INFORMATION SECURITY BUSINESS CONTINUITY AND PRIVACY POLICY

10 February 2026

Firmado digitalmente por LOGALTY PRUEBA POR INTERPOSICION SL
Fecha: 2026.02.11 10:24:38 +01'00'

GENERAL INFORMATION

Type	**General Policy** Specific Policy Procedure Technical Instruction Plan Template
Classification	**Public** Confidential Internal Use
Version	V.1
Status	Draft in progress **Approved** Withdrawn

VERSION HISTORY

Version	Approval date	Section and changes	Author
V.1	22.07.2024	First version	GRC MANAGER
V.1	09.02.2026	Reviewed, no changes applied.	GRC MANAGER

Table of Contents

1 INTRODUCTION

The LOGALTY GROUP, as a Trust Service Provider, recognises the importance of protecting our customers' information, ensuring the availability of our services at all times and complying with constantly evolving data privacy regulations.

The Group understands that while technology offers opportunities and benefits, it also exposes us to a number of challenges and risks that are inherent to an increasingly complex and dynamic digital environment. We are aware that a proactive and holistic approach to information security, business continuity and data privacy is essential to protect our most valuable assets and ensure the long-term sustainability and excellence of our operations.

The Group has therefore adopted this Policy, which should serve as a benchmark for decision-making at all levels and units that comprise the Group and guide the behaviour of employees, executives and directors in their internal and external relations.

2 PURPOSE

The purpose of this Policy is to ensure the protection, integrity and confidentiality of the company's information, as well as to establish measures for business continuity and to ensure compliance with data privacy in all the Group's activities.

The Logalty Group Information Security, Business Continuity and Privacy Policy (hereinafter, the 'Policy') sets forth the principles and guidelines to protect information, ensure continuity of operations, and oversee and continuously improve security across all areas of the organisation. This Policy represents a key commitment by senior management to safeguard the confidentiality, integrity and availability of information, comply with legal and regulatory requirements, ensure business resilience and foster a strong security culture.

3 SCOPE OF APPLICATION

This Policy applies to all employees, contractors, suppliers and any other entity that has access to, processes, stores or transfers information on behalf of the Logalty Group or any of the organisations belonging to the Group.

The scope of application also includes all information systems, data assets and technological resources used by Group companies, either internally on their premises or externally in remote environments, such as the cloud or third-party services. Furthermore, it extends to all geographic locations where the company operates, regardless of local or regional jurisdictions.

4 APPLICABLE REGULATIONS

In preparing this Policy as well as other documents, procedures or instructions related to information security, business continuity and privacy, the current regulations applicable to each field will be taken into account, as well as international standards of good practice and applicable internal regulations.

5 GOVERNANCE FRAMEWORK

The HR Department will be responsible for assigning the roles related to information security, business continuity and privacy to each employee, ensuring that they are aware of and accept each assigned role.

5.1 Board of Directors

The Board of Directors of the Logalty Group plays a crucial role in the oversight and strategic direction of the company, and is therefore ultimately responsible for overseeing compliance with this Policy. The Board also participates in shaping the Group's vision and financial strategy, ensuring that it is aligned with long-term goals and takes into account the interests of all stakeholders.

5.2 Executive Committee

The Executive Committee, as the Group's supreme executive body, has the duty to oversee and provide the necessary support for the implementation and enforcement of the Policy.

This is why its primary functions are as follows:

- Define and approve information security, business continuity and privacy goals.
- Oversee compliance with security, business continuity and privacy regulations.
- Allocate the necessary financial and human resources to ensure compliance.
- Ensure the establishment of policies and goals that are compatible with the organisation's strategic direction with regard to information security, business continuity and privacy.
- Ensure that the requirements of the management system are integrated within the Group's processes.
- Monitor and oversee the effectiveness of the management system.

5.3 Continuity, Risk and Security Committee (CRS Committee)

The organisation has a specific committee to manage the continuity, risk and security of the Logalty Group (CRS Committee), in which the Executive Committee participates. The CRS Committee is ultimately responsible for the design and implementation strategy of the information security, continuity and privacy programme and cannot delegate this responsibility to others. Its main functions are:

- Propose a security, continuity and privacy strategy, aligned with the business strategy.
- Approve and periodically review the associated policies, plans and procedures.
- Collect and analyse data relating to the performance and level of compliance of the security, continuity and privacy management system, the risk management process, and the security controls and measures adopted.
- Monitor the main deviations and security breaches, analysing and proposing possible areas for improvement in security processes and controls.
- Promote periodic audits to verify compliance with the organisation's security obligations.
- Report regularly on the status of information security, continuity and privacy to management, as well as any deviations or security breaches.

