Corporate Cyber-resilience Policy

Approved by the Board of Directors
of El Corte Inglés, S.A.
on 29 October 2025

Version 1.0 (29 October 2025)

El Corte Inglés

TABLE OF CONTENTS

NOTE: The definitions of the most frequently used terms in this document and in the regulations that make up the EL CORTE INGLÉS Cyber Resilience Management System are provided in **Annex 1.**

1. INTRODUCTION

The Board of Directors of El Corte Inglés, S.A. is responsible for defining the Strategy and Corporate Policies of the companies within the El Corte Inglés Group (hereinafter, the 'Group'), as well as for approving internal compliance and control programmes and systems.

Since its establishment, the Group's operational capacity has been considered one of its strategic assets and a key element for the sustainability and competitiveness of the Organisation. Accordingly, with the aim of establishing the general principles governing cyber resilience across all Group companies, the Board of Directors has approved this Corporate Cyber Resilience Policy (hereinafter, the 'Policy').

This Policy is aligned with the Group's values, reaffirming its firm commitment to contributing to the 17 United Nations Sustainable Development Goals and to maintaining conduct that is respectful of both the regulations applicable to its activities and the ethical standards and other rules and initiatives to which the Group has committed through certification or adherence, such as DORA, CRA, ENS, NIS2, among others, as well as recognised good practices including ISO/IEC 27001:2020, UNE-ISO/IEC 22301:2020 and UNE-ISO/IEC 22316:2020.

This Policy constitutes the basis of the Cyber Resilience Management System (hereinafter, the 'CRMS'), on which the Organisation's strategy and operational framework are built.

2. PURPOSE

The purpose of this Policy is to establish the principles, commitments and guidelines that enable the Group to anticipate, withstand, respond to and recover from threats and opportunities affecting the cyber domain that may impact operational continuity, information security and integrity, and organisational resilience.

The application of these principles enables the Group to:

- reduce the impact of incidents affecting the cyber domain;
- enhance its capacity to anticipate and respond;
- promote continuous improvement of the management system and organisational resilience;
- ensure operational continuity and maintain customer trust;
- comply with applicable legislation.

This Policy is intended to serve as an instrument that promotes informed decision-making, aligned with the Group's risk appetite, regulatory requirements and stakeholder expectations.

3. SCOPE OF APPLICATION

This Policy is mandatory and applies globally to the companies that make up the Group, as well as to employees, collaborators and third parties, across all activities related to the value chain, both upstream and downstream, regardless of the country in which such activities are carried out.

All Members of the Organisation and Business Partners, particularly those involved in the value chain, shall comply with its provisions, irrespective of their position or the territory from which they operate.

This commitment shall be formalised as set out in Section 10, 'Awareness and Statement of Compliance', of this Policy.

This Policy also applies to all resources* across the Group's various operational environments.

4. PRINCIPLES OF ACTION

The Group expects all Members of the Organisation, as well as its Business Partners and other relevant stakeholders, to comply with the following principles of action, which form the foundations of Corporate Cyber Resilience:

Principle 1. Governance and Committed Leadership.

Senior Management plays an active role in the development, supervision and continuous improvement of cyber resilience, ensuring that continuity and resilience objectives are integrated into the business strategy. Appropriate resources shall be allocated, and a clear governance framework with defined roles and responsibilities for decision-making—particularly in cyber-related crisis situations—shall be established.

Principle 2. Resilient Organisational Culture.

The Organisation promotes a culture focused on prevention, collaboration and proactive response to cyber-related threats. All personnel shall receive training, awareness and the necessary mechanisms to act consistently with resilience and security objectives.

Principle 3. Risk Management–Based Approach.

The Group's strategy is based on identifying and assessing risks that may affect critical processes, with the aim of achieving effective cyber resilience. This assessment is carried out systematically and continuously, considering both internal and external threats, in order to prevent incidents, prioritise actions and ensure business continuity in disruptive scenarios.

Principle 4. Preparedness and Response Capability.

The Organisation develops and implements plans to ensure an agile and coordinated response that limits the impact of any cyber-related event on operations and critical processes. These plans shall be tested in advance to ensure that all involved parties are aware of how to act effectively.

Principle 5. Protection of Critical Resources.

*Definition in Annex I

Differentiated security controls and measures are implemented to protect the Organisation's most valuable resources, including systems, data, people and critical processes. Protection is based on the level of criticality and the potential impact that a threat could have on operations.

