Information Security Policy

History

Version	Date	Author	Modifications
1.0	09/11/2018	Alessio Zanforlin	Initial draft created for discussion purposes
1.1	26/11/ 2018	Alessio Zanforlin	Final Version
1.2	13/02/2020	Claudia Volpato	Frame Update
1.3	31/01/2021	Valerio Savino	Frame Update
2.0	08/06/2022	Valerio Savino	Final Release

ISO 27001:2013 Related Control

Control Number	Description
A.5.2	Information Security Policy

JAKALA Group ISMS Related Documents

Document Labeling	Document Name
ISMS_PL01_Information Security Policy_1.0	Information Security Policy

Contact for this documents

Email	Function
Infosecurity@jakala.com	Security & Compliance

Approval

Approved by	Date
CISO	08/06/2022

Data Classification

Level
Internal

JAKALA Spa S.B. / Corso di Porta Romana 15 / 20122 Milano - Italy / +39 02 673361 / www.jakala.com
C.F. e P.I. e n. Iscrizione al Registro Imprese di Milano 08462130967
Cap. soc. deliberato 3.934.182,00 Euro, sottoscritto e versato per 3.602.225,00 Euro

Contents

JAKALA Spa S.B. / Corso di Porta Romana 15 / 20122 Milano - Italy / +39 02 673361 / www.jakala.com
C.F. e P.I. e n. Iscrizione al Registro Imprese di Milano 08462130967
Cap. soc. deliberato 3.934.182,00 Euro, sottoscritto e versato per 3.602.225,00 Euro

JAKALA Spa S.B. / Corso di Porta Romana 15 / 20122 Milano - Italy / +39 02 673361 / www.jakala.com
C.F. e P.I. e n. Iscrizione al Registro Imprese di Milano 08462130967
Cap. soc. deliberato 3.934.182,00 Euro, sottoscritto e versato per 3.602.225,00 Euro

1. Introduction

JAKALA Group recognizes in the information it generates, collects, manages and communicates through the services and products it provides, an asset that must be protected since any loss of its confidentiality, integrity or availability could result in:

- Damage to the corporate image;
- A lack of customer satisfaction;
- The risk of incurring sanctions related to the violation of current regulations; and
- Damage of an economic and financial nature.

An adequate level of security in terms of confidentiality, integrity and availability of information is therefore basic to the sharing of information - the term "CIA" means:

- **C**onfidentiality: ensuring that information remains accessible only to those duly authorized;
- **I**ntegrity: Safeguarding the consistency of information from unauthorized modification;
- **A**vailability: ensuring that information is accessible when needed.

Part of that program involves the design and implementation of an Information Security Management System based on the international standard ISO/IEC 27001:2013, which provides guidelines for developing, implementing, using, monitoring, auditing, updating, and improving an information security management system. This system is a tool that allows to control in a systematic and continuous way the processes concerning the security of all the company's information assets, not only from the IT point of view (electronic or paper supports used to store documents and data) but especially from the managerial and organizational point of view, defining roles, responsibilities and formal procedures for the company's operations.

1.1. Objectives

This document - Information Security Policy - is the main cornerstone of JAKALA Group's ISMS, as it outlines its main objectives:

- Express the Management Committee's intent to implement an Information Security Management System to safeguard the information used and/or held by JAKALA Group;
- Define the major roles and responsibilities to govern the management system;
- Define the operational areas of the ISMS and the high-level objectives for each;
- Define the main processes and components governing the framework of the above management system.

The Information Security Policy has as its object all the physical, logical and organizational aspects of the Information Security Management System, which defines and regulates the processes supporting the

communication and dissemination of information between JAKALA Group and the external environment for the proper conduct of business activities that must take place in compliance with the rules and regulations.
Therefore, the implementation of this policy is mandatory for all personnel and must be included in the regulation of agreements with any external party who, for any reason, may be involved with the processing of information that falls within the scope of the Information Security Management System.

1.2. Scope of the document

This policy applies to all data stored on JAKALA Group's systems. The procedure covers such specifics as the type of data to be backed up, frequency of backups, storage of backups, retention of backups, and restoration procedures.

