Tedial™
Media IT

Information Security Policy

Contents

Purpose

To establish the guidelines and principles that will govern how TEDIAL will manage and protect its information and services through the implementation, maintenance, and improvement of an Information Security Management System (hereinafter, ISMS), applying the requirements of the UNE ISO/IEC 27001 Standard and its stakeholders within the legal and regulatory framework in force, such as Royal Decree 311/2022, of May 3, which regulates the National Security Framework (ENS). This decree mandates the establishment of security policy principles and requirements for the use of electronic means that allow for the adequate protection of information.

Scope

Considering the organization's context, which determines the internal and external issues of the organization, the relevant stakeholders and their requirements for information security, as well as the interfaces and dependencies between the entity's activities and those carried out by other organizations, TEDIAL has established the following scope:

- **ISMS:** "The information systems supporting the processes of Design, Development, Implementation, and Maintenance of audiovisual and multimedia management software according to the current Statement of Applicability at the certificate issuance date."
- **ENS:** "The information systems supporting the processes of Design, Development, Implementation, and Maintenance of audiovisual and multimedia management software 'smartWork' according to the system categorization in force."

Mission, Legal and Regulatory Framework

Royal Decree 311/2022 obliges TEDIAL to protect the services provided to stakeholders using electronic means. The implementation of an ISMS under UNE ISO/IEC 27001, extended to cloud-based services under UNE ISO/IEC 27017 and integrated with the ENS, strengthens service security as well as the information and data included, necessary for proper service delivery due to the close relationship between them and the additional elements that enhance information security management.

The legal framework mentioned above will be aligned with TEDIAL's ISMS/ENS, as one of its security control groups is Compliance with Applicable Legislation.

TEDIAL processes personal data, inventoried by processing, to facilitate control, management, and protection, applying measures to comply with **REGULATION (EU) 2016/679** of the European Parliament and of the Council of April 27, 2016 (General Data Protection Regulation – GDPR) and **Organic Law 3/2018** on Personal Data Protection and Guarantee of Digital Rights.

The ISMS/ENS of TEDIAL will comply with the Intellectual Property Law regarding software use, obtaining appropriate licenses, and maintaining their records and controls for proper use.

Leadership and Committee

TEDIAL's Management is committed to providing the necessary resources for establishing, implementing, maintaining, and improving the ISMS/ENS, demonstrating leadership through the establishment of the Quality and Information Security Committee. The Committee will:

- Ensure the establishment and compatibility of this policy and security objectives with TEDIAL's strategy.
- Integrate and comply with applicable ISMS/ENS requirements in company services and processes.
- Ensure availability of necessary resources.
- Communicate the importance of effective security management.
- Ensure ISMS/ENS achieves intended outcomes.
- Support staff to contribute to ISMS/ENS effectiveness.
- Promote continuous improvement.
- Lead other relevant roles in information security responsibility areas.

Information Security Objectives

Information security objectives will be set at relevant functions and levels, focusing on improvement and using the following reference framework:

- Changes in stakeholders' needs leading to ISMS scope improvement.
- Applicable information security requirements and risk assessment results.
- Internal factors such as organizational techniques for tracking and resolving security incidents.
- External factors such as technological advancements enhancing risk treatment.
- Improved staff training and awareness affecting security performance.

The planning to achieve the established information security objectives will consider what needs to be done, the necessary resources, the responsible party, the completion deadline, and indicators to evaluate both the result and compliance. This comprehensive approach ensures that objectives are effectively implemented and measured, aligning with the organization's broader information security strategy.

ISMS/ENS Implementation, Maintenance, and Improvement and Documentation Management Guidelines

TEDIAL's ISMS/ENS deployment will begin with an information systems risk analysis, including personal data processing, to determine the security risk level and identify necessary security controls and improvement opportunities. Security controls will be implemented, maintained, and continuously improved, documented, reviewed, and approved by the Quality and Information Security Committee.

In compliance with Article 12 of the Royal Decree of the ENS, this security policy will be developed by applying the following minimum requirements to be included in the system documentation:

- Organization and security process implementation.
- Security risk analysis and management (including those derived from personal data processing).
- Personnel management.
- Authorization and access control.
- Facilities protection.
- Acquisition of security products and contracting of security services.
- Least privilege principle.
- Stored and in-transit information protection.
- Prevention of interconnected system risks.
- Activity logging and malicious code detection.
- Security incidents.
- Business continuity.
- Continuous improvement.

The CCN-STIC Security Guides, particularly Series CCN-STIC-800, will be applied alongside UNE ISO/IEC 27002 for ISMS security controls.

Additionally, this policy establishes the required levels of information security for information processed through cloud services, including:

- Security and privacy by design and by default, applying best security practices in cloud service development, deployment, operation, maintenance, and retirement.
- Staff training, awareness, and access control as part of internal risk mitigation.

