Information Security Policy

MEO Group

Index

1. Introduction

Information is an essential critical asset for the business of the MEO Group and, for this same reason, it needs adequate protection. Protection is especially important in a business environment that is increasingly interconnected. As a result of increasing interconnectedness, information is now exposed to an increasing number of different vulnerabilities and threats.

Security of Information and Communications Technology System (ICT) is ensured through the implementation of an appropriate set of controls that includes policies, processes, procedures, organizational structures, software, and hardware. These controls must be established, implemented, monitored, revised, and improved where necessary to ensure that MEO Group specific security and business objectives are met.

MEO Group's Information Security Policy includes a chapter related to managing the organization's cybersecurity risks and managing the supply chain's cybersecurity risks.

What is defined in this Policy prevails over any other document in force at MEO Group, (policy, regulation, working document, etc.).

2. Objectives

The purpose of this Information Security Policy is to establish requirements to ensure the appropriate level of protection of MEO Group Information and Communication Systems and Technologies, including the telecommunications services platforms that support its operations and business.

It is the Policy of MEO Group to prohibit unauthorized access, distribution, duplication, alteration, destruction, or misappropriation of information from its organizations, and to protect the information of external entities – entrusted to MEO Group – in a way consistent with its classification level, in accordance with all applicable legal and regulatory requirements.

In addition to this Information Security Policy, there are operational areas of MEO Group with relevant technological specificities, specific complementary procedures in terms of information security to be followed.

This Policy should be made available to all employees, suppliers, partners, service providers, internal and external entities that access MEO's Group information.

For the purposes of this Policy, information from MEO Group is equivalent to information from external entities that has been entrusted to MEO Group, or to which MEO Group has access, or that deals with any legal or contractual purposes, unless expressly or from the context it results different understanding.

3. Scope

The Information Security Policy described herein is applicable to:

a. People or entities, with access to Information and Information and Communication Systems and Technologies of MEO Group, or under its responsibility, that is, internal and external collaborators, suppliers, service providers, partners, consultants, collaborators of entities external entities and internal entities with access to Information and Information and Communication Systems and Technologies of MEO Group, or under its responsibility. The term "Users" will be used generically in reference to any of the individuals or entities referred to above.

b. People or entities with direct or indirect responsibility for the Architecture, Engineering, Operation and Maintenance, including technological evolution, of MEO's Group Information and Communication Systems and Technologies, or under its responsibility. Responsible for ensuring that the different Information and Communication Systems and Technologies are developed and maintained, throughout their life cycle, within the security requirements defined in this Policy. The term "E&O Responsible Person" will be used generically in reference to any of the individuals or entities referred to in this point.

c. External entities to whom MEO Group awards services, whenever they have access to Information or work directly on MEO's Group Systems and Technologies and Communication or have systems directly connected in a network1 with MEO's Group Systems and Technologies and Communication.

d. External entities to whom MEO Group awards "Cloud" type services, in the IaaS (infrastructure as a service), PaaS (platform as a service), SaaS (software as a service) models, etc. as long as MEO Group data is stored.

All Users and E&O Responsible Persons, regardless of their hierarchical level, function and contractual relationship – internal to MEO Group or assigned to external entities or others with whom MEO Group has contracted to supply Products/Services – must be aware of this Policy and have adequate access to the information necessary to carry out their functions, and they are required to respect the implemented security controls, which are essential for sustainable compliance with the following minimum Information Security values:

- **Information integrity** – prevention against unauthorized modification and destruction of Information, safeguarding its reliability and origin;
- **Confidentiality of Information** – prevention against unauthorized access and disclosure of Information;
- **Availability of Information** – guarantee of authorized access to Information whenever and to the extent necessary.
- **Non-repudiation** – guarantee that whoever caused an activity or event cannot deny that they caused it.
- **IAAAA** (Integrity, Authentication, Authorization, Auditing and Accounting) – guarantee of identification (who accesses), authentication (proof that it was the person who accessed), authorization (definition of permissions), auditing (recording activities and events in logs) and accounting (review of logs to detect violations).

It must also be ensured that evidence of the disclosure referred to in the previous paragraph is kept.

Information security, that is, its confidentiality, integrity, availability, non-repudiation and IAAAA, is everyone's responsibility.

The Policy described here is applicable to all MEO Group Information and Communication Systems and Technologies, as well as to communication between them. The application of this Policy must, however, be carried out in a differentiated manner according to the following classification of Information and Communication Systems and Technologies: :

- New systems and technologies;
- Existing systems and technologies.

3.1 Acquisition of new Information and Communication Systems and Technologies

For the new Information and Communication Systems and Technologies of MEO Group, full compliance with the Policy defined herein should be guaranteed, and this requirement should be ensured from the moment of search and selection of the technological solution to be adopted (RFI, RFP, ...), during the selection and negotiation phase with possible suppliers or service providers, which should be made available to them, under a confidentiality clause, pursuant to the following paragraphs.

When hiring products and services, the internal customer must safeguard that the proposal submitted by the supplier expressly states in writing that the products and services to be contracted comply with MEO Group Information Security Policy and that the provisions of confidentiality and protection of personal data contained in this Policy are explicitly reflected in this proposal, being the supplier liable for any damages arising for MEO Group due to the violation of this Policy by the supplier and its employees, agents and subcontractors.

MEO's Group internal Customer must additionally guarantee, before and after the award, that:

- The architecture, design, implementation, integration, operation, maintenance and future evolution of the solution, including any development, testing and quality control environments, comply with this Policy, as well as integrate with all official security controls of the company, such as Anti-DDoS platforms, WAF's, Forward Proxies, mail relay's, etc.;
- All necessary software development and administration scripts are based on good software development practices, recognized internationally in terms of security, in order to avoid common errors and known security vulnerabilities;
- The Cybersecurity Department was involved, whenever the risk was high, through the Operational Procedure Management of Exceptions and Opinions, published on the MEO Group document management platform, with all the security requirements that it identified being met, as well as tests being carried out security measures, appropriate to the system/software in question and accredited or validated by the Cybersecurity Department, to verify the absence of security vulnerabilities and other non-conformities with this Policy;
- Any supplier or service provider involved in the solution is committed to the confidentiality and information security clauses established in the contracts as well as other clauses that guarantee compliance with this Policy;
- Any person external to MEO Group, who has access to the solution, including the development, testing and quality environments, signs a Confidentiality Declaration that guarantees compliance with this Policy, in addition to other provisions specific to the supply in question.

3.2 Existing systems and technologies *(Legacy)*

For systems and technologies in these conditions, the necessary changes must be implemented to ensure full compliance with the Policy defined herein, except where technical, business or force majeure reasons are identified that make it impossible to implement the abovementioned amendments, for which the exception management procedure should be followed, as described in Chapter 8 of this Policy.

4. General Responsibilities

4.1 Top Management Responsabilities

Computing equipment provided by MEO to Users is for the exercise of their professional duties, so they must ensure its good maintenance and adequate use. It is the Users responsibility to safeguard its personal information and make sure that this is not illicit in legal terms or improper considering the Code of Ethics of MEO. MEO employees, as Users of MEO provided software, must abide by the terms and conditions of software use.

Any MEO employee, as a User, who commits a violation of this Policy shall be subject to disciplinary sanctioning, in accordance with the General Labor Law and the Company Agreement in force.

4.2 Responsibility of the Information Security/Cybersecurity Officer

Dependent on Top Management, the organization has a Department responsible for cybersecurity and information security issues.

4.3 General user responsibilities

Computing equipment provided by MEO Group to Users is for the exercise of their professional duties, so they must ensure its good maintenance and adequate use. It is the Users responsibility to safeguard its personal information and make sure that this is not illicit in legal terms or improper considering the Code of Ethics of MEO Group. MEO Group employees, as Users of MEO Group provided software, must abide by the terms and conditions of software use.

Any MEO Group employee, as a User, who commits a violation of this Policy shall be subject to disciplinary sanctioning, in accordance with the General Labor Law and the Company Agreement in force.

4.4 General responsibilities of administrators of systems, databases, service platforms and network equipment of the information and communication systems and technologies, technical Teams

An employee of MEO Group, as a User, who has configured accesses that allow him to manage Systems, Databases, Service Platforms, Network Equipment of Systems and Information and Communication Technologies, is responsible for:

- By safeguarding the information to which they have access, and must guarantee its confidentiality, in accordance with the Declaration of Confidentiality that you must sign.
- For assuring that the assets under its technical management comply with this Policy. Ensuring, as a minimum, and a necessary condition for the fulfillment of this policy, the application of best practices for maintaining the Cyber Hygiene 2 of the assets under its administration.

The direct management of these employees is responsible for ensuring that only those employees who need privileged access have them configured, and must authorize, review, and guarantee their removal, when they are no longer justified.

4.5 General responsibilities of officers responsible for engineering, operation and maintenance of information and communication systems and technologies

Those responsible for the Engineering, Operation, and Maintenance of Information and Communication Technologies (E&O) and Systems, throughout the lifecycle of the various Information and Communication Technologies and Systems under their supervision, must identify, plan, and obtain approval/commitment from senior management for all conditions, in terms of financial and human resources, the necessary processes and technological tools, and the technologies, in accordance with budget planning cycles, that enable their technical teams to sustainably comply with this Policy. At a minimum, this will involve avoiding technological obsolescence and ensuring the effective application of best practices regarding continuous software security updates (e.g., with the timely application of security patches, updating digital certificates, updating antivirus programs when applicable, eradicating insecure protocols, etc.).

4.6 General responsibilities of external entities

Computing equipment provided by MEO Group to external Users is exclusively meant for the execution of the contracted service, so these Users must ensure its good maintenance and adequate use. It is the User's responsibility to safeguard its personal information and make sure that this is not illicit or improper considering the existing Code of Ethics.

These users must fully comply with the terms and conditions of use of the software which may be provided by MEO Group.

In the event of a breach of this Policy by suppliers, service providers, partners and their users, MEO Group may trigger the legal means within its power and apply the contractual penalties as well as immediately revoke all rights of access to MEO Group systems and technologies to the element that fails to comply, and so should, for this purpose, change their passwords for systems access and disable their access to MEO Group facilities.

