INFORMATION SECURITY POLICY GUIDELINES

ELABORATED BY:	RAFAEL LEITÃO	REV:	00
APPROVED BY:	MARCELO LIMA		
DISCIPLINE:	INFORMATION SECURITY	DATE:	Nov. 30, 2023

1. OBJECTIVE

The objective of this Technical Instruction is to establish and specify requirements and conditions necessary for the management of Information Security in **Estaleiros do Brasil Ltda. (EBR)** environment. Its purpose is to define processes, aiming to maintain the occurrence and the impact of information security near misses at acceptable levels in relation to the corporate risk appetite.

2. REFERENCES

ISO/IEC 27001 - Information Security Management System.

Note: The standard must be used in its most recent version.

3. TERMS AND DEFINITIONS

Information Asset: means all devices that produce, process, transmit or store information, or the information itself, such as: information like business secrets, printed reports, electronic documents, professionals, digital certificates, telecommunications equipment, computers, smartphones, etc.

Information Systems: an information system is an organized set of elements, which can be people, data, activities or material resources in general, for example: email, network, internet, device, VPN, systems and/or corporate applications. These elements interact with each other to process information appropriately according to the company's objectives.

Information Owner: is responsible for creating, classifying, granting, reviewing and maintaining a certain set of information in systems, e-mail and digital and physical documents. The identified owner does not necessarily have any ownership rights to the information asset.

Custodian Area : is the area responsible for the functional and operational aspects of a certain type of configuration item (asset). Has responsibility for operational tasks delegated by the asset owner. The custodian areas of Information Technology Management mean all of its internal areas.

Responsible for the service provider: this is the contract manager or the professional authorized thereby.

Information Classification: information classification consists of assigning the level of secrecy and indicating its respective label by the Information Owner to determine which controls must be applied, aiming to preserve the information.

Information Security Term of Responsibility: is the document whose content defines the Information Security rules that professionals must follow.

Confidentiality Agreement: is a contractual clause signed between **EBR** and third-party companies, aiming to guarantee the confidentiality of information.

Network Drive: remote virtual area intended to store logical files.

Antivirus: software responsible for identifying and blocking harmful files and malicious codes (viruses) in the Information Systems environment.

Malicious Codes: are computer programs designed specifically to attack the security of computer systems, normally through the exploitation of vulnerabilities, with the aim of infiltrating and spreading automatically, causing damage, deleting data, stealing information, advertising services, etc.

Information Security Committee ("COSI"): group formed with the mission of discussing issues related to information security and the risks associated with the business.

Information Security Control: measure that modifies the risk. Controls include any process, policy, device, practice or other actions that change risk. It is possible that controls do not always exert the intended or assumed modification to risks, thus generating what is known as residual risk.

Residual Risk: is the amount of risk that remains or appears after the inclusion of additional controls and/or adjustments to existing controls.

Risk Matrix: document that establishes the implementation of an information security control or information security improvement project, or that formalizes the acceptance of the risk.

4. GENERAL INFORMATION SECURITY GUIDELINES

The Information Security guidelines can be defined as formal statements by **EBR** regarding its commitment to protecting the information it owns and/or under its custody, and its main objective is to formalize the approach related to Information Security in the company.

The Information Security Management System has the information security guidelines below:

1. Preserve the confidentiality, integrity and availability of information handled in the general administration of **EBR** and projects managed thereby;

2. Maintain the international Information Security standard in accordance with ISO/IEC 27001;

3. Meet applicable information security requirements in accordance with the business;

4. Continuously improve the Information Security Management System;

5. Minimize the risks of breaches or losses of any information technology assets;

6. Develop and improve human and technological resources under the Information Security Management System.

5. RESPONSIBILITIES

a) Information Security area

- Manage the Information Security Management System;
- Propose and support initiatives aimed at the security of **EBR's** information assets, in accordance with the recommendations of regulatory agencies;
- Promote the updating of the Information Security Policy approved by the Information Security Committee;
- Support the evaluation and adequacy of specific information security controls for new systems or services;
- Analyze together with the Information Technology Area and/or Management Areas involved in information security near misses and propose actions to deal with vulnerabilities, according to the risk analysis;
- Maintain effective communication with the Information Security Committee, highlighting matters that require intervention by the committee or board members;
- Routinely audit information security controls;
- Monitor the activity of all users when accessing networks, including *the internet* (websites visited and emails received/sent), with the aim of identifying malicious behavior;
- Support internal and/or external audits and carry out investigations and assessments of damage resulting from security breaches;
- Preventively identify and mitigate risks that compromise the security of information and services in a corporate environment;
- Carry out study, implement and manage solution/tool to be applied in the environment to raise the level of Information Security;
- Perform control and management actions on cybersecurity mechanisms/tools;
- Perform vulnerability management on systems, devices and infrastructure available on the internal and external network and adapt services that require security controls.

