INFORMATION SECURITY POLICY

1. OBJECTIVE

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

2. APPLICATION AND SCOPE

This Policy applies to all employees, interns, suppliers, service providers or any other persons who are users of Randoncorp information.

3. REFERENCES

- Randoncorp Code of Ethical Conduct.
- Consequences Policy.
- ABNT NBR ISO/I EC 27001 – Information technology – Security techniques – Information security management systems – Requirements.
- CERT.br – Center for the Study, Response and Treatment of Security Incidents of Brazil.
- NIST – *National Institute of Standards and Technology.*
- Applicable Laws.

4. DEFINITIONS

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

Backup: This is the copying of data from one storage device to another so that it can be restored in the event of the loss of the original data, which may involve accidental deletions or data corruption. **Mobile Devices:** notebooks, tablets, smartphones, among others.

Security Incident: event that can cause losses to the company or even violate security rules.

5. GUIDELINES

Randoncorp's Information Security Policy considers information security through the following aspects:

- Confidentiality: ensuring that 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 the corresponding information and assets whenever needed.

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

This policy is in line with Randoncorp's strategic objectives.

5.1 Specific Guidelines

- **Use of resources and information:** it is everyone's commitment to ensure that information and resources are used only for professional purposes, making appropriate 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 Randoncorp or third parties. These rights apply to both tangible and intangible assets, including brands, patents, source codes and licensing agreements, among others.

- **Classification and treatment of information:** all information found in Randoncorp's physical and logical environments, including that related to its suppliers, partners and clients, must be classified according to its criticality and sensitivity. It is a commitment of all employees, interns, suppliers, service providers to ensure that information receives 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 managers, employees and interns of the Randoncorp, but the external public will not be able to access this information;

  iii. **Restricted:** the restricted classification has a medium level of confidentiality. Only authorized people may have access to information;

  iv. **Confidential:** Confidential classification has the highest level of confidentiality. Information has high value for the organization.

- **Users and Passwords:** physical and logical access will be granted only to the resources and information necessary and indispensable for the performance of activities and in accordance with the interests of Randoncorp 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. It is the employee's responsibility to ensure the correct use of their identification and the confidentiality of their password.

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

- **E-mail:** it is a work tool and must be used to support the development of functional activities. The employee is fully responsible for the use of the service, and is fully responsible for any action or damage carried out, responding for any legal or illegal act. The addresses and PO boxes 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 Randoncorp 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 Randoncorp's Information Technology resources are the exclusive responsibility of the IT area. Only duly licensed and approved IT resources are permitted to be used, subject to risk analysis.

- **Confidentiality agreements and terms of responsibility:** every Randoncorp employee must attest to knowledge of the Information Security Policy through the Term of Responsibility, which succinctly describes the conditions for using Randoncorp's IT resources and information.

- **Information Security Incidents:** any events that negatively affect the confidentiality, integrity and availability of information assets are considered incidents. Everyone is committed to immediately

reporting any Information Security incident via email to si@randoncorp.com. Any incident that occurs where the cause is an employee may suffer sanctions provided for in the Consequences Policy.

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

- **Monitoring:** Randoncorp may,
  i. Monitor technological resources to identify users and their accesses, as well as manipulated material;
  ii. Make the information obtained by monitoring and audit systems public, if legally required, and make it available to managers, as requested;
  iii. Perform physical and logical inspection of the machines owned by you;
  iv. Install protective, preventive and detectable systems to ensure the security of information and access perimeters.

- **Remote Work / Home Office:** it is a modality that Randoncorp provides to its employees so that they can work from 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.

6. RESPONSIBILITIES

Board of Managers

- Approve the policy.

Risk Management and Compliance Area

- Review and approve the general definitions of information security strategies;
- Identify, by type of exposure, evaluate as to the probability of incidence and as to the impact, all the risks that may compromise the achievement of Randoncorp's objectives.

Information Security Area

- Monitor the resources and environments under its responsibility in order to ensure protection against possible threats and inappropriate use, as well as to keep them up to date with their updates and changes in legislation and/or business requirements;
- Manage Information Security controls and tools, as well as deal with incidents, problems, changes and any requests and/or reports related to Information Security;
- Promote culture in Information Security.

Information Technology Area

- Ensure the availability of the Randoncorp environment in accordance with the information security policy and procedures.

Managers

- Disseminate the culture of Information Security by example, verifying compliance with controls, as well as guiding employees and interns under its management;
- Define the access privileges of employees and interns under their management according to the activities they perform.

Staff & 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. Improper disclosures may cause disadvantages, financial losses and/or damage to Randoncorp's image. 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 Managers on 11/07/2017, coming into effect from November 2017.

Responsible for the document:

Preparation	Review	Approval
Information Technology	Risk Management and Compliance	Board of Managers

Last revision:

Date: 12/14/2023

ID

RANDONCORP