Summary of the Information and Cybersecurity Policy

CIRIONTECHNOLOGIES.COM

1. Objective

This Policy, as well as the regulatory framework that supports it, aims to protect information assets against unauthorized or accidental modification, disclosure, or destruction, and to ensure the general security principles of confidentiality, integrity, and availability.

2. References for the Preparation of this document

- **ISO/IEC 27001:2022** Information security, cybersecurity and privacy protection — Information security management systems — Requirements
- **ISO/IEC 27002:2022** Information security, cybersecurity and privacy protection — Information security controls
- **ISO 22301:2019** Security and resilience — Business continuity management systems — Requirements
- **CIS Controls v8** – Center for Internet Security Critical Security Controls for Effective Cyber Defense
- **ITIL® 4 – ITIL Foundation**, AXELOS Global Best Practice
- **Anatel Resolution Nº 740**, dated December 21, 2020
- The **NIST Cybersecurity Framework** (CSF) 2.0
- **Sarbanes-Oxley Act of 2002 (SOX)**, Public Law 107–204
- Payment Card Industry Data Security Standard (**PCI DSS**) v4.0, PCI Security Standards Council, 2022

This policy is aligned with the main global data protection standards, considering the legal frameworks in the countries where the company operates.

3. Responsabilities

Information Security and Cybersecurity are shared responsibilities across the entire organization. However, the Cybersecurity Directorate is responsible for ensuring the implementation, maintenance, and continuous evolution of applicable security strategies, policies, standards, and controls.

4. Awareness Actions

Through its organizational policies and procedures, Cirion aims to raise awareness among all employees to maintain a solid information security structure.

Currently, mandatory internal training sessions are conducted to disseminate and promote awareness of information security. Additionally, campaigns simulating security risks and threats are carried out. For external audiences, Cirion publishes content on social media and its website addressing cybersecurity topics from various perspectives.

5. General Guidelines for Security Procedures and Controls

5.1 Classification and Asset Control

Information shall be classified based on its criticality and confidentiality level. As a result of this process and according to its function, it must be managed and labeled to guarantee the appropriate protection level and prevent exposure beyond what is necessary for normal task performance.

5.2 Risk Management

The organization must establish a continuous and systematic process for managing information security risks, following ISO/IEC 27001 best practices (and specific standards such as ISO 27005). The goal is to proactively identify and assess risks that may affect information and systems to address them timely.

5.3 Logical Security and Access Control

Logical security includes mechanisms and controls to protect IT systems, applications, and data against unauthorized access or malicious activities. A core element is access control, ensuring each user or system obtains only the permissions needed for their functions and nothing more (principle of least privilege).

All systems storing or processing information must have strictly controlled access. The required access control level for a system storing or processing information or for a specific resource is determined by the potential business impact.

5.4 Network and Communications Security

The network and communications infrastructure is the backbone on which the company's information flows. Therefore, security measures must be implemented to protect internal, perimeter, and data communications networks against unauthorized access, interception, or disruption.

Controls to manage risks for information transmitted over Cirion's networks or the internet must comply with established security standards.

5.5 Business Continuity and Disaster Recovery

Measures must be defined to ensure Business Continuity in situations that affect or interrupt Cirion's normal service performance. This provides a systematic framework to prepare for, respond to, and recover from large-scale incidents caused by natural disasters, catastrophic technological failures, high-impact cyberattacks, or other crises.

5.6 Regulatory Compliance and Personal Data Protection

Legal and regulatory requirements related to information security and personal data protection must be identified and incorporated into security policies, technology service design and implementation, and audit practices. All personnel must understand and comply with applicable contractual terms.

Any personal data breach must be reported promptly, observing the guidelines and legal requirements established in data protection laws applicable in countries where the company operates.

5.7 Vulnerability Management

The company must maintain a structured vulnerability management process aimed at reducing risks associated with security weaknesses in information assets, including vulnerability identification, assessment, risk prioritization, treatment and correction, monitoring, and documentation.

5.8 Supplier Relationship

All agreements with suppliers and service providers must contain clauses obliging them to comply with the Information Security and Cybersecurity Policy.

5.9 Security Incident Management

Procedures and mechanisms must be defined to manage security incidents to minimize their impact. These must involve collaboration of areas that may be part of the process in prevention, detection, containment, and response stages, as well as continuous improvement and learning.

Personnel must report suspicious or unusual activities that may threaten Cirion's information assets, unauthorized access to customer or employee information, or any other suspected information security incident.

6. Incident Notification

Incidents may be logged in the company's ITSM tool or notified via email <Security.Incidents@ciriontechnologies.com>. Incidents classified as critical must be immediately reported to the competent regulatory bodies via the designated official platform.

If the incident involves the compromise of personal data, the guidelines and legal requirements established in the data protection laws applicable in the countries where the company operates must be observed and followed — for example, the General Data Protection Law (Law No. 13.709/2018 – Brazil).

7. Contact

Any knowledge of a security breach must be immediately reported to the immediate supervisor (if applicable) and to the Information Security area via the email <Security.Incidents@ciriontechnologies.com>. In addition, the corresponding Service Desk phone number for the country where the company operates may be used.

8. Approvals

The extract of the General Information Security and Cybersecurity Policy was approved by the company's CISO on July 8, 2025.