CHOICE EQUITY BROKING PVT. LTD

CYBER SECURITY POLICY

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
Approved	08-Jan-2025	2.2	Abhishek Vinayak	08-Jan-2025	Yogesh Jadhav

Version Control Revised Format

Version	Activity	Date	Description	Person Responsible
2.3	Amendments	05th April, 2025	Amendments done and submitted for review regarding the stages for Cyber Security Program along with minor changes in Application and Infrastructure Security	Abhishek Vinayak, Associate Information Security
2.3	Reviewed	07th April, 2025	Reviewed the changes.	Shripad Mayekar, Manager Information Security
2.3	Approved	07th April, 2025	Approved the changes	Ashutosh Bhardwaj, CISO

TABLE OF CONTENTS

1.0 Background

In light of the growing cyber security threats, Choice Equity Broking Pvt. Ltd. (Choice) has outlined the policy to protect its information, infrastructure and people resources from the risks of cyber- attacks and breaches.

A cyber-attack is an intentional exploitation of assets (people, systems, networks, processes and services) using threat agents such as exploits, denial of service, backdoors and social engineering, indirectly or directly with the intent to adversely affect or compromise the confidentiality, integrity or availability of such assets. Such attacks can be performed from both within the perimeter of the organization or from outside physical and logical boundaries.

Over the years, cyber-attacks have developed from singular manual attacks to state-sponsored attacks often launched using automated techniques. Cyber-attacks have also propagated to not simply steal or destroy information, but to penetrate the organization's defenses and continuously transmit information over a large period of time.

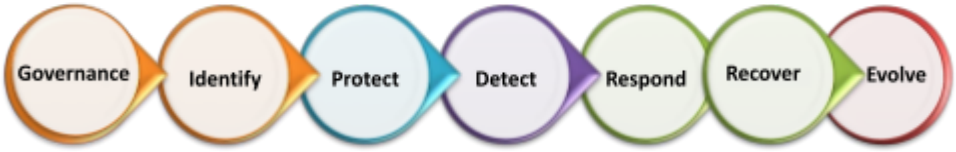
Examples of cyber-attacks are:

- Network intrusions involving sniffing, spoofing, session hijacking, man-in-the-middle attacks, foot-printing, password hacking and denial of service
- Systemic compromise using malware such as viruses, trojans, worms, advanced persistent threats to obtain unauthorized access to assets
- Application security breaches involving SQL injections, privilege escalation and gaining illegitimate access to sensitive data
- Social engineering techniques involving elicitation of people assets using telephonic, electronic (email, SMS and chat messengers) or physical communication
- Unauthorized access to sensitive data

This policy embodies the processes, practices and technologies required to emphasize the importance of cyber-security resilience across Choice Equity Broking Pvt. Ltd. (Choice) in order to protect assets critical to its businesses, from theft, damage or compromise.

2.0 Choice Equity Broking Pvt. Ltd. (Choice)'s Cyber Security Program

- The following policy has the framework based on the principles prescribed by National Critical Information Infrastructure Protection Centre (NCIIPC) of National Technical Research Organization (NTRO), Government of India.
- Choice Equity Broking Pvt. Ltd. (Choice)'s Cyber Security program shall operate in a continuously improving environment with the below stages:



#	Stage	Description
1	Governance	Establishing governance structures, policies, and procedures for cybersecurity. Defining roles, enforcing compliance and conducting cybersecurity audits and board reviews.
2	Identify	Identification of critical assets and management of cyber security risks
3	Protect	Continually safeguarding identified assets by deploying controls such as security architecture mechanisms, event correlation systems, intrusion prevention and detection systems, and enforcement of secure configurations.
4	Detect	Detecting incidents related to attacks or anomalies through continuous monitoring of critical infrastructure
5	Respond	Take steps to assess the incident impact and take appropriate response measures including escalation to relevant authorities
6	Recover	Recover from incident adequately following the organization's incident management, business continuity and disaster recovery policies
7	Evolve	Continuously assessing controls through security testing, ensuring ongoing compliance, and implementing improvements based on incident learnings.

- As new vulnerabilities are being exposed for exploitation and new threats are identified through internal and external channels, Choice Equity Broking Pvt. Ltd. (Choice) shall constantly update its Cyber Security program and security architecture with improved controls, upon completion of risk assessments by the Information Security Team.