Principle 6. Effective Communication.

The Group ensures clear, accessible and redundant internal and external communication channels for managing cyber-related crisis situations. Relevant information flows in real time among stakeholders, enabling an efficient, coherent response aligned with the principles of transparency and accountability.

Principle 7. Collaboration with Third Parties.

These principles are extended to suppliers and stakeholders as part of the management of risks affecting critical processes.

Accordingly, when contracting suppliers, it shall be ensured that the requirements arising from internal supplier regulations are conveyed both contractually and through appropriate training.

Principle 8. Regulatory and Contractual Compliance.

Cyber resilience is managed in compliance with applicable laws, regulations, standards and contractual commitments relating to information security, resilience and business continuity. Compliance is periodically audited, and regulatory changes are managed proactively.

Principle 9. Transparency and Continuous Improvement.

A review and improvement cycle is established, incorporating lessons learned, results from simulations, internal audits and changes in the technological environment. The Policy, controls and cyber resilience procedures are systematically updated to ensure their effectiveness over time.

These principles constitute the operational and strategic foundation on which the Organisation's ability to withstand, adapt to and recover from cyber threats is built, ensuring long-term sustainability and competitiveness.

5. ORGANISATIONAL STRUCTURE

The Group's Cyber Resilience Management System (CRMS) establishes an organisational structure based on three fundamental pillars: Governance, Management and Operation of Cyber Resilience.

5.1. Cyber Resilience Governance

Governance is grounded in the **Corporate Prevention and Security Department**, the governing body responsible for leading, coordinating and overseeing the global security and cyber resilience strategy, ensuring its alignment with corporate objectives and applicable regulations.

Under its supervision, the following collegiate bodies are structured:

- **Advisory Cabinet on Crises, Emergencies and Catastrophes:** the principal and most relevant body, of a consultative nature and providing strategic support to Senior Management. It is responsible for advising on critical decision-making, recommending the activation of crisis management plans and coordinating

*Definition in Annex I

liaison with authorities and external bodies.

- **ISC (Information Security Committee):** a multidisciplinary committee that meets periodically and promotes and oversees information security across the Organisation, ensuring that good practices are applied in a transversal and consistent manner.

5.2. Cyber Resilience Management

Management is articulated through the **Cyber Resilience Area,** integrated within the GRC framework. This unit coordinates, defines and regulates the Group's cyber resilience capabilities, ensuring the coherence of actions across all organisational areas and promoting the adoption of common policies, procedures and controls.

5.3. Cyber Resilience Operation

Operation lies with the **operational areas** responsible for implementing cyber resilience measures and capabilities. These areas ensure the proper application of the resources required to maintain organisational resilience, including people, locations, technology, third parties, security, and other relevant elements.

6. CRMS COMPONENTS

The Cyber Resilience Management System (CRMS) is the organisational framework adopted by the Group and is structured around four fundamental components that ensure its effective operation:

- **Cyber Resilience Strategy:** a high-level approach defined by the Group aimed at ensuring the ability to anticipate, withstand and recover from threats. It includes documents setting out the Organisation's principles and values on cyber resilience and their alignment with the corporate strategy and business objectives.
- **Cyber Resilience Regulatory Framework:** a set of Policies, Standards and general and specific Procedures that cover the requirements identified both in the Control Framework and in applicable regulations.
- **Cyber Resilience Control Framework:** establishes the technical and organisational control structure to adapt, protect assets, manage risks and ensure the recovery of the Group's business processes.
- **Cyber Resilience Scorecard:** a tool that enables the measurement and evaluation of the performance of cyber resilience-related actions and processes.

These four components are maintained and updated by the Information Security and Cybersecurity Department according to the context and needs of the Organisation.

7. LEGAL AND REGULATORY ANALYSIS

The Group recognises the need to comply with all legal, regulatory and contractual obligations related to information security, data privacy and business continuity. In this regard, the legal component of cyber resilience is considered a strategic priority.

Applicable Regulatory Framework

The Organisation undertakes to identify and comply with the legislation in force in all jurisdictions in which it operates, including, but not limited to:

*Definition in Annex I

- **Personal data protection laws**, such as the General Data Protection Regulation (GDPR) in Europe.
- **Cybersecurity regulations specific** to the retail sector or regulated industries (e.g. PCI-DSS for payment card processing, ISO standards, ENS, etc.).
- **Mandatory incident notification laws**, such as those requiring the reporting of data breaches to authorities or affected parties.
- **Requirements imposed by financial or consumer supervisory bodies,** where applicable to payment platforms, e-commerce or credit services.

