Security policy

Security Policy

Index of Contents

1 . Intro

This document sets out the Information Security Policy of MHP TIME MANAGEMENT SERVICE (MHP), as the set of basic principles and lines of action to which the Organization is committed, within the framework of the ISO 27001 Standard and the National Scheme of Security (ENS).

Information is a critical, essential asset of great value for the development of the company's activity. This asset must be adequately protected, through the necessary security measures, against threats that may affect it, regardless of the formats, supports, transmission media, systems, or people who intervene in its knowledge, processing, or treatment.

Information Security is the protection of this asset, to ensure the quality of the information and the continuity of the business, minimize risk, and allow to maximize the return on investments and business opportunities.

Information security is a process that requires technical and human resources and adequate management and definition of procedures, in which the maximum collaboration and involvement of all company personnel is essential.

The management of the company, aware of the value of the information, is deeply committed to the policy described in this document.

2 . Definitions

- **Information System**: organized set of resources so that information can be collected, stored, processed or treated, maintained, used, shared, distributed, made available, presented or transmitted.

- **Risk**: estimate of the degree of exposure to which a threat materializes on one or more assets causing damage or harm to the organization.

- **Risk management**: coordinated activities to direct and control an organization with respect to risks.

- **Information Security Management System (ISMS):** management system that, based on the study of risks, is established to create, implement, operate, supervise, review, maintain and improve information security. The management system includes the organizational structure, policies, planning activities, responsibilities, practices, procedures, processes, and resources.

- **Integrity:** System information must be available as stored by an authorized agent.

- **Authenticity:** (relative to the ENS). The identity and origin of the information must be ensured.

3 . Goal

The goal of this Information Security Policy is to protect MHP's information assets, ensuring the availability, integrity, confidentiality, authenticity, and traceability of the information and of the facilities, systems, and resources that process, manage, and process it. transmit and store, always in accordance with business requirements and current legislation.

4 . Scope

The Security Management System specified in this Manual in a manner consistent with the international standard UNE-ISO/IEC 27001: 2017 and the National Security Scheme has the following scope, however, it may be, it is also reflected in the Analysis of the Context of the ISMS Organization 02:

"The information systems that support the following services managed by the entity MHP Time Management Service, with the address located at Avenida Alcalde Ramírez Bethencourt, Nr. 12, Fuentemar Office Center, CP 35004, Las Palmas of Gran Canaria: time and attendance systems through different devices, clocking platform, hr consulting and customer service."

This Information Security Policy is applicable to all people, systems and means that access, treat, store, transmit or use the information known, managed or owned by the company for the processes described.

The personnel subject to this policy includes all persons with access to the information described, regardless of the automated support or not in which it is found and whether the individual is an employee of the company or not. Therefore, it also applies to contractors, clients, or any other third party who has access to company information or systems.

To ensure that the security process implemented will be updated and improved continuously, an Information Security Management System is implemented and documented. In this way, the content of the Information Security Policy is developed in complementary security standards and procedures.

5 . Goals and reason for the policy

The information must be protected throughout its life cycle, from its creation or reception, during its processing, communication, transport, storage, dissemination, and until its eventual erasure or destruction. Therefore, the following minimum principles are established:

- **Principle of confidentiality**: information systems must be accessible only to those users, bodies and entities or processes expressly authorized to do so, with respect to the obligations of secrecy and professional secrecy.

- **Principle of integrity and quality:** the maintenance of the integrity and quality of the information must be guaranteed, as well as the processes of treatment thereof, establishing the mechanisms to ensure that the processes of creation, treatment, storage and distribution of information they help to preserve its accuracy and correctness.

- **Principle of availability and continuity:** a level of availability will be guaranteed in the information systems and the necessary plans and measures will be provided to ensure the continuity of services and recovery from possible serious contingencies.

- **Risk management principle**: a continuous process of risk analysis and treatment must be articulated as a basic mechanism on which the management of information systems security must rest.

- **Principle of proportionality in cost:** the implementation of measures that mitigate the security risks of the information systems must be done under a proportional approach in the economic and operational costs, without prejudice to ensuring that the necessary resources for the management system information security are available.

