INTEGRATED GOVERNANCE SYSTEM (SIGG)

Plain Concepts, S.L.U. and Plain Concepts Group companies

## DOC-02

# INTEGRATED LEADERSHIP AND GOVERNANCE POLICY AND FRAMEWORK

Normative document · Extension: CORE · Model layer: C2 · Governance core (direction and rules of the game)

| | |
|---|---|
| **VERSION**<br>1.1 | **VERSION DATE**<br>13/10/2026 |
| **STATUS**<br>Approved | **NEXT REVIEW**<br>12 months from approval |
| **DOCUMENT OWNER**<br>Integrated Management System (IMS) Directorate / Compliance · iso@plainconcepts.com | **APPROVED BY**<br>Senior Management |
| **CLASSIFICATION**<br>Public · general internal and external distribution | **SCOPE OF APPLICATION**<br>Plain Concepts, S.L.U. and subsidiaries; Ardanis Technologies Ltd. included in the certified scope |
| **OFFICIAL LOCATION**<br>Handbook / Teams / OneDrive / corporate SharePoint | **RETENTION**<br>While in force and for 6 years after replacement, unless a longer legal period applies |

# Document control

## Version history

| Version | Date | Author | Description of the change | Approved by |
|---|---|---|---|---|
| Rev. 03 | 26/09/2023 | Senior Management | 'Integrated System Policy': baseline document in force, setting out the vision, mission, ten corporate values and Senior Management's commitment. Published on the corporate website. | Enrique Martínez Alén (Senior Management) |
| 2.0 | 31/07/2026 | IMS Directorate / Compliance | Comprehensive review and expansion of Rev. 03: organisational context, intellectual property, transparency and accountability, governance and responsibilities, objectives and indicators, communication and training, ethics channel in accordance with Spanish Law 2/2023, and reorganisation of the regulatory framework. | Senior Management |
| 1.0 (SIGG) | 07/09/2026 | ISO controller | Incorporation of Integrated Policy v2.0 into the SIGG structure. | Senior Management |
| 1.1 (SIGG) | 13/10/2026 | IMS Directorate | Full integration of the content of Integrated Policy Rev. 04 that had not been carried over to v1.0: organisational context, scope, values, intellectual property, transparency, ethics channel, roles, objectives and indicators, communication and regulatory framework. Strengthening of the statement with the commitments required by the standards. Proposed risk appetite and decision-making structure. Removal of the template instructions. | Senior Management |

## Review and approval

| Action | Role / Body | Name | Date and signature |
|---|---|---|---|
| **Prepared by** | ISO controller | Natalia Domínguez Peña | |
| **Reviewed by** | Security Committee · Information Security Management Officer | Alejandro Casquete Prieto | |
| **Approved by** | Senior Management · CEO | Enrique Martínez Alén | Signed / Approved |

## Relationship with other SIGG documents

| Direction | Document / record | What is taken or delivered |
|---|---|---|
| **Relies on** | DOC-01 | Scope and integrated standards |
| **Relies on** | REG-04 | Context and expectations of interested parties |
| **Relies on** | REG-03 | Obligations the Policy commits to fulfil |
| **Feeds into** | REG-05 | Reference framework for setting objectives |
| **Feeds into** | DOC-04 | Risk appetite and criteria |
| **Feeds into** | All extensions | Subject-specific guidelines |
| **Relies on** | REG-01 | Bodies, delegations and named responsibilities |
| **Feeds into** | REG-08 | Evidence of communication and training on the Policy |
| **Feeds into** | REG-10 | Risk appetite and who accepts residual risk |
| **Feeds into** | REG-13 | Breaches of the Policy and outstanding gaps |

# Contents

**Document control** ..... **2**
Version history ..... 2
Review and approval ..... 2
Relationship with other SIGG documents ..... 3
**1. Management statement** ..... **5**
Who we are: organisational context ..... 5
Scope and application of the Policy ..... 6
**2. Governance principles** ..... **6**
Purpose and corporate values ..... 6
**3. Subject-specific guidelines** ..... **7**
Quality and client satisfaction ..... 7
Environment ..... 7
Compliance and conduct ..... 7
Information security ..... 8
Security within the scope of the ENS ..... 8
Privacy and data protection ..... 8
Artificial intelligence ..... 8
Occupational health and safety ..... 8
Business continuity ..... 9
Intellectual and industrial property ..... 9
Transparency and accountability ..... 9
**4. Risk appetite and tolerance criteria** ..... **9**
**5. Decision-making and delegation structure** ..... **10**
Roles and responsibilities ..... 11
**6. Commitments to interested parties** ..... **12**
Strategic objectives and performance indicators ..... 12
**7. Breach of the policy** ..... **13**
Ethics channel ..... 13
**8. Validity, distribution and review** ..... **14**
**Annex A. Regulatory traceability of this document** ..... **15**

