Number: PL.00.34	MANAGEMENT SYSTEM POLICY	
Review: 01	Information Security Policy	
Data: 15/08/2023		

1. OBJECTIVE

The Information Security Policy aims to:

The. Establish guidelines that allow green4T's stakeholders to follow desirable and acceptable standards of behavior on the subject of information security, acting in accordance with legality and good global practices and aims to mitigate technical, financial, administrative, legal and image risks/ reputation.

B. Guide the definition of specific Information Security procedures, as well as the implementation of controls and processes to comply with it.

w. Preserve green4T's information regarding confidentiality, integrity and availability.

d. Minimize the risks of financial loss, market share, consumer and partner trust or any other negative impact on green4T's business, resulting from one or more security breaches in its environments, especially with regard to the data produced , stored, processed or treated by its professionals, whether in physical or digital format.

This Policy is complemented by procedures and attached documents, classified as confidential, which bring the guidelines to be followed in the conduct of processes related to this policy, and serve as a reference for the professionals in charge of its execution.

2. SCOPE This

document applies to all Departments and affiliated and controlled companies of green4T and covers the NBR ISO/IEC 27.001 and ISO/IEC 27.002 standards.

3. TERMS

a) Authenticity: Property that the information was produced, issued, modified or destroyed by a specific natural person, or by a specific system, body or entity. Brings non-repudiation features and warranties of only authorized and tracked modifications.

b) Confidentiality: Property that the information is not available or disclosed to unauthorized and accredited person, system, body, entity.

c) Availability: is the guarantee that the information can be obtained whenever necessary, that is, that it is always available and usable for those who need it in the exercise of their functions. When information is unavailable, the processes that depend on it are paralyzed.

d) Integrity: is the guarantee that the information stored or transferred is correct and is presented in full to the person who consults it. It means that in a communication, the information is not modified, suppressed, destroyed in an unauthorized or accidental way in the middle of the path between the one who sends the information and the one who receives it. It is a critical feature from an operational and indispensable point of view, as it validates the entire communication process at green4T. e) Legality: is the guarantee that the information is recorded in accordance with the procedures in force, that is, the use of computer and communication technology that generated the information is in accordance with the laws in force in the place or country. f) Traceability (or Auditability): is the possibility of tracking updates to sensitive information so that, in the event of a problem, it is possible to clarify exactly what happened to the information. There are situations where there is a need for mechanisms capable of tracing the process back to the source.

g) User: Collaborator or representative (service provider) who uses the technological resources belonging to the company.

4. RESPONSIBILITIES

4.1. INFORMATION TECHNOLOGY MANAGER

a) Manage the use of technologies necessary for the smooth running of green4T's business, including preventive actions and handling incidents, in order to promote a higher level of information security; b) Carry out actions directed at technical issues related to information security management;
c) Propose specific methodologies and processes for Information Security, together with the Information Security manager, such as Risk Assessment; d) Support the evaluation and adequacy of specific Information Security controls for new systems or services, together with the Information Security Committee; e) Take immediate measures to remedy any violation verified by the area and immediately cease the risk to green4T, immediately informing the DPO about the violation and the measures implemented.

4.2. PEOPLE AREA a)

Deliver the PL.00.34 - INFORMATION SECURITY POLICY upon admission to every employee or service provider. b) Deliver and collect a signature for every employee or service provider upon admission to PL.00.22 - INFORMATION TECHNOLOGY POLICY; c) Define with the area manager, the IT manager and the information security manager, the information resources necessary to carry out the activities for which the employee or provider was hired

(hardware e software);
d) Request the blocking of access to the company's information systems in case of dismissal and change of area.

4.3. EMPLOYEES AND THIRD PARTY PROVIDERS

All green4T employees and providers:

a) They undertake to faithfully comply with the Information Security Policy, rules and procedures established in this document, assuming the commitment to observe and apply them, as well as submitting to the sanctions provided for in the internal policies and in the applicable legislation; b) They agree that all operations and accesses made through magnetic media are recorded and subject to verification at any time, regardless of prior notice, as they are work tools, and there is no need to talk about invasion of privacy;

c) They are aware that green4T, in accordance with its right, may monitor all its environments, whether physical or workrooms; logical and/or electronic, including: corporate e-mail, internal network, Internet and Extranet and other systems, storing the access data of each user;

