INFORMATION SECURITY POLICY

Document code:	POL-14
Version:	2.1
Effective date:	03/02/2023
Type of security:	Public information

Author	Revised	Approved
Idoia Uriarte	Miguel Santos	Board
CISO	CTO	of Directors

INDEX

1. OBJECT

The information, services, and systems managed by MASMOVIL Group (hereinafter, the "Group") are a fundamental asset that constitutes a strategic and necessary element for its activities, and as such its managers and employees are responsible for their protection and safeguarding. For this reason, this Information Security Policy is based on the recommendations of the International Standard ISO/IEC 27001, and the good practices established by the UNE-ISO/IEC 27002 standard, as well as the principles and requirements of the Spanish National Security Framework (ENS) compliance with current legislation on personal data protection, network and IT system security, the information society, electronic commerce, cybersecurity, and telecommunications in order to maintain the security and integrity of information, establishing, at each point, appropriate controls and measures to protect it from unauthorized access or dissemination, modification, destruction, or unavailability for accidental or intentional reasons.

The purpose of this Policy is to define the general principles for regulating and guaranteeing the security of the information generated, processed and stored by the Group, as well as the systems and applications that support it, including the telecommunications network that supports the services provided to the Group's customers.

Similarly, the aim is to implement a set of actions aimed at preserving the confidentiality, integrity, availability, authenticity and traceability of information, which are the three general components of information security.

2. SCOPE

This Policy is binding on all areas, departments and teams of the Group, both in their internal relations and with third parties. It applies to all our activities, services and systems.

All users of the Group's IT resources and/or Information Systems must have permanent access to this Policy during the time they are performing their duties.

3. IMPLEMENTATION

3.1. Principles of the information security policy

This Policy and its implementation must be communicated to all Group personnel, both to the Group's own staff and those of collaborating entities and must be made available to stakeholders.

Information security is the responsibility of all Group personnel. This principle must be known, understood and taken on board by all levels of the organization.

In the course of its activities, the Group will apply preventive action criteria, both to existing assets and to the changes made to them:

- Risk prevention planning.
- Risk identification and assessment.
- Managing identified risks.
- Designing mitigation plans for identified risks.
- Monitoring and evaluating the effectiveness of risk mitigation plans, seeking continuous improvement and to minimize corporate risks at all times.

3.2. Information security organization

Cybersecurity will drive the development and implementation of information security in the Group.

A security structure will be established to:

- Ensure the implementation of controls appropriate to the type of information handled.
- Engage the cooperation and support of collaborators.
- Verify the effectiveness of this standard and those approved to develop it.

The assignment and delimitation of responsibilities to ensure that the objectives proposed in this policy are implemented and met requires the establishment of certain roles responsible for general aspects of information security management. To this end, the Group has established and documented roles and responsibilities for information security.

The security of the information must be maintained against access by third parties. Controls should be agreed and defined in a third party access contract in conjunction with the Cybersecurity department. If these third parties also have access to personal data, a Data Processor contract must be signed, in accordance with the models defined by the Data Protection Officer.

Information security shall be ensured and maintained when responsibility for information processing is entrusted to another organization.

3.3. Classification and control of information for security purposes

The objective is to protect information in a proportionate manner, ensuring its confidentiality, integrity, availability, authenticity and traceability throughout its life cycle according to its level of criticality:

- Confidentiality: attribute that prevents unauthorized disclosure or access to information.
- Integrity: attribute that ensures that the information is complete vis-à-vis alteration, loss, or destruction, whether accidental or fraudulent, and that it has not been modified or undergone variations in its processing.
- Availability: attribute referring to the authorized access and use of the information in the place, manner and time determined.
- Authenticity: attribute that an entity is who it claims to be or that guarantees the source from which the data comes from.
- Traceability: attribute that the actions of an entity can be attributed exclusively to that entity.

