Information Security Policy

26.November.2024

Versions Index

22.Apr.2015
Initial version

21.May.2019
Full revision

22.Nov.2022
Full 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.. Information Security Manager added.

26.Nov.2024
Merging the Information Security Policy with the Cybersecurity Policy. Full review.

Table of Contents

1. 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), and as an entity identified by the National Cybersecurity Centre as an essential service operator in the financial market infrastructure sector, pursuant to Article 29(1) of Law No 46/2018, constantly strives to be equipped with a comprehensive set of information security and cybersecurity management tools to ensure that its information and communication technology (ICT) assets and systems comply with international standards, references and norms, as well as legal requirements, namely:

- Regulation (EU) No 1227/2011 of the European Parliament and of the Council of 25 October 2011, on wholesale energy market integrity and transparency (REMIT);
- 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 (MiFID II) 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 (MiFIR) and amending Regulation (EU) No 648/2012, and its lower-level standards;
- 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 (RIR);
- Law No. 46/2018 (of 13 August) establishing the legal framework for cyberspace security (transposing Directive (EU) no. 2016/1148 of the European Parliament and of the Council of 6 July 2016);
- Decree-Law No. 65/2021 of 30 July, which regulates the legal framework for cyberspace security and defines the obligations regarding cybersecurity certification in implementation of Regulation (EU) 2019/881 of the European Parliament of 17 April 2019;
- Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on the digital operational resilience of the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (DORA Regulation);
- ISO/IEC 27032:2012;
- ISO/IEC 27001:2013;
- CIS Controls v8;
- National Cybersecurity Reference Framework, National Cybersecurity Centre (CNCS);
- Framework for Improving Critical Infrastructure Cybersecurity (v1.1, April 16, 2018), NIST.

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

Within information security, one of the most important areas is cybersecurity, which is concerned with maintaining the privacy, integrity and availability of information in cyberspace, i.e. the non-physical

space created by computer networks, namely the Internet, where people can communicate and interact through software, platforms or other information services.

All information is valuable. In some cases such value can be directly converted into a monetary amount, while in others it can be linked to qualitative factors, such as reputation. A breach of its confidentiality, integrity or availability, when handled by its end users, can result in significant losses for the organisation.

In view of these factors, through this Information Security Policy, OMIP establishes the foundations of its organisation regarding the management of information security and cybersecurity, with the aim of achieving the following macro objectives:

- **Confidentiality**: Ensure that information is only accessible to authorised persons or systems for the required period of time;
- **Integrity**: Ensure that the information is complete, accurate and is not modified or destroyed in an unauthorised or accidental manner during its life cycle;
- **Availability**: Ensure that information is available to all authorised persons as required.

To this end, this document sets out the main guidelines for OMIP's Information Security Management System (ISMS), based on ISO/IEC 27001, one of the international reference standards for information security management. The aim of this system is to protect the information for which OMIP is responsible, whether it is generated internally or entrusted to it as part of the functions it carries out, the services it provides to its clients and the responsibilities to which it is subject by law or regulation.

2. Scope

This Policy applies to all employees, including OMIP board members, and to all suppliers.

The scope of this Policy covers all areas of OMIP's operations, whose actions have an impact on information security and cybersecurity, and includes all of OMIP's technological assets, whether operational, inactive or under development, whether housed in OMIP's equipment and facilities or outsourced.

3. Information Security Objectives

The objectives for the protection of the confidentiality, integrity and availability of all information assets are as follows:

3.1. Ensure compliance with laws, regulations and other applicable standards;
3.2. Ensure the protection of personal data in accordance with applicable legislation;
3.3. Follow industry best practices and international security and cybersecurity references and standards;
3.4. Promote a culture of awareness and commitment to information security and cybersecurity among board members, top management and employees, motivating them to be aware of and take responsibility for their involvement in the ISMS to minimise the risk of security incidents;
3.5. Ensure the availability and reliability of the equipment, infrastructure and systems that support OMIP's activities;
3.6. To meet the confidentiality, integrity and availability requirements appropriate to OMIP's business objectives, in particular the needs of its clients;
3.7. Ensure that suppliers, in particular critical suppliers, meet OMIP's security and cybersecurity needs and requirements;

3.8. Identify, assess and manage the information security and cyber security risks inherent in OMIP's activities and to which its assets are exposed, in accordance with the risk tolerance defined by the organisation;

3.9. Establish and implement controls to protect OMIP's information assets according to their relevance and criticality so that they can be adequately protected throughout their lifecycle, and monitor their effectiveness;

