Information Security Policy

Policy No.: ROSS-IT-IS-POL-006

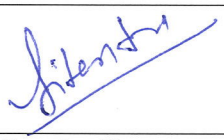
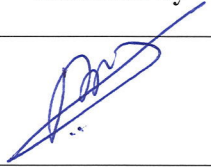
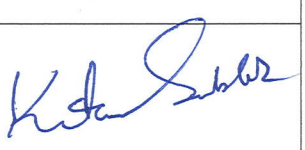
POLICY GOVERNANCE, REVISION HISTORY & REVIEW PLAN

Policy Name	ROSSARI Information Security Policy
Policy No.	ROSSARI-IT-IS-POL-006
Current Version	2.0
Effective Date	01-Jan-2026
Owner Department	Information Technology (IT)
Next Review	Every two years

Document History

Date	Description Of Change	Author	Authorized By	Verified By	Version #
01-01-2024	Initial	Rakesh Dhanda	Sunil Chari	Ketan Sablok	1.0
01-01-2026	No Changes	Jitendra Kumar	Ketan Sablok	Bhavesh Sangani	2.0

APPROVALS

Version No.	Prepared by	Reviewed by	Approved by
			
2.0 (Initial Version)	Jitendra Kumar (Asst. GM -IT)	Bahvesh Sangani (Group Head IT)	Ketan Sablok (Group - Chief Financial Officer)

1. Purpose

The purpose of the Information Security Policy is to describe the actions and behaviours required to ensure that due care is taken to avoid inappropriate risks to Rossari Biotech Limited (hereinafter referred as "the Company"), its subsidiaries & business partners, and stakeholders.

This policy outlines the mandatory minimum information security requirements for the Company and serves as an umbrella document for all other information technology (IT) policies and associated standards. This policy defines the responsibility to:

- protect and maintain the confidentiality, integrity and availability of information and related infrastructure assets;
- manage the risk of security exposure or compromise;
- assure a secure and stable IT environment;
- identify and respond to events involving information asset misuse, loss or unauthorized disclosure;
- monitor systems for anomalies that might indicate compromise; and
- promote and increase the awareness of information security.

Failure to secure and protect the confidentiality, integrity and availability of information assets in today's highly networked environment can damage or shut down systems that operate critical infrastructure, financial and business transactions and vital company functions; compromise data; and result in legal and regulatory non-compliance.

2. Policy Statement

This policy states the intent of the Company to identify and protect its confidentiality, integrity, and availability ("CIA triad") of the data employed within the Company, while providing value to the way we conduct business. Protection of CIA triad are basic principles of information security, and can be defined as:

- **Confidentiality:** Information should be accessible only to authorized personnel, many times enforced by the classic "need to know" principle.
- **Integrity:** Information should be modifiable only by authorized personnel also protecting the accuracy and completeness of information, and the methods that are used to process and manage it.
- **Availability:** Information should be made available to personnel who need it and ensuring that information assets (information, systems, facilities, networks, and computers) are accessible and usable when needed.

The Company has recognized that our business information is a critical asset and as such our ability to manage, control, and protect this asset will have a direct and significant impact on our future success.

Therefore, the Company has adopted a risk-based approach to protect its critical information assets and confidential information from likely and high-impact threats, and shall embed information security principles into the organizational culture making it the responsibility of each and every employee to ensure that a robust information security structure is maintained.

This document establishes the framework from which other IT policies are developed to ensure that the enterprise can efficiently and effectively manage, control and protect its business information assets and those information assets entrusted to the Company by its employees, partners and other stakeholders. The Company information security program is built around the information contained within this policy and its supporting policies.

3. Coverage

This policy covers all information systems operated by the Company and its group companies on-roll employees, consultants and partners. Here, the term information systems define the total environment and includes, but is not limited to, all documentation, physical and logical controls, hardware (e.g. desktop, laptops, network devices and wireless devices), software and data.

4. Policy Sections and Clauses

4.1 Document Description

It is the responsibility of all on-roll employees, consultants and partners to comply with this policy and other associated IT policies. The Company IT department is responsible for reviewing and updating this policy as and when required and /or at least once every year.

4.2 Objectives and Achievement Plan

- Protecting sensitive information from unauthorized access and disclosure.
- Minimize Security Risk by systematically managing the Company sensitive data.
- Ensuring the accuracy and completeness of information and protecting it from unauthorized alteration.
- Ensure business continuity by limiting the impact of security breaches.

Occurrence of any incident to be reported in the template, example:

Functional Objective	What will be done	Resource Requirement	Responsibility	Frequency	Results evaluation
To minimize number of information security incidents	Incident Management	People/ Process & Technology	Infrastructure Head/ CIO	Quarterly	Data on Incidents reported

4.3 Risk Management Framework

All potential risk to be captured in risk management template and reported to finance team on half yearly basis.

4.4 Security Awareness Program

It is important to implement security awareness initiatives at all levels of the organisation, including senior management, middle management, team leaders, and head of the departments, support staff, and any third parties.

The information security awareness will be an ongoing initiative that will ensure that all employees and contractors are aware of the information security policies that are relevant to them. In addition, all the procedures, guidelines, and information security best practices in conjunction with other laws, regulations, and management best practices as adopted by the Company.

Online annual information security awareness will be done in addition to an awareness session for new joiners during onboarding and induction by the respective human resources team.

4.5 Competence

The Company shall ensure that the employees and contractors in the scope of Information Security Management System (ISMS) have appropriate skills and competence to do so and maintain the records of the same.

4.6 Compliance with legal and contractual requirements

The Company shall protect its sensitive information from unauthorized disclosure. The primary laws and regulations with which it does this is as follows:

India Information Technology Act, 2000

4.7 Review

The Information Security Policy, as well as the other security policies must be periodically reviewed. This review will happen under the following circumstances:

- Once every 12 months
- If there is a significant change in the technologies in use by the Company
- If there is a significant change in the external threat environment, which mandates a review of the risk profile
- If there is a significant change in client requirements/guidelines for information security

4.9 Communication

- The Information Policy will be disseminated to all the employees, consultants and business partner using email.
- All communication related with stakeholder's media and financial markets will be done by designated person only on need basis over press event, conferences, emails. No employees of the organization until authorized by Company Secretary & Compliance Officer can connect with media or financial markets
- All employees in their daily work, should operate as representatives and ambassadors of the Company and are authorized to speak with client in align with their project and key responsibility area ("KRA"). Inside information shall be kept confidential.
- When speaking at conferences, the presentations should be checked with Company Secretary & Compliance Officer.

5. Enforcement

Necessary disciplinary action will be taken against any employee not following the policies and procedures laid down by the Company. Similarly, action will be taken against those employees encouraging/observing such an activity and not reporting the same to the concerned authority. Any employee found to have violated this policy may be subject to disciplinary action.

6. Policy Exception

Group - Chief Financial Officer is authorized to approve any exception in this Policy.

****