Choice
The Joy of Earning

CHOICE EQUITY BROKING PVT. LTD.

INCIDENT MANAGEMENT POLICY

Document Classification: Internal

Version Control

Action	Date	Revision Details	Prepared / Amended By	Approved By
Created On	17-Oct-16	1.0	Mahesh Tamhankar	Amit Jaokar
Reviewed On	21-Feb-17	1.1	Mahesh Tamhankar	Amit Jaokar
Reviewed On	13-Feb-18	1.2	Mahesh Tamhankar	Amit Jaokar
Reviewed On	20-Feb-18	1.3	Mahesh Tamhankar	Utpal Parekh
Reviewed On	10-Aug-19	1.4	Mahesh Tamhankar	Yogesh Jadhav
Reviewed On	11-Jan-20	1.5	Mahesh Tamhankar	Yogesh Jadhav
Reviewed On	15-July-21	1.6	Sunil Utekar	Yogesh Jadhav
Reviewed On	08-Jan-22	1.7	Sunil Utekar	Yogesh Jadhav
Reviewed On	10-Apr-23	2.0	Ashutosh Bhardwaj	Yogesh Jadhav
Reviewed On	31-Jan-24	2.1	Anil Ashok & Associates	Ashutosh Bhardwaj
Reviewed On	28-Mar-24	2.2	Babu Holeyara	Ashutosh Bhardwaj
Reviewed On	04-Sep-24	2.3	Abhishek Vinayak	Ashutosh Bhardwaj
Reviewed On	08-Jan-25	2.4	Abhishek Vinayak	Ashutosh Bhardwaj

TABLE OF CONTENTS

1.0 Purpose 3
2.0 Scope 3
3.0 Definitions 3
4.0 Incident Response Team 4
5.0 Sharing of Incident Information 5
6.0 Incident Handling 6
7.0 Process of handling client complaints. 7
8.0 Management Reporting 7
9.0 Incident Management Escalation Matrix 7
10.0 Incident Management Flow Chart 8
11.0 Document References 9
12.0 Annexures 9
12.1 Annexure A – Key systems/departments handling operation and assigned responsibilities at business owner and technology owner level………………………………9

1.0 Purpose

An incident management process shall be established to identify, analyze, respond and mitigate incidents effectively.

2.0 Scope

The scope of this policy is IT service owned or operated under Choice Equity Broking Pvt. Ltd.

The scope includes functions w.r.t login, order placement (including modification & cancellation), order execution, order confirmation, order status, margin updates, risk management etc.

3.0 Definitions

Incident

An incident is an unplanned interruption or quality reduction of an IT service due to operation failure or technical glitch.

Problem

A problem is a cause, or potential cause, of one or more incidents.

Crisis

Crisis is an escalated incident which breaches the manageable threshold/ severity/ impact of an incident; impacting Choice Equity Broking Pvt. Ltd. revenue, data loss, availability, customer and internal users.

Technical Glitch

'Technical glitch' shall mean any malfunction in the Member's systems including malfunction in its hardware, software, networks, processes, or any products or services provided by the Member in the electronic form. The malfunction can be on account of inadequate Infrastructure/systems, cyberattacks/incidents, procedural errors, and omissions, or process failures or otherwise, in their own systems or the one outsourced from any third parties, which may lead to either stoppage, slowing down or variance in the normal functions/operations/services of systems of the Member for a contiguous period of five minutes (5 minutes) or more.

Business Disruption

Business Disruption shall mean either stoppage or variance in the normal functions /operations of systems of Choice Equity Broking Pvt. Ltd., due to a technical glitch, for a continuous period of more than 5 minutes

4.0 Incident Response Team

Incident Response Team

An incident response team, consisting of appropriately skilled members of the organization to handle incidents, shall be formed to handle incidents through its lifecycle. The team shall support the assessing of, responding to, and managing of incidents, to a successful closure.