3.10. Identify, contain and resolve information security incidents, in particular cyber attacks, and ensure that they are reported in accordance with applicable laws and internal procedures;

3.11. Minimise the damage to the business caused by information security incidents, ensuring that OMIP is able to continue to provide its services, i.e. its critical or important business functions, in the event of serious security incidents, minimising the negative impact that may arise both for OMIP and for all stakeholders;

3.12. Promote the sharing of relevant cybersecurity information through secure channels and in a timely manner with OMIP stakeholders, the OMI Group, official bodies and other stakeholders, thereby contributing to the globalisation of cybersecurity awareness;

3.13. Promote strategies to implement improvement opportunities, namely proposals resulting from audits, intrusion tests, vulnerability analyses or other internal or external projects relevant to information security and cybersecurity;

3.14. Ensure continuous improvement of the ISMS to ensure its suitability and effectiveness.

4. Security Controls

4.1. Rules of Conduct

OMIP defines rules of conduct for information security applicable to its employees and suppliers, in particular in the following areas:

- Compliance with this Policy and other information security documents;
- Use of technological resources and systems provided by OMIP;
- Handling of information and personal data under the responsibility of OMIP.

4.2. Personal Data

OMIP undertakes to make every effort to ensure the privacy and protection of the personal data entrusted to it, in accordance with the applicable regulations and in particular the General Data Protection Regulation. OMIP classifies personal data as confidential and adopts appropriate physical, logical, technical and organisational security measures, including controls, to prevent data from being disseminated, modified, lost, misused, stolen, processed and accessed without authorisation, and to protect it against any other form of unlawful processing.

4.3. Information Systems

Since information is mostly stored in technological files, special attention must be paid to the specific procedures for managing information systems and the assets that support them.

OMIP's information systems must be planned, defined, developed, tested, implemented and managed taking into account the needs and requirements of information security - confidentiality, integrity and availability.

4.4. Asset Management

The information managed by OMIP, its supporting processes and infrastructure, employees, third parties, offices, equipment, documents, systems, applications and networks are important assets to the organisation. They are therefore properly identified, inventoried, maintained, classified and controlled according to their importance and criticality so that they can be adequately protected throughout their lifecycle (which includes their creation, handling, storage, transport and disposal) in accordance with information security and cybersecurity procedures approved by OMIP.

4.5. Human Resources

Information security applies to all OMIP employees in all departments, across the board, and specific responsibilities must be assigned to certain functions. To this end, OMIP promotes information security and cybersecurity training and awareness and provides the necessary information to enable its employees (including board members) and suppliers to fulfil their information security responsibilities. OMIP then uses event simulation campaigns, for example, to validate the success and effectiveness of these measures.

Employees in departments with privileged access to OMIP's networks and information systems also receive specific training on access management and other operational procedures before taking up their duties. Employees with a higher level of responsibility for information security and cybersecurity at OMIP also receive specialised training in these areas.

4.6. Supplier Management

In managing suppliers, particularly those whose services support a critical or important function, OMIP follows the principles set out in its Supplier Management Policy. This includes defining information security requirements to mitigate the risks associated with supplier (and ICT supply chain) access to information assets, and maintaining the level of information security and availability of services provided in accordance with the terms and conditions contracted with suppliers, by establishing procedures to monitor and evaluate the delivery of services by suppliers.

4.7. Risk Management

One of the core areas of OMIP's ISMS is the continuous management – identification, analysis, evaluation and treatment – of the information security and cybersecurity risks inherent to its activities, to which the organisation's assets are exposed, and which constitutes a corporate management tool. OMIP's risk management methodology within the ISMS includes:

- Identifying and documenting internal and external threats that could exploit vulnerabilities in OMIP's assets and compromise their integrity, confidentiality or availability;
- Assessment based on risk scenarios, measuring the probability and impact that make up the level of risk;

- Treating risks according to their criticality and to the organisation's criteria for accepting and prioritising risks.

Within the scope of the ISMS, risk management includes the implementation of security controls and mechanisms that are designed to reduce, transfer, avoid or accept the potential damage caused by the exploitation of asset vulnerabilities in order to minimise the impact and occurrence of information security incidents and to ensure an appropriate level of security which meets the risk that OMIP is prepared to accept. These measures are defined in accordance with OMIP's business objectives and responsibilities, taking into account efficiency, cost and applicability.

4.8. Incident Management

Any event that jeopardises business operations or compromise information security is treated as a security incident.