Contractual obligations

This includes the analysis of security and resilience clauses in contracts with third parties, technology partners, logistics operators and cloud service providers, ensuring that:

- responsibilities in the event of security incidents are clearly defined;
- maximum response and notification times (SLAs) are established; and
- audit rights relating to security controls are included.

8. NEEDS AND EXPECTATIONS OF INTERESTED PARTIES

The identification and management of stakeholders' needs and expectations are essential to ensure alignment with the Group's internal and external context.

The following stakeholders have been identified as key to the Organisation's performance, sustainability and resilience:

STAKEHOLDER	ROLE
Customers	End users of products and services.
Employees	Process executors, system operators and customer service staff.
Business Process Owner	Define minimum requirements to ensure critical processes can be carried out.
Senior Management and Shareholders	Responsible for corporate governance and business strategy.
Suppliers and Third Parties	Provision of critical products, technology and services.
Regulatory Bodies	Oversight of legal and regulatory compliance.
Business Partners	Strategic alliances, franchisees and logistics operators.
Community and Society	Social, environmental and economic environment.
Response Bodies	Security forces, civil protection authorities and CERTs.

*Definition in Annex I

In accordance with the principles of ISO 22301 and ISO 22316, understanding the needs and expectations of interested parties is essential to strengthen operational continuity and organisational resilience. This identification enables the alignment of response capabilities with environmental requirements and fosters trust among key stakeholders. The main needs and expectations according to the role of each stakeholder are set out below:

Customers

- Uninterrupted access to sales channels (physical and digital).
- Protection of personal and financial data.
- Transparency in the event of incidents affecting them.
- Confidence in the availability and security of services.

Employees

- Training on roles and responsibilities related to cyber resilience and continuity.
- Secure working channels, particularly in hybrid or remote working schemes.
- Clear procedures in the event of incidents or crises.
- Confidence in the Organisation as a safe and stable place to work.

Business Process Owner

- Definition and validation of business continuity requirements and applicable recovery times (RTO/RPO).
- Assurance of the availability of key resources (technology, personnel, facilities) during disruption scenarios.
- Timely information on risks and vulnerabilities affecting operations.
- Participation in simulation exercises, tests and reviews of the continuity and cyber resilience management system.
- Smooth coordination with IT, information security and crisis management functions in order to align response capabilities with business objectives.
- Informed decision-making based on Business Impact Analysis (BIA) data and risk assessments.
- Confidence that the Organisation protects and prioritises the resilience of critical processes.

Senior Management and Shareholders

- Alignment of cyber resilience with business strategy.
- Minimisation of financial, operational and reputational impacts during crises.
- Regulatory compliance and reduction of legal risks.
- Clear reporting on the Organisation’s level of preparedness.

Suppliers and Third Parties

- Clear security and continuity standards defined in contracts.
- Defined SLAs and recovery times (RTO/RPO).
- Incident communication procedures.
- Interoperability and mutual trust during contingency situations.

*Definition in Annex I

Regulatory and Compliance Authorities

- Compliance with data protection legislation (e.g. GDPR).
- Timely and appropriate notification of security breaches.
- Availability of documentary evidence on plans, tests and controls.
- Participation in audits or inspections where required.

Business Partners and Franchisees

- Assurance of continuity in shared operations.
- Integrity of transactional data.
- Access to corporate platforms with high security standards.
- Support and alignment in major incidents or reputational crises.

Community and Society

- Ethical and responsible organisational behaviour.
- Crisis management that minimises impact on consumers and employment.
- Transparency in public communication of serious events.
- Contribution to social and economic stability.

Emergency Response Bodies

- Effective coordination in the event of disasters or cyber-attacks.
- Access to key incident-related information.
- Collaboration in joint drills or exercises.

These needs and expectations are periodically reviewed through organisational context analysis, surveys and meetings with key stakeholders.

Tools such as influence and impact mapping, as well as the monitoring of complaints and non-conformities, are used to ensure continuous adaptation to environmental changes and to strengthen the Group's resilience.

9. DUE DILIGENCE

Due diligence processes refer to the management and monitoring of relationships with third parties, whether suppliers, customers, business partners or any other third party with whom a contractual relationship exists and who provide, or may potentially provide, support to the Organisation's business processes.