JAKALA Spa S.B. / Corso di Porta Romana 15 / 20122 Milano - Italy / +39 02 673361 / www.jakala.com
C.F. e P.I. e n. Iscrizione al Registro Imprese di Milano 08462130967
Cap. soc. deliberato 3.934.182,00 Euro, sottoscritto e versato per 3.602.225,00 Euro

2. Policy

The following headings outline the principles and statements around how information is managed in JAKALA Group.

2.1. Roles and Responsibilities

2.1.1. Chief Information Security Officer

Conducts periodic review activities of the implementation of the controls provided in the procedures that are part of the ISMS;
With the support of JAKALA Group's Secuand any involved/needed functions, will conduct a periodic review of this policy.

2.1.2. Information Systems

It monitors the technological infrastructure and will provide possible support to the Chief Information Security Officer in carrying out his control activities;
With respect to the general principles by which the Group is inspired in the management of security, it assigns the management of activities concerning security areas to the relative areas of competence.

2.1.3. Internal Audit

Following notification of any non-compliance, will be responsible for reviewing and potentially endorsing any improvement activities to the management system;
Will review the effectiveness and efficiency of the Information Security Management System on a regular basis, or in conjunction with significant changes, to ensure adequate support for the introduction of any necessary improvements.

2.1.4. Information Technology Area

Function dedicated to the supervision and management of issues related to the design and implementation of IT applications. In particular, it deals with implementation aspects in the areas of acquisition, development and maintenance of systems.

2.1.5. Operation and Infrastructure Management

Function dedicated to the supervision and management of issues related to the implementation and operation of infrastructures. In particular, it deals with implementation aspects in the areas of asset management, access control, cryptography and operation security.

2.1.6. Human Resources

Function dedicated to the supervision of processes inherent to the management of internal personnel and collaborators, also responsible for managing safety and physical security issues.

2.1.7. Procurement Area

Team dedicated to the supervision of processes inherent to the management of relations with third parties, such as vendors and service providers.

2.1.8. Facility Management

Area dedicated to the supervision of processes inherent to the management of security issues related to the building.

2.1.9. Crisis and Business Continuity Manager

Figure in charge of managing the continuous process of managing and overseeing aspects related to process continuity and crisis management, through the adoption of a cyclical model of planning, analysis, implementation, monitoring and updating.

2.1.10 Data Protection Officer (DPO)

A person in charge of assessing, organizing and managing the processing of personal data within the company, so that it is processed in compliance with the applicable privacy regulations. In order to ensure better control of the ISMS and avoid overlapping of security activities between the various roles, the responsibilities associated with each role are assigned in such a way as to maintain a distinction between those who define the security rules, those who implement them and those who carry out monitoring. Finally, other stakeholders, not directly/operatively involved in security management, are also interested in security management and can provide specific security requirements, with particular reference to the areas described in this policy.

The main ways in which security requirements are defined are as follows:

- Group guidelines;
- Risk analysis;

- Corporate Strategic Plan;
- Management Committees.

2.2. General Principles

The following is a summary of the general principles that will guide the main activities of planning, design, implementation and management of the System.

2.2.1. Defining Security Objectives

In order to design and plan the implementation of an effective information security management system capable of responding to the security objectives set by the Management Committee, it is essential that the company identifies the requirements, both internal and external, as well as those deriving from the mandatory to which the ISMS must respond - this activity is carried out by drawing on various sources:

- Inspiring Principles;
- Risk Analysis;
- Laws and Contracts.

2.2.1.1 Inspiring Principles

The guiding principles represent the value system in which the company believes with regard to the management of the security of its information system. These are the basic ideas that the company has developed with regard to information security, that is, what it is right to do, or not to do, in order to have an efficient, effective and adequate security management system.
The primary reference for general security principles is the ISO/IEC 27002:2005 standard

2.2.1.2 Risk Analysis

The inclusion or exclusion of any control and/or component of the entire information security management system must be justified through the performance of a risk analysis; this activity allows the Group to acquire an awareness and visibility of the level of risk exposure of its system.
The risk analysis provided through a systemic process and according to an internal methodology based on the ISO 27005:2008 standard, takes into consideration the following elements:

- Threats;
- Impact;
- Exposure.

The results of these joint assessments will allow the determination of the actions necessary to manage the identified risks and the most suitable security measures in relation to its objectives and based on the definition of the residual risk level that the Group will decide to accept.