# 1. Management statement

At Plain Concepts we drive the digital transformation of organisations around the world through software engineering, artificial intelligence, data, the cloud and emerging technologies. Our ambition is to be an organisation recognised for technological excellence, responsible innovation, digital trust and the ability to generate sustainable value for our clients, professionals, shareholders and society. We understand that sustainable growth is only possible when innovation is developed in accordance with principles of quality, security, privacy, professional ethics, protection of people, sustainability and regulatory compliance. Our purpose is to help organisations innovate, grow and transform their businesses through the responsible use of technology. The Group's Senior Management assumes ultimate responsibility for the effectiveness of the Integrated Management System and undertakes to provide the resources needed to maintain and improve it, to embed the principles of this Policy in the strategy and in operations, to promote a culture of excellence, responsible innovation and compliance, and to ensure that the Policy is communicated, understood and effectively applied. Everyone who is part of the Plain Concepts Group is responsible for actively contributing to compliance with this Policy.

As a concrete expression of this commitment, we undertake to satisfy the legal, contractual and interested-party requirements applicable to us and to continually improve the System; to protect the environment and prevent pollution; to protect the confidentiality, integrity and availability of information and the privacy of the personal data we process; to provide safe and healthy working conditions, eliminating hazards and reducing risks, with the consultation and participation of our professionals and their representatives; to fulfil our compliance obligations and foster a culture of integrity, actively supporting the Compliance function; to develop and use artificial intelligence responsibly; and to maintain the capability to continue delivering our services at acceptable levels in the event of a disruption.

| Signed by | Enrique Martínez Alén, CEO · Senior Management of the Plain Concepts Group |
|---|---|
| **Date** | Pending signature (version 1.1) |
| **Approved by** | Senior Management of the Plain Concepts Group |
| **Distribution** | Public. It is published on the internal corporate channels (Handbook, Teams, Factorial) and on the Group's public website, and is made available to clients, suppliers and other interested parties on request. |

## Who we are: organisational context

Plain Concepts was founded in 2006 by four Microsoft Most Valuable Professionals (MVPs) with the aim of building a leading technology company able to attract and retain top talent internationally. We define ourselves as a software engineering and technology consultancy boutique, committed to technical excellence, closeness and personalised service, placing people — clients and professionals — at the centre of the way we work.

The Group has an international presence in Germany, Spain, the United States, the Netherlands, the United Kingdom and Romania, and a workforce of more than 700 professionals spread across more than 26 delivery centres. Our activity is organised around four complementary business pillars:

- **Data:** organising, governing and exploiting data as the foundation of any transformation process.
- **Artificial Intelligence:** design and deployment of AI solutions applied to business processes, with active research and continuous monitoring of the state of the art.
- **Cloud:** cloud computing services focused on productivity, sustainability and the impact on the client's business.

- **Enterprise:** bespoke developments for unique needs for which no standard solution is available on the market.

Across more than 2,400 projects we have served organisations in banking and financial services, industry, energy, transport and public administration, among others, with an approach that is agnostic as to sectors and technologies; our clients include IBEX-35 companies, large multinationals and public bodies, and more than 90% of them return every year. We are a Microsoft Global Partner, with awards such as Partner of the Year in Azure, Artificial Intelligence, Mixed Reality and Power Platform, and we are progressively expanding our capabilities in AWS and Google Cloud Platform to offer a multicloud proposition. Inorganic growth — such as the integration of ApiumHub — and international expansion strengthen our position as a strategic innovation partner.

This context (markets, interested parties, capabilities and risks specific to the technology sector) is the basis on which the commitments of this Policy rest. Its detailed and up-to-date record is kept in REG-04.

### Scope and application of the Policy

The principles and commitments of this Policy constitute the general framework for action of the Plain Concepts Group and apply to all companies, subsidiaries, branches, permanent establishments, business units, workplaces, professionals and third parties acting on its behalf or under its direction, in any of the geographies in which we operate.

