Harendra D. Mehta Share & Stock Broker Pvt. Ltd.

MEMBER > NSE Equity Segment > BSE Equity Segment

Stock Exchange Rotunda Building, PG -12, Ground Floor, Mumbai Samachar Marg, Mumbai - 400 001.

Phone : 2272 2392 / 2272 2190 / 2272 2546 / 2272 2548 • E-mail : bhm264@gmail.com

CIN : U67120MH1997PTC110950 • GSTIN : 27AAACH2890J1ZE

INTERNAL SECURITY AUDIT PLANNER

HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED

15-04-2024

Author:	BAIJU HARENDRA MEHTA (DIRECTOR)
Owner:	BAIJU HARENDRA MEHTA
Organization:	HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED
Version No:	1.0
Date:	15-04-2024

Document Control

Document Title **Internal Security Audit Planner**

Version History

Version No.	Version Date	Author	Summary of Changes
1.0	15-04-2024	BAIJU HARENDRA MEHTA	NA

Approvals

Name	Title	Date of Approval	Version No
BAIJU HARENDRA MEHTA	Internal Security Audit Planner	15-04-2024	1.0

Distribution

Name	Title	Date of Issue	Version No
NA	NA	NA	NA

1.0 INTERNAL AUDIT PLANNER

1.1 PURPOSE

To conduct internal cyber security readiness audits to determine whether the controls, processes and procedures of the organization; conform to the requirements of the standards, information security requirements and relevant legislation or regulations.

1.2 SCOPE

The scope of this procedure is to audit the effectiveness of the HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED SEBI Cyber Security Resilience implementation and the continuous improvements of the same.

1.3 POLICY STATEMENTS

This document provides procedures for implementing the Internal Audit section of Security Policy for the HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED. This document can be used to conduct internal audits to determine whether the controls, procedures and security practices conform to the requirements of the security policies, standards, information security requirements and relevant legislation or regulations.

1.3.1 AUDIT SCHEDULE

- An internal audit calendar should be created based on fulfilling the following audit requirements:
  - An Internal audit should be conducted for HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED on a yearly basis.
  - A technical vulnerability assessment of the security preparedness of the facilities should be done on a yearly basis.
- The audit calendar should be created and/or reviewed and approved by the Technology Officer or Head of IT Security.

1.3.2 AUDIT PLAN

- The Company shall conduct internal audits of its security management system at planned intervals to determine if its control objectives, controls, processes, and procedures are effectively implemented and maintained, and perform as expected.
- Technology Officer shall conduct an assessment of the existing Information Technology security system, in order to establish a baseline for auditing.

H. D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

- The internal audit plan shall be created based on the following requirements:
  - Importance of processes and areas to be audited (based on a Risk based audit approach)
  - Review of closure of non-conformity from previous audits
  - Ensure that auditors shall not audit their own work

1.3.3 AUDIT PROCESS

- The auditor would need to review compliance that are applicable to HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED at the time of the audit.
- The audit calendar should be communicated to the auditee at least one week prior to the proposed date of audit in coordination with the security coordinator.
- The process and people audit will be conducted by means of interviews with the personnel from the department or process being audited; after ensuring that work performed by the personnel is not hindered.
- The technical audit for devices, servers, laptops and desktops would be conducted using vulnerability assessment tools, scripts and/or manual inspection.
- The auditor should check the implementation of the controls implemented in the environment and their effectiveness.
- The auditor should attempt to identify any new risks or improvements that can improve the security of the work environment.
- The auditor should do a sample audit for the effectiveness of the controls' implementation.
- The auditor should take notes and make observations during the audit process.
- The auditor should fill in the following in the Internal Audit Report:
  - Type of Non-Conformance (Major, minor or observation)
  - Relevant Domains and Controls for the Non-Conformance
  - Description of findings
  - Recommendations for conformance
- Then only after consulting with the Technology Officer the auditor should fill the following details in the Audit Report For:
  - Root Cause Analysis of the Non-Conformance
  - Corrective and Preventive Measures
  - Resources assigned to close non-conformity
  - Confirmatory Audit details
  - Update Non-Conformance Tracker and file after closure

H. D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

- The audit would end with a closing meeting in which the general compliance level will be revealed. The non-conformances detected in the audit will be communicated to the coordinator of the department for correction of the non-conformances
- The Technology Officer should review the recommended action and obtain management approval for the implementation of the control.
- The Technology Officer is responsible for ensuring that the non-conformances are closed by the proposed closure dates. These non-conformances should be reviewed and closed before the next scheduled audit.
- If the implementation of the recommended control is a long-term activity, an implementation plan needs to be created and tracked.

1.4 GUIDELINES FOR DETERMINING TYPES OF NON-CONFORMANCE

1.4.1 MAJOR NON-CONFORMANCE

- A major non-conformance occurs when one of the criteria of the standard is not addressed or has not been addressed adequately. Typically, major non-conformances occur when an organization has not addressed all the requirements of a specific element or criterion.
- They also occur when an organization has put a process or procedure in place but has not implemented it or cannot yet demonstrate effective implementation.
- One of the most common major non-conformances is the failure of an organization to complete a full internal audit and/or management review.
- A major non-conformance can also occur if a significant number of minor non-conformances in a given activity.
    - For example, a minor non-conformance in document control may not in itself constitute a significant problem. But if several problems are found with document control, then this points to a larger systemic document control problem and would constitute a major non-conformance.

1.4.2 MINOR NON-CONFORMANCE

- A minor non-conformance by itself doesn't indicate a systemic problem. It is typically an isolated or random incident.
    - An example is if the most current version of a document is not available at an operator's station; the updated version exists but a copy of it is not available for the operator's use and the operator is using an outdated procedure.
    - Other examples are a form without a document control number on it or an internal audit with an overdue corrective action request pending.

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

1.4.3 OBSERVATION

- An observation is, no violation of policy, standards, or procedures defined. It is typically identification that there may be a better way to perform an activity.
- The improvements may be in the monitoring of a process or in the documenting of a procedure. Observations are a potential for improvement - a way to avoid future problems.

FOR HARENDRA D. MEHTA SHARE & STOCK BROKER PVT. LTD.

DIRECTOR

H. D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

Harendra D. Mehta Share & Stock Broker Pvt. Ltd.

