INFORMATION SECURITY POLICY

1. OBJECTIVE

Establish guidelines for behavior related to information security that are appropriate to the business and legal protection needs of the company and the individual.

2. APPLICATION AND SCOPE

This Policy applies to all employees, interns, suppliers, service providers or any other people who are users of information from Randon Companies.

3. REFERENCES

- Randon Companies Code of Ethical Conduct.
- Sanctions Policy
- ABNT NBR ISO/EC 27001: 2013 Information technology - Security techniques - Information security management systems - Requirements
- CERT.br - Center for the Study, Response and Handling of Security Incidents in Brazil.
- NIST – *National Institute of Standards and Technology*.
- Current legislation

4. DEFINITIONS

Information Assets: any information that has value for the organization, including equipment, information and data.

Backup: Copying data from one storage device to another so that it can be restored in case the original data is lost, which may involve accidental deletion or data corruption.

Mobile Devices: laptops, tablets, smartphones, among others.

Security Incident: event that may cause damage to the company or even violate security rules.

5. GUIDELINES

The Information Security Policy of Randon Companies considers information security through the following aspects:

- Confidentiality: ensure that the information is accessible only by authorized persons;
- Integrity: safeguarding the accuracy and completeness of information and processing methods;
- Availability: ensuring that authorized users gain access to information and corresponding assets, whenever necessary.

Information security is achieved through the implementation of a series of controls, which can be technological, physical or administrative.

This policy is in line with the strategic objectives of Randon Companies.

5.1 Specific Guidelines

- **Use of resources and information**: everyone is committed to ensuring that information and resources are used only for professional purposes, making proper use of IT (information technology), physical (hardware) or logical (software) resources. Employees, interns, suppliers, service providers must observe and respect intellectual property rights, whether information owned by Randon Companies or third parties. These rights apply to both tangible and intangible assets, including trademarks, patents, source codes and licensing agreements, among others.

- **Classification and handling of information**: all information found in the physical and logical environments of Randon Companies, including those related to their suppliers, partners and customers, must be classified according to how critical and sensitive they are. It is a commitment of all employees, interns, suppliers, service providers to ensure that the information receives the labels consistent with its classification, divided into the following levels:
  i. **Public:** in the public classification there is no confidentiality in the information, it is open to both the internal and external public;
  ii. **Internal:** The internal use classification has a low level of confidentiality. This information will be available to all administrators, employees and trainees of Randon Companies, but the external public will not be able to access this information;
  iii. **Restricted**: Restricted classification has a medium level of confidentiality. Only authorized persons may have access to information;
  iv. **Confidential:** The confidential classification has the highest level of confidentiality. Information is of high value to the organization.

- **Users and Passwords:** physical and logical access will be granted only for the resources and information necessary and indispensable for the performance of activities and in accordance with the interests of Randon Companies, considering the principle of least privilege. Passwords and other forms of authentication are individual, secret, non-transferable and are protected with a level of security compatible with the associated information, according to item 5.3 of the document "Procedimento de Padrão de Gestão de Acesso". It is the employee's responsibility to ensure the correct use of their identification and the confidentiality of their password.

- **Internet**: is a work tool and should be used as a research method and to complement professional activities. Access to pages and web sites is the responsibility of each user, and access to sites with inappropriate content, such as pornography, games, betting, among others, is prohibited.

- **E-mail:** is a work tool and should be used to support the development of functional activities. Employees are s fully responsible for the use of the service, being fully responsible for any action or damage performed, responding for any lawful or unlawful act. The addresses and mailboxes made available to users are the property of the company.

- **Mobile devices**: it is a commitment for the employee to use them in accordance with the interests of Randon Companies and to ensure their safekeeping, taking care of their physical integrity and the inviolability of the information contained therein, as well as returning them when requested by the company.

- **Management and protection of IT resources**: the acquisition, installation, configuration, movement and maintenance of Information Technology resources of Randon Companies are the exclusive responsibility of the IT area. Only use properly licensed and approved IT resources, after a risk analysis.

- **Confidentiality agreements and term of responsibility**: every employee of Randon Companies must attest to their knowledge of the Information Security Policy through the Term of Responsibility, which succinctly describes the conditions for using IT resources and information from Randon Companies.

- **Information Security Incidents**: incidents are any events that negatively affect the confidentiality, integrity and availability of information assets. It is everyone's commitment to immediately report, through the Ethics Channel, any Information Security incident. Any incident that occurs where the cause is an employee, they may suffer sanctions provided for in the Sanctions Policy.

- **Information Security Controls**: to reduce information security vulnerabilities and incidents, Randon Companies have controls such as equipment and mobile device management, antivirus, email filters and internet access filters.

- **Monitoring:** Randon Companies may,
    i. Monitor technological resources to identify users and their access, as well as manipulated material;
    ii. Make the information obtained by the monitoring and auditing systems public, if legally required, and make it available to managers, as requested;
    iii. Perform physical and logical inspection on the company machines;
    iv. Install protection, prevention and detection systems to ensure the security of information and access perimeters.

- **Remote Work / Home Office**: this is a modality that Randon Companies provide to their employees so that they can work outside the corporate environment (e.g. residence, coworking, hotel, etc.). The employee is responsible for taking care of the equipment provided by the company, as well as the information they are accessing.

- **Disclosure of the Information Security Policy:** policy must be disclosed when hiring employees and when there is an update that affects culture or operation of Randon Companies. The policy can be disclosed through the Safe Connections awareness program and/or official internal communication channels.

6. RESPONSIBILITIES

Board of Directors

- Approve the policy.

Risk Management and Compliance Area

- Review and approve the general definitions of information security strategies;
- Identify by type of exposure, assess the probability of incidence and the impact, all risks that may compromise the achievement of Randon Companies' objectives.

Information Technology Area

- Monitor the resources and environments under your responsibility in order to ensure protection against possible threats and misuse, as well as keep them up to date with updates and changes in legislation and/or business requirements ;
- Manage Information Security controls and tools, as well as handle incidents, problems, changes and any requests and/or reports related to Information Security;
- Disclose Security Information Policy when an update that impacts the culture or the operation of Randon Companies occurs;
- Promote a culture of Information Security.

Managers

- Disseminate the Information Security culture by example, verifying compliance with controls, as well as advising employees and interns they manage;
- Define and control the access privileges of employees and interns they manage according to the activities they perform.

Employees and interns

- Know and comply with the Information Security Policy, as well as other controls, especially the procedures related to it and applicable to the activities performed.

7. GENERAL PROVISIONS

Information protection must be part of employee conduct. Undue disclosures can cause disadvantages, financial losses and/or damage to the image of Randon Companies. Whenever you become aware of the leak of confidential information, this fact must be reported through the Ethics Channel, so that the appropriate measures can be taken.

8. CONTROL INFORMATION

This Policy was approved by the Board of Directors on November 07, 2017 and has been effective since November 2017.

Responsibilities for this document:

Author	Review	Approval
Information Technology	Risk Management and Compliance	Board of Directors

Last review:
Date: Nov 10, 2022.