Information Security Policy

28.Mar.2023

Versions Index

22.Apr.2015
Initial Version.

21.May.2019
General revision.

22.Nov.2022
General revision.

28.Mar.2023
Inclusion of reference to Regulation (EU) 2016/1011 of the European Parliament and of the Council of 8 June 2016. Adjusted the text of point 3.2. and added the Information Security Manager to chapter 3.

Introduction

OMIP, as a Regulated Market Operator as defined in article 4 (1) of Directive 2014/65/EU of the European Parliament and of the Council, of 15 May 2014 (MIFID II), has the constant concern to be equipped with a comprehensive set of tools for managing information security, in order to ensure that its information technology systems and information security framework are in conformity with the principles, references and international standards and legal requirements, in particular with:

- Regulation (EU) n.º 1227/2011 of the European Parliament and of the Council of 25 October 2011 on wholesale energy market integrity and transparency;
- Commission implementing Regulation (EU) n.º 1348/2014 of 17 December 2014, on data reporting implementing Article 8 (2) and Article 8 (6) of Regulation (EU) No 1227/2011 of the European Parliament and of the Council on wholesale energy market integrity and transparency;
- Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014, on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU;
- Regulation (EU) n.º 600/2014 of the European Parliament and of the Council of 15 May 2014, on markets in financial instruments and amending Regulation (EU) No 648/2012;
- Regulation (EU) 2016/1011 of the European Parliament and of the Council of 8 June 2016 on indices used as benchmarks in financial instruments and financial contracts or to measure the performance of investment funds.

Information security is defined by the practices that make it possible to ensure that the information under the responsibility of an organisation is only accessed or modified, during its storage, processing or transmission, by the authorised individuals, entities or systems. These practices include the necessary measures to detect, document and respond to threats to integrity, availability and confidentiality of information.

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

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

- **Confidentiality**: ensure that the information is accessible only to the authorised individuals or systems, for the required period;
- **Integrity**: ensure that the information is complete and accurate and that it is not modified or destroyed from an unauthorized or accidental manner, during its life cycle;
- **Availability**: ensure that the information is available to all authorised individuals, whenever necessary.

In this regard, here are set out the main guidelines for OMIP's Information Security Management System (ISMS), based on the ISO 27001, one of the international reference standards for managing information security. This system aims to protect the information for which OMIP is responsible, whether produced internally or entrusted within its role, the services provided to its customers and the responsibilities to which is subject by legislation or regulations.

1. Scope

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

The scope of this Policy extends to all OMIP's functional areas which may impact information security.

2. Objectives

The following goals are pursued to safeguard the confidentiality, integrity and availability of all information assets:

a) Ensure the compliance with legislation, regulations and further applicable standards;
b) Comply with the requirements of confidentiality, integrity and availability satisfatory for OMIP's business goals, in particular with the needs of its members;
c) Implement controls to protect OMIP's information assets from theft, intrusion, abuse or other forms of illicit treatment;
d) Promote a culture of awareness and commitment to information security amongst the Board of Directors, Senior Management and employees, motivating them to become aware and take responsibility for their intervention in ISMS, so as to minimize the risk of security incidents;
e) Ensure the availability and reliability of the equipments, infrastructures and systems that support OMIP's activity;
f) Ensure that OMIP has the ability to continue its activity in case any serious security incident occurs, under the conditions laid down in the specific applicable rules and procedures;
g) Ensure the protection of personal data, as provided by the applicable legislation;
h) Follow industry best practices, namely those based on applicable regulations;
i) Ensure that external suppliers, namely critical suppliers, fit OMIP's, security needs and requirements;
j) Reduce the damage caused by information security incidents at OMIP, as well as ensure that they are reported under the terms defined for that purpose;
k) Ensure the continuous improvement of ISMS, in order to guarantee its suitability and effectiveness.

3. Roles and responsibilities

3.1 Board of Directors

The Board of Directors of OMIP ultimately holds the overall responsibility for information security and, in particular, for the definition and approval of the present Policy, as well as its revision, in order to ensure its continuous suitability and effectiveness. The competence of approving the remaining documents, including ISMS documentation, is delegated to the Chief Operating Officer, who shall keep the members of the Board of Directors informed and updated, on a regular basis, of the revisions, developments and improvements in the system and also of the results of audits, tests and evaluations (internal or independent).

3.2 Senior Management

OMIP's Senior Management, formed by the Chairman and Vice-Chairman of the Board of Directors and the Chief Operating Officer, holds the responsibility to endorse and support all phases of implementation and maintenance of ISMS, ensuring the adequate resources are available to guarantee the achievement of the objectives set out in this policy. It is the responsibility of senior management to submit this Policy and any amendments thereto to the Board of Directors for approval.

3.3 Security Comittee

Within the scope of ISMS's implementation, the Security Committee of OMIP was created – an internal technical Committee formed by, at least, the Chief Operating Officer, one responsible for the Information Systems department and the (Information) Security Manager. The Security Committee is responsible for implementing, maintaining and reviewing the policies and procedures of ISMS, in accordance with the objectives and principles defined in the present Policy.