4.7 General responsibilities of managers and Human Resource Management areas

Whenever there is a change in the responsibilities or functions of an internal User, the respective manager must immediately initiate the adjustment of that User's access privileges to the different Information Systems and Technologies of MEO Group. If you are an external user, this responsibility will be the responsibility of the person responsible for the internal unit where the service is or was provided.

Whenever an MEO Group employee stops working at the company, the access/identity management system must automatically trigger the appropriate application blocking requests, or at the request of those responsible for the employee, the access management team must deactivate all their access accounts, based on information received by the Human Resources Management area. This team deactivates all access accounts to applications, databases, operating systems (which supported these applications), official wireless networks, RAS (Remote Access Service) and/or VPN (Virtual Private Network) systems, Cloud services, Hosting and Housing, and physical access points to company buildings. The Human Resources Management area must also guarantee the collection of the employee card and all IT resources made available to it by MEO Group (Desktop and/or Notebook, mobile phone, ...).

If this internal employee has, within their duties, dealt with confidential information or personal data, all information on their Desktop and/or Notebook must be destroyed before it is reused for another User. You must then proceed to delete all biometric information associated with that employee and, finally, eliminate all information residing on the internal disks or "flash memory" of the collected devices, with the exception of that which may be necessary for work purposes.

Whenever an employee of an external entity stops performing functions at MEO Group, the area in which they carried out their activity must inform the access management team so that they can deactivate all their access accounts to applications and operating systems (that supported these applications), RAS (Remote Access Service) and/or VPN (Virtual Private Network) systems, as well as the voice communication system (mobile and fixed) and physical access points to the company's buildings. The internal area responsible for the service provided by the external entity must also ensure the collection of any access cards as well as the elimination of all biometric information associated with that external collaborator. If this external collaborator has, within their functions, dealt with confidential information or personal data, all information on their Desktop and/or Notebook must be destroyed before it is reused for another User.

It is mandatory to carry out a procedure that periodically re-evaluates the need to maintain accounts in all Systems, Databases, Service Platforms, Systems Network Equipment and Information and Communication Technologies.

It is MEO's Group responsibility to make its workstation (endpoint) available to external employees, and the use of workstations external to the MEO Group network is not permitted, either remotely (RAS or VPN) or locally (points of local area network (LAN) and wireless networks in company buildings). Exceptions are regulated in MEO's Group Bring your own device Policy.

5. Communication and Information Management

5.1 Classification of information

The degrees of classification of information security, corresponding to the level of sensitivity of information defined in the company are as follows:

- **Top Secret** – this Top-Secret rating is limited to information, documents and materials that require the highest degree of protection. It shall be applied solely to matters whose knowledge or disclosure by unauthorized persons may entail exceptionally serious consequences for MEO Group or for one of its subsidiaries.

  Directives, plans or strategic orders at the level of the company's top management are examples of matters classified as Top Secret. Technical information such as MEO Group PKI keys is yet another example.

  The assignment of the Top-Secret classification level is the sole responsibility of the members of the Executive Committee or equivalent, and it may not be sub-delegated under any circumstances.

- **Secret** – This level of classification applies to matters whose knowledge or disclosure by unauthorized persons, may entail serious consequences for MEO Group or for one of its subsidiaries.

  Examples of materials classified as Secret are studies and documents on the provision of new technological solutions or improvements considered strategic for the business, or other circumstances that indicate highly sensitive issues for MEO Group. This classification also includes technical information, such as e.g. passwords of critical systems of MEO Group.

  The assignment of the Secret classification level is incumbent on the members of the Executive Committee or equivalent, as well as on the Company Directors.

- **Confidential** – This level of classification applies to matters whose knowledge or disclosure by unauthorized persons, may be harmful to MEO Group or to one of its subsidiaries.

  Examples of matters to classify as Confidential are:

  - Operational, technical or commercial documents or information that may contain useful information for the competition;
  - Information or studies on large customers or market segments that may contain useful information for competitors;
    - Files with personal data of customers or other natural persons;
    - All proprietary customer information;
  - Processes of occupational or disciplinary nature;
    - Private information regarding internal and external staff.

- **Restricted** – This classification level is applied to matters limited to the internal use of the organization which, although not requiring a higher classification, should not be known to people who do not need them for the strict performance of their duties.

  Examples of subjects to be classified as Restricted:

  - Technical texts whose content requires protection in the interest of the companies;
  - Information on firms or organizations, concerning offers, proposals, or transactions whose undue knowledge may adversely affect or favor unduly third parties.

  Any company information not explicitly classified with a rating level is classified by default with Restricted level.

- **Public** – This classification level is applied to matters that are explicitly aimed at the public domain.

In the scope of this Policy, "Classified Information" always stands for information not classified as **Public**.

The attribution of the Reserved and Confidential security levels is the responsibility of the employees who sign the document or information whose security they wish to guarantee, taking into account the rules and needs defined above. This information should not be forwarded unless this is necessary and critical for the business, in which case the message and its attachments must be encrypted.

Information classified as Top Secret, Secret or Confidential, stored in databases or system files, fixed or removable, must be encrypted in accordance with the Technical Standard for Cryptography and PKI, published on the MEO Group document management platform, of in order to prevent unauthorized reading, even by those with maximum system or database administration privileges or by a possible hacker.

Equipment with access to information classified as Top Secret and Secret must, whenever possible, use a privacy filter.

MEO Group facilities in which information classified as Top Secret and Secret is stored must ensure entry control mechanisms (identification cards, restriction of access to floors, optical fingerprint detection or other biometric means), in order to identify, authenticate and record entries and movements.

The information that enters MEO Group must maintain the classification assigned by the supplier / partner / service provider, etc., and the information protection security controls accepted / agreed between the parties must be guaranteed. Unclassified information follows the principle defined for the organization's internal information, so it is classified by default as reserved.

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems – Requirements, control, 5.12 Classification of information, 8.12 Data leakage prevention

5.2 Removable media management

5.2.1 Use of removable media

Drives for removable media (USBs, external disks, DVDs, tapes, etc.) should not be available on Workstations (ET) if there is no business reason to justify it.

The Director of each area is responsible for identifying and authorizing the ETs for which drives for removable media must be made available. It must, however, be ensured that drives for removable media are not made available or permitted in the case of risky ETs.

Executing unauthorized software from any removable media is strictly prohibited.

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems – Requirements, control, 7.10 Storage media.

5.2.2 Transport of classified information

Whenever it is necessary to transport any removable medium ("USB pens", external disks, CDs, DVDs, Tapes, etc.) with classified information, all necessary measures must be taken, before, during and after transport, to protect the confidentiality, integrity and availability of Information. The information contained in the removable media to be used must be encrypted prior to transport.

The transport of classified information must be carried out by Users authorized for that purpose.

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems – Requirements, control 7.10 Storage media.

5.3 Information elimination

5.3.1 Disposal of classified documents

ll documents that have already been replaced or expired must be destroyed periodically, and as soon as convenient, except in the case of matters classified as Top Secret, for which destruction will only be carried out after a request to the archive by the issuing entity.

Whenever the holder of a material or document classified as Top Secret understands that it has become useless, he or she must propose to the issuing entity that it proceed or order its destruction. Services responsible for archiving classified materials do not need to wait for instructions to proceed with the routine destruction of classified documents. As a rule, keeping classified documents older than 5 years old, whose historical interest is not recognized, or which have become unnecessary, should be avoided. In the routine destruction of classified documents, crushing machines, shredders or incinerators must be used that effectively guarantee the effective destruction of the information contained therein.

The retention time defined for each type of information must always be considered before proceeding with its deletion, namely checking the retention period of the documentation and type of data, under the terms provided for in applicable law, particularly in accounting and tax matters and in Personal Data Processing records, within the scope of the Purposes/Data Processing defined in the GDPR (General Data Protection Regulation).

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems – Requirements, control, 5.33 Protection of records, 8.10 Information deletion.

5.3.2 Disposal of Media

All CDs/DVDs, magnetic discs, magnetic strips/cartridges, etc. that are no longer needed must be physically destroyed or placed in suitable containers so that they can be subsequently destroyed by a company duly certified for this purpose. The physical destruction process must make any recovery of information, even partial, impossible. This destruction must always be carried out by a company whose contractual relationship ensures the necessary confidentiality.

Whenever the collaboration of an employee (internal or from an external entity) ends, the respective manager or the person responsible for the area in which they carried out their activity must inform the area responsible for Equipment Management with a view to the appropriate deletion of the employee's information records, ensuring the confidentiality of information relating to the function performed.

It is the responsibility of the Employee (internal or an external entity) with whom the collaboration ended to safeguard their personal information, and MEO Group does not assume any responsibility in relation to that personal information.

Retention periods for different types of information must be strictly guaranteed in accordance with the different laws to which MEO Group is obliged.

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems – Requirements, control, 7.10 Storage media, 8.10 Information deletion.

5.4 Information storage

5.4.1 Storage of information on servers

All servers with relevant information from MEO Group must be housed in a Data Center or technical rooms of the ANG type (New Generation Areas) under the responsibility of a recognized operational entity that ensures systems administration and their physical and logical security within best practices and the provisions of this Policy.

Servers with information classified above Reserved by MEO Group, from the different environments, namely development, laboratories, tests and production, must be properly identified in the CMDB and reflect the correct operational status (e.g. productive/ slaughter/ disconnected/ etc.), in order to automatically generate alerts for the responsible teams.

Whenever a server stops being used, it must be immediately disconnected from the network and its information destroyed after checking the retention period for the type of data, in accordance with applicable law, particularly in accounting and tax matters and in Data Processing records. Personal, within the Purposes/Data Processing defined in the GDPR. In the exceptional case where this server must be kept connected to the internal network for a longer period of time, it will be mandatory to guarantee its logical security by eliminating all unnecessary logical access to prevent malicious use.

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems – Requirements, control, 7.8 Equipment siting and protection.

5.4.2 Storage of information required for management and technical administration of systems, databases, service platforms or network equipment

The information necessary for the management and technical administration of Systems, Databases, Service Platforms, Systems Network Equipment and Information and Communication Technologies, e.g. registration of passwords, certificates, keys, etc., must be stored in a system that ensure access control, namely “Password Vault Management” and “Certificate Management”.

