Information Security and Business Continuity Policy

28 November 2023

1 Introduction

The LOGALTY GROUP Information Security and Business Continuity Policy establishes principles and guidelines for protection of information, ensuring continuity of operations and supervision and continuous improvement of security across all areas of the organisation. This policy represents senior management's fundamental commitment to safeguarding the confidentiality, integrity and availability of information, complying with the requirements of laws and regulations, ensuring business resilience and encouraging a strong security culture.

2 Scope

This policy applies to all employees, contractors, suppliers and any other entity that accesses, processes, stores or transfers information on behalf of the LOGALTY GROUP or any of the organisations belonging to the group.

3 Principles

This policy outlines the principles that the company deems essential with regard to information management and processing in its internal processes as well as in the services and business processes provided to its clients. These principles are:

- **Confidentiality**: We are committed to protecting confidential information from unauthorised disclosure. Confidential information will only be disclosed to authorised parties and for legitimate purposes.
- **Integrity**: We will maintain the precision and integrity of the information throughout its life cycle. We will implement controls to prevent unauthorised or wrongful modification of the information.
- **Availability**: We will guarantee the availability of the information and the critical systems supporting commercial transactions. We will implement redundancy measures and continuity plans to minimise the impact of interruptions.
- **Authentication**: We will establish sound authentication mechanisms to ensure that only authorised parties have access to the information and systems. We will implement appropriate authentication methods, including secure passwords, two-factor authentication and other controls.
- **Traceability**: We will keep detailed records of activities and events related to information security. The records will make it possible to monitor and review actions carried out by users and systems, contributing to the detection and early response to incidents.
- **Legal compliance**: We will comply with all laws, regulations and contract conditions related to information security, business continuity and data privacy.

In addition to the above, we also adhere to the following principles aligned with the National Security Framework (ENS):

- **Security as an integral process** composed of all the technical, human, material and organisational elements related to information systems.
- **Risk-based security management**, keeping the analysis constantly up to date.
- **Prevention, reaction and recovery** in response to undesired security events.
- **Regular reassessment of security and its efficacy**.
- **Security as a distinct function**, dedicating resources and efforts in addition to those required to provide the service.

4 Leadership

The organisation will create a specific committee to manage Continuity, Risk and Security (CRS Committee) in the Logalty Group. Members of senior management will take part in this committee.

Through the CRS Committee, the company's senior management shows its clear leadership and commitment to the management system and to information security,

a) ensuring that the policies and objectives set are compatible with the organisation's strategic focus

b) ensuring that the requirements of the management system are integrated into the processes

c) ensuring that the resources needed for the management system are available

d) communicating the importance of effective continuity and information security

e) ensuring that the management system achieves the expected results

f) leading and supporting people in order to render the management system more effective, and

g) promoting continuous improvement

With respect to the responsibilities indicated in the GDPR, the CRS Committee will act as data controller for its own data and as data processor for the data of its service clients.

5 Roles and Responsibilities

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

All employees and contractors must comply with the established security measures, report any security incidents and participate in training and awareness sessions about security.

In the field of information security, the most significant roles are:

- CISO (Chief Information Security Officer): The CISO is responsible for leading the organisation's information security strategy, overseeing implementation of security controls, identifying and evaluating security risks, coordinating responses to security incidents and leading the business continuity planning.
- DPO (Data Protection Officer): The DPO is responsible for ensuring compliance with data protection and privacy laws, providing advice on matters related to data protection, overseeing the handling of personal data and acting as a liaison with the data protection authorities.
- Information and Service Manager: This person determines the requirements of the information processed and the requirements of the services provided.
- System Manager: This person is entrusted with developing the specific way in which security is implemented in the system and supervising the daily operation of the system, and may delegate tasks to administrators or operators in their charge.
- Internal Auditor: The person tasked with conducting the annual internal audit of the integrated security management and continuity system and submitting the findings to the CRS Committee.

These five roles defined by the organisation cannot be assigned to the same people, nor can there be any hierarchical ties between them that might limit the independence of their functions. These five roles shall be members of the CRS Committee.

6 Risk Management and Business Continuity

We will regularly identify and evaluate information security risks and risks related to business continuity. We will take measures to effectively mitigate them and develop continuity plans for critical scenarios.

The appraisal of information security risks and processing procedures must be aligned with the principles and general guidelines defined in ISO standard 31000 and the MAGERIT Methodology.

We will established adequate security controls based on a risk assessment to protect the information assets.

7 Frameworks of Reference

We will use ISO 27001, ISO 22301, the National Security Framework (ENS), the General Data Protection Regulation (GDPR), the NIS Directive, the DORA Regulation and the eiDAS Regulation as our frameworks of reference for ensuring information security and business continuity.

8 Prevention

Each area of the organisation must hinder, or at least prevent to the extent possible, information or services from being damaged by security incidents. To this end, adequate security controls and measures will be implemented. These controls, and the security roles and responsibilities of each staff member, must be clearly defined and documented. In this regard, the following practices are deemed relevant:

- Establishing mechanisms for authorising changes, assigning access and privileges and going from information systems to production.
- Regularly evaluating the security.
- Asking third parties for regular assessments in order to gain independent perspectives.

9 Detection

Operations must be monitored constantly to detect anomalies in service provision levels and to respond appropriately. Therefore, this policy establishes the need to create mechanisms for the detection, analysis and reporting to be submitted to the managers regularly or whenever a significant deviation is found in the parameters originally deemed normal.

10 Response

Processes will be defined and resources and tools allocated in order to effectively respond to security events and incidents.

The operating processes and procedures developed must provide this capability in a manner that is proportional to the critical nature of the affected systems and information.

11 Security incident management

Procedures will be in place to manage security incidents and weaknesses detected in the information security system. These procedures will define the detection mechanisms, classification criteria, analysis and resolution procedures, the stakeholder communication channels and records of the actions taken. These records will be used to continuously improve the system security. In particular, resources will be dedicated to detecting and reacting to malicious code.

12 Monitoring and Improvement

We will periodically review and audit the security controls and continuity plans to ensure that they are effective and adequate.

We will constantly improve our security and continuity processes based on the findings of the reviews and changes in the threat environment.

13 Communication and Awareness

We will regularly communicate details regarding information security, resilience and business continuity. We will provide training to ensure that everyone involved understands and complies with this policy.

14 Breaches of the Policy

A breach of this information security and business continuity policy may give rise to disciplinary action.

15 Approval and Updates

This policy will be approved by the CSR Committee and reviewed and updated annually as necessary to ensure that it remains relevant and effective.