Incident Handler

A dedicated Incident Handler shall be identified by/from the Incident Response team. The Incident Handler shall be responsible for the following:

- Lead the Technology and Business Services team in conducting forensic investigation and mitigation of the incident
- Identify duration and types of logs to be analyzed during the incident
- Ensure that logs and evidence being captured is following the Digital Evidence Handling Guidelines
- Communicate the scope and activities, to be undertaken as a part of forensic activities, to the Technology/ Business Services Team
- Identify compromised systems by performing root cause analysis and notify the relevant teams
- If BCP/DR is invoked, ensure teams perform their roles and responsibilities as per the Business Continuity and Disaster Recovery Plan
- Formulate recovery strategy based on the type of incidents
- Ensure all decisions being taken and actions being performed are recorded for future analysis and knowledge management
- Notify the Incident Response Team of resolution of the incident
- Ensure compliance to the Incident Management policy and procedure

The Incident Response team shall coordinate with the following teams, when required:

- Information Security Team - evidence gathering
- Technology - evidence gathering
- Business - evidence gathering & business impact assessment
- Compliance - communication to regulators
- Communications - communications to identified parties
- Legal - coordinating with law enforcement agencies
- Business Continuity - BCP/ DR issues

Incident Response Team

Sr.No.	Role	Name	Responsibilities
1	Incident Manager	Sunil Utekar (Head IT)	The incident manager is responsible for coordinating the incident response process and ensuring that all necessary resources are available to resolve the incident.
2	Technical Specialist	Shailendra Chaudhari (Sr. Manager DevOps)	Technical specialists are responsible for providing technical expertise and support to resolve the incident. This could include network engineers, application developers, or security analysts.
3	Operations Specialist	Chetan Kunder (IT)	Operations specialists are responsible for ensuring that all affected systems and processes are identified and that the incident response process does not disrupt normal operations.
4	Communications Specialist	Levin Peeyus (Sr. Executive)	Communications specialists are responsible for communicating the incident status and updates to all relevant stakeholders, including customers, employees, and partners.
5	Security Specialist	Shripad Mayekar (Manager Information Security)	Security specialists are responsible for ensuring that the incident response process does not compromise the organization's security posture, and that any vulnerabilities or threats are identified and addressed.
6	Business Continuity Manager	Ankit Jain (Senior Vice-President)	Business continuity specialists are responsible for ensuring that critical business processes and operations are not disrupted by the incident, and that the organization can continue to operate despite the incident.
7	Chairperson	Yogesh Jadhav (CTO)	Chairperson for the incident response team is responsible for the actual declaration of disaster, invoking the BCP and shifting of operations from PDC to DRS whenever required.

Incident Response Team Services

The incident response team shall be responsible for the following services:

- Implement a structured and consistent framework for the management of all incidents

- Provide response capabilities during incident lifecycle to mitigate the effects of incidents
- Facilitate communications regarding incidents
- Update senior management to enable them to make timely decisions about the incident
- Monitor compliance with policy and procedure
- Ensure compliance with required legal and regulatory requirements
- Advise on root cause analysis based on the impact of the incident
- Assist the management to envision the problem scenario that the incident can develop to.

Crisis Management Team/Incident Response Team

- Choice Equity Broking Pvt. Ltd., shall constitute an Incident Response Team as mentioned in the above table involving senior officials or management personnel of the members from different line of businesses, chaired by CTO.

- The incident response team shall be responsible to assess the incident, oversee the implementation of the corrective and preventive actions and ensure the implementation of policy and procedure.

Designated Officer

The designated officer (Compliance Officer) shall be responsible for ensuring compliance to the aforementioned exchange reporting requirements as per section 5.0 , sub section 5.

5.0 Sharing of Incident Information

1. All incidents will be reported to the Compliance, Risk Management committee and IT Steering Committee.

2. All communications with the media, other broadcasting channels and agencies shall be directed through the Communications team, in consultation with the CISO and CTO.

3. All communications regarding business disruption with clients shall be done by the Compliance/Business Risk team. There shall be an alternate means of communication including channel for communication with the clients in case of any disruption.

