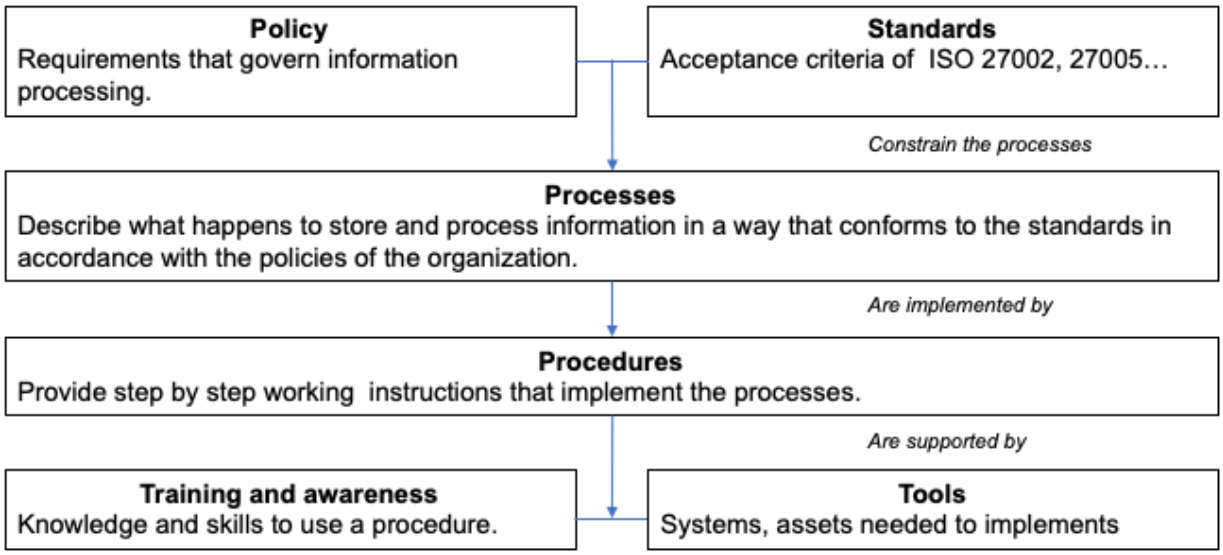
2.4 The organization holds and processes confidential and personal information on private individuals, employees, partners, clients and suppliers and information relating to its own operations. In processing information, the organization has the responsibility to protect information and prevent its misuse.

2.5 The purpose and objective of this Information Security Policy is to set out a framework for the protection of the organization's information assets:

- to protect the organization's information from all threats, whether internal or external, deliberate, or accidental,

- to enable secure information sharing,
- to encourage consistent and professional use of information,
- to ensure that everyone is clear about their roles in using and protecting information,
- to ensure business continuity and minimise business damage,
- to protect the organization from legal liability and the inappropriate use of
- information.

2.6 The Information Security Policy is a high-level document and adopts a number of controls to protect information. The controls are delivered by policies, standards, processes, procedures, supported by awareness and training campaigns, and tools.



3 Scope

3.1 This Information Security Policy outlines the framework for management of Information Security within the organization (see 1.1).

3.2 The Information Security Policy, standards, processes, and procedures apply to all staff and employees of the organization, contractual third parties and its consultants who have access to the organization's information systems or information.

3.3 The Information Security Policy applies to all forms of information including those categories of assets:

- Hardware,
- Software,
- Networks, computers,
- Organization,
- Physical and premises,
- Datas,
- Users rights.

4 Continuous improvement

4.1 Continuous improvement is a key concept of the organization's information system insofar as its information system evolves and with it the exogenous and endogenous risks associated with it.

4.2 Whenever possible, the Deming wheel will be used (PDCA). Thus the operations will be planned, developed, checked and adjusted.

4.3 This constant improvement is supported by top management and driven by the various department managers.

4.4 The various prerogatives in terms of awareness and training are an essential tool for continuous improvement.

5 Structure

5.1 This policy is based upon ISO 27001(2022) and ISO27002(2022) and is structured to include the 4 domains and 93 controls.

