CHOICE EQUITY BROKING PVT. LTD

NETWORK SECURITY MANAGEMENT POLICY

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	09-Apr-23	2.0	Ashutosh Bhardwaj	Yogesh Jadhav
Reviewed On	31-Jan-24	2.1	Anil Ashok & Associates	Ashutosh Bhardwaj
Reviewed On	20-Feb-25	2.2	Abhishek Vinayak	Ashutosh Bhardwaj

TABLE OF CONTENTS

1.0 Purpose

Networks have logically and physically extended data, processing and communication facilities across Choice Equity Broking Pvt. Ltd. (Choice). Network security assumes importance to Choice Equity Broking Pvt. Ltd. (Choice) when viewed in light of the following:

- Networks change frequently as new users and devices are added and newer data communication technology is introduced
- Usage of various networking, communications and computing technologies to effectively meet the IT needs
- Sensitive data is increasingly transmitted over networks
- Proliferation of Internet access has increased vulnerability as employees use Internet for information and knowledge

The term 'network' used in this policy section refers to all the types of networks like Local Area (LAN), and Wide Area Network (WAN).

2.0 Scope

This policy applies to all employees, contractors, consultants, and temporary staff members etc. who have access to Choice Equity Broking Pvt. Ltd. (Choice)'s network resources. All are expected to be familiar and comply with this policy.

3.0 Policy

3.1 Network Management Controls

3.1.1 Network Design

Networks shall be designed in conformance with sound security practices. The following points shall be observed:

- The hardware and software configuration of the critical servers shall be documented.
- Incorporate coherent technical standards, use consistent naming conventions and comply with statutory and industry regulations.
- Incorporate distinct sub-networks, protected by rule-based traffic filtering using firewalls and other appropriate technology.
- Minimize single points of failure and the number of entry points into the network.
- Enable network management reports and maintain audit trails.
- Network design shall be supported by a formal documentation of the network details
- Hardware redundancy mechanisms (i.e. duplicating certain or all hardware elements) shall be adopted for all applicable network devices and critical applications.
- Mechanism for High Availability (HA) need to be looked at and implemented, if possible and necessary.

3.1.2 Network Services

- A server shall be dedicated to a single network service, wherever feasible.

- The appropriate authority shall assess the security risks associated with enabling a network service to arrive at the security requirements.
- Any unused or unwanted network services shall be removed or disabled.

3.1.3 Network Connectivity

- Access to local system control utilities (e.g. Network Management System etc.) shall be controlled. Access to these utilities shall be limited to authorized personnel only
- Modems or any other connection to external network/internet shall not be used on machines when connected to the internal network. (Exception: only when the device is meant for WAN/internet connection.)
- External parties shall not be allowed to connect to the Choice Equity Broking Pvt. Ltd. (Choice) internal network. There shall not be any exception to this policy.
- For non-public information, all equipment that provides access to the network shall positively identify the user through a login sequence for providing access.
- No dial-in connections shall be allowed to connect inside the Choice Equity Broking Pvt. Ltd. (Choice) network.
- Remote Access Software shall be used over the internal network only by authorized personnel.
- All default passwords used on network devices for administrative or otherwise authorization shall be changed. All such default accounts shall be either enabled with changed passwords or disabled and new accounts created in their place.
- User access control list shall be maintained and implemented on all network equipment's. No changes shall be made to existing rules without prior approval from Head – Network.
- When access is no longer required, the requesting department within Choice Equity Broking Pvt. Ltd. (Choice) or external connecting organization shall notify the network team responsible for that connectivity. Network Team shall then terminate the access.
- Automatic connections to external remote computer systems shall not be allowed.
- Corporate wireless connectivity shall be enabled only for corporate mobile computing devices with relevant security controls implemented

3.1.4 Network Component Security

- All the network components shall be identified, and their use restricted.
- All network components shall be maintained in an inventory along with details.
- All communication equipment like cables, network devices shall be secured from unauthorized physical access. The access control may be in the form of:
  - Access control systems like RFID access cards, Biometric scanners, Keypad locks, etc.
- Access to highly sensitive processing functions shall be secured by limiting the terminals from which these functions can be executed and physically and / or logically restricting these terminals.

3.1.5 Installing Network Operating Systems (NOS)

- A documented procedure for installing a network operating system shall be developed and followed.
- A hardened version of the operating system shall be installed to prevent easier compromise of the system.

- Default passwords shall be changed as part of the installation process.

3.1.6 Network Operating System Controls

- Each network user shall have a unique user id and password.
- All user accounts shall be associated with an applicable, informative full name and description.
- All the guest account shall be disabled.

3.1.7 Updating the Network Software

- The System / Network Administrator are responsible for installing necessary security-related software updates on need basis.
- The update may cause issues with the current functionality of the network device and consequently the day to day operations.
- The Network Software upgrade is done on need basis.