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems – Requirements, control, 5.37 Documented operation procedures

5.4.3 Documentation management and use in information systems and technologies

Documentation relating to the MEO Group’s Information and Communication Systems and Technologies (e.g., operational and user manuals) must be up to date and accessible only to those authorized.

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems – Requirements, control, 5.37 Documented operation procedures.

5.4.2 Storage of information required for management and technical administration of systems, databases, service platforms or network equipment

The information necessary for the management and technical administration of Systems, Databases, Service Platforms, Systems Network Equipment and Information and Communication Technologies, e.g. registration of passwords, certificates, keys, etc., must be stored in a system that ensure access control, namely “Password Vault Management” and “Certificate Management”.

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems – Requirements, control, 5.37 Documented operation procedures

5.4.3 Documentation management and use in information systems and technologies

The documentation on the organization’s information and communication systems and technologies (e.g., operating and use manuals) must be updated and accessible only to those authorized.

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems – Requirements, control, 5.37 Documented operation procedures.

5.5 Information Communication

5.5.1 Classified Information Communication

The transmission, by electronic means of any type (including e-mail, fax, telephone, mobile phone and Internet), of material or documents classified as Top Secret or Secret, even partial, is not permitted.

Information classified as Confidential or Reserved cannot be sent to a network printer without someone authorized to safeguard confidentiality during printing and collection of the document, and must not be forwarded outside the company unless it is necessary and critical to the business from MEO, in which case the data must be encrypted before sending.

Whenever possible, the transmission of credentials must be carried out separately and through different communication channels, otherwise the risk must be assessed by the Cybersecurity area in accordance with point 8 of this Policy.

When sending documents of this nature for destruction and subsequent recycling, it must be ensured that the result is unreadable.

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems – Requirements, controls, 5.14 Information transfer.

5.5.2 Use of portable computers and other mobile devices (tablets, smartphones, ...)

Employees who use MEO Group laptops must not leave the equipment without its padlock. Password protection of documents, usually available in some applications (e.g., Microsoft Word, Microsoft Excel, Adobe), is not sufficient.

Mobile devices can be stolen or lost, and may be more subject to the interception of data and information, therefore requiring additional Information Security controls if they have to access MEO’s Group classified information.

For each type of mobile device that has to access MEO’s Group classified information, the following Information Security controls must be ensured: physical protection, access controls, encryption of stored and transferred information, data backup, virus protection , malware and intrusions.

In case of loss or theft, the procedure contained in the User support system in force at the company (e.g., OneDesk) must be activated.

MEO has an internal Bring Your One Divice (BYOD) Policy, which clearly defines the guidelines for their use, under what circumstances, when, and who can approve their use.

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems – Requirements, controls, 5.33 Protection of records, 8.1 User end point devices.

5.5.3 Policy and principles of email use

Any message sent from a MEO Group email domain or with a signature containing a reference to MEO Group companies (even if sent from an employee's personal email domain) may be considered by the "general public" as an official statement/position of the organization. Therefore, the organization's email address may not be used to create or distribute any message that is contrary to the law and the provisions of the MEO Group code of ethics.

Messages may only be sent via an MEO Group e-mail domain and/or subdomain, by servers that are duly authorized, legitimized and with defined policies, using for this purpose the security standards SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) and DMARK (Domain-based Message Authentication Reporting and Conformance).

It is acceptable for MEO Group employees to use the organization's email system for personal purposes, provided that such use is properly moderated, does not violate the MEO Group code of conduct and respects the rules established in this Policy, as well as in other MEO Group instruments on this subject.

The use of the MEO Group e-mail system is subject to the security controls necessary to combat SPAM, PHISHING, SPEARPHISHING and Virus and other Malware infections. The logging system for e-mails sent and received, and administrative acts relating to different mailboxes, follows all the requirements for safeguarding user privacy and obligations provided for by law.

5.5.3.1 Authorized Systems

E-mails are only permitted to be sent via applications (e-mail clients) installed in ETs or duly authorized systems, and cannot be automatically forwarded to e-mails external to MEO Group.

Whenever justified, Digital Certificates must be used to sign and encrypt e-mails.

5.5.3.2 Misuse

- Sending chain letters from an MEO Group e-mail;
- Sending mass emails, (e.g. to a large distribution list), except if done by authorized MEO Group areas;
- Creating e-mails by posing as third parties is a violation of this Policy and may give rise to disciplinary and judicial proceedings.

5.5.3.3 Procedures in case of suspicion

Users should never open documents, files, macros, or URLs (links) that they receive as an attachment to an e-mail whose origin is unknown, or there is suspicion that the content may be harmful, indicate password theft or usurpation of identity.

The User must immediately report it (by attaching documents or e-mails) via the User support system in place and immediately delete them. You should then empty the "Deleted Items" folder.

All spam e-mails, chain letters, and the like must be immediately deleted (including from the “Deleted Items” folder) and must never be resent.

In order to guarantee the security and performance of the systems, e-mail control tasks can be carried out randomly and filtering certain files included in e-mails, namely those affected by computer viruses or those that, due to their format (e.g. , .exe, .bmp), may represent a potential danger to the integrity of information and communications systems and technologies.

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems – Requirements, controls, 5.14 Information transfer

5.5.4 Use of Messaging Services with encryption end-to-end

Any message sent by a Messaging Service with a signature containing a reference to MEO Group (even if sent from a personal user of an internal or external collaborator) may be considered by the “general public” as an official statement/positioning of the organization. In this sense, the Messaging Service cannot be used to create and distribute any message contrary to the law and the provisions of MEO’s Group code of ethics.

The use of Messaging Services is permitted as long as end-to-end encryption is guaranteed (WhatsApp, Signal, Telegram, etc.).

These means of communication must be used as a complementary means to existing means at MEO Group, namely corporate e-mail, corporate messaging services (Microsoft Teams, Microsoft Lync/Skype for Business, etc.).

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems – Requirements, controls, 5.14 Information transfer.

5.5.5 Systems development – encryption use in communication

Standard and non-proprietary algorithms must be used, accepted by the cybersecurity community as being state of the art, and which are described in MEO’s Group Internal Technical Standard for Cryptography and PKI. Cipher key size requirements are reviewed and updated in accordance with technological developments. The use of proprietary encryption algorithms is not permitted.

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems – Requirements, controls, 8.24 Use of cryptography.

5.5.6 Information communication between systems and applications

Whenever sensitive or classified information must circulate between two applications or systems outside a secure perimeter, Secure Protocols (e.g., HTTPS, SSL/TLS, SSH or IPSec) must be used. If it is not possible to segregate classified information from different levels, all security measures of the highest classification must be adopted.

Whenever new systems or applications are acquired, it must be ensured that they all support Secure communication and administration protocols.

Exceptionally, the FTP protocol can be used in legacy systems that have to transfer classified information and that, for historical technical reasons, do not support secure file transfer versions (e.g., SFTP or SCP). In these cases, access must:

- Only be allowed among equipment that requires these services, and access must be blocked for any and all other IPs. Violations at this point must constitute events monitored by MEO’s Group Security

Operations Center (SOC);
- Be carried out whenever possible through the File Store;
- Be registered in the respective CMDB (Configuration Management Database), or equivalent, for periodic control.

Regarding legacy Systems and Technologies that, for technical reasons, cannot fully comply with the provisions, all exceptions must be documented, in an official asset register (e.g., CMDB), guaranteeing their confidentiality and that access to them is carried out only by authorized Users.

Whenever a technological renewal action does not lead to full compliance with this Policy, the identification of this system as a documented exception must be maintained.

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems – Requirements, controls, 5.14 Information transfer, 8.24 Use of Cryptography.

5.5.7 Security Guarantee at Internet/Extranet/Intranet Front Ends

For MEO's Group Internet and Extranet solutions, the https protocol must be used in areas of the application that involve classified information, the http protocol is only used in situations where all information is classified as Public.

Although in this version of this Policy the obligation of the https protocol is only restricted to areas involving classified information, in future versions this restriction will become universal and the main browsers will require it, so, by default, the https protocol must always be used in all new systems and technology implementations.

Under any circumstances, the Web front-ends of the aforementioned solutions must always be protected in an MEO Group Data Center within a secure DMZ, with internal (from the DMZ to the backends) and external (from the DMZ to the network where they are located) interfaces. Users) duly protected and monitored by MEO's Group Security Operations Center (SOC). Segregation of internal and external DMZs must be guaranteed. If the solution is critical for MEO Group, it must additionally guarantee multiple distinct Web front-ends (at least 2), in a cluster, divided by different physical infrastructures, and properly balanced by a load balancer or equivalent architecture with adequate capacity.

This ensures:

- Better resource management, as it allows scalability;
- Less exposure of IP ports to the Extranet or Internet, allowing to consolidate access from abroad and facilitate their monitoring by the Security Operations Center (SOC);
- Greater simplification in the configuration and management of DMZ security devices monitored by the SOC;
- Prevention and mitigation of possible DoS (Denial of Service) attacks at the load balancer entrance, saving the servers connected to it;
- Implementation of virtual addressing, thus preventing it from being known and accessed directly from the outside.

Cybersecurity protection mechanisms must be guaranteed for systems exposed to the internet or extranets, whose information is considered critical, namely covered by the GDPR and other legislation, regulations applicable to MEO's Group activity, namely anti-DoS and WAF (Web Application Firewall) solutions.

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 8.21 Security of network services.

5.6 "Clear desk and clear screen" Policy and Principles

MEO Group, committed to the progressive improvement of its information security practices, defines the basic principles of "Clear desk and clear screen" below:

- That aim to guarantee the correct storage and safeguarding of information in its different media, namely physical and logical with information from MEO Group;
- They intend to establish the basic requirements so that the environmental space remains clean and tidy, where information and materials containing company information are protected, particularly regarding employees, customers, suppliers and intellectual property of MEO Group;
- They apply to all Persons or Entities, with access to Information and Information and Communication Systems and Technologies of MEO Group, or under its responsibility, whether they are internal collaborators, external collaborators, suppliers, service providers, partners and consultants.

