CI&T

INFORMATION SECURITY POLICY

VERSÃO 3.0

Letter from Our CEO

The exponential evolution of technological possibilities drives an increasingly connected and digital society. Along with the benefits of digital transformation, the number of digital threats is alarmingly multiplying, which can cause severe harm to individuals and businesses. Protection against these threats is only possible with the engagement of everyone: no digital security strategy works without all involved parties being aware of the threats, safe habits, and commitment to the subject. Digital security is one of the cornerstones of a true digital society.

I invite you to become an agent of protection for our people, clients, culture, and company. It is essential to stay constantly updated, as threats also evolve at digital speed.

Take this opportunity to develop yourself and learn about the most current protection practices. And feel free to share your feedback with the Information Security team at securitytalk@ciandt.com.

Be safe, be secure!

César Gon

CEO, CI&T

TABLE OF CONTENTS

1. Definitions

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

PEOPLE OF CI&T: direct or indirect employees, including, but not limited to, individuals in labor contracting arrangements and those holding positions as directors or advisors. This definition also includes individuals acting as third-party contractors for CI&T, such as consultants or freelancers.

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

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

MATERIAL INCIDENTS: incidents with a substantial likelihood that a reasonable shareholder would consider them important when making an investment decision or if that 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 considering both quantitative and qualitative factors.

2. Objective

All our people, partners, and suppliers have the responsibility to protect CI&T and its culture against these threats, adding value to our business, reducing the possibilities of loss, and ensuring its sustainability. Therefore, CI&T is committed to maintaining a secure corporate environment that aligns with the credibility of our brand due to the high level of trust placed in us by each of our clients through CI&T's processes and teams.

This Policy is primarily intended to guide the people of CI&T on all aspects that make this type of relationship possible: business decisions, protection of CI&T's image, protection of company and client information, workplace safety, and, especially, the expected behavior of our people, suppliers, and service providers.

3. Applicability

The guidelines contained in this document must be known and followed by all people, partners, and suppliers of CI&T, as well as by anyone present in any of our CI&T offices. It is the responsibility of all individuals to ensure that the security guidelines established in this Policy are adhered to.

4. Guidelines

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 ensuring the integrity of the technological infrastructure and in compliance with the laws and regulations in effect in each location:

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

- Ensure the availability and continuity of technological services and information processing that could impair the organization’s performance;

- Ensure that the systems and data under the responsibility of the individuals in question are properly protected and used solely for the fulfillment of their functions;

- Preserve the integrity of the technological infrastructure where data is stored, processed, or otherwise handled, adopting the necessary measures to prevent logical threats such as viruses, malicious programs, or vulnerabilities that may lead to unauthorized access, manipulation, or use of internal and confidential data;

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

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

In addition to the protection measures mentioned above, it is important to highlight that the company has a Disaster Recovery Plan (DRP) that is implemented and regularly tested, with the participation of all involved areas. This ensures that, in the event of incidents that compromise the technological infrastructure and business continuity, effective procedures are in place for the quick and secure recovery of operations, thus maintaining our commitment to information security and the trust of our clients.

Access management is one of the priority areas at CI&T, aimed at ensuring that only authorized users have access to the information and systems relevant to the performance of their functions. To achieve this, we utilize tools and procedures that allow for the creation, modification, and deletion of access in a controlled manner, according to the needs of each area and user profile. Furthermore, we conduct periodic reviews of granted access to ensure compliance with internal policies and applicable regulations. With these measures, we aim to mitigate the risks of unauthorized access, information leakage, and other threats to information security.

All of this is executed through the principle of need-to-know and least privilege, meaning that only the necessary permissions are granted for the user to perform their tasks. This approach helps 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, access and security measures are adopted for the facilities. Good security practices are also implemented to ensure appropriate operating conditions for equipment and data preservation. These measures are essential to protect our personnel, physical assets, and company data, as well as to ensure the continuity of critical operations.