MEMBER ➤ NSE Equity Segment ➤ BSE Equity Segment

Stock Exchange Rotunda Building, PG -12, Ground Floor, Mumbai Samachar Marg, Mumbai - 400 001.

Phone : 2272 2392 / 2272 2190 / 2272 2546 / 2272 2548 • E-mail : bhm264@gmail.com

CIN : U67120MH1997PTC110950 • GSTIN : 27AAACH2890J1ZE

INFORMATION SYSTEMS & CYBER SECURITY POLICY

HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED

15-04-2024

Author:	BAIJU HARENDRA MEHTA (DIRECTOR)
Owner:	BAIJU HARENDRA MEHTA
Organization:	HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED
Version No:	1.0
Date:	15-04-2024

Document Control

Document Title **Information Systems & Cyber Security Policy**

Version History

Version No.	Version Date	Author	Summary of Changes
1.0	15-04-2024	BAIJU HARENDRA MEHTA	NA

Approvals

Name	Title	Date of Approval	Version No
BAIJU HARENDRA MEHTA	Information Systems & Cyber Security Policy	15-04-2024	1.0

Distribution

Name	Title	Date of Issue	Version No
NA	NA	NA	NA

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

TABLE OF CONTENT

Table of Content....3
1.0 Introduction....4
1.1 Objective & Need....4
2.0 Information Systems & Cyber Security Policy....5
2.1 Purpose....5
2.2 Scope....5
2.3 Information Security Responsibilities....5
2.4 information security audit....6
2.5 Information Security Policies List....6
3.0 Acceptable Use Policy....8
3.1 Purpose....8
3.2 Scope....8
3.3 Policy Statement....8
4.0 Patch Management Policy....13
4.1 Policy Statement....13
5.0 Data Backup & Recovery Policy....15
5.1 Policy Statement....15
6.0 Technical Vulnerability Management policy....17
6.1 Policy Statement....17
7.0 Cryptographic and Encryption Policy....18
7.1 Policy Statement....18
8.0 Application Development and Security Policy....20
8.1 Policy Statements – Systems Development Life cycle (SDLC)....20
8.2 Policy Statements – Application Security....23
9.0 User Awareness and Training Policy....28
9.1 Policy Statements....28
10.0 Teleworking Policy....30
10.1 Policy Statement....30

1.0 INTRODUCTION

Information and the supporting processes, systems and networks are important business assets. Increasingly, organizations and their information systems and networks are faced with security threats from a wide range of sources, including computer-assisted fraud, espionage, sabotage, fire or flood. Sources of damage such as computer viruses, computer hacking, and denial of service attacks have become more common, more ambitious and increasingly sophisticated. Dependence on information systems and services means organizations are more vulnerable to security threats.

Information Security Management needs, as a minimum, participation by all employees in the organization.

1.1 OBJECTIVE & NEED

- The objective for developing and implementing Information Systems & Cyber Security Policies is to provide HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED direction and support for information security in accordance with business requirements and relevant laws and regulations.
- Need for having Information Security Policies is listed below.
    - Regulatory and legal requirements – One of the most compelling reasons for developing formal policy is because it is mandated
    - Consistency – Similar problems are treated in a similar and consistent fashion
    - Fairness – Policies ensure that all users are treated fairly with respect to the level of access they may have
    - Understanding – Policies ensure that all involved parties understand clearly what is expected

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

2.0INFORMATION SYSTEMS & CYBER SECURITY POLICY

2.1 PURPOSE

The purpose of Information Systems & Cyber Security Policy is to provide guiding principles and support to safeguard the information security in the organization. HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED aims to ensure the appropriate confidentiality, integrity and availability of its data. The security policies contained in this document have been established to cover data and information assets at rest in the IT infrastructure or in transit over the communication networks owned and operated by HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED.

2.2 SCOPE

This policy applies to:

- All staff (permanent & on contractual basis) and non-employees / stakeholders (interns, contractors, consultants, suppliers, vendors etc.) of HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED and other individuals, entities or organizations that have access to and use HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED' information systems environment.
- HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED staff, who are responsible for administering and maintaining HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED' IT infrastructure.

2.3 INFORMATION SECURITY RESPONSIBILITIES

IT Committee shall be created. Chaired by a senior member of the Information Security or Information Technology management team, and will comprise the following members:

- Chair
  - Head of IT Security, or,
  - Head of Information Technology
- Members
  - Head of IT Applications
  - IT team member(s)
  - IS team member(s)
  - HR head or designated team member
  - Finance Head or designated team member

This Technology Committee should on a yearly basis review the implementation of the

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

Information Systems and Cyber Security policy approved by the Board.

The technology committee of HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED Equities should periodically review instances of cyber-attacks, if any, domestically and globally, and take steps to strengthen Cyber Security and cyber resilience framework.

2.4 INFORMATION SECURITY AUDIT

HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED Equities shall arrange to have their systems audited on an annual basis by a CERT-IN empanelled auditor or an independent CISA/CISM qualified auditor to check compliance with all areas of information security and shall submit the report to Stock Exchanges / Depositories along with the comments of the Board of HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED Equities within three months of the end of the financial year

2.5 INFORMATION SECURITY POLICIES LIST

Following policies shall be developed as part of HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED Information Systems Security guidance documentation. These policies, procedures, guidelines will be approved by HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED senior management or Board as appropriate.

POLICY NO.	POLICY NAME
1	Information Systems & Cyber Security Policy
2	Acceptable Use Policy
3	Patch Management Policy
4	Teleworking Policy
5	Data Backup & Recovery Policy
6	Technical Vulnerability Management Policy
7	Cryptography and Encryption Policy
8	Application Development and Security Policy
9	User Awareness & Training Policy
OTHER POLICIES	
10	IT Asset Management Policy
11	IT Vendor Selection Policy
12	IT Threat-Risk Assessment
13	IT Access Control Policy
14	IT Incident Handling Policy
15	IT Business Continuity Plan

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

16	IT Computer Malware Policy
17	IT Security Audits Planner
18	BYOD Policy
19	E-Mail Policy
20	IT Outsourcing Policy
21	IT Records & Documents Management Policy
22	Physical Security Policy
23	HR Security Policy
24	Change Management Policy
25	Hardening Procedure

H. D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

3.0 ACCEPTABLE USE POLICY

3.1 PURPOSE

The purpose of this policy is to outline the acceptable use of computer equipment at HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED.