d) They agree and acknowledge that, in the event of any violation of the terms and conditions of this Policy, it will be subject to the internal rules and legislation in force. It may also give rise to dismissal for just cause, pursuant to the provisions of Article 482, item “g”, of the Consolidation of Labor Laws, without prejudice to other applicable legal sanctions; e) They are aware that, upon termination of their employment relationship, or at any time upon request by green4T, they must return any and all materials provided, or that contain Information produced as a result of the employment contract;

f) They are aware that the reproduction of documents for the exclusive use of green4T, for any purpose, is prohibited, such attitude being characterized as unauthorized disclosure of confidential information and illegal production of evidence;
g) They must seek guidance from the information security manager when there are doubts related to Information Security; h) They must use a secure password, and must change it, as periodicity determined by green4T;
i) They must sign the PL.00.22 - INFORMATION TECHNOLOGY POLICY, formalizing the science of the Information Security Policy and Standards, as well as assuming responsibility for their compliance;

j) Must protect the information against access, modification, unauthorized disclosure or destruction by green4T;
k) They must ensure that the technological resources are used only

for approved professional purposes and in the interest of green4T; l) They must immediately notify the information security manager of any non-compliance or violation of this Policy and/or its related Rules and Procedures.

4.4. AREA MANAGER It

is the responsibility of every green4T area manager:

a) Be aware of and manage the accesses granted to subordinates, being, therefore, indirectly responsible for the misuse of the themselves;

b) Periodically review users with access to critical transactions under their responsibility, informing the People area of any changes in access or authorization; c) Have an exemplary attitude in relation to Information Security, serving as a model of conduct for the employees under their management; d) Comply with and enforce this Policy, the Rules and Procedures for Information security;

e) Ensure that their teams have access to and are aware of this Policy, as well as the Rules and Procedures related to the Safety of the Information;

f) Attribute in the contracting phase of third parties and partners, when they need to have contact with company information, the insertion of a liability clause, awareness of the Company's Security Policy Information, requiring the transfer of obligations to its employees responsible for providing services within green4T; g) Specify and previously request access permission, listing the information assets for employees in general who are not hired;

h) Assist the Information security manager in adapting the Norms, Processes, Procedures and systems under his/her responsibility to comply with this Information Security Policy; i) Immediately communicate to the information security manager, through a specific Channel (dpo@green4t.com), any violations of Information Security, which will be triggered and will work together with the Information Security team.

4.5. COMPLIANCE MANAGER

a) Carry out monitoring tests on adherence to the rules established in this policy; b) Assist the DPO in adapting the green4T company to the law 13.709/18 (General Data Protection Law - LGPD), the ISO/IEC 27.001, ISO/IEC 27.002 and ISO/IEC 27.701 standards, defining the improvements of internal controls to be implemented by the information technology area and other requirements described in the law.

4.6. INFORMATION SECURITY AREA

The green4T Information Security team is responsible for:

a) Submit to the Information Security Committee and LGPD the versions of the Information Security Policy and standards, and after approval, publish and promote them on the green4T intranet; b) Propose and support initiatives aimed at securing the assets of information from green4T;

c) Promote, together with the People area, the awareness of employees and partners regarding the importance of Information Security for green4T's business, through campaigns, lectures, training and other means;

d) Critically analyze incidents, with support from the IT team, if necessary;

e) Maintain effective communication with the Information Security and LGPD Committee, with the aim of keeping them adequately informed on matters related to the topic, which affect or have the potential to affect green4T; f) Receive complaints about violations of the Policy and Standards, after completion of the investigations carried out, and must promote the treatment of information, identification of the action plan, risk mitigation, activation of the Information Security Committee and LGPD and application of the appropriate sanction (Penalties).

4.7 LEGAL AREA

a) Provide guidance on the best way to collect and preserve electronic evidence, in order to maintain its effectiveness for use in court, when necessary; and b) Preparing and reviewing legal documents related to Information Security, mainly data protection defined by the LGPD and ensuring clauses that mitigate legal risks.

4.8 INFORMATION SECURITY COMMITTEE

The Information Security and LGPD Committee is made up of managers from the main areas of Green4T, who must fulfill the following responsibilities within the organization.

a) Ensure the availability of resources for all Information Security actions; b) Maintain focus and promote Information Security at green4T, approving policies that reflect its role described above by approving material submitted by the Information Security manager Information;

c) Ensure that risks to Information Security are identified, assessed, categorized and managed by the Information Security manager Responsible information for that; d) Approving cost-effective actions to manage risks and monitor their implementation; e) Give direction, review and update the Security strategy of the

Information ensuring that its Policy, rules and procedures are properly updated and continuously relevant to the green4T scenario;

f) Ensure that training and awareness on Information Security is provided to employees and, when relevant, to third parties, suppliers and customers.

