RIKHAV SECURITIES LTD
B-501, 5TH FLOOR, O2 COMMERCIAL BUILDING, ASHA NAGAR, MULUND WEST,
MUMBAI - 400080.

SEBI Registration No: INZ000157737 BSE/NSE/MCX

SEBI Registration No: IN-DP-CDSL-12051500

Cyber Security

Incident Management Procedure

Table of Contents

1. Purpose

This SOP helps in providing guidance to both technical and managerial staff to quickly respond tofor all types of cyber security events and incidents and handle it in a consistent manner with the following objectives:

- To ensure complies with applicable legislative and regulatory guidelines.
- To facilitate effective, coordinated, security incident response.
- To identify the root cause of computer security incidents, and implement measures to prevent further incidents of a similar nature.
- To enable continuous improvement of **RIKHAV SECURITIES LTD** intrusion detection capability.

2.Framework-

- SEBI Circular - Cyber Security & Cyber Resilience framework for Stock Brokers / Depository Participants for the Broking Sector dated 3rd Dec 2018. Exchange circular NSE/INSP/48163 dated May 03, 2021

3. Responsibility for Implementation

Compliance with this procedure is mandatory and implementation responsibility is with IT team and other suppoting teams.

4. Review and Deviations

The procedure shall be reviewed / updated annually against IT environment and business requirement to ascertain its appropriateness. Any deviation or exception to this procedure shall be documented and formally approved from competent authorities such as CTO, ITRO, CIO and amended procedure shall be shared with relevant stakeholders.

5. Procedure Requirements

5.1 Roles & Responsibilities

All the employees from end users, third-party staff to senior management have the responsibilities to protect the **RIKHAV SECURITIES LTD** information system from unauthorized access, modification, disclosure and security threats.
In order to minimize the adverse impact on business operations and to optimize activities undertaken to restore normal service operation, it's essential to carefully consider the roles and responsibilities within **RIKHAV SECURITIES LTD** depending on the incident type.

Below are the defined resposibilities for different team members in case of incident management:

5.1.1 IT Team

a. IT team familiar with **RIKHAV SECURITIES LTD** information systems, may often be the first to discover a security event.

b. They are responsible for immediately reporting critical events which are classified as incidents to the CISO. Additionally, they will be called upon to help determine and implement a solution, whenever applicable.

5.1.2 IT Continuity and Business Continuity Team

a. This team is responsible for IT continuity, business continuity and crisis related consulting.

5.1.3 Legal Team

a. This team is responsible for legal consulting as well as assist in cyber insurance.

5.1.4 Compliance

5.1.4.1 This team is responsible for compliance consulting, regulatory reporting and media communication to external entities.

5.1.5 HR Team

5.1.5.1 The Human Resources department must be involved in the incident management process ifan employee is suspected of causing a Cyber security incident.

Refer detailed Cyber Security Incident Management Team Structure & point of contact in case of cyber security incident management.

5.2 Threat Environment

a. Although events may take many forms and involve many devious means, there are certain types of attacks which occur more frequently than others.

b. Knowing what these types of attacks are and how the **RIKHAV SECURITIES LTD** counters them will help the **RIKHAV SECURITIES LTD** staff be best prepared to react and report all related information to the local team for further investigation.

5.2.2 Internal Threat

a. An internal threat is any instance of a user misusing resources, running malicious code or attempting to gain unauthorized access to an application. Examples include unauthorized use of another user's account, unauthorized use of system privileges, and execution of malicious code that destroys data.

b. More significant internal threats may include an otherwise authorized system administrator who performs unauthorized actions on a system.

5.2.3 External Threat

a. An external threat is any instance of an unauthorized attempts to gain access to systems or cause a disruption of services. Examples include disruption/denial of service attacks, mail spamming and execution of malicious code that destroy data or corrupt a system.

5.3 Cyber Security Incident Management Process

To protect the concerned individuals, units as well as the **RIKHAV SECURITIES LTD** as whole, cyber securityincidents must be handled as soon as possible.

5.4 Incident Detection

Timely identification and reporting of incidents is critical for their effective management and an indicator of risk culture. Incidents must be escalated to internal stakeholders as soon as possible to enable them to commence mitigation activities. This will ensure that incidents and any potential control weaknesses are addressed in a timely manner with clear accountability.

The concerned personnel should immediately bring it to the notice of the immediate supervisor/Manger and / or the Systems Administrator or the Head of the department. The incident may be reported by e-mail in case of emergency.