3.1.8 Network Security and Access Controls

- There shall be proper authorization procedure for determining who can access which networks and networked services. Proper protection shall be ensured for any such connectivity.
- Access to diagnostic ports within Choice Equity Broking Pvt. Ltd. (Choice) shall be securely controlled.
- It is the responsibility of Head Network to determine the following prior to connection:
  - Permitted network and network services
  - Elements of the network that may be accessed
  - The authorization procedure for gaining access
  - Authorized users allowed to access these network and network services
  - Controls to protect the access to the network and services

3.1.9 Login Process

- A warning banner shall be displayed at login to any Choice Equity Broking Pvt. Ltd. (Choice) system. This will constitute a special notice, which will include:
  - The system is to be used only by authorized users
  - The user represents that he/she in an authorized user by continuing to use the system
  - Use of this system constitutes consent to monitoring
- The banner shall not include any system or application identifiers, which may provide valuable information to a would-be intruder e.g. hardware and operating system present on the host, information about the organization or other internal matters
- All unsuccessful login attempts shall be recorded. The logs shall be reviewed periodically for such attempts**.**
- Only authorized users shall have access to utilities that reconfigure logging mechanisms
- The log files shall be protected from being accessed, modified or deleted by unauthorized users.

3.1.10 Terminal Timeout

- Time out duration shall be specified for all terminals inactive for a set period of time

- The timeout facility shall clear the application screen

3.1.11 Network Configuration Diagrams

- Network configuration diagrams shall be considered as sensitive information. Network configuration diagrams shall only be made available to authorized individuals strictly on a need-to-know basis.
- The network configuration diagrams shall always be kept updated.
- Any change in the network configuration shall be notified, to the officials of Choice Equity Broking Pvt. Ltd. (Choice) responsible to maintain the Disaster Recovery Plan / Business Continuity Plans.
- All changes in access control shall be accompanied by a valid business justification and are subject to security review. All such changes shall go through the change management process. The requesting department is responsible for notifying the Network and Security team when there is a material change in their originally provided information so that security and connectivity evolve accordingly.

3.1.12 Enforced Path

- Controls are in place to prevent users from accessing applications or facilities that they are not authorized to use. Controls shall be based on the Logical Access Control policy.
- Allocate specific ports for specific applications and systems.
- Enforce access restrictions at firewalls and other perimeter devices like routers.
- Create separate logical domains or Virtual LANs based on the need for segregation in the network.
- Principle of least privilege should be followed while granting users access to the network systems.

3.1.13 Clock Synchronization

- System clocks shall be synchronized regularly especially between the organization's various processing platforms. This would allow for generating time based audit trails.

3.2 Network Devices

3.2.1 Routers

Proper router security is essential for protecting Choice Equity Broking Pvt. Ltd. (Choice)'s information resources from external threats. The procedures shall be established to ensure the routers are protected adequately.

3.2.2 Firewalls

The firewall design and architecture shall be decided based on the security requirements of the internal Choice Equity Broking Pvt. Ltd. (Choice) network. Access to Choice Equity Broking Pvt. Ltd. (Choice) resources in DMZ from the public network (Internet) shall be controlled at the firewall level.

Adequate measures should be taken to isolate and secure the perimeter and connectivity to the servers running algorithmic trading applications.

Firewall Rule review need to be performed on annual basis.

3.2.2.1 Web Filtering

To enhance network security and prevent access to malicious or inappropriate content, web filtering must be implemented and enforced on all network traffic passing through the firewall. The firewall should include a web filtering mechanism that:

- Blocks access to websites known for hosting malicious content, including malware, phishing, and ransomware sites.

- Restricts access to unauthorized or non-business-related websites as defined by the organization's acceptable use policy.
- Monitors and logs all web traffic for security analysis, identifying potential threats or unusual behavior patterns.
- Enforces category-based filtering (e.g., blocking social media, streaming, gaming, and other non-essential categories during business hours) based on the organization's operational needs.
- Regularly updates web filtering rules and definitions, leveraging threat intelligence feeds to stay current with emerging web-based security threats.
- Allows for exception requests to be made, subject to managerial approval, for business-critical websites that may fall outside the standard filtering categories.

3.2.3 Network Switch

Network switches direct and control much of the data flowing across computer networks. The detailed procedures shall be established to segment networks.

3.2.4 Other network equipment's

Similar security procedures shall be established for other networking equipment's.

3.2.5 Intrusion Prevention / Detection System (IPS / IDS)

- IPS signature shall be updated on a regular basis to prevent emerging Network attacks

  IPS shall be placed in line with the internet gateway to inspect and prevent malicious traffic.

3.2.6 Mobile Devices

- Access to Choice Equity Broking Pvt. Ltd. (Choice) network using mobile devices is restricted to Choice Equity Broking Pvt. Ltd. (Choice) authorized devices

3.2.7 Network Diagnostic Tools

- The use of network diagnostic tools shall be strictly controlled to prevent unauthorized users from obtaining sensitive information about the network.
- Penetration testing tools may sometimes be deployed to assess the network's robustness to internal and external hacking. It is essential that these tools shall be run in a controlled environment, with written approval from Head – Technology.

3.3 Auditing, Logging and Monitoring

- The firewall shall be configured to generate logs on daily, weekly and monthly basis.
- All super user activities shall be logged and reviewed on a monthly basis.
- Logs of activities (e.g., resources accessed, time of action etc.) carried out by maintenance personnel, shall be generated and closely monitored by the Network Administrator.

4.0 Reference Documents

- ISO 27001:2022

ISO 27001 CONTROL NUMBERS	CONTROL TITLE
5.15	Access Control
5.29	Information Security during disruption
8.2	Privileged access rights
8.14	Redundancy of information processing facilities
8.15	Logging
8.17	Clock synchronisation
8.20	Network controls
8.21	Security of network services
8.22	Segregation in networks