Specific requirements arising from standards, certifications, regulatory obligations or contractual commitments are applied in accordance with:

- The approved scopes of the management systems implemented at any given time.
- The activities and services carried out by each Group entity.
- The risks identified in each business line and geography.
- The legal and regulatory obligations applicable in each jurisdiction.
- The contractual requirements undertaken towards clients and third parties.
- The needs and expectations of the relevant interested parties.

## 2. Governance principles

- One piece of information, several views: a fact is recorded once and consulted from each regulatory perspective.
- Evidence prevails: an approval is not the same as conformity; compliance is demonstrated through verified evidence.
- Named accountability: every governed object has an identified owner.
- Proportionality: the intensity of control is proportionate to the risk and the impact, not uniform.
- Separation of execution and verification: whoever carries out an activity does not verify their own work.
- Informed decision-making: no governance decision is taken without the consolidated information produced by the system.

### Purpose and corporate values

Our purpose rests on a business model based on technical excellence and specialist knowledge; continuous innovation and client focus; digital trust and ethical, responsible conduct; talent development and

collaboration; and sustainability as a cross-cutting decision criterion. These principles are reflected in the corporate values that define how we act:

- **People First:** our main asset is the people who make up the team. We foster a flexible, inclusive and diverse working environment that supports professional development, wellbeing and collaboration.
- **Innovation:** we drive innovation as an engine of growth and competitiveness, continuously adapt to technological advances and support our clients in their transformation processes.
- **Quality:** we pursue excellence in everything we do, with highly qualified professionals and the continual improvement of our processes.
- **Agile collaboration:** we work on the basis of communication, trust and cooperation, with agile and effective models that promote transparency, adaptability and the achievement of shared objectives.
- **Transparency:** we act with integrity, honesty and responsibility, and maintain open communication with clients, employees, partners and other interested parties.
- **Sustainability:** we integrate environmental, social and governance criteria into decision-making to reduce our environmental impact and create long-term value.

# 3. Subject-specific guidelines

## Quality and client satisfaction

Clients are at the centre of our activity. We undertake to understand their objectives, needs and expectations; to design, develop and deliver services to the highest standards of professionalism and quality, in line with the principles of ISO 9001; to provide innovative solutions that contribute to their business objectives; to comply with the applicable contractual, regulatory and legal requirements; to maintain relationships based on trust, transparency and collaboration; and to foster the continual improvement of our processes, services and capabilities, systematically incorporating the voice of the client. Quality is a responsibility shared by everyone in the Group, regardless of their role, geography or business line.

## Environment

We recognise our responsibility towards the environment and future generations. We promote the responsible and efficient use of available resources; the progressive reduction of the environmental impacts associated with our activities, in line with ISO 14001; the integration of environmental criteria into decision-making where feasible and proportionate, including the energy efficiency of the cloud and AI solutions we design for our clients; raising our professionals' awareness of good environmental practice; and the continual improvement of our environmental performance.

## Compliance and conduct

Integrity is a non-negotiable element of the way we act. We act in accordance with the principles of the Code of Ethics and maintain a culture based on regulatory compliance, corporate responsibility and respect for our stakeholders. We undertake to comply with the applicable legislation in every country in which we operate; to maintain mechanisms for preventing, detecting and responding to irregular conduct; to identify, assess and manage compliance risks; to maintain a criminal risk prevention model; to apply proportionate due diligence in our relationships with clients, suppliers, partners and collaborators; to prevent fraud, corruption, bribery and conflicts of interest; and to promote a culture of zero tolerance towards any unlawful conduct, ensuring the protection of those who report in good faith. We also respect fundamental rights and the principles of responsible conduct, foster a culture of open communication that facilitates the early identification of risks

and breaches, and protect the trust and reputation of the Group. The ethics channel and the regime for breaches are described in section 7.

## Information security

Trust is one of the Group's main assets. We undertake to promote the responsible management of information and of the assets associated with the delivery of our services; to safeguard the confidentiality, integrity, availability and traceability of information in accordance with the risks identified and the obligations undertaken, in line with ISO/IEC 27001; to implement organisational, technical and contractual measures proportionate to the nature of the information; to maintain a corporate culture of awareness and information protection; and to continually improve our capabilities to respond to a constantly evolving technological environment. We also protect clients' confidential information by applying the need-to-know principle, with a duty of confidentiality that extends beyond the term of the contractual relationship. We honour the confidentiality commitments made to clients, partners and third parties and take reasonable measures to prevent unauthorised access to, or use, disclosure or retention of, confidential information.

