RANDONCORP

信息安全政策

1. 目标

制定与信息安全有关的行为准则，以满足公司和个人的业务和法律保护需求。

2. 应用和范围

本政策适用于所有员工、学员、供应商、服务提供商或任何其他 Randoncorp 信息用户。

3. 参考文献

- - Randoncorp 道德行为守则。
- - 后果政策。
- - ABNT NBR ISO/I EC 27001 - 信息技术- 安全技术- 信息安全管理系统- 要求。
- - CERT.br - 巴西安全事件研究、响应和处理中心。
- - NIST - 国家标准与技术研究所。
- - 现行立法。

4. 定义

信息资产：对组织有价值的任何信息，包括设备、信息和数据。

备份：是指将数据从一个存储设备复制到另一个存储设备，以便在丢失原始数据（可能涉及意外删除或数据损坏）时可以恢复。

备份：是指将数据从一个存储设备复制到另一个存储设备，以便在原始数据丢失（可能涉及意外删除或数据损坏）的情况下恢复数据。

移动设备：笔记本电脑、平板电脑、智能手机等。

安全事件：可能对公司造成损害甚至违反安全规则的事件。

5. 指导原则

Randoncorp 的信息安全政策从以下几个方面考虑信息安全问题：

- - 保密性：保证只有获得授权的人才能获取信息；
- - 完整性：保障信息和处理方法的准确性和完整性；
- - 可用性：保证授权用户在必要时可以访问信息和相应的资产。

信息安全是通过实施一系列控制措施来实现的，这些控制措施可以是技术控制、物理控制或行政控制该政策与 Randoncorp 的战略目标保持一致。

5.1 具体准则

- **资源和信息的使用**：每个人都有义务确保信息和资源仅用于专业目的，并适当使用 IT（信息技术）资源，无论是物理资源（硬件）还是逻辑资源（软件）。员工、学员、供应商和服务提供商必须遵守和尊重知识产权，无论信息是属于 Randoncorp 还是第三方的财产。这些权利既适用于有形资产，也适用于无形资产，包括品牌、专利、源代码和许可协议等。

- **信息的分类和处理：**在 Randoncorp 物理和逻辑环境中发现的所有信息，包括与 供应商、合作伙伴和客户相关的信息，必须根据其关键性和敏感性进行分类。所有员工、受训人员、供应商和服务提供商都承诺确保根据信息的分类（分为以下级别）对信息进行标记：

  i. **公开**：在公开密级中，信息不保密，对内部和外部受众开放；

  ii. **内部**：供内部使用的保密级别较低。这些

  iii. Randoncorp 的所有董事、员工和受训人员都可获取这些信息，但外部公众无法获取这些信息；

  iv. **限制级**：限制级具有中等保密级别。只有获得授权的人才能获取信息；

v. **保密**：保密级别最高。信息对组织具有很高的价值。

- **用户和密码**：只有在符合 Randoncorp 利益的情况下，并考虑到最小特权原则的情况下，才可对开展活动所必需和不可或缺的资源和信息进行物理和逻辑访问。密码和其他形式的身份验证是单独的、保密的、不可转让的，并受到与相关信息相匹配的安全级别的保护。员工有责任确保正确使用其身份和密码的保密性。

- **互联网**：这是一种工作工具，应作为一种研究方法和专业活动的补充。访问网页和网站是每个用户的责任，禁止访问色情、游戏、赌博等不适当内容的网站。

- **电子邮件**：这是一种工作工具，应用于支持职能活动的发展。员工对使用该服务负全部责任，并对所采取的任何行动或造成的损害负全部责任，对任何合法或非法行为负责。提供给用户的地址和邮箱属于公司财产。
- **移动设备：**员工有义务按照 Randoncorp 的利益使用这些设备，并确保其安全保管，保护其物理完整性和其中所含信息的不可侵犯性，以及在公司要求时归还这些设备。

- **IT 资源的管理和保护：**Randoncorp 信息技术资源的获取、安装、配置、处理和维护由 IT 部门全权负责。在分析风险后，只能使用经正式许可和批准的信息技术资源。

- **保密协议和责任条款：**每位 Randoncorp 员工必须通过责任条款证明他们了解信息安全政策，该条款简要说明了该政策。

- **信息安全事故**：事故是指对信息资产的保密性、完整性和可用性造成负面影响的任何事件。每个人都有义务立即通过电子邮件向 si@randoncorp.com 报告任何信息安全

事件。任何由员工造成的事件都可能根据后果政策受到处罚。

- **信息安全控制**：为了减少信息安全漏洞和事故，Randoncorp 采取了各种控制措施，如设备和移动设备管理、防病毒、电子邮件过滤和互联网访问过滤。
- **监测**：Randoncorp 可能、
  i. 监控技术资源，以确定用户及其各自的访问权限以及所处理的材料；
  ii. 如果法律要求，公布监测和审计系统获得的信息，并应要求提供给管理人员；
  iii. i对其拥有的机器进行物理和逻辑检查；
  iv. 安装预防性和可检测的保护系统，确保信息和访问边界的安全。
- **远程办公/家庭办公**：这是 Randoncorp 为员工提供的一种工作模式，员工可以在公司环境之外（如家中、协同办公、酒店等）工作。员工负责看管公司提供的设备以及他们访问的信息。
- **人工智能：** Randoncorp的员工对人工智能的使用必须经过信息安全，信息技术和信息隐私部门的分析和批准。未经适当授权，不得上传敏感数据。必须与信息技术团队合作，以开发和监督流程，确保信息安全和符合信息安全政策。

6. 责任

董事会

- 批准该政策。

风险管理与合规领域

- - 审查和批准信息安全战略的一般定义；
- - 按风险类型确定、评估可能危及 Randoncorp 目标实现的所有风险的发生概率和影响。

信息安全领域

- 监测其负责的资源和环境，以确保免受可能的威胁和不当使用，并使其跟上立法和/或业务要求的更新和变化；
- 管理信息安全控制和工具，处理与信息安全有关的事件、问题、变更以及任何请求和/或报告；
- 促进信息安全文化。

信息技术领域

- 遵守信息安全政策和程序，确保Randoncorp 环境的可用性。

管理人员

- 以身作则，传播信息安全文化，核查控制措施的遵守情况，并指导下属员工和受训人员；
- 根据下属员工和受训人员所从事的活动，确定其访问权限。

雇员和受训人员

- 了解并遵守信息安全政策以及其他控制措施，特别是与之相关并适用于所开展活动的程序。

7. 总则

保护信息必须成为员工行为的一部分。不适当的泄密会造成不利、经济损失和/或损害 Randoncorp 的形象。一旦发现机密信息泄露，应通过道德渠道报告，以便采取适当措施。

8. 控制信息

本政策于 2017 年 11 月 7 日获得董事会批准，并于 2017 年 11 月生效。

负责该文件：

阐述	**评论**	**批准**
信息技术	风险管理与合规	董事会

版本	**RCA**	**日期**	**有效性**
1ª	841	07/11/2017	07/11/2017
2ª	869	14/03/2019	14/03/2019
3ª	940	10/11/2021	10/11/2021
4ª	955	04/07/2022	04/07/2022
5ª	981	14/12/2023	14/12/2023
6ª | 目前	999	12/12/2024	12/12/2024

最后修订： 日期：12.12.2024

ID

RANDONCORP