4. All client communication should be completed within 30 minutes from the time of disruption.

5. Technical glitches, resulting in business disruption needs to be reported to the exchange over email ID: infotechglitch@nse.co.in as under:

   1. Choice Equity Broking Pvt. Ltd. shall intimate the Exchange about the incident within 1 hour from the start of the glitch.

   2. A preliminary incident report shall be submitted to the Exchange within T+1 day of the incident (T being the date of the incident). The report shall include the date and time of the incident, the details of the incident, effect of the incident and the immediate action taken.

   3. Root Cause Analysis (RCA) of the issue in the format as enclosed in Incident Management Procedure, to be submitted within 14 working days. The RCA must include details of the incident, time of occurrence and recovery, impact, summary as well as a detailed analysis of the cause of incident, immediate action taken and the long-term plan of action.

6.0 Incident Handling

Choice Equity Broking Pvt. Ltd. has a robust system and technical infrastructure in place to provide seamless service to clients. If an incident is identified the following handling mechanism shall be adopted.

Preparation

- An incident management process comprising detection, response and recovery shall be developed.
- All relevant stakeholders shall have roles and responsibilities defined to support the incident management process.

Detection and Analysis

- A process for reporting incidents shall be implemented. Process flow and escalation matrix shall be defined, along-with resolution time and other parameters.
- Users shall be required to note and report any observed or suspected weaknesses in systems or services.
- Incidents shall be classified based on their level of impact to the organization with appropriate escalation matrix defined.
- Root-cause analysis of incidents shall be conducted, documented and response strategies formulated.
- If the incident is not resolved within 30 minutes (thirty minutes) escalate the incident to disaster and invoke BCP.

Recovery

- Adequate measures to recover from the incident shall be performed on the affected systems/services.
- The response and recovery plan should be documented for the timely restoration of systems affected by technical glitch including the Recovery Time Objective (RTO) and the Recovery Point Objective (RPO).

Recovery Time Objective (RTO) :

1. Objective: The provision of RTO is to ensure the timely recovery of critical systems and functionalities following an incident or disruption, in compliance with SEBI guidelines.
2. Defined Timeframes:
    - Trading-related Systems: The RTO for trading-related systems shall not exceed 45 minutes.
    - Clearing and Settlement-related Systems:The RTO for clearing and settlement-related systems shall not exceed 45 minutes.
3. Recovery Procedures:
    - The recovery process will include identifying the issue, and recovery will proceed via backups, failover mechanisms, or invoking the BCP DR Plan.
4. Resource Allocation:

  - Adequate resources, including personnel, technology, and infrastructure, will be allocated to ensure timely recovery within the specified RTOs.
5. Monitoring and Reporting:
   - Continuous monitoring of systems' recovery progress will be conducted during an incident.
   - Reporting mechanisms will be in place to notify stakeholders about the status of recovery efforts and any deviations from RTOs.
6. Review and Improvement:
   - A Disaster Recovery (DR) drill will be conducted annually to assess the effectiveness of the DR plan. Based on the results, the policy will be updated and improved accordingly.
   - Lessons learned from incidents or drills will be utilized for continuous improvement.

Recovery Point Objective (RPO):

1. Objective:
   - The RPO aims to ensure minimal data loss and timely data recovery in alignment with regulatory guidelines.
2. Specified Recovery Points:
   - Trading-related Systems: The RPO for trading-related systems shall not exceed 15 minutes (fifteen minutes).
   - Clearing and Settlement-related Systems: The RPO for clearing and settlement-related systems shall not exceed 15 minutes (fifteen minutes).
3. Data Backup and Recovery:
   - Robust data backup mechanisms will be implemented to achieve the specified RPOs.
   - Regular backups and replication of data will be conducted to minimize potential data loss.
4. Data Recovery Procedures:
   - The recovery process will include identifying the issue, and recovery will proceed via backups, failover mechanisms, or invoking the BCP DR Plan.
   - Verification and validation processes will be in place to ensure the integrity and accuracy of recovered data.
5. Documentation and Compliance:
   - Comprehensive documentation of data backup schedules, procedures, and compliance records will be maintained.
   - A Disaster Recovery (DR) drill will be conducted annually to assess the effectiveness of the DR plan and will ensure adherence to RPO requirements.

