INFORMATION SECURITY POLICY

VERSION 2.0

March, 2024

TABLE OF CONTENTS

1. Definitions

CI&T: all references to "CI&T" include CI&T Inc as well as all CI&T Group companies.

CI&T PERSONS: direct or indirect collaborators, including, but not limited to, people under the labor contracting regime, people who hold positions of officer or board members. This definition will also include people who act as third parties hired by CI&T, such as consultants or freelancers.

CODE OF ETHICS AND CONDUCT: it clarifies an organization's mission, culture, values, and principles, linking them to standards of professional conduct. The Code articulates the values that the organization wants to promote in leaders, in our people, and, by doing so, defines the desired behavior. As a result, codes of ethics and conduct become benchmarks by which individual and organizational performance can be measured.

INFORMATION SECURITY POLICY (ISP): it is a set of standards and guidelines to maintain the integrity, availability, and confidentiality of information.

MATERIAL INCIDENTS: there are incidents with a substantial likelihood that a reasonable shareholder would consider them important when making an investment decision or if this shareholder understands that the incidents significantly alter the total set of information available in the market about CI&T. Their assessment should take into account all relevant facts and circumstances, which may involve the consideration of both quantitative and qualitative factors.

2. Objective

All of our people, partners and suppliers have the responsibility to protect CI&T and its culture against information security threats, adding value to our business, reducing the possibilities of loss and ensuring its sustainability. Therefore, CI&T is committed to having a secure company environment, compatible with our brand credibility due to the high level of trust bestowed upon us by each of our clients through CI&T processes and teams.

This Policy is mainly intended to guide CI&T persons on every aspect that makes this type of relationship possible: business decisions, protection of CI&T image, protection of company and client information, security at the workplace and especially the behavior expected from our people, suppliers and vendors.

3. Applicability

The guidelines in this document should be known and followed by all CI&T persons, partners and suppliers and anyone who is at any of our CI&T offices. It is everyone's responsibility to ensure that everyone follows the security directives set forth in this Policy.

4. Directives

4.1. General Principles

CI&T is committed to the security and integrity of data, which is why some general guidelines are applied for the protection and use of systems and information, always guaranteeing the integrity of the technological infrastructure and in compliance with the laws and regulations that are in force in each locality:

- Protect data against unauthorized access, as well as unauthorized alteration, destruction or disclosure;

- Guarantee the availability and continuity of technological services and information processing against any security breaches which may impair the organization's performance;

- Ensure that the systems and data under its responsibility are properly protected and are used only for the fulfillment of its duties;

- Preserve the integrity of the technological infrastructure where data is stored, processed or treated in any other way, adopting the necessary measures to prevent logical threats, such as viruses, harmful programs or vulnerabilities that may lead to unauthorized access, manipulation or use of internal and confidential data.

- Continuously improve security and information technology processes and provide the necessary resources for this;

- Comply with the laws and regulations that regulate the company's activities.

In addition to the protection measures mentioned above, a highlight is that the company must have a Disaster Recovery Plan (DRP) implemented and regularly tested, with the participation of all areas involved. This ensures that, in the event of incidents that could compromise the technological infrastructure and business continuity, effective procedures are in place for the quick and safe recovery of critical operations, keeping our commitment to information security and the trust of our customers.

Access management is one of our company's priority areas, aiming to ensure that only authorized users have access to information and systems relevant to the performance of their duties. For this, we have

tools and procedures that allow the creation, modification and deletion of accesses in a controlled manner, according to the needs of each area and user profile. In addition, we carry out periodic reviews of the accesses granted, in order to ensure that they are in compliance with internal policies and applicable regulations. With these measures, we seek to mitigate the risks of improper access, information leakage and other threats to information security.
This is all done through the principle of need-to-know and least privileges, that is, granting only the necessary permissions so that the user can perform their tasks. This approach helps to reduce the risk of unauthorized access and leakage of confidential information, thus ensuring the security of the organization's data.

In terms of physical security, controlled access and security measures are adopted for the facilities. Good security practices are also adopted to ensure proper operating conditions for equipment and data conservation. These measures are essential for protecting our people, physical assets and company data, as well as for the continuity of critical operations.

4.2. Actions Performed

- All CI&T Persons and suppliers of CI&T have the responsibility to protect CI&T against threats and, thus, reduce the possibilities of losses and guarantee the sustainability of the business.

- Significant updates will be made available through CI&T's official communication channels, and we encourage everyone to review them frequently for continuous updates on our protection practices.
  Our information security team is prepared to act in:

- **Prevention**, through traditional security controls and safeguards,
- **Monitoring**, with the continuous review of events and alerts, and
- **Response**, by treating incidents quickly to remediate and mitigate impacts.

All events are treated immediately by the information security team, and for incident handling, it may be necessary to mobilize other areas such as Human Resources, IT, Legal, etc;

➢ CI&T has a team responsible for data privacy and information security. We also rely on strategic partners to ensure monitoring of the Security Operations Center (SOC), which provides us with support for anti-malware solutions and intrusion detection, as well as regular information security testing. Our environment is monitored 24 hours a day, 7 days a week. The protection practices adopted are based on internationally recognized frameworks, such as ISO 27001, MITER ATT&CK and NIST methodologies for risk management. We also work in compliance with all privacy and data protection laws in the countries where we operate;

➢ In addition to our information security policy and our data privacy policy, we have processes, standards and plans that are executed on a daily basis, helping to maintain business continuity even outside of business hours. These documents guide the CI&T People, help in mitigating risks and in the adequate treatment of the most varied types of events or security incidents;

➢ CI&T strives to ensure that:

- **100% of our employees are trained annually in ethics, security and data protection;**
- **Constant awareness and Phishing simulation campaigns are carried out;**

- **Informative content is made available to employees.**

➢ CI&T maintains several channels for reporting problems or incidents, such as chat, email, incident tool, and internal website, in order to make communication quick and effective, increasing proximity and agility in response. These channels are widely publicized, and new CI&T People are notified about them on the first day of employment;

➢ The company's information security and risk management program are reviewed annually or whenever a relevant event occurs that impacts our scenario. Risk analysis is carried out to maintain the level of residual risk appropriate to our business. These reviews take into account the external cybersecurity landscape, lessons learned, regulatory and customer requirements, and gaps identified in our security assessments. There are also reviews of our information security and risk management program, which is structured following the best market practices and the appropriate information security management system, valid internationally. In addition, the program also involves a set of policies and procedures, controls and action plans managed by the information security area that are audited by CI&T's internal audit and by renowned external audit companies in the market. This all helps to optimize the use of available resources, prioritize risks and define all safeguards to protect the organization's assets.

4.3 SEC Filing

In cases of incidents deemed material, CI&T adheres to the Material Cybersecurity Incident Disclosure rule set by the Securities and Exchange Commission (SEC).

5. Responsibilities and Violations

CI&T Senior Management and all CI&T personnel must comply with and guarantee the effectiveness of this Policy.

Any breach of this Policy, as well as the Code of Ethics and Conduct, and any other guideline, rule or policy of the company, must be reported through our Ethics Portal (ethics.ciandt.com).

A violation of the guidelines of this Policy may result in disciplinary action, including, but not limited to, a warning, suspension, or termination of employment. In addition to CI&T measures, violations may result in referral to civil or criminal authorities where necessary or otherwise appropriate.

6. Document Control

Version	Date	Description	Author
1.0	DEC/2022	Policy creation	Álvaro Santana
2.0	JAN/2024	Policy review	Álvaro Santana and Compliance Team
2.0	MAR/2024	Policy approval	Board of Directors