3.2 SCOPE

This policy applies to the use of information, electronic and computing devices, and network resources to conduct HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED business or interact with internal networks and business systems, whether owned or leased by HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED, employee, or a third party. All employees, contractors, consultants, temporary, interns and other workers at HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources.

3.3 POLICY STATEMENT

General Use and Ownership, proprietary information stored on electronic and computing devices whether owned or leased by HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED, the employee or a third party, remains the sole property of HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED.

- Employees have a responsibility to promptly report the theft, loss or unauthorized disclosure of HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED proprietary information.
- Employees may access, use or share HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED proprietary information only to the extent it is authorized and necessary to fulfil their assigned job duties.
- Employees are responsible for exercising good judgment regarding the reasonableness of personal use.
- HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

H. D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

3.3.1 SECURITY AND PROPRIETARY INFORMATION

- All mobile and computing devices that connect to the internal network must comply with the User Access Policy.
- System level and user level passwords must comply with the Password Policy Guidelines.
- All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less.
- Employees must lock the screen or log off when the device is unattended.
- Postings by employees from HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of unless posting is during business duties.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

3.3.2 UNACCEPTABLE USE

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during their legitimate job responsibilities.

Under no circumstances an employee of HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED is authorized to engage in any activity that is illegal under local, state, government or international law while utilizing HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED owned resources.

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software
- Accessing data, a server or an account for any purpose other than conducting HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED business, even if you have authorized access.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal.

H. D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others.
- Using HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED account.
- Effecting security breaches or disruptions of network communication.
    - Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access.
    - Disruption includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Executing any form of network monitoring which will intercept data not intended for the employee's host.
- Introducing honeypots, honeynets, or similar technology on the HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED network.
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session
- Providing information about, or lists of, HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED employees and customers to parties outside HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED

3.3.3 EMAIL AND COMMUNICATION ACTIVITIES

When using company resources to access and use the Internet, users must realize they represent the company. The following activities are strictly prohibited, with no exceptions:

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.
- Solicitation of email for any other email address, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

H. D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

3.3.4 ALLOWED INTERNET USAGE

Internet usage is granted for the sole purpose of supporting business activities necessary to carry out job functions. Acceptable use of the Internet for performing job functions might include:

- Communication between employees and non-employees for business purposes
- IT technical support downloading software upgrades and patches
- Review of possible vendor websites for product information
- Use of social network websites for business purpose
- Reference regulatory or technical information
- Research

3.3.5 RESTRICTIONS ON INTERNET USAGE

The company prohibits acquisition, storage, and dissemination of data which is illegal, pornographic, or which negatively depicts race, sex or creed is specifically prohibited.

The company also prohibits the conduct of a business enterprise, political activity, engaging in fraudulent activities.

Other activities that are strictly prohibited include, but are not limited to:

- Using gambling related websites
- Unauthorized downloading of any shareware/freeware programs or files for use
- Any illegal use or unauthorized access or network scanning – both internal and external
- Any ordering (shopping) of items or services on the Internet
- Downloading through torrents or bulk file sharing websites
- Browsing pornographic and any inappropriate sites
- Downloading pirated software and graphics
- Forwarding of chain letters
- Participation in any on-line contest or surveys or promotion
- Acceptance of promotional gifts
- Deliberate pointing or hyper-linking of company Web sites to other Internet/www sites whose content may be inconsistent with or in violation of the aims or policies of the company.
- Any conduct that would constitute or encourage a criminal offense, lead to civil liability, or otherwise violate any regulations, local, state, national or international law
- Use, transmission, duplication, or voluntary receipt of material that infringes on the copyrights, trademarks, trade secrets, or patent rights of any person or organization.

H.O. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

- Transmission of any proprietary, confidential, or otherwise sensitive information without the proper controls.
- Creation, posting, transmission, or voluntary receipt of any unlawful, offensive, libellous, threatening, harassing material, including but not limited to comments based on race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs.

3.3.6 CLEAN DESK POLICY

- Computer workstations must be locked when workspace is unoccupied.
- Computer workstations must be shut down at the end of the workday.
- Any Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the workday.
- File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.
- Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.
- Laptops must be either locked with a locking cable or locked away in a drawer.
- Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
- Printouts containing Restricted or Sensitive information should be immediately removed from the printer.
- Whiteboards containing Restricted and/or Sensitive information should be erased.
- Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer
- All printers and fax machines should be cleared of papers as soon as they are printed; this helps ensure that sensitive documents are not left in printer trays for the wrong person to pick up.

3.3.7 SOFTWARE INSTALLATION POLICY

- Employees should not install software on HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED computing devices without prior approvals.
- Software must be selected from an approved software list, maintained by the system admin of HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED

  For installation of software not present in approved list, employee should submit formal request to his/her manager, along with business justification for software usage.

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

4.0PATCH MANAGEMENT POLICY

4.1 POLICY STATEMENT

4.1.1 IDENTIFICATION AND VALIDATION OF PATCHES

- System administrator and Application administrator of HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED IT department are responsible for identification and validation of all patch related issues concerning their domain of work.
- Head of Information Technology, Head of IT Security, Head of IT Applications are responsible for approving all security related patches.
- To ensure that all patches are tracked, the administrator shall:
  - Subscribe to the trusted advisories, vendor's security patch mailing list or have agreements with vendors for receiving new security patches
  - Maintain an updated list of OS, application and database related patches released
  - Head of Information Technology or Head of IT Security shall validate whether the released patch is applicable to the environment
  - If the patch is affecting a service and is not implemented, system administrators shall track and keep a record of the discarded patches for future audit purposes

4.1.2 PATCH SCHEDULING & PRIORITIZATION

- Patches shall be tested and applied on priority basis based on their identified criticality.
- Criticality of Patches are as follows:
  - Critical: A vulnerability whose exploitation could severely impact the IT systems that provide services to critical business functions of HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED.
  - High: A vulnerability whose exploitation could result in compromise of the confidentiality, integrity, or availability of HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED information.
  - Medium: A vulnerability whose exploitation would affect HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED IT systems but on a controllable level.
  - Low: A vulnerability whose exploitation is extremely difficult, or whose impact is minimal.