- **Principle of awareness and training**: initiatives will be articulated that allow users to know their duties and obligations regarding the secure treatment of information. Likewise, specific training in ICT security will be promoted for all those who manage and administer information and telecommunications systems.

- **Prevention principle:** specific plans and lines of work will be developed aimed at preventing fraud, non-compliance or incidents related to ICT security.

- **Detection and response principle**: the services must continuously monitor the operation to detect anomalies in the levels of service provision and act accordingly, responding effectively, through the mechanisms established for this purpose, to security incidents.

- **Principle of continuous improvement**: the degree of compliance with the security improvement objectives planned annually and the degree of effectiveness of the ICT security controls implemented will be reviewed, in order to adapt them to the constant evolution of risks and the technological environment of the Public Administration.

- **ICT security principle in the life cycle of information systems:** security specifications will be included in all phases of the life cycle of services and systems, accompanied by the corresponding control procedures.

- **Principle of differentiated function:** the responsibility for the security of the information systems will be differentiated from the responsibility for the provision of services

The Information Security Policy is approved by the Company's Management, and it's content of the rules, and procedures that develop it is mandatory:

- All users with access to the information processed, managed or owned by the company have the obligation and duty to safeguard and protect it.

- The Information Security Policy and Standards will be adapted to the evolution of systems and technology and to organizational changes and will be aligned with current legislation and with the standards and best practices of ISO / IEC 27001: 2014 and of the National Security Scheme.

- The security measures and the applicable physical, administrative and technical controls will be detailed in the Applicability Document and the company must establish a planning for their implementation and management.

- The security measures and controls established will be proportional to the criticality of the information to be protected and its classification.

- Users who fail to comply with the Information Security Policy or the complementary rules and procedures may be sanctioned in accordance with the provisions of the contracts that protect their relationship with the company and with current and applicable legislation.

6 . Safety Requirements

This security policy will be developed applying the following requirements:

6.1 Organization and implementation of the security process

Information security compromises all members of the organization. MHP identifies those responsible and establishes their responsibilities for this purpose in the “Roles, responsibilities, and duties” section of this document. The security policy and regulations will be known to all members of the organization.

6.2 Analysis and risk management

Knowing the risks and developing a strategy to manage them properly is essential for the company, since only if the security status is known can the appropriate decisions be made to mitigate the risks it faces.

MHP uses the Magerit methodology to analyze risks, carrying out a detailed analysis of the risks that affect the assets included in an asset inventory, which is documented in a Risk Analysis document.

The entity determines the risk levels from which it takes treatment actions on them. A Risk is considered acceptable when implementing more security controls is estimated to consume more resources than the possible associated impact.

Once the risk assessment process has been carried out, the company's management is responsible for approving the residual risks and the risk treatment plans.

6.3 Personnel management

TAll MHP personnel related to information and systems are trained and informed of their duties and obligations in terms of security, essentially through the appropriate security procedures in each case and through the regulations on the use of assets.

Their actions are supervised according to the established roles to verify that the defined procedures are followed.

The accesses of the users are unique and their rights and the activities that have to do with the security of the information are periodically verified to correct or demand responsibilities in their case.

6.4 Professionalism, Awareness, and Training

The security of the systems is managed and reviewed by qualified MHP personnel and specialized external personnel, who receive and update the necessary training to guarantee the security of the information.

This Information Security Policy must be known by all internal and external users and by companies that access, manage or process company data.

The set of Policies, rules and procedures complementary to this Information Security Policy must also be adequately communicated and made known to the people, companies and institutions affected or involved in each case.

Communication, awareness and training programs will be defined periodically and a copy of the corresponding regulations will be delivered to users.

6.5 Authorization and control of access

Access to information systems is controlled, monitored, and limited to users, processes, devices, and information systems with the minimum allowed and/or authorized functionalities.

6.6 Physical protection of facilities

The MHP systems are located in protected areas, equipped with physical, redundancy, continuity, and environmental security measures, and with an access control procedure.

6.7 Default security

At MHP, systems are designed and configured always with Security by Default in mind. The system provides the minimum required functionality and MHP ensures that they are only accessible by people, and from authorized locations or equipment. This is particularly important on operating systems, where MHP removes, disables (or advises disabling or removing as appropriate) features that are not going to be used.