## Security within the scope of the ENS

Plain Concepts, S.L.U. provides services to public sector entities and is one of only two organisations certified by the National Cryptologic Centre (CCN-CERT) to implement the guidelines of the Spanish National Security Framework (Esquema Nacional de Seguridad, ENS) on Microsoft 365 and Azure. The formal security policy required by the Framework is set out in artefact ENS-DOC-01, to which this Policy refers. Process FP01 provides the context and risk framework needed to comply with the ENS requirements in the applicable category.

## Privacy and data protection

We recognise that personal data are an especially sensitive asset whose protection is essential to safeguard people's rights and freedoms and the trust placed in our organisation. We process personal data lawfully, fairly, transparently and responsibly, in accordance with the GDPR and ISO/IEC 27701; we apply the principles of accountability and privacy by design where applicable; we integrate privacy risk management into the activities and services that require it; we adopt appropriate measures to protect data against unauthorised access, loss, alteration, disclosure or destruction; and we ensure that data are properly managed throughout their life cycle. The Group has an external Data Protection Officer (Leasba Consulting).

## Artificial intelligence

Innovation is part of our corporate identity and one of the Group's main growth engines, in line with our Artificial Intelligence business pillar. We promote the development and use of emerging technologies, including artificial intelligence systems, in a manner that is responsible, secure and aligned with our values and with the requirements of the EU Artificial Intelligence Act and ISO/IEC 42001. We integrate criteria of responsibility, quality, security and privacy into our innovation processes; consider risks and opportunities from the earliest design stages; promote governance mechanisms through the Regulatory Compliance Committee; and encourage human oversight, transparency and accountability. We inform users when they are interacting with an AI system and label synthetic or artificially generated content. We seek to adapt our practices to technological, regulatory and sector developments and drive innovation that contributes to the progress of our clients and of society.

## Occupational health and safety

People are the main driver of innovation and growth at Plain Concepts. We undertake to maintain safe, healthy, inclusive and respectful working environments, in line with the applicable principles of ISO 45001; to

promote the active participation of our professionals in improving the organisation; to support continuous learning and professional development; to foster a culture of collaboration, respect and responsibility; to manage risks to people's health and safety preventively; and to promote the physical, psychological and social wellbeing of our teams.

### Business continuity

We promote management based on risks and opportunities that enables us to protect our strategic objectives and strengthen our capacity to adapt. We support organisational and operational resilience through the Group's Business Continuity Plan, which defines the critical activities, risk scenarios, recovery objectives and response strategies, supported by high-availability cloud infrastructure, encrypted backups verified through quarterly restoration tests, a 'remote-first' working policy and redundant communication channels.

### Intellectual and industrial property

The development of software, proprietary products, methodologies and AI solutions makes intellectual and industrial property a strategic asset and a source of risk that must be actively managed. We undertake to protect the assets generated by the Group — software, proprietary products, methodologies, trade marks and other creations — through the appropriate legal mechanisms; to respect the rights of third parties, including clients, suppliers, technology partners and open-source communities; to set clear criteria on the ownership of intellectual property generated in client projects, as agreed in each contract; to manage open-source and third-party software licences responsibly, verifying their compatibility with what we develop; to pay particular attention to the risks associated with generative AI — the provenance of training data and the originality of code and content — before incorporating them into client deliverables; and not to tolerate the unauthorised use, reproduction or distribution of protected works, software or materials. This commitment complements, and does not replace, the duties of confidentiality, which are of a different legal nature.

### Transparency and accountability

Transparency is a core value of our culture of integrity and a condition of digital trust. We undertake to communicate truthfully, promptly and clearly with clients, professionals, shareholders, suppliers and society, avoiding misleading, ambiguous or incomplete information; to inform users when they are interacting with an AI system and to label synthetic content, in accordance with the transparency obligations of the EU Artificial Intelligence Act; to report diligently any security or privacy incidents that may affect clients or their data, in accordance with the applicable legislation and contracts; to cooperate transparently with authorities, regulators, clients and certification bodies; to identify, disclose and manage conflicts of interest; and to make relevant information on the performance of the System available to interested parties that require it, to the extent applicable and proportionate.

