



CHOICE EQUITY BROKING PVT. LTD

CYBER SECURITY INCIDENT & PROBLEM MANAGEMENT

PROCEDURE

Version Control

Action	Created Date	Revision Details	Prepared / Amended By	Approved Date	Approved By
Initial Creation	17-Oct-16	1.0	Mahesh Tamhankar	17-Oct-16	Amit Jaokar
Revision	17-Feb-17	1.1	Mahesh Tamhankar	21-Feb-17	Amit Jaokar
Revision	09-Feb-18	1.2	Mahesh Tamhankar	13-Feb-18	Amit Jaokar
Revision	16-Feb-18	1.3	Mahesh Tamhankar	20-Feb-18	Utpal Parekh
Revision	07-Aug-19	1.4	Mahesh Tamhankar	10-Aug-19	Yogesh Jadhav
Revision	09-Jan-20	1.5	Mahesh Tamhankar	11-Jan-20	Yogesh Jadhav
Revision	13-July-21	1.6	Sunil Utekar	15-July-21	Yogesh Jadhav
Revision	05-Jan-22	1.7	Sunil Utekar	08-Jan-22	Yogesh Jadhav
Revision	06-Apr-23	2.0	Ashutosh Bhardwaj	09-Apr-23	Yogesh Jadhav
Revision	29-Jan-24	2.1	Anil Ashok & Associates	31-Jan-24	Ashutosh Bhardwaj

Version Control Revised Format

Version	Activity	Date	Description	Person Responsible
2.2	Amendments	08th April, 2025	Amendments done and submitted for review regarding the incident classification criteria and Incident/ problem Handling section 3.2 to align with SEBI CSCRf	Abhishek Vinayak, Associate Information Security
2.2	Reviewed	07th April, 2025	Changes Reviewed	Shripad Mayekar, Manager Information Security
2.2	Approved	07th April, 2025	Changes Approved	Ashutosh Bhardwaj, CISO

TABLE OF CONTENTS

Contents

1.0 Purpose	4
2.0 Scope	4
3.0 Procedure	4
3.1 Incident/ Problem Management	4
3.2 Incident/ Problem Classification	5
3.3 Reporting of Incidents/ Problems	6
3.4 Incident/ problem Handling	7
3.5 Incident/ problem Recovery	8
3.6 Incident/ problem Closure	8
3.7 Post Incident Report (PIR)	8
4.0 Incidents Indicative List	9
4.1 Information Security Incidents	9
4.2 Cyber Security Incidents	9
5.0 Reference Documents	10
6.0 Definitions / Anyms	10
7.0 Exceptions	10
Risk Acceptance Criteria	10
8.0 Annexures	11
8.1 Annexure A - CYBER SECURITY COMMITTEE	11
8.2 Annexure B - First Incident Responder Guidelines	14
8.3 Annexure C - Digital Evidence Handling Guidelines	15

1.0 Purpose

The primary use of this document is to implement the controls for cyber security incident/ problem management as specified within Incident Management Policy, to minimize impact on business operations and to ensure normal service operations are restored as early as possible. The document serves:

- As the process document for the process owners
- To define various templates to be used for incident management

Furthermore, a Technology Committee has been appointed for their valuable contribution and guidance in regards with this policy (Refer Annexure A for details on Cyber Security Committee).

2.0 Scope

The scope of this procedure is applicable to all information and cyber assets owned or operated under Choice Equity Broking Pvt. Ltd. (Choice). All users (Choice employees, contractors, vendors, or others) of information or cyber resources are responsible for following this procedure.

3.0 Procedure

3.1 Incident/ Problem Management

The Incident/ Problem Management procedure ensures handling of incidents through its lifecycle, i.e., to prepare, identify, assess, respond, and learn from security incidents.