All projects related to or affecting information systems must include, in their analysis process, an evaluation of the security requirements and define a security model agreed with the person responsible for information security.

In the design, development, installation and management of the information systems and in the projects, the concepts of security will be taken into account and applied from the design, secure coding and the controls and security measures that proceed according to the applicability document approved by the company.

6.8 Contracting and acquisitions

All contracts and acquisitions that involve or require access or treatment of information classified as non-public must be under a contract that includes clauses designed to guarantee the safeguarding of the confidentiality, integrity, and availability of information.

In those cases in which the contracted services involve access or treatment by the provider of personal data, the clauses required for compliance with the DPD and its developments must be included in the contract.

Companies and people who, due to contracting services or acquisitions of any kind, access confidential information or for internal use, must be aware of the Information Security Policy and the complementary rules and procedures that are applicable to the purpose of the contracting.

Companies and external persons who access company information must consider such information, by default, as confidential. The only information that may be considered non-confidential is that which has been obtained through the public media.

6.9 Integrity and updating of the system

At MHP, systems are periodically evaluated to know their security status at all times, taking into account the manufacturer's specifications, vulnerabilities and any appropriate updates, and thus managing their integrity.

All elements of the systems require authorization prior to their installation.

6.10 Protection of information stored and in transit

The information is classified according to the sensitivity required in its treatment and according to the levels of security and protection required.

MHP pays particular attention to information stored or in transit through insecure environments. This includes information stored or processed on laptops, tablets, smartphones, peripheral devices, information media, as well as communications over open networks or with weak encryption, where security measures are applied to ensure that the information is processed. according to their classification.

6.11 Prevention against other interconnected information systems

MHP protects the perimeter of access to its system, particularly in connections through the Internet, always analyzing the risks derived from the interconnection with other systems, and establishing the measures that guarantee the necessary level of security.

6.12 Activity Register

MHP registers the activities of its users in order to monitor, analyze, investigate, and document improper or unauthorized activities, allowing the person who acts to be identified at all times. All this with full guarantees of the right to honor, personal and family privacy and the image of those affected, and in accordance with the regulations on personal data protection and other provisions that may be applicable.

6.13 Security incidents

Any commitment to the confidentiality, integrity, availability, authenticity or traceability of company information is considered a security incident.

MHP has a system for detecting and reacting to security incidents, which are classified and managed until they are solved, collecting evidence so that they can be reported and learned to improve continuously.

In particular, the company has a system for detecting and reacting against harmful code, as well as a system for preventing and detecting intrusions, carrying out technical audits to ensure the relevant protection measures.

Users have established channels to immediately report any incident or anomaly detected.

6.14 Continuity of activity

MHP performs the backup copies that guarantee the recovery of the information, and establishes the appropriate mechanisms to guarantee the continuity of the operations in case of loss of the usual means of work.

6.15 Continuous improvement of the security process

The implemented security management system is continuously updated and improved, as established by the ISO 27001 standard and National Security Scheme certifications.

7 . Legal requirements

- Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, regarding the protection of natural persons to the processing of personal data (RGPD).

- Organic Law 3/2018, of December 5, on Data Protection and Guarantee of Digital Rights (LOPDGDD).

- Royal Legislative Decree 1/1996, of April 12, Intellectual Property Law.

- Law 34/2002 of July 11, on services of the information society and electronic commerce.

- Royal Decree 3/2010, of January 8, which regulates the National Security Scheme.

- Royal Decree 951/2015, of October 23, modifying Royal Decree 3/2010, of January 8, which regulates the National Security Scheme.

8 . Roles, Responsibilities and Duties

The management assigns, renews, and communicates the responsibilities, authorities, and roles in relation to information security, determining in each case the reasons, the term of validity, and managing the conflicts that may arise. It will also ensure that users know, assume, and exercise assigned responsibilities, authorities, and roles.

8.1 Users

Any person or system that accesses the information processed, managed, or owned by the company will be considered a user. Users are responsible for their conduct when they access information or use the company's computer systems. The user is responsible for all actions carried out using their personal identifiers or credentials.