The results of the information security risk analysis, the actions required to manage the identified risks, and the security measures defined must be shared with Risk Managers and top management.

2.2.1.3 Laws and Contracts

Within the existing regulatory framework, guidance is provided on how to deal with security issues and how to manage the use of information systems.

2.2.2. Management processes

In order for the information security management system to meet the requirements expressed by the ISO/IEC 27001:2013 standard, it is necessary that it be subject to a process of continuous improvement, based on the Deming Cycle paradigm, or Plan-Do-Check-Act model.
Therefore, downstream of the implementation of the Information Security Management System (ISMS), it must be subjected to a series of periodic and continuous activities aimed at measuring the performance of the system in achieving the objectives, as well as at correcting any gaps in it and/or improving its performance or efficiency.

2.2.2.1 Monitoring

Each component and control of the management system should be associated with a performance indicator that will be monitored by the relevant manager (or owner).
In the event of a failure to comply with the terms of the contract, the firm should be required to ensure that the client is able to comply with the terms of the contract.
Furthermore, periodic verification activities must be carried out, at least annually, of the execution of the controls foreseen in the procedures that are part of the ISMS. These activities will be carried out by the Chief Information Security Officer.

Key monitoring activities include the following:

- Utilities Monitoring;
- Monitoring and recertification of network folders;
- Monitoring Installed Software.

Finally, the Information Systems Area will monitor the technological infrastructure and provide possible support to the Chief Information Security Officer in carrying out his control activities.

2.2.2.2 Audit

In parallel with monitoring activities, the effectiveness of the ISMS and its operation should be subject to objective and independent verification. Any non-compliance should be reported to the Internal Audit function, which will be responsible for reviewing and endorsing or not endorsing any activities to improve the management system.

2.2.2.3 Review

The Internal Audit Function will review the effectiveness and efficiency of the Information Security Management System periodically and regularly, or in conjunction with significant changes, in order to ensure adequate support for the introduction of any necessary improvements and in order to facilitate the activation of a continuous process by which control and adjustment of the policy is maintained in response to changes in the corporate environment, business, and legal conditions.
The outcome of the review should include all decisions and actions related to improving the firm's approach to information security management, controls and the allocation of resources and responsibilities.

JAKALA Spa S.B. / Corso di Porta Romana 15 / 20122 Milano - Italy / +39 02 673361 / www.jakala.com
C.F. e P.I. e n. Iscrizione al Registro Imprese di Milano 08462130967
Cap. soc. deliberato 3.934.182,00 Euro, sottoscritto e versato per 3.602.225,00 Euro

2.3. General Principles Governing The ISMS Framework

2.3.1. Human Resource Security

The ISO/IEC 27001:2013 standard defines Human Resources Security as the set of controls, activities and processes whose objective is to ensure that human resources (employees and collaborators) working on behalf of the Group are fully aware of issues relating to information security.

Objectives:
The main security objectives to which this subject area refers are presented below:

- During the staff selection and induction phases, it is appropriate to assess the levels of knowledge of the objectives and issues of corporate security in relation to the activities to be carried out;
- Adequate and ongoing training is provided for personnel during their stay with the Group, regarding information security issues;
- The methods for terminating the employment relationship will be consistent with the company's security objectives.

2.3.2. Asset Management

The ISO/IEC 27001:2013 standard defines Asset Management as the set of controls, activities and processes whose objective is to ensure full knowledge of the information managed by the Group and its subsequent assessment in terms of criticality, and the information systems used to make it available, in order to facilitate the implementation of adequate levels of protection.
Objectives:
The main security objectives referred to in this security topic area implemented by the Group as part of its Information Security Management System are outlined below:

- A census system of all tangible and intangible assets to be protected (information, hardware, software, paper documentation and storage media) must exist and be kept updated over time;
- Each resource (tangible/intangible asset) must be directly associated with a responsible person;
- Information must be classified according to its level of criticality, so that it is managed with consistent and appropriate levels of confidentiality, integrity and availability. The criticality of information must be assessed as objectively as possible, through the use of appropriate working methods;
- The management methods and protection systems for information and the assets on which it resides must be consistent with the level of criticality identified.