Sr. No.	Activity	Responsibility
1	It shall be ensured that all incident/ problem related information is documented accurately and comprehensively while preserving evidence	Incident Response Team
2	Forensic methods, which shall be accepted in a court of law, shall be used while conducting root cause analysis on the incident/ problem	Incident Response Team

3.2 Incident/ Problem Classification

All incidents/ problems must be classified based on the impact they have on various aspects of the business and technology functions. All incidents must be classified in the four categories as described below:

Category	Details
Low	System probes or scans detected on external systems; intelligence received concerning threats to which systems may be vulnerable; intelligence received regarding username password compromise; isolated instances of known malware easily handled by antivirus software, etc.
Medium	Target recon or scans detected; penetration or Denial of Service attacks attempted with no impact on operations; widespread instances of known malware easily handled by antivirus software; isolated instances of a new malware not handled by anti-virus software; instances of phishing emails that were not recognized by employees and were clicked by them; instances of data corruption, modification and deletion being reported, etc.
High	Penetration or Denial of Service attacks attempted with limited impact on operations; widespread instances of a new malwares not handled by anti-virus software; unauthorized access to servers and network devices; unauthorized or unexpected configuration changes on network devices detected; impersonation of SEBI officials in email communications; data exfiltration; unusually high count of phishing emails; instances of outbound phishing emails; some risk of negative financial or public relations impact, etc.
Critical	Unauthorized access to servers and network devices; unauthorized or unexpected configuration changes on network devices detected; impersonation of SEBI officials in email communications; data exfiltration; unusually high count of phishing emails; instances of outbound phishing emails; some risk of negative financial or public relations impact, etc.

- Any cyber incident that results in disruption, stoppage or variance in the normal functions/ operations of systems of the entity thereby impacting normal/ regular service delivery and functioning of the entity, must be classified as High or Critical incident.

Nature of Incident/ problem	Reportin g Time (SOC)	Escalation for resolution	Severity	Response SLA (Tech/IS/ BU's)	Resolution SLA (Tech/IS /BU's)
Any incident/ problem which: <ul style="list-style-type: none"> Is impacting critical data confidentiality/ integrity or availability of a critical application, and; Has a noticeable impact on revenue/ critical business has a noticeable impact on the brand/ reputation has led to a known breach of legal and regulatory compliance 	15 minut es Strivin g for real time report ing with the help of auto matio n of alerts	(CISO, CTO)	Critical / High	30 min	80% of incidents/ problems to be closed within 4 hrs of reporting
Any incident/ problem which: <ul style="list-style-type: none"> Is impacting critical data/ availability of a critical application or Partially impairing critical business units 	2 Hours	(CISO)	Medium	2 Hours	80% of incidents/ problems to be closed within 8 hrs of reporting
Any incident/ problem which is: <ul style="list-style-type: none"> Not impacting critical data/ availability of a critical application or Not impairing critical business units 	5 Hours	(Cyber Security Manager)	Low	5 Hours	80% of incidents/ problems to be closed within 24 hrs of reporting

NOTE:

- The “Initial response time” denotes the time required, from the time of notification/detection of the incident/ problem, to acknowledge the occurrence of the incident and begin response procedure.
- Scheduled downtimes are excluded from the scope of Incident Management

3.3 Reporting of Incidents/ Problems

Information and cyber security Incidents/ problems shall be reported in a timely and prompt manner.

Sr. No.	Activity	Responsibility
1	Reporting of incident/ problems to Information Security Team	SOC team/ Users
2	Incident/ problem reporting shall contain the following at a minimum: <ol style="list-style-type: none"> 1. Incident/ problem Description 2. Information/ System affected 3. Damage observed 4. Evidence 5. Name of person who has reported the incident/ problem 	Users/ Cyber Security Manager
3	Users may follow the first incident responder guidelines. The guidelines outline what the user shall do and what the user shall not do, when an incident/ problem has occurred. Refer Annexure B – First Incident Responder Guidelines.	Users
4	The end user shall not attempt to resolve the incident / problem on their own. If attempted, it shall be considered as breach of security and may form a base for disciplinary actions.	Users
5	Once the incident / problem is reported, the incident response team shall classify the incident/ problem as per the Incident / Problem Classification criteria.	Incident Response Team
6	If the incident / problem is classified as Critical / High, it shall be reported to the CISO.	Incident Response Team
7	The procedure for reporting of incidents / problems shall be made aware to the new joiners by way of awareness programs at the time of induction and existing employees on a regular basis.	Information Security Manager/ HR

3.4 Incident/ problem Handling

- The actions to treat the incident/ problem once it has been confirmed as an incident/ problem is to be conducted as part of the incident/ problem handling procedure. The actions are as follows:

Sr. No.	Activity	Responsibility
1	Incident response team shall ensure that the person who reported the incident / problem is recorded over an email / phone call / in-person.	Incident Response Team
2	Refer Incident / problem Management Knowledge Base to see if a similar incident / problem has occurred before. If yes, knowledge documented for that incident / problem can be leveraged for responding.	Incident Response Team
3	Additional expertise (external/internal) shall be leveraged in cases where additional data is required to analyze the incident/ problem	Incident Response Team
4	The incident/ problem shall be escalated in a timely manner as per the incident escalation matrix	Incident Response Team
5	<p>The successful security incident/ problem shall be reported to appropriate regulatory bodies and government authorities (Refer Incident/ Problem Classification).</p> <p>SEBI ,Depositories and all exchanges - within 6 hours and quarterly reports by compliance team. CERT-In – within 6 hours.</p> <p>This information shall be shared to SEBI & CERT-IN through the dedicated e-mail id: mkt_incidents@sebi.gov.in and incident@cert-in.org.in respectively.</p> <p>1. A preliminary Cyber incident report shall be submitted to the SEBI on Incident Reporting Portal within 24 hours 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.</p> <p>2. An interim report shall be submitted to the SEBI within T+3 days & the report must contain, inter alia, the following: Details of the incident including time of occurrence, information regarding affected processes/ systems/ network/ services, severity of the incident, and the steps taken to initiate the process of response and recovery.</p> <p>3. Root Cause Analysis (RCA) of the cyber incident in the format as enclosed in</p>	Compliance Team

	<p>Incident Management Procedure, to be submitted within 30 working days.</p> <p>4. The RCA must include exact cause of the incident (including root cause from vendor(s), if applicable), exact timeline and chronology of the incident, details of impacted processes/ systems network / services, details of corrective/ preventive measures taken (or to be taken) by the entity along with timelines and any other aspect relevant to the incident. Additionally, it shall also include time when operations/ functions/ services were restored and in the event of a disaster, time when disaster was declared.</p>	
7	The incident/ problem response team shall follow the digital evidence handling guidelines while responding to the incident/ problem.	Incident Response Team
8	<p>The Incident/ problem shall be updated with the following details at a minimum:</p> <ol style="list-style-type: none"> 1. Reason of incident/ problem 2. Action taken 3. Impact of incident/ problem 4. Status 5. Date of closure 	Incident Response Team

- Cyber incidents should mandatorily be reported to Cert-In within 6 hours of noticing or being brought to notice about such incidents and also to concerned regulators / authorities whenever applicable.
- The quarterly reports containing information on incident/problem shall be submitted to Stock Exchanges / Depositories within 15 days from the quarter ended June, September, December and March of every year.
- Incidents to be reported by internal teams and end users to soc@choiceindia.com .

3.5 Incident/ problem Recovery

The actions to resume business as usual, post an incident/ problem will be carried out in the Incident/ problem Recovery phase. The actions are as follows:

Sr. No.	Activity	Responsibility
1	On successful resolution of the incident/ problem, the affected systems shall be monitored for a period to ensure that the incident / problem activity has been suspended. This can be done by monitoring the affected systems logs frequently or deploying other security monitory controls / solution	Incident Response Team
2	All actions taken for resolution of the incident/ problem shall be documented in detail and stored in the incident / problem knowledge base.	Incident Response Team

3.6 Incident / problem Closure

The formal procedure for marking the resolution of the incident/ problem reported shall be carried out as a part of the incident/ problem closure. The actions are as follows:

Sr. No.	Activity	Responsibility
1	The following resolution details shall be recorded: <ol style="list-style-type: none">1. Root cause of the incident/ problem2. Incident/ problem symptoms3. Actions taken for resolution / Changes made to application4. Preventive measures taken	Incident Response Team
2	Information documented in lessons learnt shall be considered for revisions of the Information Security Policy, Security Incident Management Policy, Risk Assessments, Business Continuity Plan and Crisis Management Plan, etc.	Cyber Security Manager
3	On successful resolution of the incident/ problem, an acknowledgement email shall be sent to the user who reported the incident/ problem	Incident Response Team
4	Any disciplinary action shall be taken as per the HR Disciplinary policy.	HR/ CISO/ Cyber Security Manager

3.7 Post Incident Report (PIR)

- Once the incident/ problem is handled, follow up activity shall be carried out for all incident / problems by the Incident Response team. Follow-up activity is intended to include the following:
 - Analyzing what has transpired and what was done to intervene
 - Was there sufficient preparation for the incident/ problem?
 - Did detection occur promptly or, if not, why not?