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

4.1.3 PATCH INSTALLATION

- All patches deployed in HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED IT infrastructure (pre-production and production environment) must be performed as per change management process.
- Respective System administrators and vendors shall check whether the patch installation affects the operating system or application's functionality in a test environment, wherever applicable.
- If the tested patch is successful, it can be applied on the production environment, only after an approval from IT Management as per the change management process.

4.1.4 PATCH TRACKING

Respective IT Administrators shall maintain a patch tracking sheet which shall detail the list of patches that have been installed and the ones that are scheduled. Unapproved patches shall also be listed in Patch Tracking Chart with business justification.

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

5.0DATA BACKUP & RECOVERY POLICY

5.1 POLICY STATEMENT

Management and system admin shall ensure that adequate data backup mechanism is in place to ensure that the data is not lost and can be recovered or restored in the event of an equipment failure, intentional destruction of data, or disaster.

5.1.1 BACKUP PROCESS

- Responsibility for data backup operations shall be assigned by System Admin.
- There shall be a documented backup and recovery procedure to back up the following:
  - Customer information
  - Source codes and executable of Application software
  - Data files of all application software
  - End-user document files like Photoshop, CAD or Microsoft Office documents etc.
  - Electronic mail
  - System software (operating system, RDBMS etc.)
  - Parameter and configuration files of networks and network devices, if applicable
  - System documentation likes user manuals, technical manuals etc.
- Backup scheduling shall be done to ensure that all critical data is backed up without affecting system operations. Preferably Backup shall be scheduled during non-peak hours
- In case of the data exceeding the daily back up limits, appropriate type of backups like full, incremental or differential shall be scheduled and taken.
- Type and frequency of backup and type of backup media to be used shall be decided by the data owner in consultation with system admin taking into consideration the following parameters.
  - Volume of data
  - Criticality of data
  - Recovery time constraints
- Data shall be retained for the period necessary to satisfy both business and legislative requirements. Data owners shall assign the retention period for essential business data and establish any requirement for archive copies to be permanently retained.
- All backup media shall be properly labelled for identification and information classification. From the labelling it shall be possible to identify the following:
  - Server Hostname/IP address
  - Application Name
  - Date of Backup

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

- Type of Backup
- Media Expiry date
- Location Name
- Classification level

- A backup register shall be maintained by system administrator to track the backup and recovery operations
- The recovery register shall have following details:
  - Application name
  - Backup administrator name and User ID
  - Date of testing
  - Status
  - Comments

5.1.2 SECURITY OF BACKUP MEDIA

- Data on backup media shall be secured against unauthorized access.
- Backup media shall be secured against environmental and physical threats.
- Backup media shall be stored in a fire resistant safe.
- Access to the fire resistant safe containing the backup media shall be restricted.
- Environmental conditions like dust, humidity, fire etc. shall be considered while selecting media storage room.
- Backup media shall not be exposed to direct sunlight or other heat radiating sources.
- Backup media shall be securely disposed.
- Backup media shall be disposed under the following conditions:
  - Media life has expired
  - Media is damaged, and data is not accessible

5.1.3 RECOVERY TESTING

- Recovery testing shall be done periodically to ensure the integrity of data being backed up and good health of backup tapes or media.
- Frequency of recovery testing shall be determined by management & system administrator.
- Frequency of recovery testing can be determined based on the following:
  - Criticality of the application
  - Existing Redundancy in place

H. D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

6.0TECHNICAL VULNERABILITY MANAGEMENT POLICY

6.1 POLICY STATEMENT

Management and system admin shall ensure that the assets are regularly verified for the vulnerabilities from the Information Security team. Adequate actions would be taken to mitigate the identified vulnerabilities.

6.1.1 CONTROL OF TECHNICAL VULNERABILITIES

Application and operating system vendors operate notification schemes which publish detailed information about any known vulnerabilities including regular updates and, normally, criticality ratings. The following points should be considered by HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED for inclusion within the vulnerability management process:

- Roles and responsibilities for the process should be defined, including; monitoring, risk assessment, patching, asset tracking and coordination,
- Sources of notifications should be identified for all HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED's critical assets,
- Risk assessment of each relevant patch should have carried out to compare the risk of installing it against the risk of not doing so,
- Patches should be tested to ensure they are effective and do not adversely affect other system components,
- If a vulnerability is discovered and no patch is available other mitigating controls should be considered, including:
  - disabling services or capabilities related to the vulnerability,
  - adapting or adding compensating controls elsewhere i.e. disabling a port at a firewall or blocking a protocol,
  - increasing monitoring to detect and react to any attempted exploit,
  - raising awareness of the vulnerability to any potentially impacted users,
- Any high risk or particularly sensitive systems should be prioritized within the process.
- In case of vulnerabilities discovered in off-the-shelf products (used for core business) or applications provided by exchange empanelled vendors, HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED Equities shall report them to the exchanges and Regulatory bodies like SEBI in a timely manner.

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

7.0 CRYPTOGRAPHIC AND ENCRYPTION POLICY

7.1 POLICY STATEMENT

- Encryption shall be used wherever it is required to protect confidentiality, integrity and authenticity of the information, data and message.
- The encryption techniques shall identify agreed and applied before implementing them in the organization.
- The algorithms used shall be suitable for the business processes they are supporting.
- The key length shall be at least 128 bits. The length shall be appropriate for the security requirements of information that will be protected, and the solutions implemented shall be consistent throughout the organization.

7.1.1 RESPONSIBILITY

- The responsibility for deciding cryptographic keys and the management of keys lies with the respective Application owners.
- The responsibility for implementing the required encryption or cryptographic techniques lies with the Application, Network and Database Managers
- The responsibility for securing the individual keys lies with the relevant managers. However, they shall hand them over before going on leave or leaving the organization

7.1.2 USE OF CERTIFICATES

- Digital certificates shall be used in transactions where there is need for authentication, non-repudiation and encryption.
- Certificates can be issued by HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED' internal Certificate Authority or by an external party.

7.1.3 KEY MANAGEMENT GUIDELINES

- The key management system shall provide protection of the cryptographic keys according to their use, the management methods that support the handling and use of keys as required by the business processes for which these controls will be used.
- The requirements for key management shall be different depending on which cryptographic technique, secret or public key technique will be used and what type of key, public, private is considered.
- The protection of secret and private cryptographic keys is different from the protection necessary for the public keys. When defining a key management system, these protection

H. D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

requirements shall be analysed and appropriate protection shall be in place before the keys are generated and used.

