Adventz Securities Enterprises Limited

Incident Reporting Process

Purpose

The purpose of this policy is to establish a standard process for the reporting of security incidents by users and subsequent reporting to the RBI.

Scope

The scope of this policy includes all personnel who have has access to the *company's* Information Assets/resources.

Policy

- A security incident can be anything from an active threat to an attempted intrusion to a successful compromise or data breach. Policy violations and unauthorized access to data such as health, financial, social security numbers, and personally identifiable records are all examples of security incidents

- In case a user anticipates an incident to be a Security Incident, he should immediately report the same. Such reporting should contain the minimum of the following

    - Date of incident
    - Time of incident
    - Location
    - Nature/Description of Incident
    - Information Assets compromised

- On receipt of report regarding a Security Incident/ On identifying a Security Incident, the CIO should report the same to RBI by way of "Security Incident Reporting (SIR)" within 24 hours. Cyber Security Incident Reporting (CSIR) Form is attached in Annexure – A.

- Subsequently the CIO shall be responsible for providing Subsequent updates to RBI as and when necessary. (updates to be provided if the earlier reporting was incomplete i.e. investigation underway or new information pertaining to the incident has been discovered or as per request of RBI).

Review of the Policy

The Company is required to review the above policy in every two years based on its own experience, business need and RBI guidelines in this regard.

Annexure - A

Cyber Security Incident Reporting (CSIR) Form

Particulars	Information
1. Particulars of reporting ▪ Name of the NBFC ▪ Date and Time of Reporting to RBI ▪ Name of Person Reporting ▪ Designation/Department ▪ Contact details (e.g. official email-id, telephone no, mobile no)	
2. Details of Incident ▪ Date and time of incident detection ▪ Type of incidents and systems affected ▪ What actions or responses have been taken by the NBFC at the time of first reporting/till the time of subsequent reporting?	
3. Impact Assessment ▪ Business impact including availability of services ▪ Impact on stakeholders ▪ Financial and market impact ▪ Regulatory and Legal impact	
4. Chronological order of events: ▪ Date of incident, start time and duration. ▪ Escalations done including approvals sought on interim measures to mitigate the event, and reasons for taking such measures ▪ Stakeholders informed or involved ▪ Channels of communications used (e.g. email, internet, sms, press release, website notice, etc.) ▪ Rationale on the decision/activation of BCP and/or DR	
5. Root Cause Analysis(RCA): ▪ Factors that caused the problem/ Reasons for occurrence, Cause and effects of incident ▪ Interim measures to mitigate/resolve the issue, and reasons for taking such measures, and ▪ Steps identified or to be taken to address the problem in the longer term. List the remedial measures/corrections affected(one time measure) and/or corrective actions taken to prevent future occurrences of similar types of incident	
6. Date/target date of resolution	