- Could additional tools have helped the detection and eradication process?
- Was the incident/ problem sufficiently contained?
- Was communication adequate, or could it have been better?
- What practical difficulties were encountered?
- Was the incident/ problem caused due to negligence or malicious intent on part of an employee? If suspected guilty, PIR shall be forwarded to HR for initiating disciplinary proceedings.
- Were any data irrecoverably lost, and, if so, what was the value of the data? Was any hardware damaged?
- Developing effective policies and procedures is an iterative process in which feedback from discussion on Post incident Report (PIR) is essential.
- Lessons learned from the security incident should be recorded by the SOC team.

4.0 Incidents Indicative List

4.1 Information Security Incidents

- Non-compliances with policy or procedure
- Breaches of physical security arrangements
- Malfunctions of software or hardware
- Access violations
- Theft or damage to computer hardware equipment
- Tailgating or piggy backing
- Access card not worn visibly
- Photography within the sensitive areas
- Attempt to access restricted areas like Servers Rooms & Electrical Rooms
- Unattended confidential document
- Downloading or Installation of unlicensed/ unapproved software
- Take and / or send any company confidential and proprietary information including any client's information outside the office without proper authorization
- Forwarding of non-business-related emails (Spamming) with large attachments
- Sharing of User ID and Password
- Browsing, Accessing, and/ or downloading any pornographic content
- Attempt to deliberately infect any device with viruses / keyloggers / malwares
- Attempt at email ID impersonation, Identify theft
- Rendering any network devices and / or critical servers unavailable or not operational

4.2 Cyber Security Incidents

- External Vulnerability Scan
- External DDOS Attacks
- External Botnet attacks
- External Port Scans - Horizontal
- External Port Scans - Vertical Scans

- Ransomware Attacks
- Virus Attacks
- Zero Day Attacks
- Malware Attacks
- Portable devices carrying customer data
- Web Site Defacement
- Alerts generated by XDR System
- Alerts generated by SIEM System
- Alerts generated by IDS/IPS System
- Alerts generated by Firewall System
- Alerts generated by DLP System

5.0 Reference Documents

- Incident Management Policy
- SEBI circular - SEBI/HO/MIRSD/CIR/P/2017/0000000100
- SEBI circular - SEBI/HO/MIRSD/CIR/PB/2018/147
- SEBI circular - SEBI/HO/MIRSD/TPD/P/CIR/2022/80
- SEBI circular - SEBI/HO/MIRSD/TPD/P/CIR/2022/93
- CERT-In - No. 20(3)/2022-CERT-In
- ISO 27001:2022
- SEBI/HO/ ITD-1/ITD_CSC_EXT/P/CIR/2024/113

6.0 Definitions / Acronyms

CISO: Chief Information Security Officer

ISSC: Information Security Steering Committee

ISMS: Information Security Management System

IRC: Incident Response Committee

PIR: Post Incident Report

LOB: Line of Business

7.0 Exceptions

- Exceptions shall not be universal but shall be agreed on a case-by-case basis, upon official request made by the information owner. These may arise, for example, because of local circumstances, conditions or legal reasons existing at any point of time.
- All exceptions during implementation shall be submitted by the concerned person responsible for implementation. These shall be submitted through the Exception Form and sign-off on the same shall be maintained as per the below grid.

Risk Acceptance Criteria

Action	High/Medium	Low
Reviewer	Level 1 - BU CTO Level 2 - BU Compliance Team	BU CTO
Approver	BU COO	

8.0 Annexures

8.1 Annexure A - CYBER SECURITY COMMITTEE

Composition of Cyber Security Committee

Sr. No	Name of the Member	Designation in the Company	Designation in the Committee
1	Mr. Ashutosh Bhardwaj	Group CISO	Chairperson
2	Mr. Ankit Jain	Senior Vice President	Member
3	Mr. Sunil Utekar	Head – IT operations	Member
4	Mr. Shailendra Chaudhari	Security Analyst	Member

TERMS OF REFERENCE

Preamble

The Management level Cyber Security Committee (hereafter referred to as the “Committee “or “CSC”), has been constituted in alignment with the requirements & guidelines laid down by the directional guidelines laid down by “Securities & Exchange Board of India” circular dated February 06, 2023 bearing No SEBI/HO/MIRSD/ MIRSD-PoD-1/P/CIR/2023/24 and as amended from time to time & for ease of doing the Business.