In compliance with them, the following specific principles must be observed:

1. People or Entities must protect all MEO information, whether physical or logical, present in their work environment;
2. Whenever he is absent from his workstation, and to prevent access to the information contained at his workstation, the employee must:
    a. Lock the screen, using the sequence of commands to do so: "Ctrl-Alt-Del"+"Lock this Computer" or Window key + L;
    b. Turn off your workstation when you are absent at the end of the working day or log off, whenever applicable;
    c. Leave the padlock on the laptop or store it in a locked cabinet.
3. Authorized mass storage devices must be considered sensitive material and must therefore be stored in a protected/locked location whenever they are not in use;
4. Printers must have logical access control (e.g. Copy Points from MEO). If it is not possible to implement such control, they must be located in reserved spaces and with physical access control;
5. Printing documents should be avoided, and priority should be given to sharing and managing documents electronically and securely. Printed copies must be collected immediately from the printers after printing; Documents on physical media, when not in use, should not be left on the desk, fax machine, printer or photocopier or in any other area of the work environment;
6. The destruction of documents and classified information must comply with what is defined in point 5.3.1;
7. Passwords must follow the guidelines defined in MEO's Information Security Policy and must not be written down or stored on any physical medium (e.g. Post-its, etc.);
8. Keys and access cards must not be left unattended;
9. Meeting boards and flip charts must be kept clean after use;
10. Internal collaborators, external collaborators, suppliers, service providers, partners and consultants must not verbalize confidential information in "open spaces" or in any public space, and must use reserved spaces, whenever it is necessary to have a telephone or video conference, ensuring the convocation/presence of only those Persons or Entities that should have access to this information;
11. All of the previously mentioned Principles apply equally when People or Entities are teleworking or when remotely accessing the MEO network or handling MEO information.

It is everyone's responsibility to ensure the application of these MEO Group "Clear desk and clear screen" Principles. Repeated or serious violations thereof may trigger disciplinary action as well as legal, civil or criminal proceedings.

If any of your devices and/or documents are missing, or if you believe that your work area has been violated, employees (internal or external) must report this situation immediately, in accordance with Point

9. Communication of Security Incidents Security of MEO's Group Information Security Policy.

Exceptions to this document must be assessed, in terms of risk, by the Cybersecurity Department, in accordance with Point 8 (Exceptions and Opinions to the Information Security Policy) of the MEO Group Information Security Policy.

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 7.7 Clear desk and clear screen.

6 Access Management

6.1 User Access Management

MEO Group must adopt, across the board, a centralized identity management system. This system must store data that identifies all Users, internal and external, defining their access privileges to different systems, technologies and applications, the validity period of each of these privileges and the authorization chain.

Access allocation must follow the RBAC (Role Based Access Control) principle, which is based on the roles and tasks that users perform in the Organization.

In order to guarantee an adequate level of security, the following rules must be implemented:

- All systems, technologies and applications must allow authenticating and validating the access privileges of each of their Users;
- Access to systems, technologies and applications must be via user/password authentication, which must be unique for each individual User, or through stronger authentication mechanisms, meanwhile adopted by MEO Group and approved by the Cybersecurity Directorate (DCY). The sharing of authentication mechanisms by groups of Users is not permitted.
- Accounts with a privileged access profile, namely AD and Domain Administration, Systems Administration, Databases, Service Platforms, Systems Network Equipment and Information and Communication Technologies, must use authorization access using additionally a two-factor authentication (2FA) or multifactor authentication (MFA) mechanism.
- In the most critical administration functions, such as, for example, "AD & Domain Admin" and Backup Systems Administration, in addition to 2FA/MFA, a "Privileged Account Security" (PAS) solution must be used , such as CyberArk.
- All access systems to MEO's Group internal network from the Internet (for example, VPN and CITRIX) must require 2FA/MFA for all users with system administration roles, with access profiles not limited in terms of what can access critical application profiles with the possibility of carrying out transactions or functions with significant impact.
- Additionally, this 2FA or MFA mechanism must be used whenever justified given the criticality of the asset accessed.
- Any situation that requires specific analysis must be observed in Point 8 (Exceptions and Opinions to the Information Security Policy) of this Policy.
- Whenever possible, the interface presented for authentication should include the following warning:

  "This system should only be used by authorized Users. By continuing to use this system, the User acknowledges that they are an authorized User, acknowledges that uses of this system are recorded and understands that violations of this Policy may trigger disciplinary action as well as civil or criminal legal proceedings."

- Any anonymous access to MEO Group systems or applications (e.g., through Guest Users) is prohibited. These accounts must all be deactivated.
- Requests for new Users or changes to privileges must go through a validation process that includes the Human Resources area, in the case of internal users, and the areas responsible for hiring, in the case of external users, and must be made in writing, using pre-written templates. -defined or specific computer applications for this purpose and approved by the respective manager before being

implemented.

- All Users who are inactive for 60 days (maximum) must be automatically blocked;

  Users who are inactive for 1 year (maximum) should, if technically possible and without impact on User traceability, be automatically removed, otherwise they should be kept blocked;

- Privileges granted to Users external to the organization must automatically expire after a maximum of 90 days.

  Exceptions to this rule may be implemented, as long as they are identified by the respective authorized MEO interlocutor, who will define the appropriate period for the respective access. Whenever it is necessary to extend this period, a new request must be authorized by the same entity;

- Whenever there is a change in a User's responsibilities or functions, their supervisor must request the corresponding adjustment of the User's access accounts.
- For critical systems and applications, it is imperative to carry out a procedure that periodically requires the revalidation, by those responsible, of the need to maintain access to Users. This revalidation must occur at least once a year for each user.
- Whenever a technician with active access to administration accounts on any equipment ceases to function, it is mandatory to suspend all accounts on these systems or equipment. It is mandatory to carry out a procedure that periodically re-evaluates the need to maintain accounts with administration privileges in all technologies, systems and applications, whether information (BSS or OSS) or communication.
- All employees with access to systems/technology/application administration accounts must be covered by a Declaration of Confidentiality or contractual or legally equivalent provision.
- The granting of access must respect the "need to know" principle, that is, access must be provided based on the functional needs of each employee.
- Whenever possible, granting access must ensure the segregation of roles for development, test and production Users. Users on the development team should not have write access privileges to the production environment.
- If a User, who is not part of the technical area of Operation, Management and Maintenance, Systems, Applications, Databases, etc., and within the scope of their functions needs access to them, with Administration privileges, must present the respective justification and approval from the direct manager and this must be duly documented in the CMDB or application used to manage accounts and profiles.

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 5.16. Identity management, 5.18 Access rights, 8.12 Data leakage prevention.

6.2 User Password Policy

All users must have their own password to access MEO's Group computer systems, this password being personal and non-transferable. Passwords are used for the most diverse purposes: application access accounts, system administration accounts, service platform accounts, network equipment administration accounts, web accounts, e-mail accounts, screen saver protections, protections voice-mail, etc. In this sense, the following rules must be implemented:

- After installing any application/system/technology, it must be ensured that all factory passwords (assigned by default by suppliers) of accounts with administration privileges are changed in accordance with the rules defined in this Security Policy; likewise, all Guest accounts or others not necessary for the operation of MEO Group must be immediately inhibited;
- Passwords assigned by default to new Users of applications/systems/technology must comply with the robustness rules defined in this Policy and must be changed after the first login. If the password is not changed, new Users will be valid for 48 hours, after which the account must be blocked;

- In order to prevent possible attacks on information security, the number of consecutive attempts to authenticate to a system/application/technology must be a maximum of five. Whenever possible, after five failed authentication attempts from the same point, the system must block access to that User from the identified point until the administrator resets the respective password (password reset) and the authentication process must continue. if prevented for a period of no less than 10 minutes;
- The presentation by an application/system/technology of any password on the screen or printed on paper is prohibited, and it must always be hidden during its insertion;
- Whenever applications/systems/technology allow, the initial password assigned to a User must only be valid during the User's first authentication. During this access, the User must be forced to change this first password. This process must also be applied whenever a User forgets their password and it has to be reset by the support/maintenance team (password reset);
- Automatic mechanisms must be implemented in systems/applications/technologies that force the User to periodically change the password in accordance with the following rules:
- A maximum of one password can only be used for 90 days, after which it must expire and be forced to be changed;
    - It must not be possible to reuse any of the last 10 passwords previously used;
    - After defining the new password, the User will only be able to change it again after at least 1 hour;
    - Systems/applications/technologies must only allow passwords that comply with the construction rules defined in point 6.5 or 6.6.

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 5.17. Authentication information.

6.2.1 Specific Guidelines for User IDs and Passwords for Application Use

Whenever a target system, application or database allows direct access to other "client" systems or applications, through a login using a user-id and password, the target system/application must guarantee:

- Different user-ids and passwords, for each system or application that is your "client", regardless of the access method used;
- The passwords used must follow the guidelines for creating robust passwords (point 6.6);
- The target system/application/database must refuse the logon if the source IP does not belong to a recognized range;
- In order to prevent possible attacks on information security, the number of consecutive attempts by a system/process to authenticate to another system/application/technology must be at most one;
- When a login fails either because the password is wrong or because the IP does not belong to the expected range, it must fail without returning any feedback to the "client" entity;
- All logons, whether successful or not, must be recorded in an appropriate log, kept in a secure area.
- In order to guarantee traceability, user-Ids and Passwords for application use must not be used outside the scope of established application processes and/or procedures (e.g. interfaces, schedulers, pools, etc.) regardless of the environment's function. Therefore, they cannot be used for direct connections by individual users, particularly from equipment outside the datacenter environment.

If all the previous points are met and the "client" applications/processes and the target system/application or database reside in secure areas within MEO Group Data Centers, the passwords do not have to be changed on a mandatory periodic basis. Otherwise, those responsible for the "client" system or process must assume a password expiration period (maximum one year), and ensure a reliable update process following the recommendations referred to in point 6.6 for robust passwords.

In any case, whenever there is a well-founded suspicion that a certain password has been revealed beyond the team responsible for operating the systems or technologies involved, the administrator responsible for the system/application/technology must replace it.

The purpose of using these accounts is to enable Systems, Databases, Service Platforms, Systems Network Equipment and Information and Communication Technologies to communicate with each other, so they should only be used automatically, not its use being permitted by a nominal person.