The third-party due diligence process is based on the following pillars:

- Before entering into a relationship with a third party, the impact of the agreement on Cyber Resilience shall be assessed and, where such impact exists, the corresponding risk analysis shall be carried out.
- The Organisation shall establish a framework of controls and measures to enable the security risks associated with working or contracting with third parties to be managed in a standardised and systematic manner.
- The third party shall be contractually required to comply with the Cyber Resilience Policy and to implement the technical and organisational measures necessary to ensure adequate protection of the Organisation's resources.

*Definition in Annex I

- On a periodic basis and depending on the level of risk associated with the agreement, monitoring and audit processes shall be conducted to ensure that the third party maintains a security ecosystem equivalent to that contractually committed.
- Upon termination of the contractual relationship, the Organisation shall ensure the return of resources, the destruction of information and the revocation of any access to information by the third party

10. AWARENESS AND STATEMENT OF COMPLIANCE

Compliance with ethical rules and standards represents both a corporate commitment and a strategic objective for the Organisation. Therefore, all Members of the Organisation are expected to be familiar with and adhere to the contents of this Policy. Likewise, all Business Partners are expected to act in accordance with its principles.

This commitment shall be formalised through:

i. Statements of compliance with the principles set out herein by Members of the Organisation, confirming their acceptance of **High Ethical Standards.**

ii. **Compliance clauses included in contracts** with Business Partners

iii. **Formal agreements or acknowledgement** by the governing bodies of the companies within the El Corte Inglés Group, in accordance with applicable internal regulations.

Such agreements and their renewals shall be notified to the El Corte Inglés Group's Compliance and Risk Control Department.

In the event of significant changes to this Policy, – i.e. changes that require formal approval from the Board of Directors at El Corte Inglés, S.A. – the preceding commitments shall be formally renewed.

As compliance with ethical rules and standards is a corporate commitment and a strategic goal for the Organisation, all Members of the Organisation are expected to know and respect the contents of this Policy. Likewise, all Business Partners are expected to act in accordance with its principles.

The Organisation shall respond promptly to any breach of the provisions set out in this Policy, in accordance with its internal regulations and in compliance with all applicable legislation.

11. REPORTING OF NON-COMPLIANCE

11.1 Non-Compliance with Information Security Regulations

Any Member of the Organisation, Business Partner or Third Party with a direct relationship and a legitimate commercial or professional interest who becomes aware of a breach of this Policy, or who has doubts as to whether an observed practice may constitute an unlawful act, whether in the public or private sector, shall immediately contact the Compliance and Risk Control Department of the El Corte Inglés Group via the Ethics Channel, using any of its available means of communication:

- **Digital Channel:**

  The El Corte Inglés Group's digital channel can be accessed via the following website:

  https://www.elcorteingles.es/informacioncorporativa/es/gobierno-corporativo/etica- and-compliance/

  This access is available on the corporate website and additionally on the NEXO intranet for Members of the Organisation.

*Definition in Annex I

- **Postal address:**

  El Corte Inglés, S.A.
  Compliance and Risk Control
  Hermosilla, 112
  28009 Madrid

- **Compliance and Risk Control Department – Phone number:** 91 401 85 00

- **Request for a face-to-face or remote meeting**

The information communicated through this Channel is confidential, as is the identity of reporting persons acting in good faith, whose cooperation the Organisation appreciates and in respect of whom it guarantees the absence of retaliation of any kind.

In addition, the Compliance Function may act on its own initiative by investigating any indication of non-compliance with this Policy.

12. APPROVAL, EFFECTIVE DATE AND UPDATING

This Policy shall enter into force on the date of its approval by the Board of Directors of El Corte Inglés, S.A.

This Policy shall be kept up to date over time. To this end, it shall be reviewed regularly, on an annual basis, and on an extraordinary basis where necessary, and in any event as promptly as possible in the event of changes to the Group's strategic objectives or to internal or external regulatory requirements that require its update or amendment.

Proposals for amendments shall be submitted to the Audit and Control Committee by the Corporate Finance Department, following validation by the Compliance and Risk Control Department and under the corresponding supervision of the internal control body entrusted with such function.

Where such changes are significant, they shall be submitted for approval to the Board of Directors, following a proposal from the Audit and Control Committee.

13. DISSEMINATION AND IMPLEMENTATION

Once approved by the Board of Directors of El Corte Inglés, S.A., this Policy shall be made available on NEXO for all Members of the Organisation and on the corporate website for all ECI Group stakeholders.