The Board shall be responsible for reviewing the “Cyber Security” policy for the Company. The Board of Directors (hereafter referred to as the “Board”) may delegate the monitoring and reviewing of the Cyber Security policy to the committee as deemed fit. This section covers the roles and responsibilities of the Cyber Security Committee.

PRIMARY OBJECTIVES

The Committee is constituted by, and accountable to, the Board of Directors of “Choice Equity Broking Private Limited “committee shall assist the Board in monitoring and reviewing:

- I) The Company’s technology landscape, competitive assessment and roadmap for future development.
- II) The Company’s cyber security and other information technology (IT) risks, controls and procedures, including high level review of the threat landscape facing the Company and the Company’s strategy to mitigate cyber security risks and potential breaches.
- III) The Committee shall also review the recovery and communication plans for any unplanned outage or security breach.
- IV) The Company’s technology planning processes to support its growth objectives as well as acquisitions and the system integrations required in support of such activities.
- V) The integrity of the Company’s IT Systems’ operational controls to ensure legal and regulatory compliance

VI) Review the Company's Cyber insurance policies, if applicable, to ensure appropriate coverage and that all insurance terms and conditions are being met

VII) Review the Company's development and training plan for critical IT staff as well as succession planning and employee training of cyber security risks.

CYBER SECURITY COMMITTEE COMPOSITION

The Board of Directors has constituted a sub-committee – Cyber Security Committee (CSC) Committee (Management Level) to assist the Board in framing policy, monitoring and reviewing the Cyber Security policy and framework. The Committee shall act as a forum to discuss, manage and assist the Board with its oversight of the cyber security program and risks.

The **Chairperson of the Committee** shall be responsible for overseeing the functioning of the Committee.

QUORUM

The quorum for a meeting of the Cyber Security Committee shall be either two members or one third of the members of the committee, whichever is higher, including at least one member of the Board in attendance.

MEETINGS AND REPORTING

I) The Committee shall meet at least twice in a year with a gap of not more than one hundred and eighty days shall elapse between any two consecutive meetings;

II) All or any members may participate in a meeting by video conferencing or by other audio-visual means. A member so participating is deemed to be present in person at the meeting and shall be counted for the purpose of quorum at the meeting;

III) The Secretary to the Committee shall be responsible, in conjunction with the Chairperson for compiling and circulating the agenda and papers for the meeting;

IV) Formal decisions shall be made by simple majority; in case of equality the Chairperson of the meeting shall have the casting vote;

V) The Secretary to the committee shall prepare minutes of all the meetings of the committee and shall circulate the same to the Board and committee for consideration;

VI) Committee shall report the outcomes of all its meetings to the Board periodically

ROLES AND RESPONSIBILITIES OF THE COMMITTEE

The Committee shall have the following roles and responsibilities:

1. Review the Company's cyber security program.
2. Oversee the Company's risk management with respect to cyber security.
3. Review the Company's adoption and implementation of systems, controls and procedures designed to prevent, detect and respond to cyber-attacks or security breaches involving the Company.
4. Review updates regarding the Company's cyber security threat landscape

5. Review Management's responses to noteworthy cyber security incidents, developments and threats as identified by Management
6. Receive reports on the Company's network and data security architecture
7. Review the Company's technology resilience, including business continuity and incident response.
8. Review the budget and resources allocated to the Company's cyber security program.
9. Review the Company's cyber security insurance program.
10. Prevention of cyber security incidents through continuous threat analysis, network and host scanning for vulnerabilities and breaches, deploying adequate and appropriate technology to prevent attacks originating from external environment and internal controls to manage insider threats etc
11. Monitoring, detection and analysis of potential intrusions/security incidents in real time and through historical trending on security-relevant data sources
12. Review reports from management concerning the implementation of the Company's significant programs and initiatives, including the cost, the expected benefits and the timelines of implementation.
13. Conducting cyber-attack simulation on quarterly basis to aid in developing cyber resiliency measures and test the adequacy and effectiveness of the framework adopted.
14. Conducting awareness and training programs for its employees with regard to cyber security and situational awareness on quarterly basis.
15. Prevention of attacks similar to those already faced
16. Operating network defence technologies such as Intrusion Detection Systems (IDSes) and data collection/analysis systems.
17. Review reports from management and provide input on how information technology impacts, or is needed to implement, strategic and business initiatives.

