APPROVAL AND ENTRY INTO FORCE

Text approved on July 02, 2026 by **DIRECCION.**
This Information Security Policy is effective from that date until it is replaced by a new Policy.

INTRODUCTION

CHEIL SPAIN depends on ICT (Information and Communication Technologies) systems to achieve its objectives. These systems must be managed diligently, taking appropriate measures to protect them against accidental or deliberate damage that may affect the availability, integrity or confidentiality of the information processed or the services provided.
The objective of information security is to guarantee the quality of information and the continuous provision of services, acting preventively, monitoring daily activity and reacting promptly to incidents.
ICT systems must be protected against rapidly evolving threats with the potential to impact the confidentiality, integrity, availability, intended use and value of information and services. To defend against these threats, a strategy that adapts to changes in environmental conditions is required to ensure the continuous delivery of services. This implies that departments must apply the minimum security measures required by the National Security Scheme, as well as continuously monitor the levels of service provision, monitor and analyze reported vulnerabilities, and prepare an effective response to incidents to ensure the continuity of the services provided.
Different departments must ensure that ICT security is an integral part of every stage of the system's lifecycle, from conception to decommissioning, development or acquisition decisions and operational activities. Security requirements and funding needs should be identified and included in planning, in the request for proposals, and in tender documents for ICT projects.
Departments must be prepared to prevent, detect, react to, and recover from incidents.

PREVENTION

Departments should avoid, or at least prevent as much as possible, information or services from being harmed by security incidents. To do this, departments must implement the minimum security measures determined by the ENS, as well as any additional controls identified through a threat and risk assessment. These controls, and the safety roles and responsibilities of all personnel, must be clearly defined and documented.
To ensure compliance with the policy, departments must:

- Authorize systems before they go into operation.
- Regularly assess security, including assessments of configuration changes made on a routine basis.
- Request periodic review by third parties for the purpose of obtaining an independent evaluation.

DETECTION

Because services can degrade quickly due to incidents, ranging from a simple slowdown to a halt, services must continuously monitor operation to detect anomalies in service delivery levels and act accordingly.
Detection, analysis and reporting mechanisms will be established that reach those responsible regularly and when there is a significant deviation from the parameters that have been pre-established as normal.

ANSWER

Departments must:

- Establish mechanisms to respond effectively to security incidents.
- Designate a point of contact for communications regarding incidents detected in other departments or in other agencies.
- Establish protocols for the exchange of information related to the incident. This includes two-way communications with Emergency Response Teams (CERTs).

RECOVERY

To ensure the availability of critical services, departments should develop ICT continuity plans as part of their overall business continuity plan and recovery activities.

SCOPE

This policy applies to all **CHEIL SPAIN** ICT systems and to all CHEIL SPAIN members, without exceptions.

MISSION

CHEIL SPAIN's mission is to provide comprehensive marketing, advertising, communication, creativity and digital transformation solutions that add value to its clients, through the development and execution of innovative strategies, communication campaigns and technological services adapted to the needs of the business.

The organization focuses its activity on offering high-quality services, guaranteeing compliance with applicable contractual, legal and regulatory requirements, as well as the protection of the information managed during the provision of its services.

In this context, **CHEIL SPAIN** considers information security to be a strategic element to preserve the confidentiality, integrity, availability, authenticity and traceability of the information and systems that support its activity, contributing to business continuity, the trust of its customers and collaborators and compliance with the National Security Scheme and the rest of the applicable regulations.

REGULATORY MARCO

Below are all the legal requirements applicable to the organization:

- Royal Decree 311/2022, which regulates the National Security Scheme
- Law 40/2015, on the Legal Regime of the Public Sector
- Regulation (EU) 2016/679 (GDPR)
- Organic Law 3/2018 (LOPDGDD)
- Law 34/2002 (LSSI-CE)
- Regulation (EU) 910/2014 (eIDAS)
- Regulation (EU) 2024/1183 (eIDAS 2)
- NIS2 Directive (EU) 2022/2555
- Regulation (EU) 2022/2554 (DORA)
- Law 9/2017 on Public Sector Contracts
- Law 39/2015 on the Common Administrative Procedure
- Law 56/2007 on Measures to Promote the Information Society
- Royal Legislative Decree 2/2015 (Workers' Statute)
- Law 31/1995 on the Prevention of Occupational Risks
- Royal Decree 171/2004
- Royal Decree 1215/1997
- Law 10/2021 on Remote Work
- Law 1/2019 on Trade Secrets
- Criminal Code (articles relating to computer crime and disclosure of secrets)
- Royal Legislative Decree 1/1996 (Law on Intellectual Property)
- General Telecommunications Law 11/2022