7.1.4 CERTIFYING AUTHORITY KEY MANAGEMENT

- If HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED sets up an internal CA, the system shall be installed in secure location and the private keys shall be protected from unauthorized access.
- There shall be a secure backup of CA private keys.

7.1.5 KEY USAGE PERIODS

- All certificates shall have pre-defined validity periods.
- Certificate renewal shall be processed as per new certificate generation guidelines.

7.1.6 KEY COMPROMISE

- If the CA private key has been compromised all subscriber certificates shall be revoked.
- If a subscriber private key is compromised CA shall immediately revoke the certificate.

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

8.0APPLICATION DEVELOPMENT AND SECURITY POLICY

8.1 POLICY STATEMENTS – SYSTEMS DEVELOPMENT LIFE CYCLE (SDLC)

Security shall be considered and included in all phases of the SDLC process namely Initiation / Requirement, Acquisition / Development, Testing, Implementation, Operations/Maintenance and Disposal. Depending upon the size and complexity of the project, phases may be combined or may overlap.

To ensure the segregation of roles involved in application development, testing and production, there may be three separate environments.

8.1.1 INITIATION / REQUIREMENT PHASE

- The business (the requesting department) is expected to provide the approved Business Requirements. All requirements need to be measurable and testable and relate to the business need.
- A risk analysis shall be performed to determine the threats associated and the corresponding security and quality controls required for the requested system or system application under development.
- It shall be ensured that there is a balance between user requirements and Security & Quality controls.
- Specifications for the new system shall be documented to provide the development group with specific requirements. This enables HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED in identifying, reviewing and testing the security functionalities of the system or software.

8.1.2 ACQUISITION/ DEVELOPMENT PHASE

- The following points shall be considered at a minimum while preparing the detailed requirements for the system application:
    - Impact on existing systems
    - Security vulnerabilities involved when connecting with other systems and applications
    - Operating environment security
    - Cost of providing security to the system over its life cycle (includes hardware, software, personnel and training)
- While purchasing a system or software, the security requirements shall be specified in the Request for Proposal and the selection criteria shall be based on secure functionality.
- There shall be a separation between the operational, test and development facilities.

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

- Application controls shall be designed into all application systems to prevent loss, modification or misuse of user data. These controls shall include:
    - Validation of input data
    - Control of internal processing
    - Message Integrity
    - Validation of output data
- Where software development is outsourced, the following points shall be considered:
    - Licensing arrangements, code ownership and intellectual property rights
    - Certification of the quality and accuracy of the work carried out
    - Escrow arrangements in the event of failure of the third party
    - Rights of access for audit of the quality and accuracy of work done
    - Contractual requirements for quality of code
    - Testing before installation to detect backdoors or Trojan code
    - Meeting compliance regulations

8.1.3 TRAININGS AND MANUALS

- Manual: The updated system manual should be available for both users and technical team to use and/or support the system effectively.
- Training: The business/functional trainings to be provided for business users, UAT In-charge, Application Support and Technical training to be provided for other peers-in-Development, Application Support, and Technical Support/Operation, etc., for managing and supporting the system

8.1.4 TESTING PHASE

- All modifications, enhancements and installation of new systems shall be subject to testing for sanity, capacity, peak load, etc.
- The appropriate users shall do design testing and unit testing on the new systems prior to installation into the production environment.
    - Test Cases & Unit Test: The developers should prepare the test cases and do the adequate unit tests of their work before placing the work to the team leader
    - System Integration Test: The team leader should review/update test cases and test to ensure various components of the system are integrated and functioning as per the functional requirements.
- User Acceptance Testing

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

- During User Acceptance Test, actual business user shall test the system to ensure that the business requirements, are satisfied by the developed or modified system
- The implementation of operating systems, patches/upgrades, or standards systems in which there were no-customizations, however, must undergo compatibility check or certification to ensure that the production environment shall not be disturbed.

8.1.5 IMPLEMENTATION PHASE

Before the implementation of any new system, a security procedure document shall be prepared for the new system. It should contain hardware specification, prerequisites, implementation steps for client, server (UNIX, Windows, etc.), database, proposed system architecture showing interaction with other subsystems and data flow, application server, etc.

- For software packages, system default settings shall be reviewed prior to installation to determine potential security holes.
- The system or system modifications shall be installed and made operational in a production environment using approved 'Implementation Specification'. The phase is initiated after the system has been successfully tested and accepted by the user and concerned parties during User Acceptance Phase.
- Different implementation approach such as Pilot, Soft Live, Parallel Run or Complete Live shall be selected depending on the project nature and complexity. The approach shall be approved by Section Head – Business Applications, Head of Information Security.
- The project manager shall arrange the handing over the system to 'Application Support' and hands over the details required for application support team required to carry out the support.

8.1.6 OPERATIONS/MAINTENANCE PHASE

- HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED IT Department shall maintain the system and perform identified IT Operations activities.
- The system shall be monitored by the users for continued performance in accordance with user requirements. The users shall record issue/problems and system modifications to the IT Department.
- All requisite procedures for operational tasks shall be documented. Access to this documentation shall be restricted.
- All changes to the system shall be carried out in line with the Change Management Procedure.
- Libraries containing application source code, production executable, and systems audit tools shall be secured from unauthorized access.

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

- The development staff shall not have access to operational systems. For occasional and essential support purposes, the development staff may be granted special access for a limited period.
- An audit log shall be maintained of all updates to operational systems and system applications.

8.2 POLICY STATEMENTS – APPLICATION SECURITY

Applications deployed in HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED IT Department shall have controls for secure input, processing, storage, and output of data. Applications must be tested for security and performance before deployment and shall be managed for high availability.

8.2.1 APPLICATION ACCESS

- Application shall have authentication and authorization controls.
    - Application shall authenticate all users before allowing access
    - Application shall have the provision for allocating access rights based on the principle of least privilege
    - Role based access controls shall be defined. The access level shall be documented by the Senior Business Analyst in coordination with Head of Business Applications
    - The application shall restrict menu options based on a need to know and need to do basis
    - Access shall be granted only after adequate authorization by the application owner
- All applications enabling business transactions shall facilitate maker and checker role.
- No individual irrespective of his/her grade, title or function shall be allowed to complete a transaction involving sensitive, valuable, or critical information from initiation to the final authorization.
- Applications shall not allow end-users to invoke operating system level commands through the application interface.
- Application shall use secure channel for transmission of sensitive user credentials and financial information.
- SSL shall be configured to ensure that all sensitive information is encrypted and sent from client to server.
- For web-based applications, application shall redirect the login credentials to another page for authentication purposes.