3.0 Governance

- The ownership and responsibility for the maintenance of the Cyber Security Policy and Choice Equity Broking Pvt. Ltd. (Choice)'s Cyber Security program lies with the Chief Information Security Officer (CISO).

- The responsibility for cyber security operations across the organization rests with the corporate Information Security Team. The Information Security Team must be contacted in the event of any queries on the contents of this policy, suggestions for improvements, exceptions and any other areas relating to the cyber security environment at Choice Equity Broking Pvt. Ltd. (Choice). 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)
- Information Security Team shall assess, identify and reduce cyber security risks, respond to incidents, establish appropriate standards and controls on an ongoing basis to direct the implementation of the Cyber Security Policy.
- The policies outlined in this document are the foundation of Choice Equity Broking Pvt. Ltd. (Choice)'s cyber security strategy. Cyber Security defenses will be built on the foundation of these policies, in addition to the organization's Information Security Policy and procedures.
- Information Security Team is responsible for enforcing the Cyber Security program and continually ascertain the security posture of Choice Equity Broking Pvt. Ltd. (Choice) against cyber threats & report on cyber resilience to senior management
- An Information Security Steering Committee (ISSC) shall be formulated comprising of key technology and business stakeholders, to review the implementation of Cyber Security Policy on an annual basis. This review shall encompass the current cyber resilience capabilities and controls, impact of noted cyber security incidents, and results of cyber security assessments and exercises, to assist Information Security Team in developing plans to improve the overall cyber security readiness for the organization.
- Choice Equity Broking Pvt. Ltd. (Choice) shall set up partnership and/or membership with various security-related entities such as CERT-In (Computer Emergency Response Team - India).

4.0 Policy Review and Approval

- This policy document shall be reviewed at least annually, or in the event of any significant change(s) in the existing cyber security environment at Choice Equity Broking Pvt. Ltd. (Choice).
- The CISO will be responsible to approve changes to the Cyber Security policy document, with the view to continually improve the cyber security resiliency program. The Cyber Security policy shall be shared with ISSC for review and approval
- In-case there are any changes that are proposed to the Policy document by any user other than the CISO or Information Security Team, the proposed

changes shall be formally communicated to and subsequently discussed, reviewed with the Information Security Team and approved by CISO .

5.0 Policy Exceptions

- All exceptions or deviations from the policies outlined in the Cyber Security Policy document are mandated to be formally approved by the Chief Information Security Officer (CISO).
- Approval for such exceptions or deviations, wherever warranted, will be provided only after an appropriate assessment of the risks arising out of providing the exception. This assessment will be conducted by the Information Security Team and/or authorized persons designated by it.
- Exceptions will be granted for a maximum of one calendar year from the date of approval.
- Business must formally accept/reject risks identified as part of Information Security Team assessment.

6.0 Cyber Security Operations

6.1 Critical Cyber Asset Identification

- Respective teams shall identify and categorize critical information, system, service, software, application and people assets in the Information Asset Register. The assets should be identified & classified on the basis of the organization's risk assessment methodology. The Information Security Team shall provide guidance and support as required.

6.2 Cyber Risk Identification and Assessment

- Information Security Team shall identify cyber security risks, i.e. threats to and vulnerabilities in its critical cyber assets and business environment. The Information Security Team must also assess the likelihood and impact of such threats on various business processes.
- Information Security Team shall maintain a library of controls that can be or have been implemented to mitigate or transfer specific cyber security risks, and implement the relevant controls as risks evolve (Refer next section for list of primary Cyber Security controls and their operations).

- Special attention shall be given to potential reputation risks such as:
    - Leakage of company information to the public domain
    - Inappropriate actions by disgruntled employees on the public domain, such as social media and recruitment websites
    - Misrepresentation of Choice Equity Broking Pvt. Ltd. (Choice) identity

6.3 Security Controls Management and Monitoring

Physical Access Security

- Physical access to critical cyber assets must be limited only to duly authorized end-users, especially for third-party vendor and service-provider personnel.
- Adequate monitoring controls shall be implemented to ensure protection of critical cyber assets from natural and manmade disasters impacting environmental factors like temperature, water, smoke, access alarms, service availability alerts (power supply, telecommunication, servers), access logs, etc.
- Access shall be granted based on need to know and least privilege basis,no person shall have inherent access to critical cyber assets, irrespective of rank, position or business-as-usual activities.
- Employees must immediately report lost or stolen devices to the local IT teams.