- Promote continuous improvement, communication and training for employees, in order to prevent security, continuity and privacy risks.

The CRS Committee must meet on a quarterly basis, and extraordinarily whenever required.

5.4 Chief Information Security Officer (CISO)

The CISO, together with his/her team, is responsible for leading the organisation's information security strategy, overseeing the implementation of security controls, identifying and assessing security risks, and coordinating responses to security incidents, inter alia.

5.5 Business Continuity Manager (BCM)

The BCM, together with his/her team, is responsible for ensuring the business continuity of the organisation, identifying critical business processes and functions and developing plans to maintain and quickly re-establish or restore operations in the event of disruption, managing the associated risks and ensuring organisational resilience.

5.6 Data Protection Officer (DPO)

The DPO is responsible for overseeing compliance with data protection and privacy regulations and privacy policies within the Group, providing advice on data protection issues and performing data protection impact assessments, as well as cooperating and acting as a liaison with the data protection supervisory authority.

5.7 Other roles

The Logalty Group has also appointed certain roles that are of significant importance within the information security, continuity and privacy management system:

- **Information and Service Manager:** They will determine the requirements for the information processed and the requirements for the services provided.
- **System Manager:** They will be tasked with developing the specific way in which security is implemented in the system and with overseeing the day-to-day operation of the system, and may delegate tasks to administrators or operators under their responsibility.
- **Internal Auditor:** They will be responsible for performing the annual internal audit of the integrated security and continuity management system and submitting the findings to the CRS Committee.

6 PRINCIPLES OF ACTION

This Policy outlines the principles that the Group considers essential in the management and processing of information, both in its internal processes and in the services and business processes provided to its customers. These principles are:

1. We conceive security as a **comprehensive process**, consisting of all technical, human, material and organisational elements related to information systems.
2. We perform **risk**-based security, continuity and privacy management, keeping the analysis constantly up to date.
3. We implement **prevention, reaction and recovery** measures to protect against undesired security incidents.

4. We **regularly reassess** the security, business continuity and privacy measures adopted and their effectiveness.
5. We view security as a distinct function, deploying **resources and efforts in addition** to those required for the provision of the service.
6. We ensure the availability of critical information and systems to support business operations, implementing redundancy measures and continuity plans to minimise the impact of disruptions.
7. **We understand that legal compliance is the cornerstone of business activity and therefore the Group takes all the necessary actions to comply with** laws, regulations and contractual requirements related to information security, business continuity and data privacy.
8. We communicate and conduct internal training on an ongoing basis.

The Group also undertakes the commitment to establish annual goals for the improvement of information security, business continuity and privacy processes, duly documented and reviewed.

7 REPORTING FRAMEWORK

Establishing an appropriate reporting framework is critical to meeting the Logalty Group's security, continuity and privacy commitments.

The main goals of the reporting framework are as follows:

- Provide senior management and the Board of Directors with accurate, clear and adequate information in a timely manner, in order to facilitate decision-making and verify compliance with the proposed goals.
- Respond to requests for information from supervisory bodies, if any.
- Provide the heads of the different departments and the control areas with the necessary data to be able to monitor compliance with the strategy defined within the Group in relation to security, continuity and privacy.

In this regard, the Management Committee will receive regular information on:

- The strategy adopted in relation to information security, business continuity and privacy.
- Corrective actions to be implemented or improvements affecting the business strategy.
- Breaches detected or vulnerabilities, as well as the corrective plan.
- Regulatory changes that significantly affect the processes already implemented in relation to information security, business continuity or privacy.

8 REVIEW AND CONTINUOUS IMPROVEMENT

In compliance with the Code of Ethics approved by the Group's Board of Directors, this Policy will be reviewed when:

- There is a change in the applicable regulations.
- Adaptations to recommendations made by a competent authority are required.
- Where the Group wishes to make improvements and/or clarifications to the document.

- In any case, the Policy will be reviewed annually.

Any revisions and/or updates must be approved by the appropriate body and effectively notified to staff if such changes are material to the understanding of this Policy. Updates purely for formatting purposes or for the correction of errata will not be notified.

9 PUBLICATION, COMMUNICATION AND TRAINING

This Policy must be public and accessible to all employees of the Group. The organisation will effectively inform the entire workforce and this communication may be published on the website(s) of all the companies that comprise the Logalty Group.

In addition, those employees who use or whose duties specifically require them to address the obligations of this Policy will receive specific training to ensure that they are properly informed with regard to all aspects of this document.

10 APPROVAL AND VALIDITY

This text has been approved by the Executive Chairwoman on behalf of the Board of Directors and after ratification by the Executive Committee. This Information Security, Business Continuity and Privacy Policy is effective from the date of approval until it is replaced by a new policy.