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

8.2.2 DATA SECURITY

- Sensitive data including application user login credentials shall be stored in secure manner.
- User login passwords shall be stored in an encrypted format. The user passwords shall be stored in such a way that it is not retrievable even by system administrators / application developer.
- Application shall have facility to check the integrity of the data.
- Application owner shall define the retention period for all data handled by the application.
    - This shall be done after considering relevant statutory and regulatory requirements
    - Retention period is required for determining the backup media rotation cycle and for deciding on erasing old data for creating free disk space

8.2.3 INPUT CONTROLS

- All user inputs shall be checked by the application to ensure it is both appropriate and expected:
    - Application shall have additional controls to identify duplicate transaction records
    - The application shall have adequate controls to ensure that, data has been accurately input e.g., range checks, validity checks, missing or incomplete data

8.2.4 PROCESSING CONTROLS

- The application shall ensure processes cannot be initiated out of sequence.
- Application shall ensure that all tasks associated with a process are completed and cannot be manipulated or bypassed.
- The application shall have built-in checks to ensure that if there are any pre-requisites for executing a process, these are met before initiating the same.

8.2.5 PERFORMANCE TESTING

- Head of Applications shall ensure that application is tested for peak load conditions before deployment.
- For all multi-user applications, the load testing needs to be done in environments which simulate real life conditions.

8.2.6 SECURITY TESTING

- Head of Application along with Head of Information Security shall ensure that application code review and security testing is carried out at least annually.
- Web user access restricted to the front-end web servers only. Also, it shall be reviewed for:

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

- Protection against common vulnerabilities (such as Parameter Manipulation, SQL Injection, Command Injection, Cross Site Scripting, Directory Traversal, Buffer Overflow, Cookie Snooping, Authentication Hijacking, Log Tampering, Attack Obfuscation, Error message Interception, Denial of Service, etc.)
- Web applications shall be secured against the key vulnerabilities that have been identified in latest OWASP (Open Web Application Security Project) standards.
- Internet facing application shall be subjected to external penetration testing / vulnerability assessment by a qualified Cert-In empanelled auditor
- The application system shall have Multi-tier Architecture

- HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED Equities shall ensure that off the shelf products being used for core business functionality (such as Back-office applications) should bear Indian Common criteria certification of Evaluation Assurance Level 4.
  - The Common criteria certification in India is being provided by (STQC) Standardisation Testing and Quality Certification (Ministry of Electronics and Information Technology).

8.2.7 RESTRICTIONS ON CHANGES TO SOFTWARE PACKAGES

- Vendor/OEM supplied software packages shall be used without modification as far as possible.
- Vendor shall not have any access to production environment.
- If it is necessary to make changes in the software package, the required changes shall be made with the consent of the vendor.

8.2.8 PROTECTION OF TEST DATA

- Test data shall be selected carefully, protected and controlled.
- The use of operational data containing personally identifiable information or any other confidential information for testing purposes shall be avoided.
- The following guidelines shall be applied to protect operational data, when used for testing purposes:
  - The access control procedures, which apply to operational application systems, should also apply to test application systems
  - There should be separate authorization each time operational information is copied to a test environment
  - Operational information should be erased from a test environment immediately after the testing is complete

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

- The copying and use of operational information should be logged to provide an audit trail
- All the test data should be cleaned from the database and applicable folders, and configuration files.

8.2.9 AUDIT LOGS & MONITORING

- The application shall have the facility to log all transactions and security related events. including the following:
  - User account management
  - User privilege changes
  - User login/logout time
  - Changes in application configuration
  - Authentication failures
- Auditing mechanism deployed shall have tamper proof, continuous logging systems. The logs shall be available in "Read Only" mode only to authorized user.

8.2.10 ERROR HANDLING

- The error messages generated by the application shall not disclose any information related to installed packages, OS, Databases and / or security setup.
- The error shall not reveal information to the end user of what the correct input might be.
- Custom error messages shall be used by modifying the default error messages.

8.2.11 FIREWALL

- All critical multi-user applications shall be placed behind a firewall to adequately segregate access from internal and external users.
- IT Managers shall review any request for Firewall rule base change pertaining to the applications (IP addresses, ports and users) and Head of Information Security shall approve the request.
- Access to the system audit tool, which is used to test the applications, shall be restricted.

8.2.12 VENDOR DECLARATIONS

- The vendor shall agree on (by declarations/acceptance or contract)
  - Not to violate any Intellectual Property Rights, licensing rights, etc. while producing the system and subsequently providing it to HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED IT Department.

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

- Must agree to provide fix for all the concerns raised and elimination of existing vulnerabilities before launching on the internet.
- Not to deploy techniques to covertly gather information about individuals at the time of access authentication.
- Installation according to best practices such as remove unnecessary services, files or programs, disable anonymous user account, according to business needs of HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED Technologies.
- Protection against source code vulnerabilities for the system such as hard coded passwords, time/events triggers, loops, trap doors, etc.

8.2.13 DOCUMENTATION

- Application owner shall ensure that detailed documentation is available for the following activities:
  - Application installation
  - Configuration Settings
  - Privilege levels and associated roles
  - User procedures
  - Backup and recovery procedure
  - Data retention period
- All settings mentioned in the secure configuration document shall be incorporated in the application documentation.
- Adequate backups of all documentation shall be maintained.
- Every new system/application shall have the step by step user manual for better understanding and navigation of the system