3.4 Information Security Manager

OMIP's Information Security Manager is assigned the following duties and responsibilities:

- Responsible for implementing and maintaining the ISMS;
- Responsible for liaising between the Security Committee and all other areas within the scope of the ISMS;
- Ensure that the ISMS complies with OMIP's business objectives, ISO 27001:2013 requirements and other regulatory requirements arising from OMIP's activity;
- Develop and implement, whenever necessary, training and awareness programmes for information security among employees;
- Ensure that ISMS non-conformities are corrected in the shortest possible time;
- Comply with and ensure compliance with all ISMS requirements, policies and procedures.

3.5 Employees

OMIP's employees are responsible for:

- Complying with all standards, requirements, policies and procedures laid down under the scope of information security;
- The information assets entrusted to them, proactively contributing to their adequate protection;
- Reporting to the Security Committee the occurrence of information security incidents or anomalies in OMIP.

3.6 Suppliers

Suppliers shall conduct and proceed in accordance with the present Policy. In particular, the contracts between OMIP and contractors with access to information, systems and/or to OMIP's technological environment shall include clauses that assure confidentiality between parties and guarantee that the professionals under the contractors' responsibility comply with the present Policy, standards and further applicable procedures.

Suppliers are also responsible for reporting to OMIP the occurrence of incidents related to the security of OMIP's information or to OMIP's information systems.

Suppliers that are considered critical to OMIP should be subject to greater control and monitoring, as well as additional security requirements in the contractual relationship between the parties.

4. Principles of Information Security

4.1 Code of Conduct

OMIP should define rules with respect to information security in its Code of Conduct, applicable to all employees and suppliers, specifically in the following principles:

- Compliance with the present Policy and further information security documentation;
- Usage of technological resources and systems provided by OMIP;
- Treatment of information and personal data under the responsibility of OMIP;
- Treatment of breaches or violations of the present Policy or of further information security policies and procedures.

4.2 Human Resources

Information security is applicable to all OMIP's employees, across all departments, and specific responsibilities shall be assigned to certain functions. OMIP should promote the necessary training and duly inform its employees, as well as employees of suppliers, so that they are able to assume their responsibilities under the scope of information security.

4.3 Asset Management

The information managed by OMIP, its processes and support infrastructures, employees, third parties, offices, equipment, documents, systems, applications and networks are valuable assets to the organisation. As so, each of these assets should be properly protected in compliance with the information security procedures approved by OMIP, throughout its entire life cycle, which includes its creation, handling, storage, transportation and disposal.

The information managed by the OMIP should be used in a transparent manner and only for the purpose for which it was created or entrusted.

4.4 Information Systems

Since information is mostly stored in technological files, special attention should be paid to the specific procedures that manage the information systems, as well as the assets that support them.

OMIP's information systems should be designed, specified, developed, tested, deployed and managed taking into account the needs and requirements of information security – confidentiality, integrity and availability.

4.5 Personal Data

OMIP is committed to make every effort to ensure the privacy and protection of personal data entrusted to it, in compliance with the applicable regulations and, in particular, with the General Data Protection Regulation. OMIP classifies personal data as confidential, adopting proper physical, logical, technical and organisational security controls, in order to protect personal data from being

disseminated, changed, lost, misused, processed and accessed without authorisation, or stolen, as well as to protect it against any other form of illicit processing.

4.6 Risk Management

One of the key areas of OMIP's ISMS is the continuous risk management – identification, evaluation and treatment of risks, inherent to its activity, to which the organisation's assets are exposed – as a tool of management of the company. Within the scope of ISMS, risk management includes the implementation of security controls and mechanisms that aim to mitigate or limit the potential damages caused by the exploitation of assets' vulnerabilities, in order to minimize the occurrence of incidents and ensure an adequate security level which meets the risk level that OMIP is willing to accept. Such measures should be designed in accordance with OMIP's business goals and responsibilities, considering efficiency, cost and applicability.

4.7 Incident Management and Business Continuity

All events that may jeopardize business operations or compromise information security will be treated as security incidents, in accordance with the incident management procedures approved by OMIP.

The availability of information, not neglecting the responsibility towards the remaining information security commitments, shall be assured by the implementation of a response plan to disruptive incidents, integrated in the framework of OMIP's Business Continuity Management System.

4.8 Cybersecurity

Being aware of the growing importance of cybersecurity as a specific area within the framework of information security, OMIP shall develop and apply a Cybersecurity Policy in line with best practices and benchmark standards, enabling it to comply with the applicable regulatory requirements on cybersecurity matters, particularly those applicable to its activity as a Regulated Market Operator and also as an operator of essential services in the financial market infrastructure sector. Additionally, OMIP shall establish, whenever possible, protocols and processes of cooperation with entities acting as competent national authorities and specialised in cybersecurity.

5. Final Provisions

The present Policy should be reviewed by the Board of Directors of OMIP whenever there is any change in the framework of information security, in OMIP's internal organisation, in the regulatory or legal framework or in industry best practices.

The present Policy is available on OMIP's corporate website.

Approved by the Board of Directors on the 28th of March of 2023