ARYA FIN-TRADE SERVICES (INDIA) PRIVATE LIMITED

STANDARD OPERATING PROCEDURE
INFORMATION SECURITY AND DATA PROTECTION & HANDLING INCIDENT REPORTING

Version	2024/01.02	Original Adoption Date:	31/05/2021
Review Date	05/04/2024		
Review & Approved by		Reviewed by Technology Committee & Approved by Board of Directors	

Summary: Describes the procedure for reporting information security incidents to the regulators & System to handle incidents by Stock Broker & DP (herein after referred as "Member").

1 Background and purpose

Member has implemented a number of technical and procedural controls and staff training to help protect the Member's information from a breach in the confidentiality, integrity or availability of the information. Where these measures fail, either deliberately or accidentally, the requirements of this Procedure must be followed.

The purpose of this Procedure is to ensure that all actual and potential information security incidents are reported in order to:

- Facilitate a fast response to incidents in order to contain or minimize the impact of the incident;
- Clarify the responsibilities of those involved in reporting incidents;
- Provide support to those who are affected by the incident; and
- Provide information regarding the causes of incidents so that improvements can be made to mitigate the risk of a further occurrence.

Reporting of incidents and "near misses" should be viewed positively as it will allow the member to analyze trends, rectify vulnerabilities and thereby reduce the likelihood or impact of future incidents.

2 Definitions and scope

For the purpose of this Procedure the following definitions apply:

Highly Restricted and Very Sensitive Information – the unauthorised or accidental disclosure of this type of information would result in a significant financial, regulatory, reputational or legal impact on the Member. Examples of information which fall into these categories are Client KYC and Financial details, trading data and securities holding data.

Information – means all information created or received in the course of Members' business which must be protected according to its sensitivity, criticality, and value, regardless of the media on which it is stored, the location of the data, the manual or automated systems that process it, the methods by which it is distributed or the locations from which it is accessed.

Information Security Incident – is an event which results or has the potential to result in the compromise, misuse, or loss (confidentiality, integrity or availability) of information or information assets at the Member, including actual or suspected incidents, as well as any perceived weaknesses that may cause an incident to occur.

A Data Protection Incident includes person-identifying information. Incidents include, for example:

Confidentiality losses:

- The accidental or deliberate unauthorised disclosure of information, such as person-identifying information;
- The unauthorised access to information or systems;
- The theft of information systems/equipment or data;
- Breach of policy - such as the information security policy or data protection policy

Integrity losses:

- The accidental or unauthorised deliberate modification of information;
- The incorrect processing of data.

- The accidental or unauthorised deliberate destruction of information;
- Actions which make an information system unavailable;
- The inability to access an information system when needed for operations

Further examples are listed in Appendix A.

Person - identifying information - any data which relates to a living individual who can be identified from that data, or from that data in conjunction with other readily available information.

Special category and criminal conviction personal data (previously known as Sensitive Personal Data): a sub-category of personal data that could cause harm or distress to an identifiable individual if generally released, including information relating to an individual's:

- Basic KYC Information
- Trading Data
- Securities Holding Data
- Financial Data viz Income Range, Occupation, etc

Additional conditions and safeguards must be applied to ensure that special category and personal data is handled appropriately by Member and is treated as Highly Restricted information. Member also recognizes other personal data besides special category data as Highly Restricted information.
This Procedure applies to all members of staff, as well as individuals conducting work at or for the Member and/or its subsidiaries, who are duly authorized to have access to Members' IT facilities ("staff"). This includes suppliers/vendors. This Procedure also applies to all third parties who have access to information classified as Very Sensitive, Highly Restricted or Restricted or critical systems, related to the conduct of Members' matters, such as Members' Back office Access, front end database access, etc.

3 Procedure and responsibilities

Consequences of non-compliance with this Procedure

Compliance with this Procedure is mandatory and non-compliance must be reported to the Head of Information Governance who will determine the action to be taken.

Staff must note that any breach of this Procedure may be treated as misconduct under relevant disciplinary procedures and could lead to disciplinary action.