H. D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

9.0 USER AWARENESS AND TRAINING POLICY

9.1 POLICY STATEMENTS

9.1.1 GENERAL STATEMENTS

- HR department in coordination with Head of Information Technology shall ensure that information security awareness programs are conducted as a part of employee induction training apart from general orientation for every new staff joining HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED.
- HR department shall ensure that relevant awareness, training and education programs are conducted on a continuous basis to raise and maintain the employee awareness with regards to information security.
- The information security awareness, training & education programs are:
  - Useful to counter threats through a basic knowledge of IT security principles
  - Useful to make staff capable of performing their IT security-related tasks effectively and efficiently
- The information security awareness, training & education programs shall aim at achieving the following:
  - Improve awareness across staff on the need for information security
  - Develop skills to perform jobs in a secured manner
  - Build in-depth knowledge to maintain and improve IT security of HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED
  - Enable HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED staff and third-party users to adhere to Acceptable Usage Policy
  - Educate HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED staff and third-party users about the disciplinary action if user actions found not complying with the HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED IT Security Policies.
- This training shall include subject areas like organizational security requirements, organizational security policies and procedures, security threats and concerns, legal responsibilities and business controls, as well as correct use of information processing facilities.
- Head of Information Technology shall periodically review the security awareness program to verify that it provides awareness to all personnel about the importance of data security.
- HR department in coordination with Head of Information shall ensure:

H. D. MEHTA SR. & ST. BR. PVT. LTD. MUMBAI

- Relevant awareness materials are developed in compliance with the information security policies, procedures and standards of HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED.
- Evaluate existing levels of employee knowledge with regards to information security issues and identify areas of improvement based on business needs.
- Obtain employee training feedback so that the awareness, training, and education program can be further enhanced.

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

10.0 TELEWORKING POLICY

10.1 POLICY STATEMENT

All access to the network from mobile computing devices shall be authorized and provided in a secure manner only. Policy also ensures that minimum necessary access rights are provided based on business requirements.

10.1.1 GENERAL STATEMENTS

When using mobile devices, special care shall be taken to ensure that business information is not compromised.

Following parameters shall be considered:

- Registration of mobile devices
- Requirements for physical protection
- Restriction of software/app installation
- Requirements for mobile device software versions and for applying patches
- Restriction of connection to information services
- Access controls
- Cryptographic techniques
- Malware protection
- Remote disabling, erasure or lockout
- Backups
- Acceptable usage of web services and web apps
- Theft of asset

10.1.2 REMOTE ACCESS

- On approval from Management and Security team, authorized staff and non-employees shall be allowed to remotely access HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED network with minimum necessary access rights while delivering their official duties.
- All remote connections initiated to/from remote / branch networks made to the HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED' network shall be done through the approved secure methods such as IPSec, virtual private network and should not be initiated from open or non-trusted public Wi-Fi networks.
- Strong authentication mechanism, such as two factor authentications, shall be used while remotely accessing information.

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

- Sharing of login credentials for Remote Access shall be strictly prohibited among HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED staff and non-employees.
- All user activities through remote access shall be monitored for any malicious activities.
- All hosts connecting to HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED network remotely shall have the anti-virus with latest AV updates, host-based firewall, latest OS and application patches installed.

FOR HARENDRA D. MEHTA SHARE & STOCK BROKER PVT. LTD.

DIRECTOR

Harendra D. Mehta Share & Stock Broker Pvt. Ltd.

MEMBER > NSE Equity Segment > BSE Equity Segment

Stock Exchange Rotunda Building, PG -12, Ground Floor, Mumbai Samachar Marg, Mumbai - 400 001.

Phone : 2272 2392 / 2272 2190 / 2272 2546 / 2272 2548 • E-mail : bhm264@gmail.com

CIN : U67120MH1997PTC110950 • GSTIN : 27AAACH2890J1ZE

BYOD POLICY

HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED

15-04-2024

Author:	BAIJU HARENDRA MEHTA (DIRECTOR)
Owner:	BAIJU HARENDRA MEHTA
Organization:	HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED
Version No:	1.0
Date:	15-04-2024

Document Control

Document Title **BYOD Policy**

Version History

Version No.	Version Date	Author	Summary of Changes
1.0	15-04-2024	BAIJU HARENDRA MEHTA	NA

Approvals

Name	Title	Date of Approval	Version No
BAIJU HARENDRA MEHTA	BYOD Policy	15-04-2024	1.0

Distribution

Name	Title	Date of Issue	Version No
NA	NA	NA	NA

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

1.0 BYOD POLICY

1.1 PURPOSE

Many employees and other contractors / vendors of the HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED uses personally owned computing devices to accomplish their work. This policy addresses the rights and obligations of both owners of a device used for official work and the HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED's rights and obligations to protect and secure its data residing on these devices.

1.2 SCOPE

This policy applies to:

- All Staff (Permanent & on contractual basis) and non-employees (contractors, consultants, suppliers, vendors, etc.) of HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED and other individuals, entities or organizations that uses or brings their own devices to accomplish official work

All mobile computing devices (Laptops, Smart phones, Tablets, PDAs etc.) that are used to access HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED network environment

1.3 POLICY STATEMENTS

Company employees and contractors may use their personal electronic devices (e.g., smart phones, tablets) for conducting company business, provided that they understand and agree with the "Bring Your Own Device" (BYOD) policy, have been granted express permission, and act in accordance with the policy.

1.3.1 BACKGROUND

HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED management fully understands that Bring Your Own Device (BYOD) program is associated with a few information securities risks such as:

- Loss, disclosure or corruption of corporate data on Personally Owned Devices (PODs)
- Incidents involving threats to, or compromise of, the HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED network infrastructure and other information assets (e.g. malware infection or hacking)
- Non-compliance with applicable laws, regulations and obligations (e.g. privacy or piracy)

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

1.3.2 GENERAL STATEMENTS

- Due to HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED management's concerns about information security risks associated with BYOD, individuals who wish to opt-in to BYOD must be first authorized by Technology Officer and must explicitly accept the requirements laid out in this policy beforehand.
- HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED Management reserves the right not to authorize individuals, or to withdraw the authorization, if they deem BYOD program is not appropriate for them and in the best interests of the organization.
- The HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED shall continue to provide its choice of fully owned and managed mobile computing devices (Laptops or smartphones) as necessary for work purposes, so there is no compulsion for anyone to opt-in to BYOD if they choose not to participate in the scheme.
- The HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED and the owners and users of Personally Owned Devices (POD) share responsibility for information security.
- Personally, Owned Devices must not be used to create, modify, store or communicate corporate data without prior approval.
- Personally, Owned Devices (POD) must use appropriate forms of device authentication approved by Technology Officer, such as digital certificates created for each specific device. Digital certificates must not be copied to or transferred between PODs.
- BYOD users must use appropriate forms of user authentication approved by Technology Officer, such as user IDs, passwords and authentication devices.
- The following classes or types of corporate data are not suitable for BYOD and are not permitted on PODs:
    - Anything classified as Confidential or above (Restricted)
    - Other currently unclassified but highly valuable or sensitive corporate information which is likely to be classified as Confidential or above
    - Large quantities of corporate data on single device (i.e. greater than 1 GB in aggregate on any one POD or storage device).