Logical Access Security

- Electronic access to cyber assets should be limited to end-users using valid approved requests.
- Access-levels granted to end-users (employees, vendor & customers) on cyber assets should be commensurate with the respective users' business roles and should be granted strictly on a 'need-to-use' and 'least-privilege' principle. Administrative access on systems viz desktops /laptops/servers etc and software's shall be controlled and monitored to prevent unauthorized software installation and modifications to baseline configuration settings implemented
- Access (authentication and sign-out) and activity logs should be stored for audit and review purposes for 180 days at minimum, and should be archived at an offsite location. These records of user access should be completely safeguarded from tampering and destruction, using controls which shall be reviewed by the Information Security Team on an annual basis.

- Access to application, software, network, database and other system assets should be restricted using secure authentication measures. Effective password management is critical to securing applications and systems from cyber security risks.
    - Information Security Team shall perform annual review on password parameters for all types of accounts in accordance with the Logical Access Control Policy.
    - The Information Security Team shall validate that passwords are not stored in plaintext form for any cyber assets; they shall be stored only using strong hashing/encryption algorithms.
    - Information Security Team shall assess risk associated with remote access to specific cyber assets and enforce implementation of mitigating / compensating controls, wherever necessary.
- Information Security Team shall monitor the access provisioning, modification and de-provisioning processes for cyber assets on an annual basis.
    - The Information Security Team shall also assess risk associated with findings and perform further analysis where required .
- Information Security Team shall monitor privileged roles on all cyber assets and enforce implementation of additional controls for accounts with such entitlements on an annual basis. Controls can include, without limitation:
    - Restricting number of privileged accounts
    - Periodic and independent review of sample privileged account activity
    - Restricting remote access to approved privileged accounts
    - Denying access to update/delete activity logs, for privileged accounts
    - Monitoring access deprovisioning process for privileged accounts to ensure no such dormant accounts exist on the infrastructure
- The Information Security Team shall monitor user access review processes for all cyber assets (as identified based on the risk assessment methodology) on an annual basis. Information Security Team shall ensure that all noted discrepancies should be targeted for remediation. Alternatively capture exceptions for such discrepancies.
    - Information Security Team shall also assess risk associated with findings and perform further analysis where required (e.g. analyze activity logs for a user for whom access-levels granted and reviewed are elevated as compared to the required privilege).
- The CISO / Information Security Team shall assess the overall risk posture based on the security monitoring outlined above, and take adequate measures to secure access to all critical cyber assets, in a manner

proportionate with the sensitivity and criticality of the asset.

- Information Security Team shall issue secure configuration guidelines for applicable platforms and review at least annually.

.

Internet Usage

- Guidelines for acceptable use of internet services shall be enforced across the Choice Equity Broking Pvt. Ltd. (Choice) network, spanning all office locations including branches.
- Employees shall have clear knowledge of what types of websites are deemed unacceptable by the internet usage policies and why their web activities can be monitored.
- Defined rules on Proxies/Content filtering solutions should be monitored by the Information Security Team. Changes to the configurations based on this review shall be implemented by the respective Technology Teams.
- Guidelines for employees' acceptable behavior on social networking forums and using company email addresses to register or get notices from social media sites, shall be enforced to make clear what kinds of discussions or posts could cause risk for the organization.
- Guidelines shall be published for handling social media risks and threats. As Social Media is vulnerable to account takeovers and malware distribution, proper controls, such as encryption and secure connections shall be implemented to mitigate such risks.
- The Information Security Team shall perform configuration review on all infrastructure components on an annual basis.
- Information Security Team shall implement control to monitor cyber space in order to detect fraudster activities by sourcing monitoring & take down services to protect its customers and employees. Any issues detected shall follow a standard process towards closure & shall be reported to senior management.

Network and Host Security

- Configuration of all network devices, appliances & critical infrastructure components viz database, servers at Choice Equity Broking Pvt. Ltd. (Choice) should be reviewed on an annual basis at minimum.
- Information Security Team shall monitor compliance of critical infrastructure components against defined baseline standards.
- Information Security Team shall assess risk associated with terminals, servers and services connecting internally and externally to the corporate

network, and document the boundaries of corporate wired and wireless networks clearly.

