**Standard Operating Procedure for Handling Cyber Security Incidents**

# Scope

This SOP applies to all employees of Member.

# Objective

The objective of this SOP is to establish a framework for the timely and effective handling of cyber security incidents by Member. This SOP aims to ensure that Member is able to identify, contain, and mitigate cyber security incidents in a manner that minimizes the impact on its operations and the securities market as a whole.

# Roles and Responsibilities

The following are the key roles and responsibilities for handling cyber security incidents:

* Chief Information Security Officer (CISO)/Information Security Officer: The CISO/Information Security Officer is responsible for developing and implementing Member's cyber security policies and procedures. The CISO is also responsible for leading the response to cyber security incidents.

|  |  |
| --- | --- |
| **Designation** | **Name** |
| Information Security Officer | Mr. Arvind M Vinchhivora |

* Incident Response Team (IRT): The IRT is responsible for responding to cyber security incidents. The IRT should be composed of representatives from Member's IT, legal, and compliance departments.

|  |  |
| --- | --- |
| **Incident Response Team (IRT)** | |
| **Name** | **Designation** |
| Mr. Arvind M Vinchhivora | IT Head/ Information Security Officer |

* Employees: All employees are responsible for reporting any suspected cyber security incidents to the IRT immediately.

# Incident Response Process

The following are the steps involved in the incident response process:

1. Detection: The first step is to detect a cyber-security incident. This can be done through a variety of means, such as monitoring network traffic, reviewing system logs, and conducting vulnerability assessments.
2. Categorization: Member shall examine the Cyber Security incident and classify the Cyber Security incidents into High/ Medium/ Low by IRT as per incident’s impact on business, vulnerability caused in the system.
3. Containment: Once an incident has been detected, it is important to contain the damage. This may involve isolating the affected system or network, removing malicious code, and changing passwords.
4. Mitigation: The next step is to mitigate the impact of the incident. This may involve restoring data from backups, notifying customers or clients, and filing a report with CERT-In.
5. Recovery: The final step is to recover from the incident. This may involve restoring systems and networks, rebuilding data, and implementing new security controls.

# Reporting

Member is required to report all cyber security incidents to CERT-In within 6 hours of detection. CERT-In is the Indian Computer Emergency Response Team, and it is responsible for coordinating the response to cyber security incidents in India. Member is also required to report cyber security incidents to SEBI within 24 hours of detection.

Member shall provide the reference details of the reported Cyber Security incident with CERTI n to the Exchange and SEBI. Members shall also provide details, regarding whether CERT-In team is in touch with the Member for any assistance on the reported Cyber Security incident

Member shall submit details whether Cyber Security incident has been registered as a complaint with law enforcement agencies such as Police or its Cyber Security cell.

# Compliance

Member is required to comply with all applicable cyber security regulations, including the SEBI Cyber Security Framework. The SEBI Cyber Security Framework sets out the minimum requirements for cyber security that Member must meet.

# Testing and Exercises

Member is required to test and exercise its cyber security incident response plan on a regular basis. This will help to ensure that the plan is effective and that employees are familiar with their roles and responsibilities.

# Documentation

Member is required to document all cyber security incidents. This documentation should include the date and time of the incident, the affected systems or networks, the impact of the incident, and the steps taken to respond to the incident.

# Review and Improvement

Member is required to review and improve its cyber security incident response plan on a regular basis. This review should be conducted in light of any new cyber security threats or vulnerabilities.

Training - Member is required to train its employees on cyber security. This training should cover the following topics:

* The importance of cyber security
* The different types of cyber security threats
* The steps that employees can take to protect themselves from cyber security threats
* Member's cyber security incident response plan

# Conclusion

This SOP provides a framework for the timely and effective handling of cyber security incidents by Member. By following this SOP, Member can help to protect its systems and networks from cyber security threats and minimize the impact of any incidents that do occur.

**FOR PINNACLE FOREX & SECURITIES PVT. LTD.**

**DIRECTOR**

|  |  |
| --- | --- |
| Policy reviewed by: | Mr. Mehul Prakash Bhadra |
| Policy Approved by: | Mr. Arvind Vinchhivora |
| Approved by the Board on: | April 13, 2024 |
| Name of the entity: | Pinnacle Forex & Securities Pvt Ltd |