All application accounts must have a nominal person responsible (not an entity, support e-mail or department acronym) duly registered on the centralized identity management platform (MEO's Group Identity Management).

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls , 5.18. Access rights, 5.16 Identity management

6.2.2 User Specific User ID Guidelines for IS/IT and Telco Technical Support Accounts

The existence of IS/IT and Telco technical support Accounts is permitted, either under the responsibility of internal collaborators or under the responsibility of external collaborators, the latter as long as they are duly contracted with the entities that provide support for the assets in question. They must always have one identified:

- Nominated internal person responsible (name and number of MEO employee);
- Nominated person responsible for the external entity.

These accounts must be accessed via VPN and have a profile strictly necessary to use the platforms required, within the scope of what is contracted, also including 2FA if they have access to the administration of Systems, Databases, Service Platforms, Network Equipment of Information and Communication Systems and Technologies.

Whenever necessary, a jump box must be used to access these applications and whose profiles are equivalent to administration accounts.

Included in the IS/IT and Telco technical support accounts are, namely, those "that come from the factory", those that are essential to Operate, Maintain and Manage them, access in the event of a serious incident, and with access to administration of Systems, Databases, Service Platforms, Systems Network Equipment and Information and Communication Technologies.

6.2.3 Specific Guidelines for Creating Passwords for Named Users (internal or external)

All Users should be aware of the importance of choosing a password that is not weak.

Weak passwords jeopardize information security and therefore prohibited by this Policy. Passwords should never be written or recorded on any media type.

User passwords must be at least 15 characters long and include 3 characters from the following 4 character3 sets:

- Lowercase letters (a...z)
- Uppercase letters (A...Z)
- Numbers (0...9)
- Special characters: ~!@#$%^&*()+|` -=\{}[]:";'<>?,/

As additional good practice, the User should make sure that passwords do not contain:

- A word in any language, dialect or slang;
- Personal information;
- The corresponding username;
- And that the password for access to MEO Group environments must be different from passwords used for authentication in personal applications (e.g. Linkedin, Gmail, Home Banking, etc.).

Alternatively, they may consist of long text phrases or excerpts known to the User, adding special characters in substitution of some letters (e.g.: S by $, B by 3, a by 4, o by 0, etc...), without a ' space ' character and with a minimum of 40 characters.

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 5.16 Identity management

6.2.4 Specific Guidelines for Building Robust Passwords for Users with Administrative Privileges

Passwords for nominal users with administrative privileges must be strong according to the characteristics above and additionally have at least 22 characters.

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 5.16 Identity management

6.2.5 Specific Guidelines for Building Robust Passwords for Users/ "User-IDs and Passwords for Application Use"

Passwords for nominal and application Users with administration privileges, and for application integration, must be robust in accordance with the characteristics above and additionally have at least 22 characters.

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 5.16 Identity management

6.3 Specific Responsibilities of Users

6.3.1 Workstation security (VDIs, desktops and notebooks)

Users are prohibited from:

a. Carry out actions that may damage, interrupt or generate errors in computer systems;
b. Carry out unauthorized uploads, downloads or transmission of any program or file subject to copyright, related rights or other intellectual property rights, namely music files, videos, etc., for non-professional purposes;
c. Install cookies.

All ETs, regardless of whether they are VDi's, Desktops or Notebooks, must be installed by the MEO Group structure responsible for desktop management, and must guarantee active support for the set of protection mechanisms stipulated by the security rules in force at MEO Group: Anti -Spam, Anti-Malware, Personal Firewall, Active Screen-saver with password, XDR/EDR, DLP, etc. These mechanisms must always be active and must be automatically updated. Users cannot change these settings on ET in order to guarantee the security of information when using it. Exceptions to this rule must be authorized by the entity responsible for ET.

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 8.7 Protection against malware, 5.17 Authentication information, 8.12 Data leakage prevention

6.3.2 Development Station (DT) Security (desktops or notebooks)

All DTs must be installed by the MEO Group structure responsible for desktop management, and must guarantee active support for the set of protection mechanisms stipulated by the security rules in force: Anti-Spam, Anti-malware, Personal Firewall, Screen-saver active with password XDR/EDR, DLP, etc. These mechanisms must always be active and updated automatically. Changing these settings, as well

as installing/uninstalling software, is the responsibility of the User to whom the development station was assigned.

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 8.7 Protection against malware, 5.17 Authentication information, 8.12 Data leakage prevention

6.3.3 Security of ET workstations with access to privileged management accounts

In ETs with access to privileged Administration accounts, in principle, the data stored on their disk must be subject to an encryption process, and this principle must be applied to any other Mobile Device (e.g. Tablets, etc.) that have access to classified data from MEO Group.

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 8.7 Protection against malware, 5.17 Authentication information

6.3.4 Security of devices not managed by the technical areas of MEO Group

Any and all devices that attempt to connect to the MEO Group network, whether via a fixed network or a wireless network, must comply with the security requirements defined for ETs managed by MEO Group. If you do not meet these requirements, you must be limited to the public Internet and any access to MEO Group systems, technologies and applications must be carried out using an official MEO Group VPN (Virtual Private Network) classified to deal with unmanaged devices. or via a Citrix-like interface.

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 8.7 Protection against malware, 5.17 Authentication information, 8.12 Data leakage prevention

6.3.5 Workstation Lock and Logout

Users who leave their workstation unattended must first ensure that they lock or Logout their computer.

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 5.17 Authentication information

6.3.6 Password protection

All passwords must be treated as classified information of the organization.

Passwords should never be shared with anyone.

Users must not use the same password to access MEO Group and for external access to it, and must not:

- Reveal your password to anyone over the phone;
- Reveal your password in any e-mail message;
- Reveal your password to your manager;
- Talking about a password in the presence of other people;
- Reveal clues about your password (e.g., “my family name”);
- Reveal your password in surveys or other means;
- Reveal your password to colleagues when you go on vacation;
- Share your password with family members;
- Use the “Remember Password” functionality available in some applications (e.g., OutLook, Netscape Messenger);
- Write the password and save it in the office or on any device, including the computer or mobile device in an unencrypted form.

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 5.17 Authentication information

6.3.7 Information sharing

Sharing disks with read/write privileges is prohibited. To share information, the organization's existing systems must be used (e.g., Shares, Intranets, MEO Cloud, Sharepoint, etc.) for which the necessary access policies have been defined and implemented.

If information sharing has to be carried out using an external storage device (due to technical impossibility), the device must be encrypted or protected by a password.

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 8.2 Privileged access rights, 5.17 Authentication information, 8.12 Data leakage prevention

6.3.8 Anomalous situation reporting

Whenever a user suspects the misuse of an access account to a system/application/technology, or that the password has been disclosed, the User must immediately inform the Security Operations Centre in accordance with the procedures described in Chapter 9 of this Policy – Security Incident Reporting.

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 6.8 Information security event reporting

6.3.9 Destruction and/or unauthorized modification of application or system logs

Users may not destroy, alter or compromise any application or system logs. Failure to comply with this rule constitutes a serious violation of this Policy.

LOGs must be stored in a secure and segregated environment from the environments where these events were generated and digitally signed. It is recommended to separate the teams that manage the environments where these events originate and the teams that manage the storage of LOGs. LOGs must record relevant events according to the CRUD principle (Create, Read, Update, Delete), as well as allow answers to the questions: Who did it?; When did you do it?; How did you do it?; Where did it come from?; What did you do?; Why did he do it?

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 5.17 Authentication information

6.3.10 Conducting unauthorized security testing

Testing and demonstration programs that do not belong to MEO Group can only be used after examination and prior authorization by the entity responsible for Information Security.

Users may not carry out computer operations that constitute a violation of any applicable legal provisions. Users may not test or compromise the security measures associated with the systems.

Incidents involving traffic capture and analysis (network tapping or sniffing), attempted unauthorized access to systems, applications or communications platforms, password cracking, decryption of third-party files, or other similar activities generally classified as hacking, which may compromise the security of information and communication systems and technologies, are considered serious violations of this Policy.

6.3.11 JumpBoxes

If it is impossible to identify all authorized IPs (e.g., IPs assigned via DHCP), access must be made via an administration warehouse (known as a Jump Machine or JumpBox) recognized by the entity responsible for operationalizing and managing IT services.

Only authorized technicians, nominally identified and subject to signing a Confidentiality Declaration or confidentiality rules within the scope of the employment relationship with MEO Group, must have administration privileges (Systems, Database, Applications, etc.).

Direct login to root must be prohibited on all UNIX family systems. System administrators or those responsible for the operation must first log in to their own nominal account, which only has the privileges strictly necessary for their role, and whenever necessary, and only in these circumstances, SUDO root from their nominal account.

SNMP access is strictly prohibited to unauthorized entities. Insecure SNMP access is prohibited.

All new systems and technologies must support SSH for interactive access to the system, even within a secure perimeter. Access using insecure protocols should be avoided.

When carrying out RFPs (Request For Proposal) it must be taken into account that:

· All new information and communication systems and technologies must support Secure Protocols for remote management (e.g., SSH);

· All new information and communications systems and technologies must support the latest version of SNMP.

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 8.20 Networks security, 8.24 Use of cryptograph

6.3.12 Remote shells, SNMP and administration of information and communication systems and technologies

In situations where it is unfeasible to use JumpBox-type technologies to access legacy systems and technologies that, for historical technical reasons, only have Telnet or another identical remote shell protocol, non-secure SNMP, access should only be allowed within a secure perimeter and from the specific IPs of the authorized consoles, and access must be blocked from any other IP.

6.3.13 Other provisions

As part of this Policy, MEO Group installs security systems such as anti-virus/anti-malware on all managed devices of its employees (e.g., ET). The fact that these security systems examine the User's CDs/DVDs or information storage devices, their operation does not imply their authorization.

Computer and communication resources are made available by MEO Group as auxiliary work instruments for the performance of the contracted activity, with the possibility of their use for private purposes being a liberality of the company. MEO Group reserves the right, without prejudice to the continued validity of this Policy, to revoke at any time, and without prior notice, the use of these resources for professional and/or personal purposes, with the inherent obligation of the User to deliver them immediately.