## 4. Risk appetite and tolerance criteria

We manage the System with an approach based on risks and opportunities: we periodically assess the relevant risks, consider the needs and expectations of interested parties, review the effectiveness of the System and take well-founded decisions proportionate to the context. Appetite is expressed against the residual risk level of the DOC-04 scale and is applied in REG-10.

| Risk category | Stated appetite | Tolerance threshold | What happens if it is exceeded | Who may accept the excess |
|---|---|---|---|---|
| Quality and client service | Low | Residual ≤ Medium | Treatment plan in REG-13 and escalation to the IMS Directorate | IMS Directorate; above High, Senior Management |
| Environmental and environmental legal compliance | Low; zero for legal non-compliance | Residual ≤ Medium; no legal non-compliance | Immediate treatment and notification to Senior Management | Senior Management (legal non-compliance is not accepted) |
| Regulatory compliance and conduct | Zero for unlawful conduct; low for the rest | No unlawful conduct tolerated; rest residual ≤ Low | Investigation by Compliance and notification to the Regulatory Compliance Committee | Not acceptable; rest, Regulatory Compliance Committee |
| Information security | Low | Residual ≤ Medium | Treatment plan and escalation to the Security Committee | Security Committee; above High, Senior Management |
| Privacy and data subjects' rights | Low | Residual ≤ Low in high-risk processing | DPIA, consultation with the DPO and escalation to the Regulatory Compliance Committee | Senior Management, with a report from the DPO |
| AI systems and fundamental rights | Zero for prohibited practices; low for the rest | No prohibited practice; rest residual ≤ Medium | Suspension of deployment and assessment by the Regulatory Compliance Committee | Regulatory Compliance Committee; high risk, Senior Management |
| Health and safety of people | Zero for serious consequences | No intolerable or significant risk without measures | Stoppage of the affected activity and immediate measures | Not acceptable |
| Operational continuity | Low | Within the recovery objectives of the Continuity Plan | Activation of the Continuity Plan and escalation to the Security Committee | Senior Management |
| Innovation and technology | Medium | Residual ≤ High, with security and privacy controls | Review of the business case and the controls | IMS Directorate; above High, Senior Management |
| Financial and reputational | Low | Residual ≤ Medium | Escalation to Senior Management | Senior Management |

# 5. Decision-making and delegation structure

Senior Management reserves the decisions that set the direction of the System and delegates their execution to the following bodies and roles; the named details of bodies, members and thresholds are kept in REG-01.

| Type of decision | Who decides | Who must be informed | Limit of delegation |
|---|---|---|---|
| Approval and amendment of this Policy | Senior Management | Everyone in the Group and interested parties | Not delegable |
| Risk appetite and acceptance of residual risk above appetite | Senior Management | Security Committee and Regulatory Compliance Committee | Not delegable |
| Acceptance of residual risk within appetite | Risk owner | IMS Directorate | Up to the tolerance threshold in section 4 |
| Annual System objectives and allocation of resources | Senior Management | IMS Directorate and area managers | Not delegable |
| Approval of normative documents (DOC) and extensions | Senior Management | IMS Directorate | Procedures and instructions: IMS Directorate |
| Deployment of high-risk AI systems | Senior Management, with a report from the Regulatory Compliance Committee | DPO and Security Committee | Other AI systems: Regulatory Compliance Committee |
| Management of serious security or privacy incidents and activation of continuity | Security Committee (crisis session) | Senior Management and DPO | Until the service is restored; thereafter, report to Senior Management |
| Investigation of ethics channel reports and resulting measures | Compliance Function | Regulatory Compliance Committee and Senior Management | Disciplinary measures: People Directorate, with a report from Compliance |

## Roles and responsibilities

The effectiveness of this Policy depends on a clear allocation of responsibilities at every level of the organisation:

| Role | Main responsibility |
|---|---|
| **Senior Management** | Approves the Policy, allocates resources and assumes ultimate responsibility for the effectiveness of the System. Embeds its principles in the strategy, drives continual improvement and actively supports the Compliance function and a culture based on integrity, legality and risk prevention. |
| **Integrated Management System (IMS) Directorate** | Coordinates the implementation, monitoring and continual improvement of the System across all the Group's geographies, and maintains, updates and distributes this Policy. |
| **Compliance Officer / Compliance Function** | Oversees the Code of Ethics, the Criminal Risk Prevention Model, the ethics channel and the management of compliance risks. |
| **Chief Information Security Officer (CISO)** | Leads the information security and cybersecurity strategy, including the relationship with the ENS and ISO/IEC 27001. |
| **Data Protection Officer (DPO)** | Monitors compliance with the GDPR and advises on privacy and personal data protection. |
| **Regulatory Compliance Committee** | Assesses the risks and regulatory compliance of the artificial intelligence systems developed or used by the Group, in accordance with the EU AI Act and ISO/IEC 42001. |
| **Area, business unit or project managers** | Apply the principles of this Policy within their remit and pass its requirements on to clients, suppliers and teams. |
| **Everyone in the Group** | Know, understand and apply this Policy in their day-to-day work and report any risk or breach they detect. |

# 6. Commitments to interested parties

| Interested party | Commitment undertaken | How it is demonstrated | Where it is published |
|---|---|---|---|
| **Clients** | Design, develop and deliver services to the highest quality standards; comply with contractual, regulatory and legal requirements; protect the confidential information entrusted to us; report diligently any security or privacy incidents that may affect them. | Satisfaction index and NPS surveys; client retention rate; compliance with contractual deadlines and requirements; certifications in force. | Contracts, service level agreements, corporate website and supplier approval processes |
| **People in the Group** | Maintain safe, healthy, inclusive and respectful working environments; support continuous learning and professional development; promote active participation in improving the organisation. | Workplace climate and wellbeing surveys; participation in training; voluntary turnover below 15%. | Handbook, Factorial, Teams and All Hands sessions |
| **Shareholders** | Reporting and alignment of annual objectives; compliance with the budget; information on climate risks, ESG compliance and environmental performance. | Strategic plan, management review and Non-Financial Information Statement. | Corporate reporting and Non-Financial Information Statement (EINF) |
| **Suppliers and partners** | Apply proportionate due diligence measures; pass on the requirements of the system; honour confidentiality commitments. | Supplier evaluation and re-evaluation; percentage of strategic suppliers with environmental certification. | Contracts and purchasing processes (FP13) |
| **Public authorities and supervisory bodies** | Comply with the applicable legislation in every country in which we operate; cooperate transparently with authorities, regulators and certification bodies. | Register of external communications; audits and approvals passed; CCN-CERT certification on the ENS. | Each body's electronic office and register of communications |
| **Society** | Responsible innovation; transparency on the use of artificial intelligence; progressive reduction of environmental impact. | Non-Financial Information Statement; ESG indicators; UN Global Compact communications. | Corporate website and Non-Financial Information Statement (EINF) |

## Strategic objectives and performance indicators

This Policy is deployed through specific, measurable objectives, reviewed annually and recorded in REG-05. By way of guidance, each area has objectives and indicators such as the following:

- **Quality and client satisfaction:** level of satisfaction and compliance with contractual deadlines and requirements.
- **Information security:** number and impact of incidents, response time and closure of vulnerabilities, and progress of the ENS and ISO/IEC 27001 certifications.
- **Privacy:** personal data breaches notified and average time taken to handle data subjects' rights requests.

- **Responsible artificial intelligence:** percentage of AI projects assessed by the Regulatory Compliance Committee before deployment.
- **People:** participation in training, results of workplace climate and wellbeing surveys, and health and safety indicators.
- **Sustainability:** trend in resource consumption and in the Group's environmental footprint.
- **Compliance:** reports received through the ethics channel and average resolution time.

The specific objectives, their annual targets and the results are reviewed in the management review of the System.

# 7. Breach of the policy

Breaches of this Policy, of the Code of Ethics or of the applicable legislation are handled in accordance with the Code of Ethics and the Group's Compliance Model. Every report received through the ethics channel is analysed and, where appropriate, investigated by the Compliance function, within the response times laid down in the corresponding internal procedure, ensuring protection against retaliation for those who report in good faith.

For people in the Group, a breach may give rise to the disciplinary measures provided for in the employment legislation and collective agreement applicable in each jurisdiction; for clients, suppliers and other third parties, to the measures provided for in the contract, including its termination. Breaches detected are recorded and handled in REG-13.

## Ethics channel

The Group has an ethics reporting channel, in accordance with Spanish Law 2/2023 on the protection of persons who report regulatory breaches and on the fight against corruption, through which anyone may report in good faith possible breaches of this Policy, of the Code of Ethics or of the applicable legislation.