OMIP's information security and cybersecurity incident response process is systematised in its Incident Management Procedure, which defines the detection, identification, classification, response, handling, communication, recording and reporting tasks to be performed following the detection of an information security incident. The aim is to ensure a rapid and effective response, minimising potential damage to the confidentiality, integrity and availability of information systems.

The availability of information, particularly in the event of disruptive incidents, is also ensured by the Business Continuity Plans defined as part of OMIP's Business Continuity Management System (BCMS).

4.9. Access Control

Identity and access credentials to OMIP's networks and information systems are issued, managed, verified, reviewed, revoked and audited according to the principles of least privilege, minimum functionality, and segregation of duties. These principles apply to all internal (employee), external (supplier or client) and remote (internal or external) access.

The authentication mechanisms in OMIP's networks and information systems are defined and maintained according to their characteristics, using authentication management technology via the web and directory services to access company information. To this end, authentication mechanisms such as the use of passwords, cryptographic tokens, single sign-on (in the case of the internal network) and multi-factor authentication have been implemented to maintain information integrity and confidentiality.

4.10. Data and Communication Security

OMIP's networks and information systems must ensure the security (confidentiality, integrity and availability) of the data stored, in circulation, in use and in the information transfer flows. To this end, OMIP has implemented the following controls:

- Management of physical and logical access and authentication;
- Backup and recovery;
- Event logging;
- Classification, handling and disposal of information;
- Cryptography;
- Data Loss Prevention (also known as DLP);
- Secure software development and restricted use of software;

- Prevention and detection of malicious activity.

4.11. Security Event Detection

OMIP outsources specialised services in cybersecurity to manage network events (logs) to identify cyber threats and regularly assess vulnerabilities in information systems through automated processes to detect, identify, catalogue and monitor malicious activity. The results and treatment of any vulnerability identified are then incorporated into OMIP's internal action plan so that they can be analysed as part of the risk management process.

4.12. Backups

OMIP makes backups of the information stored in its information systems, stores them in an alternative location where possible and ensures that the confidentiality of the information is ensured. OMIP also ensures the integrity and availability of backups by establishing recovery procedures that guarantee the efficient replacement of backups when needed, within the recovery time objective. These procedures are regularly tested to validate their suitability and the integrity and availability of the backups made.

4.13. Tests

As part of the risk management process, OMIP performs tests to assess the effectiveness of controls implemented to mitigate identified risks:

- It has a security testing plan in place to ensure that the integrity, availability and confidentiality of information is maintained whenever its infrastructure is updated, either through the integration of a new information system or a significant change to an existing system;
- It outsources specialised services to carry out regular vulnerability assessments and intrusion tests on its infrastructure. The results and vulnerabilities identified are then incorporated into OMIP's internal action plan so that they can be analysed as part of the risk management process;
- It regularly tests its incident management procedures and business continuity plans (defined as part of the Business Continuity Management System – BCMS) against plausible scenarios to assess their effectiveness and identify weaknesses and areas for improvement.

4.14. Collaboration and Sharing of Information

Sharing relevant cybersecurity information not only with stakeholders, but also with other interest groups, associations and industry bodies, will help to raise awareness of cybersecurity more widely.

Some examples of OMIP's commitment to contribute to this objective include the establishment of a Cybersecurity Committee, the outsourcing of specialised services to manage network events (logs) and identify cyber threats, and the collaboration protocol with the National Cybersecurity Centre. Compromise indicators, best practices, risk indicators and lessons learned on threats, vulnerabilities and cyberattacks are shared with these parties in a timely manner through secure channels.

4.15. Continuous Improvement

OMIP recognises not only its dynamic reality - in terms of business processes, assets and people - but also the constant evolution of security threats and the exploitation of new vulnerabilities. In addition, information and cybersecurity is a cross-cutting issue in all the organisation's activities, and OMIP is committed to continuously improve it.

To this end, OMIP updates its procedures, policies, plans and processes in light of the latest industry best practices and international cybersecurity references and standards. In addition, this review includes opportunities for improvement suggested by audits, intrusion tests, management reviews or other internal or external security and cybersecurity projects, as well as lessons learned from responding to and recovering from information security incidents.

5. Roles and responsibilities

5.1. Board of Directors

In accordance with applicable regulations, OMIP's Board of Directors is responsible for the company's operational resilience strategy, which includes setting information security and cybersecurity objectives, defining and monitoring OMIP's risk profile and approving an appropriate budget for the implementation of security practices.

As the body ultimately responsible for information security and cybersecurity, the Board is responsible for defining and approving this Policy and all documents implementing it, and for reviewing them to ensure their continued suitability and effectiveness.