6.3.14 Obligations at the time of termination of employment or contractual bond

a. Deliver to your superior the equipment, software and other work tools and information prepared and/or in your possession, not being able to keep or use said information for any purpose, without prior written authorization from MEO Group;
b. Delete all personal information that you have stored or that is available in the company's systems and electronic resources made available by the company;
c. Deliver professional e-mails to your superior, in digital format.

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection Information Security Management Systems – Requirements, controls, 5.17 Authentication information

6.4 Network Access Control

6.4.1 Internet access

User access to the internet must be done through the MEO Group Proxy and accept the groups and categories already defined. Exceptions must be evaluated in accordance with Point 8 (Exceptions and Opinions to the Information Security Policy) and approved by the Cybersecurity Department.

6.4.2 Simultaneous use of multiple networks

While a Desktop or notebook is connected to one of MEO's Group internal networks, it cannot be connected to any other network.

The use of ADSL kits, Modems or mobile internet access devices to connect Desktops or notebooks simultaneously to the Internet and to any of MEO's Group internal networks (including management networks) is prohibited.

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 5.15 Access control

6.4.3 Use of wireless networks

The area responsible for the operational security of internal networks must ensure that only wireless accesses that guarantee the security of Users' information are authorized to operate on company premises, with a request for authorization to connect the devices having to be submitted in advance.

Access Points, within MEO Group installations and with MEO Group ET or TD, to unauthorized wireless networks are considered serious violations of this Policy.

Any installation of unauthorized wireless equipment (e.g., routers with a WiFi interface) that provides other equipment with direct access to MEO's Group internal network is considered a serious violation.

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 5.15 Access control, 8.20 Networks security

6.4.4 Outward tunnels

The opening of tunnels that allow data communication from MEO's Group internal network to the outside, without being properly analyzed, documented and authorized by the corresponding managers and the entity responsible for the Information Security Policy, is expressly prohibited.

The use of internet browsing anonymization mechanisms, such as the use of TOR Networks, by MEO Group user accounts is not permitted. Since this type of mechanism makes it impossible to trace those who use MEO's Group resources.

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 5.15 Access control, 8.20 Networks security

6.4.5 Remote accesses

Remote accesses within the company must always use official VPNs managed by the entity responsible for Infrastructure.

Access requests from outside must be duly analyzed, documented and authorized by management. These requests are supported by a procedure that guarantees the traceability of allocated access and the preservation of these records for a period of 2 years.

When accessing equipment remotely, only Secure Protocols should be used, whenever the systems allow it.

The use of anonymization mechanisms for remote access to MEO Group, such as via TOR Networks, is not permitted. Since these types of mechanisms make it impossible to trace those who use MEO's Group resources.

All Users with administration privileges and non-restricted access profiles on the Corporate VPN must use 2FA to authenticate on the VPN.

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 5.15 Access control, 8.20 Networks security, 6.7 Remote working, 8.12 Data leakage prevention

6.4.6 Remote access through CITRIX

Remote access, from abroad, to corporate applications via the Citrix platform, must be properly analyzed, documented and authorized by management. These requests are supported by a procedure that guarantees the traceability of allocated access and the preservation of these records for a period of 2 years.

The use of anonymization mechanisms for remote access to MEO Group, such as via TOR Networks, is not permitted. Since these types of mechanisms make it impossible to trace those who use MEO's Group resources.

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 5.15 Access control, 8.20 Networks security, 6.7 Remote working, 8.12 Data leakage prevention

6.4.7 Extranet access

All requests for new connections to an extranet must be formalized in writing by the requesting entity with the team responsible for the extranet, including a justification of the underlying business requirement. This access must be reviewed and authorized to ensure that it is in accordance with business requirements and defined policies and that the principle of "access only to what is necessary" is complied with. Changes to an existing access are requested following the same process as a new request.

The provision of new connections between third parties and MEO Group must be formalized through a contract, which must comply with the terms of this Policy.

When extranet access is no longer necessary, the requesting entity must notify the responsible team to deactivate that access. This action may correspond to a modification of existing permissions or the complete deactivation of this connection.

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 5.15 Access control, 8.20 Networks security

6.5 Access Control to Operating Systems

6.5.1 Workstation configuration guidelines (ET/ TD)

The ET of all employees must have Antivirus, Anti-Spyware and Personal Firewall active and with automatic updates. The TD User must be prevented from changing the configuration of these programs. In the case of Virtual Workstations (VDi's), equivalent protection mechanisms must be implemented at the level of the virtualization platform and not necessarily at the level of each Virtual Desktop.

The screen saver must be configured so that, after five minutes of inactivity at the workstation, it is activated, protecting access by password.

When authenticating Users who wish to use a workstation, domain servers must validate and enforce the security configuration mentioned above. If the job does not meet any of the criteria, entry into the network must be refused.

Under no circumstances should Desktops or Notebooks be allowed to be connected to the internal network unless they have authorized User.

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 8.3 Information access restriction

6.5.2 Risk ET workstation configuration guidelines

Any ET must be installed in accordance with the security rules in force at MEO Group, including activations of Anti-Spam, Anti-Malware, Personal Firewall, active Screen-saver with password, XDR/EDR, DLP, etc., as well as automatic updates, with Users prohibited from changing the respective settings, except with prior authorization from the entity responsible for the application in question.

Risk ET is understood as those that are most exposed to threats and as such present a greater risk of use by unauthorized Users, such as MEO Group stores and call centers, which have more restricted access and usage privileges. . Any User who authenticates in one of these ETs will only have access to the functionality and applications defined for the profile of this workstation.

The screen saver must be configured to activate after two minutes of inactivity at the workstation, protecting access by password, in order to prevent unauthorized access due to the User's absence.

These risky Workstations must not have drives for removable media available, thus reducing the risk of unauthorized copies of information.

In the case of virtual workstations (VDIs) without any possibility of reading or writing data and programs from USB drives, CD/DVD or others, equivalent protection mechanisms can be implemented at the level of the virtualization platform and not at the level of each " Virtual Desktop".

Whenever these risk ETs are supported on Laptops/Notebooks, in principle, the data stored on their disk must be subject to an encryption process, and this principle must be applied to any other Mobile Device (e.g. Tablets, etc.) that have access to classified data from MEO Group.

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 5.15 Access control, 8.3 Information access restriction, 8.12 Data leakage prevention.

6.5.3 Access to servers and other information technologies

All servers, storage and backup systems and other critical information technologies for MEO Group must be under the responsibility of an operational group that ensures their administration, operability and security. Servers must always be located in an environment where there is strict physical access control, as well as adequate environmental conditions for the maintenance of equipment/systems, as well as ensuring availability in terms of redundant energy sources, according to the risk of the asset in question.

6.5.4 Network element accesses and network security

All routers, switches, firewalls, IDS's, IPS's and other network elements at MEO Group must be under the responsibility of operational groups that ensure their administration and security. These network elements must always be located in environments where there is physical access control, and suitable environmental conditions for their operation and maintenance, as well as ensuring availability in terms of redundant energy sources, in accordance with the risk of the asset. concerned.

6.5.5 Configuration guidelines

The configuration of operating systems must always be carried out taking into account the security standards issued by the respective suppliers and drawn up by the operational areas.

Access to services must be protected by access control mechanisms, for example Host Firewalls.

Security patches must be installed in accordance with current distribution policies, except when it is found that their immediate application interferes with a business requirement. Trust relationships between systems are a security risk and should be avoided. This solution can only be used if there is no alternative communication option.

Access privileges must be defined based on the principle that each User can only perform actions strictly necessary in their role.

Whenever a secure communication channel is available (if technically feasible), privileged access should only be carried out over these channels (e.g., encrypted connections using: HTTPS, SSH, SSL/TLS, SFTP, SCP, IPSec, etc.).

Administrators of servers and network assets are prohibited from:

a. Carry out actions that may damage, interrupt or generate errors in computer systems;
b. Carry out unauthorized uploads, downloads or transmission of any program or file subject to copyright, related rights or other intellectual property rights, namely music files, videos, etc., for non-professional purposes.

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 5.15 Access control, 8.3 Information access restriction, 7.8 Equipment siting and protection

6.5.6 Database passwords

Applications available on the MEO Group network that need to access one or more Database servers must authenticate themselves by presenting the necessary credentials. These credentials must not reside in the text body of the application code, nor be stored in a location accessible through a web server or the use of insecure protocols.

6.5.7 Storage of User Names and Passwords for accessing Databases

- User Names and Passwords for accessing Databases can be stored in a secure area in a file separate from the application code.
- If they are saved in a file, the User Names and Passwords for accessing Databases must be read before using them. Immediately following authentication in the Database, the memory containing the User Name and Password must be cleared or freed.
- Database credentials can reside on the server. In this case, a hash number that identifies the credentials may be included in the application code.
- Database credentials may reside on an authentication server, such as an LDAP server used for User authentication. Application authentication against the Database can occur as part of the User authentication process on the authentication server. In this case, there is no need to use credentials when programming the application.
- Database credentials cannot reside in the document tree of a web server.
- Authentication of Oracle Database Users should never use the Oracle mechanism that delegates this task to the client's operating system, also known as OPS$ authentication.
- For languages executable from code, the respective credentials must not reside in the same directory as the source code.
- Passwords used to access the Database must comply with the guidelines for creating Robust Passwords.

6.5.8 Database passwords

Each application that implements a business function must have unique Database credentials.

The teams responsible for Databases must have a defined process that ensures that Database passwords are controlled and also include a method to restrict knowledge only to those who need it. Sharing credentials across multiple applications is not permitted

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 8.3 Information access restriction

6.5.9 Application Access Passwords

Even in applications residing in secure zones within a Data Center, there must not be passwords directly written in the application code, in scripts or in tools and/or automation mechanisms. If there is no practical alternative, given the technological base in use (e.g. obsolete technologies), it must be ensured that the passwords reside in a properly protected and encrypted file and only accessible to the application or script that needs it.

Whenever applications store their Users' identifiers and their respective passwords, within a table in a database, they must do so in encrypted form, for both columns (login and password). The encryption key should not be stored within the database, and it is recommended to use an application configuration file with protected access.

When the "client" component of an application, running on a desktop/notebook, needs to directly access another secondary application, it must force the User to do so explicitly or use MEO's Group Single-Sign-On process.