- It is available to employees, clients, suppliers and other third parties related to the Group.
- Reports are handled confidentially and, where the applicable legislation so provides, may be submitted anonymously.
- Protection against retaliation is guaranteed for those who report in good faith, in accordance with the Code of Ethics and the Group's Compliance Model.
- Every report is analysed and, where appropriate, investigated by the Compliance function within the time limits of the corresponding internal procedure.

# 8. Validity, distribution and review

| Entry into force | From its approval and signature |
|---|---|
| **Review frequency** | Annual |
| **Triggers for extraordinary review** | Significant changes in the Group's strategy, its operating context, the needs of its interested parties or the applicable legal, regulatory or normative requirements |
| **Internal distribution channels** | Handbook, Teams, Factorial, corporate email, All Hands sessions and onboarding processes for new joiners. It is adapted and, where necessary, translated into the main languages of the Group's geographies to ensure it is understood |
| **External availability** | The Policy is a public document in its entirety and is published on the Group's corporate website |
| **Evidence of communication** | Periodic training adapted to each person's role, with particular attention to those who handle client information, personal data or AI systems. Evidence of senior management and employee training from December 2025 in REG-08. |
| **Approval of revisions** | Every revision is approved by Senior Management and communicated through the channels indicated |
| **Ownership and custody** | Integrated Management System Directorate, which ensures its custody, updating and distribution |
| **Controlled version** | The version in force is the one published on the official corporate channels; any printed copy is considered uncontrolled |

# Annex A. Regulatory traceability of this document

This Policy forms part of the Group's Governance, Risk and Compliance (GRC) System and complements the Code of Ethics, the Criminal Risk Prevention Model and the Information Security, Privacy, Artificial Intelligence, Human Resources and Environmental policies, among other corporate rules that develop its principles. Its content is aligned with the following standards and frameworks.

| Standard / framework | Requirement or clause | How this document satisfies it | Status |
|---|---|---|---|
| ISO 9001:2015 | 5.2.1, 5.2.2 | Establishing, communicating and making available the quality policy. | Covered |
| ISO 14001:2015 | 5.2 | Environmental policy with its mandatory commitments. | Covered |
| ISO/IEC 27001:2022 | 5.2, 6.1.2 a); A.5.1 | Information security policy, risk criteria and topic-specific policies. | Covered |
| ISO/IEC 27701:2019 | 5.2 | Extension of the policy to the protection of personal information. | Covered |
| ISO/IEC 42001:2023 | 5.2; A.2 | AI policy and related policies. | Covered |
| ISO 37301:2021 | 5.2, 4.6 | Compliance policy, obligations and compliance risk appetite. | Partial |
| ISO 45001:2018 | 5.2 | OH&S policy, including the commitments to consultation and participation. | Partial |
| ISO 22301:2019 | 5.2 | Business continuity policy. | Partial |
| ENS (Royal Decree 311/2022) | Art. 12; org.1 | Security policy approved by the competent body. | Partial |
| GDPR (EU 2016/679) | Art. 24.2 | Implementation of appropriate data protection policies. | Covered |
| Cyber Essentials | Certification scheme (United Kingdom) | Section 3, Information security: general protection commitment. | Partial |
| Directive (EU) 2022/2555 (NIS2) | Arts. 20 and 21, to the extent applicable | Sections 3, 4 and 5: cybersecurity governance and risk management. | Partial |
| Regulation (EU) 2024/1689 (AI Act) | Art. 50 | Section 3, Artificial intelligence and Transparency: information and labelling. | Partial |
| Spanish Law 2/2023 | Art. 5.2 h) | Section 7: principles of the internal reporting system and whistleblower protection. | Partial |
| Consolidated Text of the Spanish Intellectual Property Act (Royal Legislative Decree 1/1996) | Book I, Title VII (computer programs) | Section 3, Intellectual and industrial property. | Partial |

| Standard / framework | Requirement or clause | How this document satisfies it | Status |
|---|---|---|---|
| Directive (EU) 2019/790 (copyright in the Digital Single Market) | Arts. 3 and 4 (text and data mining) | Section 3, Intellectual and industrial property: AI training data. | Partial |
| UNE 19601:2017 | 5.2 | Sections 3 (Compliance and conduct) and 7. | Partial |
| Group Code of Ethics and Compliance Model | Internal integrity framework | Sections 3, 5 and 7. | Covered |