2.3.3. Access Control

The ISO/IEC 27001:2013 standard defines Access Control as the set of controls, activities and processes whose objective is to ensure secure access to information in order to prevent unauthorized processing of information or its viewing by unauthorized users.

Objectives:
The main security objectives referred to in this security topic area implemented by the Group as part of its Information Security Management System are outlined below:

- Access to information by each individual user must be limited to only the information he or she needs to perform his or her duties (need-to-know principle). The communication and transmission of information internally, as well as externally, must be based on the same principle;
- Access to information in digital format by authorized users and systems must be subject to the successful completion of an identification and authentication procedure;
- Authorisations to access information must be differentiated on the basis of the role and responsibilities of individuals and must be periodically reviewed;
- It is necessary to define a process for managing authorization credentials and the relative access profiles;
- It is necessary to define a process for managing authorization credentials and related access profiles;
- The systems that make up the ICT infrastructure must be suitably protected and segregated, so as to minimize the possibility of unauthorized access.

2.3.4. Cryptography

ISO/IEC 27001:2013 defines Cryptography as the set of controls, activities, and processes whose objective is to ensure the use of techniques to encrypt information during processing, transit, and storage in order to preserve its confidentiality, authenticity, and/or integrity.

Objectives:
The main security objectives referred to in this security topic area implemented by the Group as part of its Information Security Management System are outlined below:

- The use of specific encryption techniques must be functional for the purpose for which it is selected;
- Specific procedures must be in place to ensure the security of encryption keys throughout their lifecycle.

2.3.5. Physical and Environmental Security

The ISO/IEC 27001:2013 standard defines Physical and Environmental Security as the set of controls, activities and processes whose objective is to prevent unauthorized access to company offices and premises, ensuring adequate levels of security to the areas and assets through which information is managed.
Objectives:
The following are the main security objectives to which this security topic area implemented by JAKALA Group as part of its Information Security Management System refers:

- Security management for areas and premises must be ensured by:
  - The definition of appropriate levels of protection;
  - The identification of areas and their classification based on the criticality of the information processed.
- The security of equipment must be guaranteed by:
  - The definition of an adequate location for information processing equipment;

- Providing the necessary resources for their operation;
- The provision of adequate maintenance.

2.3.6. Operations Security

The ISO/IEC 27001:2013 standard defines Operations Security as the set of controls, activities and processes whose goal is the proper management of IT infrastructures in their operational and threat prevention phases.

Objectives:
The main security objectives referred to in this security topic area implemented by the Group as part of its Information Security Management System are outlined below:

- The presence of procedures that protect systems from malware such as viruses, Trojans and backdoors must be guaranteed;
- There must be procedures in place to back up and restore information in the event of loss and/or corruption;
- There must be procedures in place to promptly monitor and detect infrastructure vulnerabilities that may expose systems to attack.

There must be procedures in place to track system activity so that any anomalies can be identified through post-mortem analysis.

2.3.7. Communications Security

The ISO/IEC 27001:2013 standard defines Communications Security as the set of controls, activities and processes whose objective is to ensure the correct routing of information during the internal and external transit phases of the Group's infrastructure.

Objectives:
The following are the main security objectives referred to in this security topic area implemented by JAKALA Group as part of its Information Security Management System:

- The presence of procedures and mechanisms to protect communication flows within and outside the infrastructure must be guaranteed;
- The presence of procedures and formal agreements governing information exchange processes must be guaranteed.

2.3.8. System Acquisition, Development and Maintenance

ISO/IEC 27001:2013 defines System Acquisition, Development and Maintenance as the set of controls, activities and processes whose objective is to ensure that security is included in all phases of design, development, operation, maintenance, support and decommissioning of systems and services.

Objectives:
The following are the main security objectives referenced in this security topic area implemented by JAKALA Group as part of its Information Security Management System:

- Security aspects must be appropriately considered in the design and development phase, in particular:
  - Inclusion of security requirements in the functional specifications of services, systems and software;
  - Adoption of best practices for software development and maintenance;
  - Separation of development and test environments with the use of formal acceptance procedures when switching between environments.
- The operations phase must appropriately consider security aspects - specifically:
  - Capacity management of the technology infrastructure;
  - Creation of a change management process that includes securing systems;
  - Adoption of system backup/restore and decommissioning procedures;
  - Adoption of network security practices, such as network segmentation and gateway monitoring.
- Security aspects should be appropriately considered in the management of services, in particular:
  - Processes for monitoring the performance of systems and services;
  - User management.