b) Information Security Committee

- Act in accordance with the Internal Regulations of the Information Security Committee;
- Evaluate material made available monthly by the Information Security Analyst;
- Assess security risks, near misses and vulnerabilities and propose corrective actions;
- Whenever necessary, discuss any serious or relevant near miss for **EBR** and make recommendations to the Director of Governance and Integrity;
- COSI may use internal or external experts, to support issues that require specific technical knowledge.

c) Managers of EBR's internal areas

- Have an exemplary stance in relation to information security, serving as a model of conduct for professionals under their management (leadership and commitment);
- Inform the Information Security area of the termination of service providers, including third parties in the "Legal Entity" format;
- Immediately report any non-compliance or violation of the guidelines, procedures and/or technical instructions to the Information Security area.

d) Professionals from different areas

- Comply with Information Security Policies;
- Seek guidance from their immediate superior in case of questions related to information security;
- Sign the Information Security Responsibility Term, formalizing awareness and acceptance of the Information Security Policy, as well as assuming responsibility for its compliance;
- Protect information against unauthorized access, modification, destruction or disclosure;
- Ensure that the technological resources at their disposal are used only for purposes approved by the company's guidelines and procedures;
- Immediately report any non-compliance or violation of information security procedures to the Information Security area.

e) Information Technology

- Ensure the recovery of corporate data, in addition to managing, protecting and testing backup copies of programs and data related to critical and relevant processes;
- Generate and maintain audit trails in accordance with established specifications to track possible failures and fraud in critical systems of the Information Systems Continuity Plan;
- Configure equipment and systems granted to users with all necessary controls to comply with corporate information security requirements;
- Ensure that all servers, computers and other devices with access to the company's network operate with clocks synchronized with the Brazilian government's official time servers;
- Administrators and operators of computer systems can, due to their privileges, access the files and data of other users. However, this action will only be permitted when carrying out activities exclusive to their work routine that require such access, just like, for example, maintaining computers, making backup copies or testing the environment. Access must be duly authorized and documented.
- When any user changes its computer, ensure that the previous user's information is irretrievably removed before making the asset available to the next user;
- The process of acquiring and developing systems and access to production must meet security requirements set out in **EBR's** security specifications.

f) Supply area

- Include the information security clause as an integral part of all service provision contracts.

g) Property Security area

- Create protection mechanisms for information assets in the company's physical locations.

h) Human and Organizational Development Area / Human Resources and Personnel Administration Areas

- Make every professional, upon being accepted, sign the Information Security Term of Responsibility of **EBR.**
- Immediately report to the Information Security area any and all dismissals, as well as promotions and other changes in position and area, including name and registration number.

i) Privacy and Data Protection area

- Have an exemplary stance in relation to information security, serving as a model of conduct for the company's professionals;
- Immediately report any non-compliance or violation of the guidelines, procedures and/or technical instructions to the Information Security area;
- Conduct, together with the Information Security area, an action plan when there are information security near misses involving personal data.

6. SPECIFIC INFORMATION SECURITY GUIDELINES

The specific Information Security guidelines were defined as an extension of the general guidelines, regarding the implementation of applicable information security controls:

- **Information Processing**: **EBR** must create, manage and evaluate criteria for the treatment and classification of information that belongs to it, or is under its responsibility, in accordance with the required secrecy, relevance, criticality and sensitivity, observing current legislation and other applicable standards.

- **Management of Near Misses**: Information security near misses must be identified, monitored, communicated and properly handled, to prevent the interruption of the company's activities and not negatively affect the achievement of its strategic objectives.

- **Risk Management**: An Information Security Risk Management process was established with the purpose of minimizing possible impacts associated with assets, enabling the selection and prioritization of assets to be protected, as well as the definition and implementation of controls to the identification and treatment of possible security breaches.

- **Continuity Management**: Business Continuity Management was established within **EBR**, aiming to reduce the possibility of interruption of activities and services, caused by disasters or serious failures in technological resources that support critical operations.

- **Logical Access Control**: Rules were formalized to establish procedures, guaranteeing access control to information, facilities and information systems, making use of verification mechanisms and a second authentication factor, when applicable.

- **Physical Access Control, Physical Security and Environmental Security**: The company's assets are protected against physical access by unauthorized persons, as well as against damage, loss, theft and internal and external interference. Protections are aligned with the identified risks related to the asset.

- **Safe Storage, Disposal and Transport of Information**: Secure procedures have been established with appropriate mechanisms, which guarantee the security of information handled by **EBR**, whether physical or digital, guaranteeing the security and inviolability of its content, preventing the access of unauthorized persons.