5.2 This policy is a high-level policy which is supplemented by additional security policies which provide detailed policies, guidelines and working instructions relating to specific security controls.

6 Risks

6.1 Information which is collected, analysed, stored, communicated, and reported upon may be subject to theft, misuse, loss and corruption.

6.2 Information and assets may be put at risk by poor education and training, misuse, and the breach of security controls.

6.3 The organization will undertake risk assessments to identify, quantify, and prioritise risks. Controls will be selected and implemented to mitigate the risks identified.

6.4 Risk assessments will be undertaken using a systematic approach to identify and estimate the magnitude of the risks.

7 Information Security Policy

7.1 The Information Security Policy document sets out the organizations approach to managing information security.

7.2 The Information Security Policy is approved by management and is communicated to all staff and employees of the organization, contractual third parties and agents of the organization.

7.3 The security requirements for the organization will be reviewed at least annually by the Information Security Manager and approved by the Board. Formal requests for changes will be raised for incorporation into the Information Security Policy, processes, and procedures.

8 Organization of the information security

8.1 It is the policy of the organization to ensure that Information will be protected from a loss of:

- Confidentiality: so that information is accessible only to authorised individuals.
- Integrity: safeguarding the accuracy and completeness of information and processing methods.
- Availability: that authorised users have access to relevant information when required.

8.2 The Information Security Manager reviews and make recommendations on the security policy, policy standards, directives, procedures, Incident management and security awareness education.

8.3 Regulatory, legislative, and contractual requirements will be incorporated into the Information Security Policy, processes and procedures.

8.4 The requirements of the Information Security Policy, processes, and procedures will be incorporated into the organization's operational procedures and contractual agreements.

8.5 The organization will work towards implementing the ISO27000 standards, the International Standards for Information Security.

8.6 Guidance will be provided on what constitutes an Information Security Incident.

8.7 All data breaches of information security, actual or suspected, must be reported and will be investigated.

8.8 Business continuity plans will be produced, maintained, and tested.

8.9 Information security education and training will be made available to all staff and employees.

8.10 Information stored by the organization will be appropriate to the business requirements and regulatories requirements such those concerning data privacy.

8.11 The security of information will be managed within an approved framework through assigning roles and co-ordinating implementation of this security policy across the organization and in its dealings with third parties.

8.12 Specialist external advice will be drawn upon where necessary to maintain the Information Security Policy, processes, and procedures to address new and emerging threats and standards.

8.13 The Information Security Manager is the designated owner of the Information Security Policy and is responsible for the maintenance and review of the Information Security Policy, processes, and procedures.

8.14 Heads of Department are responsible for ensuring that all staff and employees, contractual third parties and agents of the organization are made aware of and comply with the Information Security Policy, processes, and procedures.

8.15 The organization's auditors will review the adequacy of the controls that are implemented to protect the organization's information and recommend improvements where deficiencies are found.

8.16 All staff and employees of the organization, contractual third parties and agents of the organization accessing the organization's information are required to adhere to the Information Security Policy, processes, and procedures.

8.17 Failure to comply with the Information Security Policy, processes and procedures will lead to disciplinary or remedial action.

9 Human resources security

9.1 The organizations security policies will be communicated to all employees, contractors and third parties to ensure that they understand their responsibilities.

9.2 Security responsibilities will be included in job descriptions and in terms and conditions of employment.

9.3 Verification checks will be carried out on all new employees, contractors and third parties.

10 Asset Management

10.1 The organization's assets will be appropriately identified and inventoried.

10.2 The organization's assets will be appropriately protected regarding the results of the risk assessments.

10.3 All assets (data, information, software, computer and communications equipment, service utilities and people) will be accounted for and have an owner.

10.4 Owners will be identified for all assets, and they will be responsible for the maintenance and protection of their assets regarding and respecting the risk management methodology.

10.5 Information will be classified on based on the criticality and sensitivity requirements.

10.6 Each information will be labelled using the classification scheme of the organization.

11 Access Control

11.1 Access to all information will be controlled and based on the Classification Policy.

11.2 Access management will be based on the principle of need-to-know.

11.3 Access to information and information systems will be driven by business requirements. Access will be granted, or arrangements made for employees, partners, suppliers according to their role, only to a level that will allow them to carry out their duties.