The information will be classified by its owner taking into consideration the following criteria:

Classification level	Persons auth.	General description
Secret	1 / 2	Critical or highly sensitive information, intended for very specific people in the organization. This information, if compromised, could cause serious or very serious damage to the Group, resulting in an abrupt loss of business or severe penalties. Access to this information is very limited and is only granted to named persons. The person responsible for this information must guarantee extraordinary security measures to help protect its confidentiality within the organization, completely preventing access to it or distribution to the outside world.
Restricted	n < 30	Confidential information of high value or sensitivity, intended for a very limited and controlled group of people. This information, if compromised, could be highly detrimental to the interests of the Group, its customers or the third parties with which it collaborates, resulting in the loss of competitive advantages, increased direct fraud, strong direct impact on the income statement, etc. Access to this information is restricted to certain persons within the organization and must be controlled and expressly authorized by the person responsible for the information. The person responsible for the information shall ensure adequate security measures to help protect its confidentiality both outside and inside the organization, limiting its access and distribution to a controlled group of persons, on a strict need-to-know basis.

Confidential	Limited group	Information intended for a limited and controlled group of people. This is information that could be detrimental to the interests of the Group, its customers or the third parties with which it collaborates, if compromised. Access to this information is limited to certain persons within the organization and must be controlled by the person responsible for the information. The person responsible for the information shall ensure adequate security measures to help protect its confidentiality both outside and inside the organization, limiting its access and distribution to a controlled group of persons, on a strict need-to-know basis.
Internal	MM Group	Information intended solely for use within the organization, either by the internal personnel of MASMOVIL Group or by third parties to be determined, without prejudice to its confidential nature, who are authorized to access it for a limited time and under the supervision of the person responsible for the information. In general, this is information that if compromised would not cause significant disruption or reputational damage to the Group or external stakeholders. It requires security measures that limit access by persons outside the Group who do not require such information to meet the objectives of their collaboration with the Group. This will be the default classification for previously unclassified Group information.
Public	∞	Information open internally to all MASMOVIL Group personnel and externally to the general public. In general, this is information that might or might not specifically concern the Group, might be disclosed or published through official channels, and does not require access limitations. It does not require specific security measures, since the information is intended for publication and/or disclosure without restrictions or limitations on access.

The security measures to be applied in processing the information will be directly related to its classification levels according to the rules and procedures on information management that define and classify it.

3.4. Security linked to Group staff

All employees and external users with access to classified information must sign a confidentiality and non-disclosure agreement.

All employees and collaborators of the Group shall receive appropriate information security training and awareness training, through which they are made aware of their security responsibilities. Likewise, users will be kept abreast of existing information security threats so that they are trained to support the Organization's security policy in the course of their normal duties.

Incidents affecting information security should be reported as quickly as possible through the established channels and procedures. Employees and third parties that may be involved should be informed of the procedures for reporting different types of security incidents, as well as the procedures to be followed in the event that the incident involves personal data.

In the event that any user (internal, external, supplier, etc., providing any type of service to the Group) engages in conduct contrary to that described in this Policy or in its internal implementation regulations, such conduct must be reported to the whistleblower channel through the channels established in the *Compliance Officer and whistleblower channel charter*.

3.5. Physical security

Physical spaces where classified information or information containing personal data is processed or stored must be adequately protected by means of defined security perimeters and appropriate access controls. The protection provided must always be proportional to the risk.

Security measures shall ensure the protection of information against loss, theft, access, disclosure, copying, and unauthorized distribution. Employees must be aware of the need to protect the confidentiality of information. The measures adopted must be such that, while maintaining the availability of the information, they prevent unauthorized access.

3.6. Security in communications and in the use of information

Routine procedures should be established to ensure the integrity and availability of processing, storage, and communications services, carrying out the defined backup strategy, backing up data and testing its timely restoration.

The necessary procedures must be established and the necessary solutions implemented to guarantee the confidentiality of corporate information, considering the requirements of the classification levels existing in the Organization, as well as the necessary measures established for each one.

The security of the telematic networks and the protection of the supporting infrastructure must be guaranteed. It is of the utmost importance to manage security on networks and infrastructures located outside the organization's perimeter, especially in the case of shared resource infrastructures, such as cloud solutions. It shall be ensured that sufficient controls are applied by network, infrastructure, and cloud service providers to the information that is transmitted and/or hosted by them. Activities must be closely coordinated to ensure that controls are applied uniformly across the organization's data processing infrastructure,

whether this is within the corporate perimeter or provided by third parties through cloud solutions.

The security of information must be guaranteed both when communicating it and storing it using personal devices not belonging to the Group, in cases where this is permitted at all.