New applications that deal with classified information must guarantee network authentication using cryptographically based Secure Protocols (e.g., HTTPS, SSH, SSL/TLS, or IPSec). .

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 8.3 Information access restriction

6.5.10 Access Monitoring

Operating systems, databases and applications must work with the access monitoring system active. At the minimum level of operation, this system must record inputs and outputs as well as access to classified data (Confidential, Reserved, customer data, business data or other types of data protected by legislation).

The most critical systems and technologies, all DMZs, all security devices, and all the most relevant systems and network elements, must be monitored in the MEO Group SOC.

Monitoring processes must be established that allow:

- Detect illegitimate entries or attempted entries into systems;
- Detect authentication failures;
- Detect practices that put the safeguarding of access control at risk;
- Detect attempts to increase assigned privileges;
- Ensure that there is sufficient evidence when an incident occurs;
- Define abnormal behavior models, which allow the detection of anomalous scenarios.

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 8.15 Logging

6.6 Standards for Application Development or acquisition of applications from third parties

Development teams and internal entities responsible for the acquisition and implementation of applications acquired from third parties must ensure that the solutions they develop, acquire/implement contain the following security precautions:

1. Applications must support the authentication of individual Users (namely identified) and not groups;
2. Applications must be able to authenticate and authorize all users and devices, including controlling access to systems and applications, namely Front-ends, and should be used whenever possible and for new systems:
    a. the use of TLS (Transport Layer Security), in its most recent version;
    b. the use of a password, preferably in combination with another factor (Two Factor Authentication -2FA), such as:
        - Password + SMS Token
        - Password + Smartcard
        - Password + Biometrics
        - Password + Graphic pattern

- Password + Coordinates card
- Password + Temporary random code (less than 5 minutes valid) sent in the form of QR -Code.

1. They must provide a level of profiles that allows the different business functions of Users to be supported, ensuring segregation of functions and thus guaranteeing the associated level of authorization.
2. They must provide some type of profile management, so that a User can assume the functions of another without having to know the colleague's password;
3. The development process must ensure that the entity responsible for development carries out security tests, in addition to functional tests. Additionally, applications exposed to the Internet or different extranets that deal with classified information must be periodically tested against security vulnerabilities (e.g., buffer overflows, sql injection, etc.) by an entity independent of the development;
4. System events and Event log events from systems, Databases, Applications, Network Assets, etc., must be stored in LOGs, digitally signed, in a secure and segregated environment from the environments where these events were generated. It is recommended to separate the teams that manage the environments where these events originate and the teams that manage the storage of LOGs. LOGs must record relevant events according to the CRUD principle (Create, Read, Update, Delete), as well as allow answers to the questions: Who did it?; When did you do it?; How did you do it?; Where did it come from?; What did you do?; Why did he do it? This principle must be used, by default, in any type of LOG.
5. Applications that deal with classified information must guarantee an audit trail that complies with the CRUD principle, in particular changes to that classified information indicating, at a minimum:
    - Operation carried out (only mandatory for information classified above Confidential);
    - Change made (old value, new value);
    - Status of the operation (e.g., success or failure);
    - Operation timestamp;
    - Who performed the operation (user-id);
    - Source IP/Port.
8. This information must be available for a minimum period to be defined for each of the applications, and the maximum period for which it will be kept must also be defined, depending on the purpose and need for collecting this information, in order to guarantee compliance with the data protection laws, particularly regarding the deletion of information containing personal data. Log retention periods may also vary depending on what is contracted with each client or for each service;
9. Must support TACACS+, RADIUS, LDAP, Single Sign On or similar whenever possible;
10. It must ensure that personal data from a productive environment is not used in a non-productive environment, and if necessary, they must be subject to a masking process, not allowing the unequivocal identification of the holder of the personal data directly or indirect, equivalent to anonymization
11. Separation between environments, namely Development, Testing and Production, must be guaranteed and that the source code is not available in Production environments.
12. Non-productive environments must have patches and antiviruses updated as is the case in productive environments.

    Access to non-productive environments must comply with the requirements of this Policy in terms of access, namely in the component of nominal accounts for access to Systems, Databases, Service Platforms, Systems Network Equipment and Information Technologies and Communication.

In the case of Laboratory and Development environments for Operational Support Systems (OSS) in telecommunications areas, the following requirements must be guaranteed:

· Adequate separation, ideally at HW level, between development/laboratory and production environments;
· Adequate separation between the laboratory network and the corporate network;
· Adequate isolation (e.g. through VDI) between access devices to laboratory environments, production environments and the corporate network/external networks.

If the above conditions are met, development/testing suppliers/subcontractors may use desktop sharing applications for debugging in the laboratory and development environment.

The Departments responsible for implementing new projects, which may result in new applications or new Information and Communication Systems and Technologies, are responsible for ensuring compliance with this Policy.

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 8.3 Information access restriction, 8.26 Application security requirements, 8.10 Information deletion

7 Additional provisions in systems, database and application management and administration

7.1 Secure zone guarantee (secure perimeters)

All relevant systems and applications must be, whenever possible, in secure perimeters, both physically and logically. Only application front-ends should be exposed in a DMZ.

In terms of physical security, for a perimeter to be considered secure, it must be fully protected within an MEO Group Data Center and physical access to it must involve the identification, authorization, control and monitoring of whoever intends to access it. Access.

The places where the infrastructures are located must have mechanisms that allow events to be generated relating to physical access made or attempted.

At the level of logical security, for a perimeter to be considered secure, it will have to ensure that all network access to any of the systems or technologies within or on that perimeter are previously known, monitored and controlled by operational security systems (Firewalls and IDS's/IPS's) and duly integrated into MEO's Group SOC. Additionally, a perimeter will only be considered secure if all systems and network elements contained therein are secure in accordance with the best information security practices and there is no trust relationship between a system within the secure perimeter and another system outside that perimeter. perimeter. A secure perimeter requires that your administration, when remote, uses Secure Protocols and secure consoles.

The entity responsible for this Information Security Policy must, whenever it deems necessary, carry out assessments of the logical and physical security of MEO's Group secure perimeters.

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 8.3 Information access restriction, 8.22 Segregation of networks.

7.2 Hardening of Systems, Databases, Applications and Network Elements

It must be ensured that the greatest number of possible security risks are eliminated in all systems, databases, applications and network elements, disabling accounts, services, interfaces (including IP ports) that are unnecessary for their final function.

In particular, Web application front-ends exposed on the internet/extranet must be subject to security hardening, in accordance with internal regulations that follow best international practices, e.g., NIST (www.nist.org), SANS (www.sans. org) or CIS (https://www.cisecurity.org/). Systems that no longer have operational functions, because they have been replaced by more current systems, or for any other reason, must not remain accessible on MEO's Group internal networks. Until they are definitively disconnected or reused for other functions, they must remain under the control of the operational security of the respective Data Center or ANG type technical rooms (New Generation Areas).

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems – Requirements, controls, 8.7 Protection against malware.

7.3 Access to Command Execution

Only technicians who are nominally identified and subject to the signature of a Confidentiality Declaration or to confidentiality rules within the scope of the employment relationship with MEO Group.

For UNIX/Linux family systems, remote root access should not be performed directly.

In Windows family systems, direct access with Administrator privileges must be guaranteed through updated PowerShell and configured with best practices, namely complying with the principle of minimum privilege necessary for the action to be performed, and whenever possible via JumpBoxes.

Access should always be done as a nominal user and then elevate privileges to root, ensuring that there are audit logs of the process.

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 8.3 Information access restriction.

7.4 Patch Application

Those responsible for each system must ensure that all patches released by the manufacturer, especially security-related patches, are properly installed on the system, with the exception of causing an impact on the proper functioning of the systems.

These updates must be formally planned, associated risks must be identified and test plans and fall-back procedures must be defined, in accordance with the internal procedure of the team responsible for IT.

Patches include all those applicable to Endpoints, Servers, Databases, Service Platforms and Networking, in the Operating System and Application components, and the detail of their applicability must be defined in specific standards of those who guarantee the Operation, Maintenance and Management, upon opinion from the Cybersecurity Department.

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 8.7 Protection against malware, 8.32 Change management, 8.8 Management of technical vulnerabilities.

7.5 Discontinuation of Systems and Network Elements

The discontinuation of Systems and Network Elements is defined in MEO's Group specific procedures.

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems – Requirements, controls, 5.9 Inventory of information and other assisted assets, 5.11 Return of assets, 5.23 Information security for use of cloud services, 8.20 Networks security, 8.21 Security of network services.

8 Exceptions and comments to the Information Security Policy

For any of the provisions defined above, the exception management procedure may be used to justify activities that do not comply with the provisions of this Policy.

There may be cases of exceptions, which due to business requirements or because there are compensatory controls are previously approved. These situations are detailed in the Exception Management Procedure. In relation to any situation related to the Information Security Policy that is not covered by it, a binding opinion may be requested from the Cybersecurity Department.

Whenever justified, specific policies may be defined, which cannot derogate from any of the guidelines defined in this Policy. Their approval is carried out by the Cybersecurity Department.

8.1 New or existing systems and technologies not included in the Internal Control Manual

For new systems and Technologies or for existing ones not included in the Internal Control Manual, it is the responsibility of the team responsible for that system or technology to identify the exception, which must be documented and registered in the CMDB or elsewhere. equivalent. Whenever a technological renewal action does not lead to compliance with this Policy, the identification of this system as a documented exception must be maintained, ensuring that no change may lead to a situation of increased security risk compared to the situation previously in production.

8.2 Existing Systems and Technologies Included in the Internal Control Manual

For existing Systems and Technologies included in the Internal Control Manual, in which there are situations in which the Security Policy is not applicable for technical and functional reasons, exceptions must be documented and subject to the opinion of the entity responsible for this Policy, accompanied by a proposal for measures that can mitigate the risks in question.

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 5.2 Information security roles and responsabulities.

9 Security Incident Reporting

Whenever an anomalous situation is identified that may be related to the logical security of MEO's Group IT, IS and NETWORK, it must be immediately reported to MEO's Group SOC/CSIRT (Computer Security Incident Response Team) through the following contact points:

- Onedesk (Workplace/Cybersecurity channel);
- Email: csirt@meo.pt
- In case of phishing, the email may also be used: phishing@meo.pt

The CSIRT team must handle incidents in a way that minimizes their impact on the organization, ensuring information security.