11.4 A formal user/accounts registration and de-registration procedure will be implemented for access to all information systems and services.

11.5 Privileged accounts will only be used for the purposes that their use requires.

12 Cryptography

12.1 Wherever is it possible, the use of cryptography is the basic rule.

12.2 A key management procedure will be set up based on a lifecycle and storage requirements.

13 Physical Security

13.1 Critical or sensitive information processing facilities will be housed and stored in secure areas.

13.2 The secure areas will be protected by defined security perimeters with appropriate security barriers and entry controls.

13.3 Critical and sensitive information will be physically protected from unauthorised access, damage, and interference.

14 Operations security

14.1 The operational procedures will be transmitted to all employee involves with direct or indirect security matters.

14.2 Change management will carried out security constrains such as risk assessment, evaluation of the security side effects and will be controlled by the Information Security Manager.

14.3 Capacity management will be considered, and the resources will be monitored.

14.4 Environments will be separated in terms of development, acceptance, and production.

14.5 Detect malware and malicious software will be a continuous improvement during the operations.

14.6 Tools for prevention against malware and malicious software will be installed at each strategic nood.

14.7 The organization ensures that a backup plan will be in place.

14.8 Logging management of events will be established with a special plan for the users or accounts with wide rights.

14.9 Monitoring solutions will be put in place according to the criticality of the events.

14.10 The organization pays particular attention to the synchronization of clocks and will establish controls in this regard.

14.11 To prevent exploitation of technical vulnerabilities, the organizations will establish a plan for gathering, evaluating, and testing technical vulnerabilities.

14.12 Regular audits will be performed to evaluate the risks and reduce its attack surface.

15 Communications security

15.1 The organization will operate its information processing facilities securely.

15.2 Responsibilities and procedures for the management, operation and ongoing security and availability of all data and information processing facilities will be established.

15.3 Appropriate operating procedures will be put in place.

15.4 Segregation of duties will be implemented, where appropriate, to reduce the risk of negligent or deliberate system misuse

15.5 Transfer of information will be based on a Classification Policy that will determine how the information will have to be transferred internally and externally.

16 System acquisition, development and maintenance

16.1 The information security requirements will be defined during the development of business requirements for new information systems or changes to existing information systems.

16.2 Controls to mitigate any risks identified will be implemented where appropriate.

16.3 Information security requirements will be considered on each development. Those requirements will be based on risk assessment report.

16.4 A development lifecycle will have to be followed based on the risks contained by the project. This lifecycle will include registered documentation.

16.5 All the phases of the development lifecycle will be monitored and supervised.

17 Supplier relationship

17.1 Just as suppliers can be a major vector of risk, the organization can also be a source of risk for its partners; therefore, everything will be done to prevent the spread of threats.

17.2 Communication channels specially established for security aspects will have to be put in place and imposed on partners and suppliers.

17.3 Any change that would have an impact on the level of security of the organization must be reported to the organization.

17.4 The organization will ensure that audit agreements are in place with suppliers.

18 Information security incident management

18.1 information security incidents and vulnerabilities associated with information systems will be communicated in a timely manner. Appropriate corrective action will be taken.

18.2 Formal incident reporting and escalation will be implemented.

18.3 All employees, contractors and third-party users will be made aware of the procedures for reporting the different types of security incident, or vulnerability that might have an impact on the security of the organization's assets.

18.4 Information security incidents and vulnerabilities will be reported as quickly as possible to the ICT Service desk.

19 Information security aspects of business continuity

19.1 The organization will put in place arrangements to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

19.2 A business continuity management process will be implemented to minimise the impact on the organization and recover from loss of information assets. Critical business processes will be identified.

19.3 Business impact analysis will be undertaken of the consequences of disasters, security failures, loss of service, and lack of service availability.

20 Compliance

20.1 The organization will abide by any law, statutory, regulatory, or contractual obligations affecting its information systems.

20.2 The design, operation, use and management of information systems will comply with all statutory, regulatory, and contractual security requirements.

END.