Post-Incident Activity

- Evidence related to incidents such as audit trails, logs, etc. shall be collected and maintained securely.
- Learnings from incidents shall be documented in the form of a knowledge base for handling of similar incidents in the future.
- Proactive action shall be taken to prevent incidents and failures by ensuring appropriate monitoring systems.
- The crisis management mechanism shall be tested periodically to understand its adequacy and relevance.
- All employees and outsourced staff shall be made aware of the policy and procedure requirements, their responsibilities and incident reporting mechanism.
- The organizational disciplinary process shall be referred for dealing with employees who commit

security breaches.

- There shall be appropriate disciplinary actions initiated by Exchange:
    - In case of repeated instances of non-compliance on 2 or more occasions,
    - In case of failure to move to DR site within the timeline,
    - In case of failure to timely address technical glitch.

7.0 Process of handling client complaints.

Clients shall lodge complaints through telephonic calls/emails. All the complaints received which qualify as Incident shall be checked immediately and replied/resolved.

Incidents raised through various above modes will be handled and resolved by the Incident Response Team who have the necessary skill sets to redress the issues.

a. All complaints are tagged and captured in CIP (Client Information Portal) or CRM

b. The Support Team shall establish contact with customers (via call or other medium) and understand the issues.

c. Incident Response Team shall initiate follow up with the respective cross functional/business team / department / branch to close issues / concerns/ queries.

d. Response and resolution of all incidents shall be done within defined timelines. If the incident results in business disruption the Response should be given to the client within 30 minutes.

8.0 Management Reporting

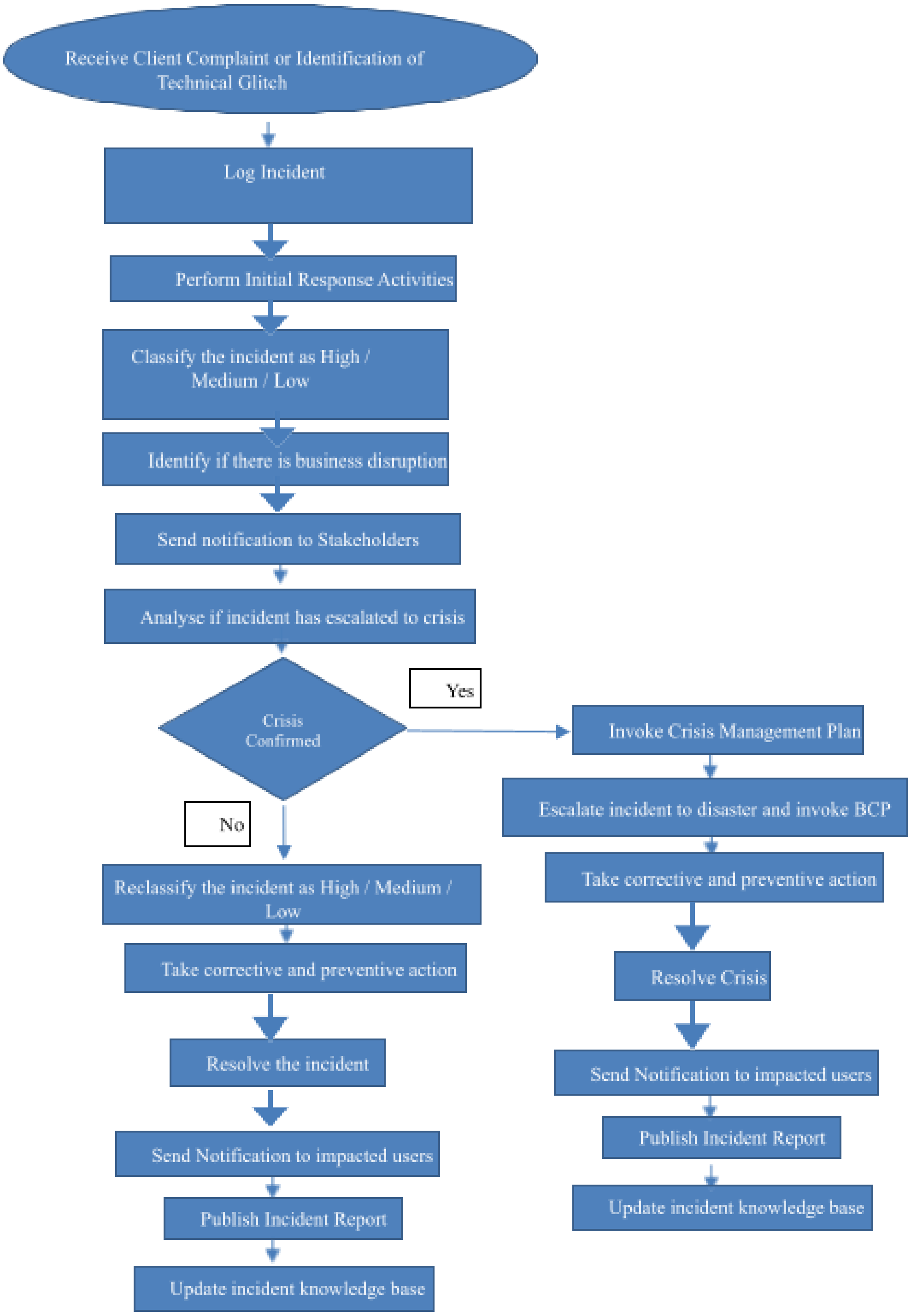
A quarterly MIS shall be put up to the Board, on incident reported, the corrective actions taken and the future plan of action. Reasons for delay in deployment of the corrective measures shall also be discussed along with the action to be taken.