- Customer information separation through cloud storage service isolation.
- Alignment with regulatory compliance and cloud service provider security requirements.
- Access control procedures with strong authentication for cloud service administrators.
- Customer communication regarding planned degradations or service interruptions due to change management.
- Server virtualization and service configuration security.
- Protection of customer data using access control, backup, and activity monitoring techniques.
- Cloud customer account lifecycle management from creation to deletion.
- Communication of privacy and information security incidents, with information-sharing guidelines based on GDPR/LOPDGDD requirements to aid forensic investigations.

he system security in our company includes prevention, detection, and response actions to minimize vulnerabilities and protect information and services:

- **Prevention:** We implement measures aimed at deterring and reducing exposure to risks. These measures eliminate or reduce the impact of threats that may materialize.
- **Detection:** Mechanisms are established to quickly identify the presence of cyber incidents and any suspicious activity that could compromise the system.
- **Response:** Procedures are developed to act efficiently and promptly in case of incidents, in order to restore affected information and services.

Our information system is based on a multi-layered protection strategy. This strategy ensures that if one layer is compromised, the following objectives are achieved:

- **Incident Response:** Mechanisms are implemented to develop an appropriate response to incidents that could not be avoided, reducing the likelihood of the entire system being compromised.
- **Impact Minimization:** Measures are taken to minimize system impact and limit adverse effects on information and services.

The lines of defense comprise organizational, physical, and logical measures, creating a robust and effective security environment.

Continuous monitoring is essential to detect anomalous activities or behaviors and enable timely responses. Additionally, we conduct ongoing security assessments of our assets, measuring their evolution, identifying vulnerabilities, and detecting configuration deficiencies.

Security measures are periodically reevaluated and updated to ensure their effectiveness aligns with evolving risks and protection systems. If necessary, a security reassessment is performed to maintain a secure and protected environment.

In our information systems, the roles of those responsible are clearly defined, including the Information Officer, Service Officer, Security Officer, and System Officer. Security responsibility is distinctly separated from operational responsibility.

The attributions of each responsible party are specified, along with coordination mechanisms and conflict resolution processes.

Functions and Responsibilities of Information Security

The Quality and Information Security Committee will review and propose the approval of this Information Security Policy to the Management, which will be the highest authority for information (also part of the Committee). Additionally, the Quality and Information Security Committee will centralize coordination mechanisms and resolve conflicts between the following responsible parties through debate during Committee meetings:

- TEDIAL's Management will be responsible for approving the policy and authorizing its modifications, as well as all documented information of the ISMS/ENS of the entity.
- The Information Security Officer will notify staff of this policy and any changes, determine the system's security category, and coordinate the implementation, maintenance, and improvement actions of the ISMS/ENS (including the Statement of Applicability formalizing the applicable security measures from UNE ISO/IEC 27001, the Royal Decree regulating the ENS, and those derived from Risk Analysis and Management) and its audits, in coordination with the System Officer, who will manage the technical security requirements of the information systems based on the system's security category, and the Service Officer, who will manage the security requirements of service provision activities.
- In compliance with the ENS security measure on Information Qualification, the following will apply regarding information system categorization:
    - The information and service responsible parties affected by the Risk Analysis and Management will be indicated in the ISMS/ENS Risk Analysis (risk owners and members of the Quality and Information Security Committee). The Risk Analysis will include criteria for determining the required security level within the framework established in Article 40 and general criteria in Annex I of the ENS Royal Decree.
    - Each information and/or service responsible party must follow the determined criteria to assign the required security level to each information, documenting and formally approving it.
    - The information and service responsible parties will have exclusive authority to modify the required security level at any time.
- In compliance with the ENS security measure on Media Labeling, information media containing information requiring specific security measures according to its qualification will carry labels indicating the highest security level of the contained information (Confidential, which may include a label or watermark if applicable). This will be detailed in the Information Media Management and Information Protection Procedure.
- The Data Controller's representative will supervise compliance with TEDIAL's Data Protection Policy, working in coordination with the Compliance Officer and the System Officer.
- All personnel, both internal and external, will be responsible for complying with this Information

Security Policy within their work area, as well as applying all documented information on ISMS/ENS controls and security measures in their job activities affecting information security performance.

Information Security Policy Review

This Information Security Policy will be reviewed by Management during system reviews through the Quality and Information Security Committee whenever significant changes occur, at least once a year.

Approval, Dissemination, and Implementation of the Information Security Policy

This Information Security Policy will be approved by TEDIAL's Management and disseminated to interested parties. Management will also provide the necessary resources for the effective implementation of this policy and its proper development in both implementation activities and the subsequent maintenance and improvement of the entire ISMS/ENS of the entity.