- Adequate controls shall be implemented for protection from security exposures, such as next-gen firewalls, Network Access Control, WPA-2 encryption for wireless networks, and Intrusion Prevention and Detection systems.
- Information Security Team shall monitor processes for deployment, updation and reporting of endpoint protection tools.

Information Protection

- Information owners must be formally defined for all critical information assets.
- All critical information assets identified in the Information Asset Register shall be classified at all times in line with the Information Classification Policy.
- Wherever deemed necessary by risk assessment results, data in-motion and in- rest shall be encrypted using strong encryption methods assessed and approved by Information Security Team. Please refer Cryptography Control policy for details.
- Monitor the compliance of all Business Function-specific critical information assets with the defined policies and enforce annual review of classification, to accommodate changes to sensitivity and criticality of the asset.
- The Information Security Team shall also monitor the implementation and operational effectiveness of controls defined in the Information Classification Policy for creation, storage, transfer, retention and disposal of information assets.
- For critical information assets transferred outside the network by Business Function s, Information Security Team shall enforce adequate compensating controls to ensure secure transfer of information (covering physical, telephonic, facsimile and electronic channels).

Security Architecture

- Choice Equity Broking Pvt. Ltd. (Choice) shall prepare and maintain Enterprise Architecture (EA) diagram covering its network and critical perimeter device setup.
- Security architectures should be developed for all platforms, technologies and devices hosting or supporting critical cyber assets.
- These architectures consist of mandatory security controls, secure configuration, hardening standards, auditing requirements and

operational requirements.

- Technology and relevant business stakeholders should review compliance of applicable assets to the defined security architecture standards on an annual basis at minimum. Any deviations in control implementation within architecture shall be documented for future assessments.
- Open ports and services which are not in use or can potentially be used for exploitation, should be blocked, unless authorized using a documented record.
- All generic accounts (which can be used to login to a system) should be replaced by named accounts; else formal ownership should be defined by the asset owner. All such cases should be routed to the Information Security Team before the creation of these accounts for risk assessment and implementation of adequate logging and monitoring controls.
- Shared and generic Accounts should be permitted only through PAM if there is a technology limitation. Also, exceptions around such accounts should be obtained and flagged to business/asset owners for their review and approval. Generic accounts should be permitted only if authorized by the Information Security Team, after assessing the sensitivity of applicable assets. Information Security Team shall monitor usage and accountability of permitted generic accounts on production systems periodically.
- Information Security Team shall perform an annual review to ascertain implementation of appropriate baseline security standard on critical infrastructure assets

Application and Infrastructure Security

- Maintain a single, complete, accurate and up-to-date inventory of all application and infrastructure component assets at Choice Equity Broking Pvt. Ltd. (Choice).
- Information Security Team and application development teams shall collaborate annually and/or on a need basis, to aid in incorporating security as part of the ongoing software design, implementation, testing, maintenance and up-gradation activities. Application development shall adopt and adhere to industry best practices ensuring alignment to the principle of defence-in-depth to provide layered security mechanisms.
- Critical infrastructure asset owners shall be responsible for maintaining a list of all available and deployed patches, and a deployment schedule including status of each patch deployment activity. Patches should be rigorously tested before deployment into production environments to ensure no adverse impact to other systems and shall adhere to the

organization's change management process. Any deviation on patch deployment shall be approved by CISO & Head IT. All application and infrastructure components deemed as critical cyber assets shall be covered in regular vulnerability assessment and penetration testing exercises.

- Remediation activities should be documented and immediately commenced to address the identified gaps within agreed timelines.
- Information Security Team shall conduct adequate vulnerability scanning and penetration testing assessment prior to any internet-facing applications, network interfaces, and new or major changes to existing systems deployed in production environments.

Social Engineering

- Information Security Team shall conduct social engineering exercises on an annual basis at multiple Choice Equity Broking Pvt. Ltd. (Choice) premises.
- Such exercises are crucial to assess peoples' related vulnerabilities in the Choice Equity Broking Pvt. Ltd. (Choice) business environment and strengthen the holistic Cyber Security posture by supplementing technical and procedural controls.
- Social engineering exercises can include techniques such as, but not limited to Phishing, pretext calling and physical elicitation at various Choice Equity Broking Pvt. Ltd. (Choice) office locations.