The Board must be kept informed and must monitor developments and improvements to the ISMS, as well as the results of audits, tests and evaluations (internal or independent) and developments that have been explicitly discussed by the Board.

5.2. Top Management

OMIP's Top Management, consisting of the Chairman and Vice-Chairman of the Board of Directors and the Chief Operating Officer, is responsible for approving and supporting all ISMS implementation and maintenance activities, including the cybersecurity strategies established by the Board of Directors, and for ensuring that adequate resources are available to ensure the achievement of the objectives set out in this Policy and compliance with the activities undertaken by the company.

5.3. Cybersecurity Committee

The OMIE, OMIP SGMR and OMIClear Cybersecurity Committee is an internal technical committee established at the level of the OMI Group and consists of the persons listed in the Rules of Procedure of the OMIE, OMIP SGMR and OMIClear Cybersecurity Committee. Other employees may be invited to attend the Committee meetings as required, including risk officers, legal departments representatives, compliance officers and the companies' internal auditors.

The Cybersecurity Committee is responsible for proposing cybersecurity strategies and guidelines to the Boards of Directors of the companies that make up the OMI Group, promoting synergies in the implementation, compliance and monitoring of these policies and requirements in the various companies and in the various areas of Management, Protection, Monitoring and Resilience, and, through the Chief

Operating Officers, keeping the executive members of the Boards of Directors of the various companies informed of all relevant cybersecurity matters.

5.4. Information Security Committee

OMIP's Information Security Committee has been established as part of the Information Security Management System (ISMS) at OMIP. This is an internal technical committee that supports management and decision making and consists of at least the Chief Operating Officer, by a representative of the Information Systems department and OMIP's Information Security Manager.

Other OMIP employees may be invited to attend the Committee meetings as required, namely the Head of Legal or other members of the Information Systems Department.

The Security Committee is responsible for overseeing the practical implementation and maintenance of the ISMS policies and procedures, and for proposing their revision to the Board in accordance with the objectives and principles set out in this Policy.

5.5. Information Security Manager

As part of the implementation of the ISMS, OMIP's Board of Directors has appointed an Information Security Manager whose main responsibilities are to:

a) promote information security and cybersecurity training and awareness programmes for employees to ensure that their actions are in line with all ISMS requirements, policies and procedures;
b) ensure that ISMS non-conformities are resolved as quickly as possible;
c) ensure that the ISMS meets its objectives, the requirements of ISO 27001 and other regulatory requirements arising from OMIP's activities;
d) liaise between the Information Security Committee and other business units and departments within of the ISMS;
e) as part of OMIP's Information Security Committee, to raise the need to review existing policies and procedures on information security and cybersecurity;
f) Manage and monitor information security and cybersecurity risk
g) manage and oversee the information security and cybersecurity measures adopted by the OMIP Board of Directors;
h) ensure that ICT incidents are reported to the appropriate authorities in accordance with applicable legislation.

The Information Security Manager participates in OMIP's Information Security Committee and reports directly to the Chief Operating Officer and, where appropriate, to the Board.

5.6. Employees

OMIP's employees, including, for the purposes of this Policy, the members of OMIP's governing bodies, must clearly understand the information security and cybersecurity risks to which they are exposed in the performance of their duties and their roles and responsibilities in mitigating those risks and protecting OMIP's assets as a result.

In particular, OMIP's employees are responsible for:

- complying with all information security and cybersecurity standards, requirements, policies and procedures;
- proactively protecting information assets entrusted to them;

- reporting any information security incidents at OMIP, in accordance with the internal procedures established for this purpose.

5.7. Suppliers

Suppliers are required to behave and operate in a manner consistent with this Policy. In particular, the contracts between OMIP and third party providers with access to its information systems and/or OMIP's technological environment shall include clauses and requirements that ensure the confidentiality between the parties and guarantee that the professionals under the suppliers' responsibility comply with this Policy, the standards, the codes and other applicable procedures.

Suppliers are also responsible for reporting to OMIP any information security incidents that occur in OMIP's information systems or in their own systems, to the extent that these may compromise OMIP's cybersecurity.

Suppliers whose services support a critical or important function of OMIP must be subject to greater control, monitoring, and additional information security requirements in the contractual relationship between the parties, as set out in the Supplier Management Policy.

6. Final Provisions

This Policy shall be reviewed by the OMIP Board of Directors whenever there are changes in information security or cybersecurity, in OMIP's internal organisation, in the legal and regulatory framework or in the best practices applicable to OMIP.

This Policy is available on OMIP's corporate website.

Approved by the Board of Directors on 26 November 2024