IT Risk Management Procedure

SOP No.: ROSS-IT-SOP-004

SOP GOVERNANCE, REVISION HISTORY & REVIEW PLAN

SOP Name	IT Risk Management Procedure
SOP No.	ROSS-IT-SOP-004
Current Version	2.0
Effective Date	24-Jul-2023
Owner Department	Information Technology (IT)
Next Review	Every two years

Document History

Date	Description Of Change	Author	Authorized By	Verified By	Version #
24-07-2023	Initial	Jitendra Kumar	Rakesh Dhanda	Santosh Mahadik	1.0
08-01-2026	No Changes	Atul Ghadigaonkar	Jitendra Kumar	Bhavesh Sangani	2.0

APPROVALS

Version No.	Prepared By	Reviewed By	Approved By
2.0 (Initial Version)	AtulGhadigaonkar (Asst.Manager - IT)	Jitendra Kumar (Asst. GM- IT)	Bhavesh Sangani (Group Head IT)

1. Purpose

The purpose of this SOP is to perform risk assessments during all stages of the system's life cycle and to evaluate the effectiveness of the security controls in place. This SOP applies to all Rossari Biotech Limited and its group Companies.

2. Definitions

2.1. IT Risk

IT risk is the potential that a certain threat will exploit vulnerabilities in an asset or group of assets, resulting in harm to the Organization.

2.2. Threat

This is any event, action, or incident with the potential to compromise system security. It can be intentional and accidental, including malware, equipment failure, human error, and natural disaster.

2.3. Vulnerability

This denotes the shortcomings or gaps in the information assets that attackers can exploit to steal sensitive information. Identifying information system weak points and their exploitation methods is critical in mitigating overall IT risks.

2.4. Asset

This is a broad term referring to organisations' software, hardware, stored data, IT security policies, privileged users, and even file folders containing sensitive data.

2.5 IT Risk Assessment

It is a process of identifying and mitigating the risks and threats that can compromise the IT infrastructure, network and database.

3. Need for IT Risk Assessment

1. Understanding the Risks
2. Evaluating the existing security controls and tools
3. Lower downtimes
4. Cost control
5. Ensure compliance

4. Type of IT Risks

1. Malware/Ransomware/Viruses
2. Spams
3. Phishing
4. Weak Authentication and Access Controls
5. Human Errors
6. Hardware /Software Failures
7. IT Asset Disposal
8. IT Asset Lost / Stolen
9. Cloud Security
10. Unauthorised access of Data Centre

5. Risk Assessment

Sr. No.	Risk	Risk Level	Impact	Control Measures	Action Point
1	Malware/ Ransomware /Virus	Moderate to High	1. Data corruption/Loss 2. Data Theft 3.Financial Loss 4. Damage to devices 5. System crash. 6. Disrupts operations	1. Regular backups 2. Be careful when downloading files or clicking on links. 3. Update software and OS regularly. 4. Install & Update Antivirus regularly.	1. Backup is taken regularly. 2. OS and applications are updated regularly. 3. Seqrite Antivirus software is installed and updated regularly. 4. The infected asset has been isolated from the network, and a thorough antivirus scan has been completed. 4. IT awareness training sessions are held at regular intervals or whenever necessary. 5. IT policies and procedures are implemented and strictly adhered. 6. Computer users should stay Vigilant & report suspicious activities to IT.
2	Spams	Low to Moderate	Floods Email accounts & consumes storage space.	1. Spam filters to automatically move spam emails to separate folders. 2. Verify that no valid emails have been incorrectly flagged as spam. 3. Awareness Training to Users	1. IT awareness training sessions are held at regular intervals or whenever necessary. 2. IT policies and procedures are implemented and strictly adhered. 3. Computer users should stay Vigilant & report suspicious activities to IT.
3	Phishing	High	1. Data theft. 2. Financial Loss. 3. Stolen credentials lead to unauthorized transactions.	1. Need to be cautious when receiving unexpected emails, especially those requesting sensitive information. 2. Prior to clicking, ensure the authenticity of the links. 3. Training on various methods used in phishing and emphasize on staying vigilant.	1. IT awareness training sessions are held at regular intervals or whenever necessary. 2. IT policies and procedures are implemented and strictly adhered. 3. Computer users should stay Vigilant & report suspicious activities to IT.

Sr. No.	Risk	Risk Level	Impact	Control Measures	Action point
4	Weak Authenticati on & Access Controls	Moderate to High	1. Sensitive information is exposed. 2. Financial loss. 3. Damage to reputation.	1. Grant unique IDs and credentials. 2. Control all enterprise applications through proper authorization mechanism. 3. Data centre entries are restricted. 4. IT security policy	1. Conducted IT security awareness training. 2. Applications frequently remind users to change their passwords at regular intervals. 3. Security policies are applied on Firewall. 4. Ensures compliance with IT security policy.
5	Human Errors	Moderate to High	1. Intentionally or accidentally opening an email containing viruses. 2. Data deletion either intentionally or accidentally. 3. Incorrect data processing. 4. Data breach	1. Implement Email, Internet usage & Cyber security policies in organization. 2. IT awareness training. 3. Install & update Antivirus Software. 4. Ensure compliance of Data backup & restoration policy and IT security policy.	1. IT policies are implemented and strictly adhered. 2. The infected asset has been isolated from the network and a thorough antivirus scan has been completed. 3. Email, Application & Data server password is changed immediately. 4. Data is restored from the backup drive.
6	Hardware / Software Failure	Low to Moderate	1. System Downtime 2. Lost productivity 3. Missed Deadlines 4. Financial Loss	1. Backup Data 2. Update application and OS patches. 3. Install and update Antivirus software.	1. A standby computer is provided in the event of hardware/software failure. 2. User credentials are restored. 3. Data server access is provided on standby system. 4. Data is restored from the backup drive.
7	IT Asset Disposal	High	1. Data security breach 2. Environment compliance	IT asset disposal process must be documented and adhered.	1. Asset is disposed through an authorized E-Waste vendor. 2. IT Assets Management Policy to be followed. 3. E-waste Disposal Certificate to be maintained.
8	Lost / Stolen of IT Asset	High	1. Data theft. 2. Financial Loss.	Implement IT asset management policy.	1. IT Assets Management Policy is implemented. 2. Email, Application & Data server password is changed immediately.
9	Cloud Security	High	1. Data security breach 2. Operations disruptions 3. Financial Loss 4. Can lead to significant damage to business reputation.	Data Backup & Restoration policy	We are using Google private cloud platform. Private cloud provides enhanced cybersecurity by allocating dedicated resources to a single organization, thereby minimizing the risk of external threats.