Vendor Management

- Senior management shall evaluate the need for outsourcing critical processes and selection of vendor / partners in line with regulatory requirements. Business Function shall periodically assess & monitor vendor performance & risk arising from outsourced services. Any such material risks and exceptions shall be formally documented.
- Contractual agreements with vendors shall consider confidentiality, background verification & regulatory requirements. In addition, agreement shall include provision on Right to audit by Choice Equity Broking Pvt. Ltd. (Choice) & its regulators to ensure vendor processes are adequate
- The Information Security Team shall conduct a comprehensive risk assessment on the vendor.

6.4 Cyber Security Metrics and Measurement

- Information Security Team shall monitor various people, process and technology controls across the environment
- Information Security Team shall use systems and/or processes to facilitate continuous monitoring and timely detection of security events, unauthorized transactions or other malicious activities by internal and external entities.
- Activity logs for critical application, system and network device assets should be aggregated and correlated to generate alerts and actionable event information.
- Capacity utilization of critical system and network assets should be monitored by respective asset owners using suitable mechanisms.

6.5 Detection and Response

- Security Operations Center shall be established to enable log aggregation and correlation for providing analysis and overarching situational awareness of cyber threats.
- Notifications from multiple sources, such as alerts generated from event monitoring mechanisms, process reviews and raised incidents shall be managed in line with Choice Equity Broking Pvt. Ltd. (Choice)'s Incident Management Policy.
- Security Incident Management Portal must be in place for all employees/outsourced to log information security incidents.
- Once detected and preliminary checks are performed, the Information Security Team should be notified immediately via incident reporting tools (or verbally, in case of severe potential impact) and consulted for resolution support.
- The impact of cyber security events should be ascertained in order to take precise and apt response measures. Response plans should aim at timely restoration of systems affected by incidents of cyber-attacks or breaches, in line with defined RTOs and RPOs.
- Response plans for the Cyber Security incident shall clearly outline the activities to be performed, and the responsibilities of people involved in them.
- Incidents of compromise, theft or destruction of data, sensitive information, or systems due to a cyber-attack or breach, should be analyzed by conducting a root cause analysis of the incident and ensuring that the actions items identified are tracked to closure. Information Security Team will liaise with specialized partners / vendors to aid in

investigation processes like forensics & active mitigation services. Cyber Incidents will be communicated to respective regulators as per regulators requirements and Compliance review.

6.7 Audits

- Information Security Team shall ensure Cyber Security & VAPT Audits to confirm the cyber security controls and test their effectiveness as per regulatory guidelines.
- Matrix to conduct different types of audits is as below:-

Asset Type	Applicable to Assets classified as	Audit Type	Audit Frequency
Web Applications	Critical	Internal- VAPT	- After every major release
Web Applications	Critical	External - CERT-IN Empanelled - VAPT	- Bi Annually (As per regulatory guidelines)
Mobile Applications	Critical	Internal- VAPT	- After every major release
Mobile Applications	Critical	External - CERT-IN Empanelled - VAPT	- Bi Annually (As per regulatory guidelines)
Firewalls	Critical	Internal- VAPT	Quarterly (Rule Reviews)
Firewalls	Critical	External - CERT-IN Empanelled - VAPT	- Bi Annually (As per regulatory guidelines)
Infrastructure (Servers) - On Prem	Critical	Internal- VAPT	- As need basis (on provisioning of new server)
Infrastructure (Servers) - On Prem	Critical	External - CERT-IN Empanelled - VAPT	- Bi Annually (As per regulatory guidelines)
Infrastructure (Servers) - Cloud	Critical	Internal- VAPT	- As need basis (on provisioning of new cloud service / application - Configuration reviews, cloud deployment reviews)
Infrastructure (Servers) - Cloud	Critical	External - CERT-IN Empanelled - VAPT	- Bi Annually (As per regulatory guidelines)
Infrastructure (Network - Switches, Wifi Routers, Network Segmentation)	Critical	External - CERT-IN Empanelled - VAPT	- Bi Annually (As per regulatory guidelines)
API Security	Critical	Internal- VAPT	- After every major release
API Security	Critical	External - CERT-IN Empanelled - VAPT	- Bi Annually (As per regulatory guidelines)

6.8 Cyber Security Drills

- The Information Security Team shall conduct periodic drills or exercises to test the readiness of the people, process and technology aspects to detect, respond and recover from cyber attacks.
- The scope and frequency of such drills shall be determined based on the scale of operations, threat landscape, and resource availability.