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems – Requirements, controls, 6.8 Information security event reporting.

10 Cybersecurity Risk Management

10.1 Organizational Risk Management

The Organization has established a Risk Identification and Assessment methodology to identify and respond to risks to the security of network and information systems. Risk assessments are conducted and documented, and corresponding risk treatment plans are implemented. The risk assessment results and residual risks are approved by Senior Management or, where applicable, by those responsible and authorized to manage risks.

10.2 Supply Chain Risk Management

The organization has established a Purchasing Policy, which recognizes the importance of the supply chain as a key component in achieving its business strategy. This Policy applies internally to all employees directly or indirectly involved in supplier procurement activities within Group companies, and externally to all suppliers and their employees, as well as to companies they may subcontract.

As part of monitoring and follow-up, the organization reserves the right to assess suppliers' compliance with accepted principles through verification activities, such as self-assessment audits or visits to the locations where the activities are carried out.

The evaluation criteria considered may cover topics such as proactivity and innovation, compliance with agreed deadlines, service quality, response times and quality to requests, compliance with information security requirements, environmental, social, and governance (ESG) criteria, compliance with ethical and conduct standards, among others deemed relevant.

11 Information Security Guidelines applicable to the use of Artificial Intelligence

The organization complies with current legal and regulatory requirements. The use of duly authorized artificial intelligence is permitted. Otherwise, Section 8 (Exceptions and Opinions to the Information Security Policy) of the MEO Group Information Security Policy applies.

12 Review of the Information Security Policy

The Information Security Policy is reviewed annually whenever significant incidents or significant changes in operations or risks occur, resulting from changes in applicable legislation and regulations, the MEO Group's business strategy, and its risk profile.

Changes to this policy are approved by the MEO Group's Senior Management, and the new version is published and disseminated to all employees and third parties involved in the MEO Group's activities.

ISO / IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection -Information Security Management Systems – Requirements, controls, 5.1 Policies for information security

This Policy was approved at the Executive Committee meeting on 10/03/2025, in accordance with Service Order 3/2025.

13 Glossary

A

Access Control – System that restricts the activities of Users and processes based on what is strictly necessary to know/do. It allows implementing function segregation.

API - Application Programming Interface Asset - all Configuration Items necessary for the provision of contracted services, namely servers, routers, firewalls, switches, databases, Operating Systems, etc.

Audit Trail – Logfile that in a chronological manner records the sequence of auditable events, containing evidence of the execution of transactions or system functions. It shall contain information relating to: "Who did?", "When was it done?", "How was it done?", "Where was it done?", "What was done?", "Why was it done?", saving the previous and new parameter/values.

Active - all Configuration Items required to provide contracted services, namely servers, routers, firewalls, switches, databases, Operating Systems, etc.

B

BSS – Business Support Systems.

C

Critical System – For the purposes of this Policy, systems are considered critical systems where unauthorized access, or the execution of an unauthorized operation, may result in a negative financial impact on the organization.

Cyber Hygiene - Cyber hygiene concerns basic preventive security precautions in cyberspace. A good cyber hygiene reduces the chance of success of cyber-attacks. It typically Involves the following vectors of good technical practices: 1) continuous elimination of known security vulnerabilities in different assets (e.g. via upgrades, security hardening, patching, updating digital certificates, closing unduly open IP ports, anti-virus updates, ...), 2) rapid correction of compromised systems (e.g. by malware) and elimination of their primary causes, 3) strict management of accesses with administration privileges and risk accesses to the Internet, and finally 4) management of inventories (e.g. CMDB) and authorized software.

CMDB – Configuration Management Database

Chain letters - Message sent to several people, requesting of each one to forward copies to their contacts and friends, and it may in certain situations refer to a threat that something ominous might happen if the message is not forwarded.

D

Data – Representation of a fact, measurement, concept, or idea using letters, numbers, special characters, images or sounds, stored on a computer allowing its subsequent consultation, transmission or processing using its means.

Database – Set of data logically linked to each other, supported on a medium that allows storage of large amounts of data and managed by a specialized program called Database Management System. This software takes care of storing and searching the data, ensures independence between the storage structure and other programs using the data, ensures its security of access as well as redundancy and fault tolerance of the query software.

Data Center or technical rooms of the NGA type (New Generation Areas) – Location with environmental and technical conditions, including physical and logical security, suitable for equipment/systems accommodation, with a rigorous control of physical and logical accesses.

Default Password or Factory Default Password – Initial password assigned when a new User is created, or an initial password made available by a hardware/software vendor.

Development Station (TD) – Personal Computer, fixed and or portable, and respective software, provided by MEO to a restricted group of Users, for professional use at MEO, with privileges of local administration
of the device.

DMZ (Demilitarized Zone) – It is a physical or logical security perimeter used to place frontends of the company's services that are intended to be exposed to a larger and less trustworthy target public, usually on the Internet.

DoS (Denial of Service) and DDoS (Distributed Denial of Service) – Type of attack on an information system or network with the intention of causing the service to be unavailable to other Users, usually through the loss of connectivity and services by aggressive consumption of the bandwidth of the attacked network or overload of the resources of the attacked systems. It is designated DDoS when the attack involves multiple systems distributed on the Internet.

E

Encryption – Process that involves data coding in order to ensure confidentiality, authenticity, anonymity, time-stamping (recording of time of creation and modification of a document) and other security objectives.

F

File Share (Public, Private) – disk spaces, for file sharing for a restricted number of Users (Private), or for the entire network they are in (Public).

Firewall – A logical barrier that aims whose goal is to prevent Users or processes from accessing beyond a certain point on the network, without having previously passed a security validation (example, providing a password).

FTP – File Transfer Protocol

H

http/https – World Wide Web communication protocols, with https being the securest and most recommended version for web/Intranet applications involving classified or sensitive information.

I

IDS – Intrusion Detection System

IPS – Intrusion Prevention System

L

Load balancer – Techniques and/or solutions that allow distributing workload for the resources concerned. Resources can be categorized as follows: Storage, Network or CPU.

M

Malware – It includes all kind of malicious software (viruses, spyware, worms, ...) designed to infiltrate in the computer, taking advantage of security vulnerabilities, without the User's consent, and which usually has illicit
and harmful goals.

N

NDA – Non-Disclosure Agreement Networking – Series of dots or nodes (computers, network assets, printers, etc.) interconnected by a communication medium (copper, optical cable, etc.)

Networking – Series of dots or nodes (computers, network assets, printers, etc.)

Network TAPs – Hardware Device that enables access to data passing through the communication network between computers.

O

OSS – Operational Support Systems

P

Personal Data – Information concerning an identified or identifiable individual (data subject). An identifiable individual is the person who can be identified, directly or indirectly, by reference to an identifier, such as a name, an identification number, location data, electronic identifiers or to one or more specific elements of their physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (RGPD, art. 4, paragraph 1).

R

Remote Shell – Software that allows to remotely access another computer. The use of remote shells will take place in the strict terms and requirements of this.

RFI – Request for Information

RFP – Request for Proposal – Market Consultation to obtain a technical and commercial proposal concerning a particular product/service.

Router – Performs routing of network traffic. Core Routers are those located in the network backbone i.e. neuralgic centers of the network.

S

Sensitive personal data – are those that are subject to special processing conditions, namely racial or ethnic origin, religious conviction, political opinion, membership of a trade union or organization of a religious, philosophical or political nature, data relating to health or sexual life, genetic or biometric data, when linked to an individual.

SCP – Secure Copy Protocol

Service Platform – technical platforms that allow making available functionalities associated with parameterization of any type of services in the networks – copper, fiber, etc. (create/activate/deactivate, session control, protocols, etc.).

SFTP – Secure File Transfer Protocol

SMTP – Simple Mail Transport Protocol

SNMP – Simple Network Management Protocol

SpyWare and SpyWare Bots – Software infiltrated on a computer that collects information from an organization or person without their knowledge and transmits it from another computer, usually on the Internet. A SpyWare Bot is a more sophisticated SpyWare controlled by remote computers on the Internet (Bot Controllers).

Spam – Unsolicited email sent, primarily with advertising objectives, in large quantities to individuals, lists, groups, etc.

SSH – Secure Shell

Strong Authentication – Also called T-FA (Twofactor authentication), it is an authentication protocol that requires two forms of authentication to access a system, where the first form of authentication corresponds to something the User knows (e.g. a PIN or a password) and the second form corresponds to something the User has (e.g. magnetic card or fingerprint)

T

TLS - Transport Layer Security

Tunneling – Technology that allows encapsulating packets from one protocol into packets from another protocol. There are tunnels to establish securer communications when the involving protocol allows encryption. There are also tunnels designed to conceal communications with prohibited protocols in an organization encapsulating them into common protocols such as https. This last use is strictly prohibited at MEO.

V

VDI (Virtual Desktop Infrastructure) – Workstation based on a screen, keyboard, and mouse but whose processing is delivered to a virtual machine that runs centrally on a server in a Data Center environment.

Virus – Program that replicates, copying itself to the code of another program, computer startup system or document, and that usually pursues illicit and harmful goals.

W

Wireless network – A wireless network is a computer network that does not require cable connections – whether they are telephony, coaxial or optical cables – using equipment that uses radio frequency (communication via radio waves) or infrared communication, such as on IrDA compliant devices.

Workstation WS (ET) – Personal Computer, virtual (VDI), fixed and/ or portable, and respective software, made available by MEO to most Users, for professional use at MEO, without any privileges of local administration of the device.

14 Annex I – ISMS Objectives

MEO defined the following strategy that was presented and shared with the entire organization:

- Focuses on three axes: investment, Inovation, Service Quality.
- Based on: Proximity, Social Intervention with our internal and external stakeholders.
- Materializes into five strategic pillars: Service Quality, Inovation, People, Brand, Sustainability.

The strategy is reflected in objectives mapped out for the Information Security Management System (ISMS) to ensure management focused on results and continuous improvement, ensuring Quality of Service.

The Information Security Policy also applies to the Service management System (ISO2000), considering the service requirements.