PREMIER FERRO ALLOYS & SECURITIES LIMITED

Cyber Security Policy

1. Introduction

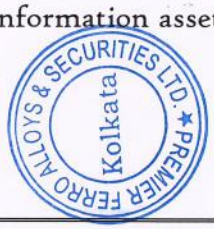
1. In addition to assessment and mitigation, a robust risk management system includes ongoing evaluation and assessment of cyber security risks and controls throughout a system development life cycle (SDLC) and organizational arrangement.
2. This Policy is framed in accordance with Master Direction - Information Technology Framework for the NBFC Sector by Reserve Bank of India dated 8th June, 2017.
3. For the purposes of this Policy references to the following shall be construed as:

Cyber Assets	Programmable electronic devices and communication networks, including hardware, software, and data.
Tailgating	It is a security breach that happens when an employee opens and holds a door for others, visitors without badges, or passively accepted uniformed employee.
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. An alternate definition of threat is an actor / adversary who may carry out an attack against the organization.
Vulnerability	A specific weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
Vulnerability Assessment	Formal description and evaluation of the vulnerabilities in an information system.

2. Scope

1. While the Information Security Policy of the Company deals with the mechanism of securing information that within the organizational structure, this Policy aims at securing the information assets and the critical business activities of the Company from external threats, more suitably termed as 'cyber attacks'.

2. This Policy covers all the functional areas within the organisation structure, which are essentially based on electronic mechanism and information technology framework, and all the employees of the organisation from Senior Management to clerk-level staff, which may directly or indirectly have access to information assets and interact with



the external environment through computer operated devices or any other electronic device which is capable of storing information or software.

3. The scope of this Policy extends to damaging actions of individuals or a group of two or more individuals, whether knowingly or unknowingly, which have a bearing on the operations of the Company.

4. The scope of this Policy would extend to all other areas, as deemed appropriate by the Board or such other authority as may be delegated by the Board.

3. Authority and Delegation

1. The primary responsibility to ensure cyber security within the organisational arrangement of the Company rests with the IT Strategy Committee ('the Committee'). Adequate authority must be delegated by the Board in order to authorise and enable the Committee to perform its functions efficiently.

2. The Committee should review the organisational arrangements, distribution of adequate authority amongst the middle and supervisory staff, periodical analysis of risks and should work in consonance with Chief Risk Officer (CRO) of the Company so that any potential threats are timely recognised and controlled.

4. Responsibilities

1. Individual responsibilities

a) Individual users must set passwords that are not easily associated with the user (e.g. Date of birth, employee number, address, numerical equivalent of names, pet names). They must not contain words from a dictionary, movie and geographical location.

b) The password must not be given to an unknown person. It must also mot be given out over phone or e-mail. The user should confirm the person's identity, who is claiming to be an IT employee, from the IT Department before allowing him to access your workstation.

c) The individual must not put any unwanted flash drive or any other electronic or storage media device into their work machines unless authorised so and the source of such device is reliable.

PREMIER FERRO ALLOYS & SECURITIES LTD. Kolkata

d) The users must not use corporate laptops in public places. However, if the same cannot be avoided, the user must make sure that it is not plastered with company logos, business card or his/her password.

e) Users should avoid Tailgating while entering or exiting a secure area.

2. Departmental responsibilities

a) A catalogue of all information assets should be maintained by all stake holders who are in-charge of the system in hard as well as soft copies, in read only mode. This catalogue may be updated and reviewed annually. The responsibility to prepare and review this catalogue rests with the IT Strategy Committee along with the Chief Security Officer.

b) The catalogue may include the following (non-exhaustive) list:

a. Item Type (H/W, S/W, databases, web contents, training material etc.)
b. Date of Procurement
c. Cost
d. Owner
e. Purpose

c) Users may also maintain their own asset catalogue and include the following in the list (non- exhaustive):

a. Service Provider contacts
b. Annual Maintenance Contract (AMC) start and expiry dates
c. Power supply information
d. Criticality and use

d) Government guidelines shall be followed to decide upon and execute the scrapping process.

5. Risk Assessment

1. Operational Risk

The Committee shall:

a) Establish internal and external information sources for cyber threat intelligence and vulnerability data, monitoring them regularly and taking appropriate actions for high-priority items.

b) Perform periodic risk assessment and mitigation, including threat analysis and Vulnerability Assessments.

c) Must refer to incident management process as laid under Information Security Policy.