5. GUIDELINES OF THIS POLICY

5.1. GENERAL GUIDELINES

The information produced or received by green4T professionals must be used with a sense of responsibility and in an ethical and safe manner, for the exclusive benefit of the corporate business and based on the following principles of integrity, availability and confidentiality. At green4T, information is considered the most valuable asset. Without confidentiality you lose competitive advantage, without integrity you lose profitability and without availability you lose the ability to operate. In addition to the three attributes mentioned, authenticity, legality and traceability are also considered, since without authenticity, confidence in the reliable origin of information is lost, without legality, there is a risk of non-adherence to internal and external regulatory standards and without traceability, you lose control of updates to sensitive data.

Information Security in the organization establishes the main guidelines and controls for the protection of information:

The. The information owned by green4T must be treated in an ethical, confidential and legal manner and always paying attention to the terms agreed with employees, customers and partners, thus avoiding the misuse and undue exposure of such information;

B. The information must be used in a transparent manner, only for the purpose for which it was designated and for the time necessary to achieve its purpose;

w. All users agree to use the Information solely in the performance of their duties and properly classified according to the classification criteria defined by the organization;

d. During your working relationship or partnership with green4T - and even after it ends - the user may not publish, reveal, or otherwise make available to any third party, any Information classified as Restricted or Restricted Confidential, except: (i) when expressly authorized in writing by green4T, or (ii) to other active employees who are known to be authorized to receive

Confidential Information and need to know it in order to use it to meet business needs;

It is. All users of the information are aware of and agree to act with all necessary diligence to protect the integrity and secrecy of information owned by green4T, being prohibited the subtraction or removal, in any form, of any materials, except for what is necessary due to rules or laws in force;

f. All persons within Green4T's physical premises should be identified by visible badges (or other visual means of identification). The identification (badge, login, password, etc.) of each employee is unique, personal and non-transferable, qualifying him as civilly and criminally responsible for the actions taken;

g. The access password is for personal use and non-transferable and must be kept confidential, with its sharing being expressly prohibited, except in cases pre-approved by the Information Security areas;

H. All risks identified in relation to green4T information must be reported to the information security team through a specific channel (dpo@green4t.com), so that the necessary measures can be taken to assess and mitigate the risk eventually identified. As well as all incidents that affect information security, they must also be reported to the information security team through a specific channel (dpo@green4t.com), which will analyze the incident and prepare the report;

i. Every procedure will follow the guidelines and rules for security incidents and, if necessary, take the report to the board so that the appropriate sanctions are applied to those involved;

j. User access control to information assets must be duly approved by the person responsible for the information, either for simple consultation or for alteration. All information relating to the request, approval and effective granting of access must be stored in a secure Drive, with access control configured by those responsible for each area;

k. The use of corporate e-mail made available by green4T is its property and will be allowed for users only for corporate purposes and for a determined period of time, defined by the management of the requesting area. As for data transmission, this feature must be used to ensure privacy in data communication;

l. All Information Security requirements, including the need for business continuity plans, must be identified in the scoping phase of a project or system. These requirements must be justified, agreed, documented, implemented and tested during the execution phase;

m. The rules for the secure development of systems and software must be established and applied to developments carried out inside or outside the organization, subject to the adequacy assessment and approval of the Information Security team. In the case of development outside of green4T, the system must contain tools that allow security auditing regarding: informational self-determination of data holders, audit trails, access policies (authentication, authorization and traceability) and analysis of source codes;

n. The granting of remote access to green4T's systems and Drives to employees, partners and suppliers must be formally authorized. The request must be sent to the IT area, by the manager of the requesting area, at which time the type of access, permission and information to be accessed must be indicated. Every procedure must be presented to the information security manager so that he is aware of the authorizations;

O. The use of the internet environment at green4T is only allowed for professional purposes, where employees must be aware of the sites they access and be aware that they will be monitored;