SAFETY ORGANIZATION

COMMITTEES: ROLES AND RESPONSIBILITIES

The ICT Security Committee will be made up of:

- Information Controller:	Marcos Velasco
- Service Manager:	Marcos Velasco
- Security Manager:	Óscar López
- System Manager:	Óscar López

ROLES: ROLES AND RESPONSIBILITIES

The designation of the roles and responsibilities defined in this document has been made taking as a reference the CCN-STIC Guide 801 "Responsibilities and Functions", adapting its content to the organisational structure and the needs of the organisation, especially in relation to the definition of the functions of the Security Manager and their relationship with the Security Committee.

Its functions are reflected in the Minutes of the Security Committee dated 02/07/2026.

APPOINTMENT PROCEDURES

The Information Security Officer will be appointed by Management at the proposal of the ICT Security Committee. The appointment will be reviewed every 2 years or when the position becomes vacant.
The Department responsible for a service that is provided electronically in accordance with Law 11/2007 will designate the System Manager, specifying their functions and responsibilities within the framework established by this Policy.

INFORMATION SECURITY POLICY

The Security Committee's mission will be the annual review of this Information Security Policy and the proposal for its revision or maintenance. The Policy will be approved by **MANAGEMENT** and disseminated so that it is known to all affected parties.

PERSONAL DATA

CHEIL SPAIN processes personal data. All **CHEIL SPAIN**'s information systems will comply with the security levels required by national and European regulations for the nature and purpose of the personal data stored and processed in **CHEIL SPAIN**'s systems.

RISK MANAGEMENT

All systems subject to this Policy shall conduct a risk analysis, assessing the threats and risks to which they are exposed. This analysis will be repeated:

- regularly, at least once a year
- when the information handled changes
- when the services provided change
- When a Serious Security Incident Occurs
- when serious vulnerabilities are reported

For the harmonisation of risk analyses, the ICT Security Committee will establish a reference assessment for the different types of information handled and the different services provided. The ICT Security Committee will boost the availability of resources to meet the security needs of the different systems, promoting horizontal investments.

DEVELOPMENT OF THE INFORMATION SECURITY POLICY

This Information Security Policy complements the security policies of **CHEIL SPAIN** in different areas:

- Access Control Policy
- Password Management Policy
- Cryptographic Controls Policy
- Acceptable Use of Assets Policy
- Year 2026 Global Management Guideline (IT)

This Policy will be developed by means of security regulations that address specific aspects. The security regulations will be available to all members of CHEIL SPAIN who need to know them, in particular for those who use, operate or manage information and communications systems.

STAFF OBLIGATIONS

All members of **CHEIL SPAIN** are obliged to know and comply with this Information Security Policy and Security Regulations, and it is the responsibility of the ICT Security Committee to provide the necessary means for the information to reach those affected.

All members of **CHEIL SPAIN** will attend an ICT security awareness session at least once a year. A continuous awareness programme will be established to serve all members of **CHEIL SPAIN**, in particular those who have joined the company.

Persons with responsibility for the use, operation or administration of ICT systems shall be trained in the safe handling of the systems to the extent that they need it to carry out their work. The training will be mandatory before assuming a responsibility, whether it is your first assignment or if it is a change of job or responsibilities in the same

THIRD PARTIES

When **CHEIL SPAIN** provides services to other bodies or handles information from other bodies, they will be made participants in this Information Security Policy, channels will be established for reporting and coordination of the respective ICT Security Committees and action procedures will be established for the reaction to security incidents.

When **CHEIL SPAIN** uses third-party services or transfers information to third parties, they will be made aware of this Security Policy and the Security Regulations that apply to such services or information. This third party will be subject to the obligations established in said regulations, and may develop its own operating procedures to satisfy it. Specific procedures for reporting and resolving incidents will be established. It will be ensured that third-party personnel are adequately aware of the
security matters, at least at the same level as that established in this Policy.

Where any aspect of the Policy cannot be satisfied by a third party as required in the preceding paragraphs, a report from the Security Officer shall be required specifying the risks incurred and how to deal with them. Approval of this report by those responsible for the information and services concerned will be required before proceeding.

In Madrid, 02/07/2026
DIRECCION