PREMIER FERRO ALLOYS & SECURITIES LTD. Kolkata

d) Control, monitor, and log all access to protected assets. The organization should aggregate its logging data in a central system or repository to allow for detection, correlation, and reporting of cyber security events.

e) Redeploy or dispose of protected assets securely.

f) Define and enforce secure change control and configuration management processes.

g) Create and document contingency plans and procedures, based on a business impact analysis and per-system recovery time objectives. The contingency plans should be reviewed, exercised, and updated regularly.

2. Insecure software development life cycle ("SDLC") risks

The Committee shall:

a) Document misuse/ abuse cases and any security requirements which may arise.

b) Build a threat model and perform architecture risk analysis.

c) Define secure implementation, deployment and operations guide.

d) Perform secure code reviews and risk-based security tests, including the penetration testing.

3. Physical Security Risks

The Committee shall make sure the following:

a) Document, implement, and maintain a physical security plan.

b) Document and implement the technical and procedural controls for monitoring physical access at all access points at all times.

c) All physical access attempts (successful or unsuccessful) should be logged to a secure central logging server.

d) Physical access logs should be retained for at least 90 days.

e) Each physical security system must be tested at least once every three years to ensure that it operates correctly.

f) Testing and maintenance records must be maintained at least until the next testing cycle.

g) Outage records must be retained for at least one calendar year.

4. Third Party related risks

The Committee shall ensure the following:

a) Due diligence on each customer and partner organization to understand its business, financial, and security track record.

PREMIER FERRO ALLOYS & SECURITIES LTD. Kolkata

b) Ask questions during the request for proposal (RFP) process to understand the security posture and practices of a partner organization, and whether its offerings meet security requirements. Compare the security policies and procedures of a third party against your organization's own security policy to ensure compliance.

c) Identify and prioritize external dependencies, both upstream (the organization depends on whom?) and downstream (who depends on the organization?). The organization should pay special attention to critical dependencies; for example, relying on a single external party for a key function/service with no secondary party readily available as backup.

d) Review the hiring practices and personnel background checks of your vendors and partners to ensure that they comply with your organization's policies.

e) Ensure that service-level agreements (SLAs) and other contractual tools are properly leveraged so that vendors and partners live up to their obligations. For instance, if a breach occurs at a partner organization, there needs to be a provision to have your organization notified of the full extent of the breach.

f) Conduct periodic audits and monitoring of the third-party organization to ensure adherence to its security policies and procedures.

g) For software purchases, request a trusted independent third-party review, to include a report outlining the discovered security weaknesses in the product.

h) Ask your organization's vendors and partners about the process they use to ensure the security of the components and services that they receive from their own suppliers in order to ascertain appropriate due diligence.

i) Actively manage cyber security risks related to third parties, including formal tracking of these risks, addressing such risks in contracts and agreements, and facilitating the two-way exchange of cyber security and threat information with trusted third parties.

j) Identify external sources of cyber security information and expertise that can be consulted when required.

k) Set up and maintain secure communication channels for the exchange of sensitive data, along with any required legal protections (such as non-disclosure agreements).

5. Network Risks

The Committee shall ensure the following:

a) Restrict user-assigned devices to specific network segments.

PREMIER FERRO ALLOYS & SECURITIES LTD. Kolkata

b) Firewalls and other boundary security mechanisms that filter or act as a proxy for traffic moving from one network segment to another of a different security level should default to a "deny all" stance.

c) The flow of electronic communications should be controlled. Client systems should communicate with internal servers; these internal servers should not communicate directly with external systems but should use an intermediate system in your organization's Demilitarized Zone (DMZ) / perimeter network. The flow of traffic should be enforced through boundary protection mechanisms.

d) Ensure that all settings used on your network hardware have been set to their secure settings and that concerned personnel fully understand the settings provided by each piece of hardware. Do not assume that default settings are secure.

e) Disable all unneeded network services.

f) Ensure that the source of network time is accurate and that accurate time is reflected on all network nodes for all actions taken and events logged.

g) Requests for allowing additional services through a firewall or other boundary protection mechanism should be approved by the information security manager.

h) Protect data in transit and domain name service (DNS) traffic.

i) Usage of secure routing protocols or static routes.

j) Denial use of source routing.

k) Ensure availability of data traversing your networks. If a proper acknowledgement (ACK) is not received from the destination node, ensure that provisions are in place to resend the packet. If that still does not work, reroute the packet via a different network link. Implement proper physical security controls to make your network links harder to compromise.

l) Before granting users access to network resources, ensure that they are authenticated and authorized using their own individual (i.e., non-shared) credentials.

m) Limit remote access to your networks to an absolute minimum. When required, use technologies like Virtual Private Networks (VPNs, IPSec) to create a secure tunnel after properly authenticating the connecting party using its individual credentials. In addition to a user name and password, also use an RSA ID-like device to provide an additional level of authentication.

n) All equipments connected to your network should be uniquely identified and approved for use in the organization's network.

o) Ensure that encryption keys are changed periodically and that they can be changed right away in the event of compromise.

p) Ensure that only standard, approved, and properly reviewed communication protocols are used on the network.