Likewise, the Information Security Committee shall be responsible for promoting the actions necessary to ensure the appropriate dissemination of and awareness of this Policy.

*Definition in Annex I

14. CONTROL, MONITORING AND SUPERVISION

14.1 Control and Monitoring

The Cyber Resilience Sub-Committee shall periodically assess compliance with and the effectiveness of this Policy through internal and external reviews, controls and audits coordinated by the Information Security and Cybersecurity Department, and shall report the results to the Information Security Committee.

The Information Security Committee shall be responsible for the ongoing supervision of the implementation of the provisions of this Policy by the Group companies.

14.2 Supervision

The Internal Audit Function shall review the adequacy and effectiveness of the measures implemented within the CRMS to supervise compliance with the regulations applicable to the different activities of the Organisation, to the extent that the Annual Audit Plan approved by the Audit and Control Committee includes work related to this System, and, on an extraordinary basis, as a result of the occurrence of incidents or the identification of irregularities. Following such audits, the Internal Audit Function shall issue the corresponding report, including recommendations where opportunities for improvement are identified.

Any opportunities for improvement that may be identified as a result of these reviews shall be considered as part of the continuous improvement process of the System.

The assessment of any potential breach of the Corporate Information Security Policy shall be determined in accordance with the applicable procedure and the provisions in force, without prejudice to any legal responsibilities, including disciplinary measures in the employment sphere, that may be applicable to the infringing party.

*Definition in Annex I

VERSION HISTORY

Version 1.0 approved by the Board of Directors on 29/Oct/2025

Version	Date of amendment	Purpose of the amendment	Sections affected
		-	-

Last revision, 29 October 2025

*Definition in Annex I

Annexes

Annex 1 - Definitions

Below are the definitions of the terms most frequently used in this document.

Availability: The ability of a service, system or process to be accessible and usable by authorised users or processes when required.

Confidentiality: The protection of data and systems to prevent threats such as unauthorised access or data leakage, which could result in the disclosure, alteration or destruction of sensitive information.

Crisis: Any event, incident or set of circumstances that seriously disrupts the availability or integrity of business processes, with an impact on the cyber domain, significantly affecting the Organisation's ability to operate normally and requiring an immediate and coordinated response to mitigate damage, restore critical functions and protect resources.

Cyber Resilience / Cybersecurity Resilience: The ability of an organisation to anticipate, resist, respond to and recover from adverse events, ensuring the continuity of its operations and the protection of its critical assets and resources against threats affecting the cyber domain.

Effective: Producing the expected effect. It refers to the result achieved, regardless of the means, time or resources used.

Efficacious: Achieving the intended objective. It focuses on attaining the result, without considering the cost or resources involved.

Efficient: Achieving an objective using the minimum possible resources (time, money, effort, etc.).

Event: Any identifiable occurrence within a system, network or technological environment that may be relevant to information security or the normal functioning of processes. An event does not necessarily imply a threat or damage but may indicate a potential incident or anomalous activity.

Information Asset: Any information or information processing system that has value for the organisation, including business processes, data, applications, IT equipment, personnel, information media, networks, auxiliary equipment or facilities.

Information Security: The set of technologies, practices and measures designed to protect the confidentiality, integrity and availability of information.

Information Security Policy: A high-level executive document through which a company establishes its guidelines, decisions and security measures regarding the protection of its information systems, following an assessment of the value of its assets and the risks to which they are exposed.

Integrity: The property of information that guarantees the accuracy of data during transmission or storage, ensuring that it has not been altered or lost.

Management System: A set of interrelated elements of an organisation that interact to establish policies, objectives and processes.

Resilience: The ability of an organisation to build, ensure and review its operational integrity and reliability in order to sustain the continuous delivery of services.

*Definition in Annex I

Resource: All assets (including infrastructure and equipment), people, skills, technology, premises, supplies and information that the Organisation must have available for use when necessary in order to operate and achieve its objectives.

Risk: The possibility that incidents or events may occur that compromise the confidentiality, integrity or availability of the Organisation's data and systems.

Security Incident: Any event that affects the confidentiality, integrity or availability of the company's information assets, including unauthorised or attempted access to systems, or the unauthorised use, disclosure, modification or destruction of information.

Threat: An unfavourable circumstance that may occur and which, if it materialises, has negative consequences for assets or resources, causing their unavailability, malfunction or loss of value.

*Definition in Annex I