To ensure the integrity of CI&T's data, the company's equipment and resources must be used solely for activities related to CI&T. That is, personal use or use for the benefit of third parties is prohibited. This measure aims to protect confidential information and ensure that all employees use CI&T's equipment and resources for purposes that are in the company's interest.

To preserve the intellectual property of CI&T and its clients, copying, using, or sharing repositories, source code, or any other data with unauthorized individuals is not permitted.

The use of a password manager, such as LastPass or similar tools, is highly recommended. These solutions allow for the secure storage of passwords, facilitate the generation of strong and unique passwords, and reduce the risk of unauthorized access.

In addition to this Information Security Policy, we maintain complementary policies that address specific aspects of security and data protection. It is essential that all CI&T personnel are aware of and understand these policies, as they are fundamental to promoting a safe environment and compliance with current regulations.

4.2. Actions taken

- ➢ All employees, partners, and suppliers of CI&T have the responsibility to protect CI&T and its culture against threats, thereby reducing the possibilities of losses and ensuring the sustainability of the business.

- ➢ Significant updates are made available through CI&T's official communication channels, and we encourage everyone to review them frequently to stay informed about updates on our protection practices.

Our information security team is prepared to act:

- in **Prevention**, through traditional security controls and safeguards,
- in **Monitoring**, by continuously reviewing events and alerts, and
- in **Response**, by addressing incidents quickly to remediate and mitigate impacts.

All incidents are addressed immediately by the internal security team, with the support of other areas such as Human Resources, IT, Legal, etc.;

➢ CI&T has a team responsible for data privacy and information security. We also have strategic partners to ensure the 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. Monitoring of our environment is conducted 24 hours a day, 7 days a week. The protection practices adopted are based on internationally recognized frameworks, such as ISO 27001, MITRE ATT&CK, and NIST methodologies for risk management. We also operate 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 daily, helping to maintain business continuity even outside of business hours. These documents guide the people of CI&T, assist in risk mitigation, and ensure the proper handling of various types of security events or incidents.

➢ CI&T guarantees that:

- **Our employees are trained annually in security and data protection;**
- **Constant awareness campaigns and phishing simulations are conducted;**
- **Informative content is made available to employees.**

➢ CI&T maintains various communication channels for reporting problems or incidents, such as chat, email, incident management tools, and an internal website, aiming to make communication quick and effective, increasing proximity and agility in response. These channels are widely publicized, and new CI&Ters are informed about them on their first day of work.

- The company's information security and risk management program is reviewed annually or whenever a relevant event occurs that impacts our landscape. Risk analysis is conducted to maintain an appropriate level of residual risk for 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 according to market best practices and an internationally recognized information security management system. Additionally, the program involves a set of policies and procedures, controls, and action plans managed by the information security area, which are audited by CI&T's internal audit and by renowned external auditing firms. All of this helps to optimize the use of available resources, prioritize risks, and define all safeguards to protect the organization's assets.

4.3. Communication channels

You can contact us to submit suggestions, ask questions about this Policy, or any situation related to security, and to report incidents or non-compliance (actual or potential).

The available channels are:

Chat (available only for internal CI&T personnel): securitytalk@.

Email (available for anyone): securitytalk@ciandt.com.

4.4. SEC Registration

In cases of incidents considered material, CI&T adheres to the material cybersecurity incident disclosure rule defined by the Securities and Exchange Commission (SEC).

5. Responsibilities and Violations

Top management and all CI&T employees must comply with and ensure this Policy.

Any violation of this Policy, as well as the Code of Ethics and Conduct, and any other guideline, rule, or company policy, 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's measures, violations may result in referral to civil or criminal authorities when necessary or appropriate.

6. Document Control

Version	Date	Description	Author
1.0	DEC/2022	Creation	Álvaro Santana
3.0	FEB/2025	Revisão	Information Security Team and Compliance Team
3.0	APR/2025	Audit Committee Review	Committee members
3.0	MAY/2025	Final Approval/Effective Date	Board of directors