PREMIER FERRO ALLOYS & SECURITIES LTD. Kolkata

q) Ensure that sufficient redundancy exists in the network links so that rerouting traffic is possible if some links are compromised.

r) Implement remote attestation techniques for your field devices (e.g., smart meters) to ensure that their firmware has not been compromised.

s) Require a heartbeat from your field equipment at an interval known to the piece of equipment and to the server on your internal network. If a heartbeat is missed or comes at the wrong time, consider treating that piece of equipment as compromised/ out of order and take appropriate action.

t) Document the network access level that is needed for each individual or role at your organization and grant only the required level of access to these individuals or roles. All exceptions should must be properly documented.

6. Vulnerability Management

1. Vulnerability Assessments would be performed by independent third parties at regular intervals, covering all of the organization's key systems, based on its threat model.
2. Vulnerability and threat data are tracked via a formal risk register, and the organization tracks and manages its response to published vulnerabilities.
3. The critical Cyber Assets should be identified and classified by the Committee.
4. The Committee shall perform a Vulnerability Assessment.
5. The Committee shall assess risks to Cyber Assets. The assessment shall combine the likelihood of a successful attack with its assessed potential impact on the NBFC's mission and goals. It shall help ensure that mitigation efforts target the highest security risks and that the controls selected are appropriate and cost-effective for the organization.

7. Cyber Security Preparedness and indicators

1. The Committee shall subscribe to a threat and vulnerability information sharing source(s) that will provide timely information on threats.
2. Such information provided shall be used to enhance internal risk management and controls and shall also be shared with applicable internal employees of the Company.
3. The Company should engage an independent IT auditor, who shall based upon the risk indicators, conduct an independent check to analysis the soundness and adequacy of control systems in place.
4. Such auditor shall submit the audit/ check report to the Committee along with the list of actionable/ suggestions, which shall be forthwith acted upon by means of review and revisions in the control systems.
5. The Management must organise awareness programmes or training among the stakeholders to spread awareness about cyber security threats, magnitude of risks

PREMIER FERRO ALLOYS & SECURITIES LTD. Kolkata

associated with them, their likely impact and the remedial course of action in case of impact.

8. Cyber Crisis Management Plan ("CCMP")

1. As soon as a cyber crisis is detected in the organisation, the Committee shall the Information Technology Officer shall immediately switch off all the networks connected to the device or server that is compromised.
2. The magnitude of the attack and as per the indicators, their likely impact must be identified and such assets/ information must be blocked from any usage.
3. All servers must be secured by hardening. And ensure that antivirus solution is installed, updated and available on all the System(s).
4. The amount of data lost or damage must be calculated and fresh networks and systems must be installed. The degree of theft or compromise must be analysed and recorded.
5. The Committee must immediately devise a reporting plan and the incident must be reported and shared with the Board of the Company, if deemed appropriate.
6. Options to recover the data and the damage done along with any required legal action must be explored from regulatory viewpoints.
7. Finally, all the systems must be updated to prevent occurrences of such incidents in future.

9. Reporting

1. The Company is required to report all types of unusual security incidents in the form **Appendix A** to the DNBS Central Office, Mumbai (Reserve Bank of India), which shall include both successful and unsuccessful attempts.
2. Fraud reporting such as suspicious transaction analysis, embezzlement, and theft or suspected money-laundering, misappropriation of assets, manipulation of financial records etc. must also be reported.
3. All regulatory/supervisory returns should be system driven.
4. There should be seamless integration between MIS system of the Company and reporting under COSMOS.

10. Policy Review

This Policy must be reviewed at such intervals as may be decided by the Board or the Committee.

APPENDIX - A

RBI Form for reporting of an incident

Template for
reporting cyber incide

PREMIER FERRO ALLOYS & SECURITIES LTD.
Kolkata