Los usuarios tienen la obligación de:

- Comply with the Information Security Policy and the complementary rules, procedures and instructions.
- Protect and safeguard company information, avoiding accidental or unauthorized disclosure, emission abroad, modification, erasure or destruction or misuse regardless of the support or means by which it was accessed or known.
- Know and apply the Information Security Policy, the Information Systems Use Rules and the rest of the applicable security policies, rules, procedures and measures.

8.2 Responsible for Data (National Security Scheme)

The Data Controller is ultimately responsible for any error or negligence that entails an incident of confidentiality or integrity (in terms of data protection) and availability (in terms of information security).

The Data Controller has the following responsibilities:

Ensure the proper use of the information and, therefore, its protection.

Establish the information requirements regarding security.

Determine the security levels of the processed information, assessing the consequences of a negative impact.

Given the above, the role of Responsible for Information in MHP is assumed by the Manager of the Organization.

8.3 Head of the Service (National Security Scheme)

The owner of the assets of the Service, understood as the person responsible for said service, will have the following general responsibilities:

- Establish service requirements in terms of security, including interoperability, accessibility and availability requirements.

- Determine the security levels of the service, in agreement with the Security Manager and the System Manager.

- Maintain the security of the information handled and the services provided by the information systems in their area of responsibility.

The figure of the Service Manager in MHP is assumed by the Manager of the Organization.

8.4 Management

The management of MHP is deeply committed to the policy described in this document and is aware of the value of the information and of the serious economic and image impact that a security incident can produce.

In the context of the National Security Scheme, the Management assumes the responsibilities described for the Information Manager and the Service Manager.

The Management is, therefore, the owner of MHP's own information assets, and also the owner of the risks.

The management also assumes the following responsibilities:

- Demonstrate leadership and commitment regarding the information security management system
- Ensure that the information security policy and objectives are established and that they are compatible with the strategic direction of the organization.
- Approve and communicate the Information Security Policy, the Information Systems Use Rules and the importance of their compliance to all users, internal or external, to customers and suppliers.
- Meet quarterly, and when any event or extraordinary request so requires, with the Security and Systems Managers, to be informed about the ISMS and update the Information Security strategy.

- Promote a corporate culture of information security, promoting Awareness and approving training plans.

- Support the continuous improvement of information security processes and projects.

- Ensure that the necessary resources are available to comply with the information security policy, the rules of use of the systems and for the operation of the information security management system.

- Define the approach for the analysis and management of information security risks and the criteria for assuming the risks and ensuring their evaluation at least once a year, exercising the role of owner of the risks.

- Ensure that internal information security audits are carried out and that their results are reviewed to identify opportunities for improvement.

- Define and control the budget for information security.

- Approve documentation up to its second level of rules and procedures.

- Determine the measures, be they disciplinary or of any other type, that could be applied to those responsible for security violations.

8.5 Security Manager

The person with the position of Responsible for Information Security will assume the following functions:

- Promote the security of the information handled and the electronic services provided by the information systems, with the responsibility and authority to ensure that the Information Security Management System complies with the requirements of the National Security Scheme and the UNE-ISO/IEC 27001 standard.

- Supervise compliance with this Policy, its regulations, derived procedures and the security configuration of the systems.

- Establish adequate and effective security measures to meet the security requirements established by the Management, following at all times what is required in Annex II of the ENS, declaring the applicability of such measures.

- Promote security awareness and training activities in their area of responsibility.

- Carry out the coordination and monitoring of the implementation of the projects of adaptation to the specified standards (ISO 27001 and ENS), in collaboration with the Systems Manager.

- Carry out, with the collaboration of the System Manager, the mandatory risk analysis, select the safeguards to implement and review the risk management process. Likewise, together with the System Manager, accept the residual risks calculated in the risk analysis.

- Promote periodic audits to verify compliance with the information security obligations and analyze the audit reports, drawing up the conclusions to be presented to the System Manager so that he can adopt the appropriate corrective measures.

- Coordinate the Security Management process, in collaboration with the Systems Manager.

- Sign the Declaration of Applicability, which includes the list of security measures selected for a system.