9.0 Incident Management Escalation Matrix

Refer incident management procedure for escalation matrix for incident without business disruption. Following is the escalation matrix for technical glitch:

Level of Escalation	Escalation to:	Resolution Timelines
First Level	Business Head/BCM	Not resolved within 15 minutes
Second Level	CTO – Chief Technology officer / CISO – Chief Information Security Officer	Not resolved within 30 minutes
Third Level	COO – Chief Operating Officer	Services are not up within defined RTO

10.0 Incident Management Flow Chart


Receive Client Complaint or Identification of Technical Glitch
Log Incident
Perform Initial Response Activities
Classify the incident as High / Medium / Low
Identify if there is business disruption
Send notification to Stakeholders
Analyse if incident has escalated to crisis
Crisis Confirmed
Yes
Invoke Crisis Management Plan
Escalate incident to disaster and invoke BCP
Take corrective and preventive action
Resolve Crisis
Send Notification to impacted users
Publish Incident Report
Update incident knowledge base
No
Reclassify the incident as High / Medium / Low
Take corrective and preventive action
Resolve the incident
Send Notification to impacted users
Publish Incident Report
Update incident knowledge base

11.0 Document References

- Incident Management Procedure
- NSE circular - Circular Ref. No: 108/2021 related to futures and options
- ISO 27001:2022
- SEBI/HO/MIRSD/CIR/PB/2018/147
- NSE/COMP/54876
- SEBI/HO/MRD1/DTCS/CIR/P/2021/33
- SEBI/HO/ ITD-1/ITD_CSC_EXT/P/CIR/2024/113

ISO 27001 CONTROL NUMBERS	CONTROL TITLE
5.5	Contact with authorities
5.24	Responsibilities and Procedures
5.25	Assessment of and decision on information security events
5.26	Response to information security incidents
5.27	Learning from information security incidents
5.28	Collection of evidence
6.8	Reporting information security events

12.0 Annexures

12.1 Annexure A – Key systems/departments handling operation and assigned responsibilities at business owner and technology owner level.

Business	Key System	Business Owner	Technology Owner
Choice Equity Broking Pvt Ltd	All Trading and Risk Management system	Ajay Kejriwal	Yogesh Jadhav