All the incidents shall be reported through appropriate management channels as quickly as possible.

5.5 Investigating cyber-security events

In the early stages of investigating a cyber-security incident, the precise nature of the incident may be unknown and initial analysis will be required. When investigating a cyber-security event, the approach taken can be either:

- Intelligence driven, based on information gathered from: Monitoring of internal resources, open source information or data provided internally
- Evidence-driven, based on information gathered from corporate infrastructure or applications (typically event logs)

Investigators will often wish to:

- Examine important alerts or suspicious events in logs or technical security monitoring systems (eg. IDS, IPS, DLP or SIEM)
- Correlate them with network data (including data from cloud service providers)
- Compare these against threat intelligence.

When carrying out an investigation, each possible trigger event should be thoroughly investigated, including:

- Date/time
- Internet protocol (IP) address (internal or external)
- Port (source or destination), domain and file (eg. exe, .dll)
- System (hardware vendor, operating system, applications, purpose, location).

Consequently, it is important that cyber security monitoring and logging process enables us to provide all the information needed to carry out a fast and effective investigation.

Events should be assessed and it should be decided if they are to be classified as information security incidents or Cyber Security incidents.

The Incident Owner should complete the investigation and compile an Incident Report which should provide a full and consolidated account of the Incident with true, accurate, complete and non-misleading information and in sufficient details, based on the investigation and all the relevant details and supporting documents and materials.

The Incident Report should be reviewed by the Designated Officer and Technology committee members from a risk perspective and by Relevant Officers from a regulatory compliance perspective to assess whether the Incident is fully investigated.

Below are the mandatory attributes which must be captured for each incident.

- Date and Time of the Incident
- Reported by (Name/department/designation)
- Reported to (Name/department/designation)
- Incident Description
- Incident type
- Location of the incident
- Severity level
- Impact Assessment
- Resulting damage
- Immediate action taken
- Planned action and resulting preventative measures

Incident Severity level

The severity scale defines the impact and scope of a cyber-security incident on a 4 level scale from the less significant to the most critical.

- Negligible
- Minor
- Significant
- Critical

All incidents must be analysed during the phase of investigation and the severity of the incident classified according to the several criteria.

5.6 Cyber Security Incident Response

Security event reports should be produced for cyber security incidents (particularly those with a high priority), which should cover a range of important details, such as:

- Activity date and time
- External endpoints affected
- Activity details (symptoms of the event)
- Risk (details about a possible attack)
- Collecting evidence as soon as possible after the occurrence
- Escalation as required
- Dealing with Cyber security weaknesses found to cause or contribute to the incident

Cyber security incident response capability, enabling us to assess state of readiness to:

1. Prepare for a cyber-security incident: performing a criticality assessment; carrying out threat analysis; addressing issues related to people, process, technology and information; and getting the fundamentals in place.

2. Respond to a cyber-security incident: covering identification of a cyber-security incident; investigation of the situation (including triage); taking appropriate action (eg. containing the incident and eradicating it's source); and recovering from a cyber-security incident.

3. Follow up a cyber-security incident: considering our need to investigate the incident more thoroughly; report the incident to relevant stakeholders; carry out a post incident review; build

on lessons learned; and update key information, controls and processes.

5.7 Incident Closure

The Cyber security incident is closed when all the counter measures and analyses intended to eradicate the incident have been performed.

The Incident Owner should finalize the Incident Report with the details of investigation results and action plan after obtained the confirmation from designated officer and Relevant/Monitoring team.

Before closing the Incident, Designated Officer should classify the risk cause type and risk event type of the Incident in Incident report.

6 Recording and Reporting

The IT Security Architect is accountable for the maintenance of cyber security metrics for periodic reporting to Management. The metrics will cover the following aspects of Practical Financial Services P Limited cyber security management:

- Current risk level;
- Control effectiveness;
- Maturity of the Practical Financial Services P Limited approach to cyber security against best practice frameworks;
- Financial status.

Quarterly cyber security incident reports will be provided to the Designated Officer, Technology Committee and relevant authorities.

7 Retention of Incident Records

Incident records should be maintained for minimum 5 years.

8 Enforcement

Failure to follow the organisation policies and procedures may result in internal disciplinary action, which may include fines, suspensions, and/or termination. The organisation reserves the right to reflect any violation of its policies and procedures on a supervised person's. The Organisation, through its IT Head/DO, is committed to implementing and enforcing these procedures.