Report and contain potential harm

Reporting of the Cyber Security incident shall be done to Indian Computer Emergency Response Team (CERT-In) in accordance with the guidelines / directions issued by CERT-In from time to time. Additionally, the Members, whose systems have been identified as "Protected system" by National Critical Information Infrastructure Protection Centre (NCIIPC) shall also report the incident to NCIIPC.

Designated Official can report an adverse activity or unwanted behavior which they may feel as an incident to CERT-In. They may use the following channels to report the incident.

E-mail: incident@cert-in.org.in
Helpdesk: +91-1800-11-4949
Fax : +91-1800-11-6969

Contents of Incident Report

The following information (as much as possible) may be given while reporting the incident

- ➤ Time of occurrence of the incident
- ➤ Information regarding affected system/network
- ➤ Symptoms observed
- ➤ Relevant technical information such as security systems deployed, actions taken to mitigate the damage etc.

To SEBI within within 6 hours of noticing / detecting such incidents	Email to sbdp - cyberincidents@sebi.gov.in

Reporting to Exchange to be done via Quarterly Incident Reporting mechanism within 15 days from the end of Quarter.

Confidentiality

Any discussion of the incident or circulation of any related documents or emails must be restricted to those directly involved in the investigation.

Actions and notifications

Any further actions to be taken will be determined following the investigation.
The communication of any data breach which involves person-identifying information must be handled with care and sensitivity, and appropriate advice will be provided.
Wider communication of an incident, including notification to any regulatory authorities, such as Vendor/SEBI/Exchange/DP/Cert-in, will be managed by the Designated Technology Commit- tee.

Incident evaluation and follow up

The incident may highlight remedial action which is required in relation to procedures, IT systems or the incident reporting procedure. Any agreed actions and target dates for completion will be recorded. The Designated Tech Committee will:

- ➤ liaise with regulators & Vendors to ensure that local actions are completed;
- ➤ escalate any actions which have not been completed by the target date; and
- ➤ ensure that guidance material is revised to reflect any learning outcomes.

4 Monitoring compliance with the Procedure

Enforcement

Directors & Designated Officer are responsible for ensuring that all staff within their area act in accordance with this Procedure.

Audit

Audit shall be conducted as specified by regulatory.

Reporting

Quarterly MIS on Incident shall be prepared & placed before board. Quarterly Incident Re- porting shall be done (even if) Nil Incidents to Exchanges and DP within 15 Days from the end of Quarter.

5 Review of procedure

This Procedure will be reviewed at least every two years or when significant changes are required.

APPENDIX A

EXAMPLES OF INFORMATION SECURITY INCIDENTS

The examples provided below are a guide and not a defined list.

Actual unauthorised disclosure of Very Sensitive, Highly Restricted or Restricted information1 for example:

- by sending an email or Teams chat/post to the wrong internal or external recipient
- by attaching incorrect attachments to emails
- by including data in the attachment or in the thread of the email which shouldn't be provided
- uploading information to to a website which can be accessed by unauthorised persons
- uploading information to a SharePoint site which should not be available to those who have access to the site
- sharing a sharepoint link outside the security classification including need to know
- including live data in testing or training materials
- papers collated incorrectly and sent to an incorrect recipient
- phishing/ransomware

Potential disclosure of Very Sensitive, Highly Restricted or Restricted information1 for example information in digital, paper or other format which is:

- held in unlocked cabinets/cupboards
- missing from archives, cupboards, desks, printers
- left on desks, printers, whiteboard or flipchart displays in meeting rooms
- left, lost or stolen - for example:
  - stolen from premises or cars
  - left on public transport
  - lost in transit
  - left behind during office removals
- Incorrectly disposed of eg papers not shredded on disposal or left in insecure locations prior to shredding; digitally stored information not securely wiped

Lost or stolen equipment which provides access to Members' information for example:

- Laptops, desktop PCs, trading PCs, tablets, removable storage devices such as USB sticks and removable hard drives
- Member issued or supported smart phones

Technical Incidents

- Backup failure
- Unplanned system downtime
- Patch management process failure