- Prepare periodic security reports that include the most relevant incidents in each period, in coordination with the Systems Manager.

- Determine the category of the system according to the procedure described in Annex I of the ENS and the security measures to be applied in accordance with the provisions of Annex II of the ENS.

- Verify that security measures are adequate to protect information and services.

- Prepare the topics to be discussed in the meetings of the Security Committee, in coordination with the System Manager, providing timely information for decision-making.

- Responsible for the direct or delegated execution of the decisions of the Directorate, will meet with it and with the System Manager, at least once a year, to ensure the strategy.

Regarding the documentation, and relying on the System Manager, the following are functions of the Security Manager:

- Propose to the Management and the Systems Manager for approval the second level security documentation (ICT Security Standards –STIC– and General Procedures of the Information Security Management System –SGSI–) and sign said documentation.

- Approve the third level security documentation (STIC Operating Procedures and STIC Technical Instructions).

- Keep the documentation organized and updated, managing the access mechanisms to it.

- For the development of any of its functions, the Security Manager may request the collaboration of the System Manager.

The MHP Safety Committee assumes the functions of Safety Manager.

8.6 EData Protection Officer

Following what is indicated in the GDPR and in the DPO, the Data Protection Delegate will have at least the following functions:

- Inform and advise the data controller and its employees of their obligations in relation to the GDPR and other data protection provisions.

- Monitor compliance with the provisions of this Regulation, other data protection provisions of the Union or of the Member States and the policies of the person in charge or the person in charge of the treatment regarding the protection of personal data, including the assignment of responsibilities , the awareness and training of the personnel involved in the treatment operations, and the corresponding audits.

- Offer the advice that is requested on the impact assessment related to data protection and supervise its application in accordance with article 35.

- Cooperate with the control authority, in this case, the Spanish Data Protection Agency.

- Act as the contact point of the control authority for questions related to the treatment, including the prior consultation referred to in article 36, and carry out consultations, where appropriate, on any other matter.

MHP has designated an internal Data Protection Delegate for its Organization.

8.7 System manager

The functions of the System Manager will be the following:

• Develop, operate and maintain the Information system throughout its life cycle, its specifications, installation and verification of its correct operation.

• Define the topology and management system of the Information System, establishing the criteria for use and the services available in it.

• Make sure that the specific security measures are properly integrated into the general security framework.

• Carry out exercises and tests on security operating procedures and existing continuity plans.

• Monitoring of the systems life cycle: specification, architecture, development, operation, changes.

• Implement the necessary measures to guarantee the security of the system throughout its life cycle, in accordance with the Security Manager.

• Approve any substantial modification of the configuration of any element of the system.

• Suspend the handling of certain information or the provision of an electronic service if it is informed of serious security deficiencies, with prior agreement with the Security Officer and the Management.

• Carry out, with the collaboration of the Security Officer, the mandatory risk analysis, selecting the safeguards to be implemented and reviewing the risk management process. Likewise, together with the Security Manager, accept the residual risks calculated in the risk analysis.

8.8 Data Security Committee

Composed of the security manager, the system manager, the figure of the Data Protection Officer, and the management, it meets at least quarterly to coordinate information security at the organization level functions are as follows:

- Address the concerns of those present regarding Information Security.
- Receive a picture of the information security status.
- Promote continuous improvement of the ISMS. Elaborar la estrategia de evolución
- Review the Policy, Regulations and procedures at least annually
- Approve training and awareness requirements
- Prioritize actions
- Promote the performance of ISMS and technical audits.
- Check that Information Security is present in all projects.

9 . Review and audits

The security officer will review this policy annually or when there are significant changes that so advise, and will submit it again for approval by management.

The reviews will verify the effectiveness of the policy, assessing the effects of technological and business changes.

The management will be responsible for approving the necessary modifications in the text when a change occurs that affects the risk situations established in this document.

The security management system will be audited at least every year, according to an audit plan developed by the security manager for the ISO 27001 (annual) and National Security Scheme (every two years) standards.

Integrated Time Management

mhpsc.co.uk/ info@mhp.es +34 900 363 834

SPAIN | PORTUGAL | UK | NETHERLANDS| GERMANY