P. A set of rules should be created to guarantee the standardization of cryptographic techniques, their proper application and responsibilities to maintain security in the transport or storage of information, regardless of the means used. Responsibility for the rules rests with the IT manager in partnership with the information security manager;

q. The development, approval and production environment must be segregated and properly controlled. The use of real personal data and sensitive personal data is not allowed in the test environment;

r. A change management process ensures that controls and modifications to systems or information processing resources are carried out with planning, in order not to cause operational or security failures in the organization's productive environment;

s. Risks are identified through an established process for analyzing vulnerabilities, threats and impacts on processes in terms of information security (confidentiality, integrity and availability);

t. All information that is on the physical medium (paper) must be classified with the same content, stored in a safe place, locked, protected against natural, voluntary and involuntary risks, with formal access control by users aiming at possible audit trails;

u. When technological reasons or superior determinations make it impossible to apply the requirements set forth in this Policy, the person in charge and/or requester must immediately report them to the information security manager, so that he/she can enable the adoption of alternative measures that mitigate the risks, as well as an action plan to correct, mitigate, monitor or eliminate them;

v. All green4T employees must periodically undergo training and awareness about security procedures and correct use of assets made available by green4T, in order to minimize possible security risks, explain their responsibilities and communicate procedures for reporting incidents;

w. All green4T employees must ensure that intellectual property rights are you preserved, such as projects, trademarks, patents and that the use of proprietary software products is in compliance with the respective license for use;

x. All green4T employees must ensure compliance with the “Clean table, clean screen and clean trash policy”, whose objective is to avoid:
1) papers and removable storage media on top of desks; 2) wastebaskets containing readable confidential information;
3) screens with information on active sessions or sessions already deactivated.
This care extends to common areas, such as corridors, closets, material storage areas, meeting rooms, waiting areas, community areas (pantry, kitchen, leisure, etc.).

5.2. DISCLOSURE

The Information Security Policy is known to all users and disclosed as follows:

a) Via periodic Information Security campaigns; and b) By digital means, through the corporate intranet.

The policy is available in an easily accessible location for employees and protected against unauthorized changes.

All employees, in addition to service providers, partners and suppliers who access or manipulate information (digital or physical) in any way or use green4T's technological resources, must formally adhere to "PL.00.22 - INFORMATION TECHNOLOGY POLICY", undertaking to act in accordance with the rules described therein. (Material available as one of the volumes of the Information Security Policy).

PL.00.34 - Information Security Policy is reviewed and updated periodically, at least every 01 (one) year and/or whenever any relevant fact or event occurs that motivates its early review, according to the Committee's analysis and decision Information Security and LGPD.

5.3. MONITORING

green4T, through its Information Security area, monitors and records all the use of information generated, stored or transmitted in it, which reserves the right to:

a) Implement systems for monitoring access to workstations, internal and external servers, electronic mail, Internet, mobile or wireless devices and other network components. The information generated by these monitoring systems may be used to identify users and their respective accesses.

b) Inspect any file that is on the network, on the station's local disk or any other environment, in order to ensure strict compliance with this Information Security Policy.

c) Install protection and intrusion detection systems to guarantee the information security and access perimeters.

d) Monitor the physical installations through cameras.

5.4. GUIDELINES FOR LGPD

Green4T companies have defined and implemented internal controls necessary to comply with the LGPD, regarding the protection of data of customers, employees, suppliers or others involving data of individuals, as provided for in law 13,709/18.

5.5. PENALTIES

When deemed necessary and relevant, the Information Security team will submit violations of the Information Security Policy and Information Security Standards to the board of directors, as well as the result of the verification validated through the information security committee and LGPD and other areas relevant, in accordance with green4T's Complaint Investigation Policy.

The suspect of committing violations of the Information Security Policy and Regulations must be ensured fair and correct treatment, and any and all measures resulting from his/her infraction must be applied proportionally to the occurrence based on the Infractions and Penalties Regulation.

green4T disclaims any and all liability arising from the improper, negligent or reckless use of the resources and services granted to its employees, reserving the right to punish offenders, analyze data and evidence to obtain evidence to be used in investigative processes and adopt the appropriate legal measures

6. REFERENCE DOCUMENTS

P.12.01 - Backup_green4T
P.12.04 - Shutdowns_green4T
P.00.22 – Information Technology Policy_green4T
P.00.31 – Internal Privacy Policy_green4T P.00.32 – External Privacy Policy_green4T

7. CONTROL OF RECORDS

NA.

8. REVISION HISTORY

Revision	Data	Description of change	Approved by the Manager	Approved by Certifications
00	30/05/2022	Issuance	Edward Marines	Adriana Moyses
01	15/08/2023	General review of the policy, item 5.1.f amended	LGPD Committee: Claudio (DPO), Alan Baldo, Eduardo Rasi and Thais Almeida	