6.9 Awareness and Training

- Choice Equity Broking Pvt. Ltd. (Choice)'s Cyber Security Policy is the foundation for its cyber security strategy, and of training initiatives that can truly help the firm collectively upgrade its cyber security posture.
- Periodic training and initiatives shall be undertaken for augmenting the awareness among Choice Equity Broking Pvt. Ltd. (Choice) employees, third-party staff and its vendors about areas such as:
    - The organization's Cyber Security policies
    - Peoples' obligations towards Choice Equity Broking Pvt. Ltd. (Choice)'s Cyber Security program
    - Appropriate use of Critical Cyber Assets
    - Physical and logical controls for Critical Cyber Assets
    - Guidelines for identification of Cyber Security incidents
- The Cyber Security policy should be included as part of the employment agreement to ensure that employees understand the guidelines.
- Awareness training shall also be imparted.
- Specific awareness mailers should be sent periodically to all Choice Equity Broking Pvt. Ltd. (Choice) employees regarding Cyber Security basics such as avoiding writing of passwords on sticky-notes at their workstation, and usage of same passwords for their public email and other accounts.
- Periodic mailers to customers shall be communicated by business management to create awareness with reference to cyber security risks, reporting of phishing mails & social engineering attacks

7.0 Continual Improvement

- Information Security Team shall periodically monitor the Choice Equity Broking Pvt. Ltd. (Choice) technological environment by evaluating Cyber Security metrics covering critical areas, including but not limited to:
    - Incident Management
    - Vulnerability Management
    - Patch Management

  - Configuration Management
  - Change Management
  - Application Security
  - Identity & Access Management
- Information Security Team shall assess compliance to defined policies, as part of ongoing operations as well as ISMS Internal Audit channels.
- The performance results shall be reported annually, to the CISO and Senior Management, and shall be used to improve the overall Cyber Security program, policies and standards.
- Lessons learnt from Cyber Security incidents shall be documented and inputs should be fed into response plans to improve recovery planning and operations, as well as the risk assessments performed.
- Information Security Team shall review the Cyber Security training program on an annual basis at minimum and ensure that the content and delivery mechanisms are relevant and easy-to-understand

8.0 Reference Documents

- ISO 27001:2022
- SEBI/HO/ ITD-1/ITD_CSC_EXT/P/CIR/2024/113

9.0 Glossary

Cyberspace
The interdependent global network of information technology infrastructure that comprises of the Internet, telecommunications networks, computer systems, tools, end-users and other entities.

Cyber Security
The capability and processes where information technology and communication systems, and the information contained therein are protected against damage, compromise, unauthorized use or modification, or exploitation in cyberspace.

Cyber Security Event
An event or an anomaly detected by a security device, service, application, process or human on a technology infrastructure environment.

Cyber Security Attack
A Cyber Security attack is an intentional exploitation of assets (people, systems, networks, processes and services) using threat agents such as exploits, denial of service, backdoors and social engineering, indirectly or directly with the intent to adversely affect or compromise the confidentiality, integrity or availability of such assets.

Such attacks can be performed from both within the perimeter of the organization or from outside physical and logical boundaries.

Cyber Attack Vector
An attack vector is a mechanism, channel or means by which an entity (such as a hacker) can gain access to a computer or network server in order to deliver a payload or cause a malicious outcome. Attack vectors enable hackers to exploit system vulnerabilities, including the human element.

Cyber Security Incident
Any malicious act or suspicious event that compromises or attempted to compromise the electronic, physical and logical security of a critical cyber asset or the operation of service(s) involving critical cyber assets.

Cyber Security Breach
A Cyber Security Incident that has successfully accomplished its malicious task of exploiting technology and/or communication systems, by overcoming or bypassing the deployed Cyber Security controls in the environment.

Cyber Security Readiness Exercise
An activity or event, during which an organization simulates a cyber-attack to assess capabilities and refine controls, for preventing, detecting, responding to or recovering from planned disruptions.

Cyber Program Operations

The activities performed by a person or a team of designated persons to deliver the cyber program plans and continually gather evidence to mitigate possible or real-time threats and protect the organization against security breach, espionage, sabotage, and other cyber threats.

10.0 Annexures

10.1 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.