2.3.9. Supplier Relationships

ISO/IEC 27001:2013 defines Supplier Relationships as the set of controls, activities and processes whose objective is to ensure compliance with legal requirements and principles related to information security in contracts with third parties, in accordance with the specific characteristics of the relationship that the Group must establish with those third parties.

Objectives:
The main security objectives referred to in this security thematic area implemented by JAKALA Group as part of its Information Security Management System are declined below:

- Agreements with third parties and outsourcers who access information and/or the tools that process it, and/or that may impact the effectiveness of the ISMS, must be based on formal contracts containing appropriate security requirements;
- Agreements with third parties and outsourcers, where necessary, must ensure compliance with legal requirements regarding the protection of personal data.

2.3.10 Information Security Incident Management

The ISO/IEC 27001:2013 standard defines Information Security Incident Management as the set of processes whose objective is to ensure that anomalies and incidents affecting the company's security levels are promptly recognized and correctly managed through efficient prevention, communication and reaction systems in order to minimize the impact on the business.

Objectives:
The following are the main security objectives referenced in this security topic area implemented by JAKALA Group as part of its Information Security Management System:

- All employees and contractors are required to detect and report any information security issues to appropriate parties in accordance with appropriate procedures;
- Incidents that may have an impact on security levels must be detected and any damage, potential or otherwise, must be handled promptly and according to specific procedures where possible;
- There must be a system for recording and classifying incidents and anomalous events in order to carry out analyses aimed at improving security levels in line with the actual problems encountered.

2.3.11 Information Security Aspects of Business Continuity

The ISO/IEC 27001:2013 standard defines Information Security aspects of Business Continuity as a set of controls, activities and processes whose objective is to ensure the continuity of the Group's activities and the eventual timely restoration of the services provided and affected by events and/or incidents of a certain severity, reducing the consequences both inside and outside the business context.

Objectives:
The following are the main security objectives referred to in this security topic area implemented by JAKALA Group as part of its Information Security Management System:

- All events on which an interruption of business continuity may depend must be carefully identified and assessed in terms of probability of occurrence and possible consequences;
- A continuity plan must be prepared that allows the organization to deal, in a planned and efficient manner, with the consequences of an unforeseen event, guaranteeing the restoration of critical services in a timeframe and in a manner that allows the reduction of negative consequences on the company's mission;
- All operational and organizational procedures necessary to ensure the implementation of the business continuity plan must be prepared, validated and appropriately disseminated;
- Testing must be periodically conducted for all components of the continuity plan;
- The maintenance and updating of the plans and procedures referred to in the previous points must be ensured in order to guarantee the effectiveness of the system over time in the face of any organizational and technological changes.

2.3.12 Compliance

The ISO/IEC 27001:2013 standard defines Compliance as the set of controls, activities and processes whose objective is to ensure compliance with legal provisions, statutes, regulations or contractual obligations and any requirements inherent to information security, while minimizing the risk of legal or administrative sanctions, significant losses or reputational damage.

Objectives:
The following is a breakdown of the key security objectives referenced in this security topic area implemented

by JAKALA Group as part of its Information Security Management System:

- All regulatory and contractual requirements relating to information system security and having an impact on the Information Security Management System must be identified and analyzed, in order to assess their impact on the Organization and its information systems;
- The managers of the various areas must ensure, each within their own sphere of competence, that all policies, procedures, standards and, in general, all documentation relating to information security are applied and complied with;
- Failure to comply with what is indicated in this document and all others that derive from it will be handled in accordance with applicable legislation or, in the case of non-compliance by third parties, in accordance with existing contractual relationships.

2.4. Revision and Control

The Chief Information Security Officer, with the support of any functions involved/required, will conduct a periodic review of this policy so that it is aligned with any significant changes in the organization and/or in the technologies used to protect information.
This review will be carried out at least annually and/or on the occasion of significant organizational and/or technological changes relevant to information management.
Monitoring of compliance with this policy shall be carried out as provided in section "2.2.2.1. Monitoring" of this document.