FORMULATE A DETAILED INFORMATION TECHNOLOGY POLICY WHICH SHALL STRIVE TO:
--

To formulate a detailed policy outlining the Role, Responsibility, Authorities, Periodic evaluation & Performance of the Committee along with architecture of system developed to mitigate the Cyber Security Risks & the procedures adopted for the smooth functioning of the Company.

POWERS OF THE COMMITTEE

The Committee shall have powers to seek information from any employee, obtain outside legal or other professional advice and secure attendance of outsiders with relevant expertise, if it considers necessary.

8.2 Annexure B - First Incident Responder Guidelines

First responder is the first person who is identified to handle the incident once it has been detected.

- i. The First Responder is responsible for collecting information regarding the symptoms from the person who reported the incident and understand the chronology of events that lead to the incident.
- ii. Affected systems shall not be powered on once they have been switched off until it is certain that the affected system is clean and vice versa.
- iii. The first responder shall capture the infrastructure affected by the incident accurately. The affected infrastructure (servers/workstations/devices etc.) shall be photographed from all sides, keeping in mind all connections to the infrastructure shall be clearly visible in the photographs
- iv. The first responder shall document the details of the infrastructure accurately. Details such as location of the infrastructure, connections, power status, peripheral equipment, storage properties, network connections etc. shall be captured.
- v. All actions taken by the first responder which may affect the state or change the status of the affected infrastructure, shall be documented so that it can be admitted as forensic evidence in a court of law and not corrupt the same.
- vi. All evidences shall be gathered keeping in mind applicable regulatory and legal laws.
- vii. Access to affected infrastructure and evidence shall be on a need-to-know basis.

Incident handling training on topics like phishing, vishing, malware attacks, DDoS attack, etc. shall be provided to users to recognize and adequately react to emergency incidents.

8.3 Annexure C - Digital Evidence Handling Guidelines

- i. If the affected infrastructure is off, do not turn it on
- ii. If the affected infrastructure is on, do not turn it off
- iii. Remove the network cable from the affected infrastructure if it is plugged in
- iv. Infrastructure device shall be isolated and not connected to any network
- v. Do not format / delete / modify any contents on the affected infrastructure
- vi. Full forensic disk images shall be taken instead of file system backups
- vii. Volatile data (data that is stored in memory, or exists in transit, that will be lost when the computer loses power or is turned off) from the affected infrastructure shall be obtained as preserved. Volatile data consist of network connections, processes, login sessions, open files, network interface configurations, and the contents of memory.
- viii. Affected infrastructure shall not be used until instructed by the Incident Response team
- ix. Once volatile data is captured and preserved, the Incident Response team may take a decision to unplug the power supply from the system. In case of laptops or mobile devices, the battery shall be directly removed.
- x. The following details shall be documented for all suspicious/affected systems/evidence
 - a. Device model number
 - b. Serial numbers
 - c. Hostname
 - d. IP Address
 - e. Owner(s) – Full name
 - f. Location
 - g. Date and Time, preferably system date and time
- xi. All cords and devices shall be disconnected to isolate the affected infrastructure
- xii. If any additional storage media is connected to the affected infrastructure, the storage media shall be captured as evidence as well
- xiii. Keep all media away from magnets, radio transmitters and other potentially damaging elements. Collect instruction manuals, documentation, and notes
- xiv. All steps followed for obtaining evidence shall be documented
- xv. Evidence captured shall adhere to requirements as per Indian IT Act 2000 and its applicable amendments and rules. Especially sections 65 A and 65 B which mentions that whoever knowingly or intentionally conceals, destroys, or alters or intentionally or knowingly causes another to conceal, destroy, or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force shall be liable to legal action against the provisions of the act
- xvi. If required evidence from non-IT resources such as CCTV footage, premises access logs etc. can also be captured as evidence
- xvii. All evidence shall be handled by skilled digital forensics personnel only
- xviii. Chain of custody shall be maintained for all evidences.
- xix. Access to evidence shall be strictly on a need-to-know basis