Sufficient controls must be implemented to ensure the security of information when any work device (laptop, cellphone, or similar), whether personal or corporate, processes Group information through external networks not controlled by the Group. Specific rules must be established for the specific use of these devices, setting out the security measures that these devices must implement in order to meet the Group's security objectives.

Exchanges of information and software between organizations should be controlled, so that they are consistent with applicable legislation and existing agreements. Procedures and standards must be established to protect information and assets both at rest and in transit, considering principally the need to reduce the security risks posed by the flow of information outside the Group's perimeter or systems.

Adequate mechanisms shall be in place to control vulnerabilities and malware.

3.7. Access control

In systems where this is possible and required by the business, access controls based on segregation of duties should be established, applying the principle of least privilege specifically for necessary functions, and avoiding as far as possible the use of user accounts with excessive or unnecessary privileges. Access administration and maintenance should be performed in cases of changes or modifications to the functions.

Unauthorized access to information systems and assets shall be prevented by implementing appropriate controls for managing user access rights.

Access to the Group's services or systems, either internal and external, must be controlled, ensuring the implementation of adequate interfaces with public networks, robust authentication mechanisms, and appropriate access controls.

Monitoring systems will be established to check the effectiveness of the controls in place and to detect deviations from internal access control regulations.

Information security should be ensured in the use of mobile devices and remote work facilities. The protection required shall be proportional to the risk involved in the type of work.

3.8. Application development, acquisition and maintenance

Guidelines will be developed to ensure that security is incorporated into the design, development, acquisition, maintenance, and commissioning of new projects to prevent loss, modification or unauthorized use of information.

Security requirements should be identified and approved by the Cybersecurity department at the information systems design stage.

For setting security requirements, the business needs, the state of the art, application costs, the nature, scope, context, and purposes of the information processing, as well as the requirements of the legislation in force will all be taken into account, as driven by the applicability of the same to each project.

A security and risk analysis should be developed for each new project and for substantial modifications to the same, to identify the threats and risks they are exposed to, so that it is possible to decide whether to deal with them or assume them.

3.9. Business continuity

The continuity of the organization's critical activities will be ensured through the implementation of guidelines and preventive and corrective controls by the Business Continuity department in order to protect critical business processes from the effects of significant failures or disasters.

The contingency plan for automated information should be developed and implemented to ensure that critical business processes can be restored in a timely manner, including controls to identify and reduce risks, limit the consequences of adverse incidents, and ensure the response time of essential operations.

3.10. Processing of personal data

Any processing of personal data must be founded upon a legitimate basis. The most important points to take into account are:

- Consent.
- Contractual relationship.
- Vital interests of the data subject or other persons.
- Legal obligation upon the data controller.
- Public interest or exercise of public powers.
- Overriding legitimate interests of the data controller or third parties to whom the data are communicated.

The processing of personal data is under special regulatory protection, so measures and controls must be applied to ensure its security and compliance with current regulations.

Any processing of personal data by third parties must be reviewed by the Data Protection Officer and a data processor contract signed in accordance with the established models.

3.11. Information security planning

Each year, security objectives will be set based on the business needs or on identifying the risks detected.

The security objectives set and projects defined will also take into account the results of the risk assessment conducted.

3.12. Risk management

Preventive action criteria should be applied to information assets in conjunction with the Cybersecurity department, by identifying existing risks and assessing their impact, to establish the appropriate security measures, in order to combat risks at their source following the Risk Management procedure.

The effectiveness of the security controls and measures implemented should be verified through continuous monitoring and audits.

3.13. Information security control and audits

In order to control and evaluate compliance with legal requirements and internal procedures, the necessary internal and external supervision and audits shall be carried out with the periodicity established, respecting in all cases the legally established criteria.

The results obtained will be taken into account in the review and evaluation that Information Security must periodically conduct of the implementation of this Policy.

4. RESPONSIBILITIES

- It is the responsibility of all MASMOVIL Group staff to ensure that they have access, know and apply the current versions of the Information Security Policy.
- Those responsible for the preparation of the documents are responsible for communicating the availability of such documentation in the organization and reviewing its content at least annually.

5. VERSION LOG

Current version	*3.0*		
Change history	**Date**	**Version**	
	02/05/2020	*1.0*	*Creating the document*
	09/29/2022	*2.0*	*Unification of Group Policies and update*
	02/03/2023	*3.0*	*Adaption of ENS requeriments*