omiclear

Information Security Policy

Definition of OMIClear ‘s Information Security Policy

11.05.2016

Versions Index

11.05.2016
Initial Version

Introduction

Information security is defined by the practices that assure that the information (which is) under the responsibility of an organisation is only accessed, modified, conveyd or used by individuals, entities or systems who have the right or the necessary permissions to do so, preserving the integrity, availability and confidentiality that is adequate to its purpose.

All information is valuable. In some cases, such value can be directly converted in a monetary amount and in others is associated to certain qualitative factors, such as reputation. The breach of its confidentiality, integrity or availability while being acessed by the end users may result in significant losses for the organisation.

Considering these factors, through the present Information Security Policy, OMIClear establishes the foundations of the its organisation and action within the management of information security, aiming to achieve the following goals:

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

1. Purpose

The purpose of the present Information Security Policy is to establish the concepts and guidelines with respect to OMIClear's Information Security Management System (ISMS), which aims to protect the information under OMIClear's responsibility, wheter internally originated or entrusted within the scope of its business functions, services provided to its clients and legal or regulatory responsibilities.

In specific, the following goals are established to guarantee the confidentiality, integrity and availability of all information assets, physical or electronic, thus assuring the compliance of OMIClear's legal, regulatory, operational and contractual requirements:

a) Assure the compliance with the legislation, regulamentation and further guidelines;
b) Comply with the requirements of confidentiality, integrity and availability satisfatory for OMIClear's business goals, in particular with the needs of its members;
c) Comply with the requirements of confidentiality, integrity and availability suitable for OMIClear's employees, permanent or temporary;
d) Set up controls to protect OMIClear's information and information systems from robbery, intrusion, corruption and other forms of misconduct and potential losses;
e) Motivate the Board of Directors and employees to become aware and take responsibility in intervening in the ISMS, thus minimizing the risk of security incidents;
f) Assure the availability and reliability of the equipments, frameworks and systems that support OMIClear's activity;

g) Assure that OMIClear has the capacity to continue its activity in case of serious security accidents, in the conditions defined in the specific and applicable guidelines and procedures;
h) Assure the protection of personal data, particularly as provided by the applicable legislation;
i) Follow the industry best practices, namely the ones based in the applicable regulation;
j) Assure that OMIClear's service providers comply with the security needs and requirements of the organisation;
k) Reduce the damage caused by information security incidents in OMIClear, as well as assure that such incidents are reported to all relevant parties.

2. Scope

The present Policy applies to all OMIClear's employees, interns, service providers and other parterns, as well as all assets and information systems, operational, inactive or in development, whether lodged in OMIClear's equipments and facilities or from outsourcing suppliers.

3. Information Security Documents

The internal regulatory framework consists of the following set of documents:

- **Policy**: defines the structure, guidelines and responsibilities with respect to information security;
- **Procedures**: detail and incorporate in the daily operations the principles laid out in the Policies, allowing their swift implementation in OMIClear's activities.

4. Roles and responsibilities

4.1 Senior Management

OMIClear's Senior Management holds the overall responsibility for the information security, specifically for the Policy. The role of approval of all remaining documents, including ISMS documentation, is delegated to the Chief Operational Officer, that shall keep informed and updated the Board of Directors of such changes.

4.2 Security Manager

The Security Manager is responsible for the operational coordination of the ISMS as well as its maintenance.

4.3 Employees

OMIClear's employees are responsible for beeing continuously aware of ISMS, complying with the internal procedures defined in the scope of Information Security.

4.4 Service Providers and other external entities

The service providers and other persons outside the organisation should conduct and proceed in accordance with OMIClear's Information Policy. Particularly, the contracts signed between OMIClear and outsourcing companies which have acess to OMIClear's information, systems and/or technological environments should assure not only the confidentiality between both parties but also the compliance of the Policy, guidelines and further procedures of ISMS by its employees.

5. Principles of Information Security

5.1 Information Management Policy

OMIClear's Senior Management should assure that the Policy, as well as the remaining procedures, are acknowledged and followed, guaranteeing the necessary conditions for that purpose, specifically communication, trainning and the resources necessary to such tasks.

The Policy should be reviewed everytime a change is observed either in OMIClear's organizational structure, in legal and regulatory requirements or in the industry best practices and regulations.

5.2 Code of conduct

OMIClear should define the code of conduct with respect to information security, applicable to all employees, outsourcing suppliers and other persons outside the organisation, specifically in the following chapters:

- Compliance with the information security policy and procedures;
- Protection of the information against unauthorized access, modification, disposal or disclosure;
- Usage of technological resources and systems provided by OMIClear;
- Usage and processing of information accessed by a third party while cooperating with OMIClear;
- Compliance with the legislation and guidelines that regulate intellectual property;
- Treatment of noncompliances or violations of this policy or the information security procedures.

5.3 Human Resources

OMIClear should promote and implement the necessary training and awareness program to inform and ensure that its employees, suppliers and other persons outside the organisation are able to assume their responsibilities in the scope of information security.

For this purpose, OMIClear should include the necessary procedures, actions and documents to such training program and information flow in the employee hiring and dismissal processes.

5.4 Risk Management

OMIClear's ISMS should be based on the identification, assessment and management of the risks underlying OMIClear's activity, whenever applicable. Particularly, the necessity to implement mitigation measures should be periodically assessed and such measures should be designed in accordance with OMIClear's business goals and responsibilities, considering efficiency, costs and applicability.

Information security risk assessment should identify, quantify and prioritize the risks in accordance with the relevant criteria for the acceptable risks and should be conducted at least once a year or whenever changes impact information security.

5.5 Classification and control of assets

The information and its framework should be classified in accordance with their confidential and critical level to OMIClear's business, as well as acess control.

The assets should be assigned to an owner, formally designated as responsible for authorising the access to the information and frameworks under his responsibility.

All information should be properly protected in compliance with the information security policy and procedures approved by OMIClear, throughout the entire life cycle of information, which includes its creation, handling, storage , transportation and disposal.

The information should be used in a transparent way and only for the purpose to which is was created or compiled.

5.6 Information systems

OMIClear's information systems should be planned, specified, developped, tested, implemented and managed considering the needs and requirements of information security, confidentiality, integrity and availability.

Since information is mostly kept is technological files, special attention is given to the specific procedures that manage the information systems and its supportive assets.

Particularly, OMIClear should implement a business continuity plan focusing on its critical activities.