- **Information Classification**: A systematic and objective classification was established to qualify the information circulating within **EBR**, considering its importance for the development of the company's activities, the need to protect the privacy of persons to whom the data refers to, and the criticality, sensitivity and relevance of information.

- **Use of own devices *(Bring Your Own Device - BYOD)***: **EBR** reserves the right to delete company-owned information on lost devices or those of professionals who are no longer linked to the company. In the case of using devices belonging to **EBR**, they will be monitored and information belonging to the company will be preserved. Company information should not be accessed through devices that are not owned by the company, except under express authorization from the Information Security Management or provision of the means of access controlled by the company.

- **Code of Conduct** : The **Code of Conduct** is only applicable to professionals who work directly at **EBR**, excluding suppliers, customers and third parties. All **EBR** professionals sign the Code of Conduct.

- **Authentication Guidance**: To create secure passwords, it is recommended to use at least (08) eight characters, which are made up of numbers and letters. Passwords that are easy to associate with users, such as date of birth, surname, telephone numbers, spouse's name, etc., should not be used.

  If the user does not use the second authentication factor, access will be blocked after 05 (five) incorrect attempts and will need to open a request in the call opening tool. Furthermore, the use of password managers not approved by **EBR** is not permitted . To ensure greater security, the second authentication factor must also be used whenever the system or application allows it.

- **Backup Management**: To ensure the proper functioning of backup management, it is determined that systems are classified according to their criticality and have backup routines compatible with the risk appetite of the business. Backups must be monitored by those responsible and their execution must be evidenced. Furthermore, to preserve the reliability of the restoration process, periodic restoration tests must be adopted, which simulate a near miss so that it is necessary to restore the environment to its original state. This simulation must be run in a test environment, to prevent files contained in the production environment from being overwritten.

- **Technological Change Management**: Change management within IT is necessary to ensure that the most appropriate standardized methods and procedures are used for the efficient handling of all changes occurring in **EBR's** organizational environment.

  Changes must be proposed using a specific form that details: scope, execution window, execution plan and restoration plan. This form must go through an approver, be registered in the call opening tool and evidence of its execution must be attached.

- **Approval of Applications:** To ensure the security and proper functioning of **EBR's** information assets, only applications and software accepted by the company may be installed and run on notebooks, VDIs (Virtual Desktop Infrastructure) and other systems used by professionals. Any other software will, in principle, be blocked, but its execution or installation can be accepted upon request via the call opening tool.

- **Approval of Cloud Services** : To guarantee the correct and functional approval of cloud services, only services accepted by the company may be used by professionals.

  The use of other services will, in principle, be denied, considering that the environments have data that is frequently consulted or updated. Furthermore, they have high access response time requirements and the preservation of these environments is necessary. However, the use of other solutions, systems or services not listed can be accepted upon request via the call opening tool, after testing in an isolated environment.

- **Remote work**: Remote work, when authorized, is only permitted using devices owned by **EBR**. These will be monitored and information belonging to the company will be preserved.

  Remote working professionals must use their corporate login to access the systems necessary to carry out their work, and the use of anonymous logins is not permitted. The login is personal and non-transferable and cannot be shared with other users or revealed to anyone, so that all activities carried out can be tracked and identified.

  The development of remote work activities must take the same diligence and follow the same safety rules applied to in-person work. Care regarding the undue exposure of information, especially in relation to confidential and personal data, must be carried out in the same way as in face-to-face work. Information should not be displayed on tables or stored in unsafe and unattended locations.

  The equipment/device provided by **EBR** must always be locked in the temporary absence of the professional, as well as turned off at the end of the working day.

7. SANCTIONS AND PUNISHMENTS

The following sanctions and punishments are applicable to the respective cases described:

- Violations of this policy and/or other safety standards and procedures, even if due to mere omission or unsuccessful attempt, are subject to the penalties provided for in **EBR's** Disciplinary Measures Policy.
- The application of sanctions and punishments must be carried out in accordance with the recommendation of the Information Security Committee, based on **EBR's** Disciplinary Measures Policy.
- In the case of violations that involve illegal activities, or that may cause damage to **EBR**, the offender must be held responsible for the losses as provided for in internal regulations, and the relevant legal measures must also be applied.
- Omitted cases must be evaluated by the Information Security Committee for subsequent recommendation, in accordance with **EBR's** Disciplinary Measures Policy.

The guidelines established in this policy and in other Information Security standards and procedures are not exhausted due to continuous technological evolution and the constant emergence of new threats. Therefore, an enumerative list is not constituted, and it is the obligation of the user of **EBR** information to adopt, whenever possible, other security measures in addition to those provided here, with the aim of guaranteeing the protection of **EBR** information.

8. APPLICABLE STANDARDS

SQ-00-SSI-01-FOR-01	Information Security Term of Responsibility