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

- The HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED has the right to control its information. This includes the right to backup, retrieve, modify, determine access and/or delete corporate data without reference to the owner or user of the POD.
- The HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED has the right to seize and forensically examine any POD believed to contain, or to have contained, corporate data where necessary for investigatory or control purposes.
- Suitable antivirus software approved by Technology Officer must be properly installed and running on all PODs.
- POD users must ensure that valuable corporate data created or modified on PODs are backed up regularly, preferably by connecting to the corporate network and synchronizing the data between POD and a network drive, otherwise on removable media stored securely.
- Any POD used to access, store or process sensitive information must encrypt data transferred over the network (e.g. using SSL or a VPN) and while stored on the POD or on separate storage media, whatever storage technology is used (e.g. hard disk, solid-state disk, CD/DVD, USB/flash memory stick, floppy disk etc.).
- Owners should report theft or lose of POD or mobile devices to Technology Officer or IT Service Desk

1.3.3 RESPONSIBILITIES

- While HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED users (employees / non-employees) have a reasonable expectation of privacy over their personal information on their own equipment, the organization's right to control its data and manage PODs may occasionally result in support personnel unintentionally gaining access to their personal information. To reduce the possibility of such disclosure, POD users are advised to keep their personal data separate from business data on the POD in separate directories, clearly named (e.g. "Private" or "BYOD").
- It is responsible for issuing digital certificates to authenticate authorized PODs, and for monitoring network security for unauthorized access, inappropriate network traffic etc.
- Technology Officer is responsible for managing the security of corporate data and configuring security on authorized PODs.

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

- IT Help/Service Desk is responsible for providing limited support for BYOD on PODs on a 'best endeavors' basis for work-related issues only. Information security incidents affecting PODs used for BYOD should be reported promptly to IT Help/Service Desk in the normal way.

FOR HARENDRA D. MEHTA SHARE & STOCK BROKER PVT. LTD.

DIRECTOR

Harendra D. Mehta Share & Stock Broker Pvt. Ltd.

MEMBER ➤ NSE Equity Segment ➤ BSE Equity Segment

Stock Exchange Rotunda Building, PG -12, Ground Floor, Mumbai Samachar Marg, Mumbai - 400 001.

Phone : 2272 2392 / 2272 2190 / 2272 2546 / 2272 2548 • E-mail : bhm264@gmail.com

CIN : U67120MH1997PTC110950 • **GSTIN :** 27AAACH2890J1ZE

BUSINESS CONTINUITY POLICY

HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED

15-04-2024

Author:	BAIJU HARENDRA MEHTA (DIRECTOR)
Owner:	BAIJU HARENDRA MEHTA
Organization:	HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED
Version No:	1.0
Date:	15-04-2024

Document Control

Document Title **Business Continuity Policy**

Version History

Version No.	Version Date	Author	Summary of Changes
1.0	15-04-2024	BAIJU HARENDRA MEHTA	NA

Approvals

Name	Title	Date of Approval	Version No
BAIJU HARENDRA MEHTA	Business Continuity Policy	15-04-2024	1.0

Distribution

Name	Title	Date of Issue	Version No
NA	NA	NA	NA

H. D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

BUSINESS CONTINUTY POLICY

1.1. PURPOSE

The purpose of this BCM policy is to:

- State the senior management commitment to Business Continuity at HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED.
- Define the overall approach to the development, implementation, testing and maintenance of a Business Continuity Management program.
- Provide direction for management to prepare company-wide business continuity plans and pre-position personnel and resources to mitigate the effect of a business interruption.
- Develop business continuity management programs to support HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED business objectives and continued delivery of essential services during a business interruption.
- Protect critical HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED infrastructure and assets necessary to sustain business continuity.
- Establish HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED wide guidelines for the identification, analysis and treatment of potential business continuity risks to HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED services, programs or operations.
- Continuously promote HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED wide business continuity practices, training and awareness for employees.

1.2. SCOPE

- All staff (permanent and on contractual basis) and non-employees (interns, contractors, vendors, suppliers and consultants) and other individuals, entities or organizations responsible for administering and maintaining Information processing systems.
- All Information assets involving data, applications, network, security devices, servers and other IT system.

1.3. POLICY STATEMENT

Ensuring the continuity of our services is essential to uphold the interests of key stakeholders, reputation, brand and value creating activities.

1.3.1 GENERAL STATEMENTS

BCM plays a vital role in achieving this vision by ensuring the right framework is in place to:

- Protect our people, systems and infrastructure
- Identify and mitigate risks to an acceptable level
- Manage any disruption to minimize its impact

HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED Business Continuity Management Policy requires:

- Human safety to be our first priority under all circumstances.

H.O. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

- Senior Management to own the management of key risks to the continuity of the HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED operations.
- Development of appropriate plans and procedures that enable us to continue to provide our customers with required services or products, within an agreed time frame
- Heads of business units and support functions to own the management of key risks to their respective functions, and to develop, review and rehearse their own continuity plans at least annually.

1.3.2 BCM LIFECYCLE

The BCM lifecycle shall include the following stages:

Business Impact Analysis

- A comprehensive Business Impact Analysis must be conducted to evaluate the impact of an interruption in terms of damage scale and recovery period.
- The Business Impact Analysis must consider financial, operational, reputational impact of an interruption along with risks arising out of non-compliance with legal, contractual, or regulatory requirements.
- Business Impact Analysis must also include identification of potential risks and threats to critical business activities both internally and from the external environment.

Business Continuity Plans

- Business Continuity plans must be developed and implemented to mitigate the impact of a disruption on critical processes identified through Business Impact Analysis.
- Disaster Recovery procedures must be developed to quickly recover and restore business operations in the required time scales following interruption to, or failure of, critical business processes.

Testing

- Business Continuity plans must be tested at least annually to identify incorrect assumptions, oversights, or changes in people, processes, or technology.
- Test results should be used to revise the plans.
- Observations noted during tests should be remediated and tracked until closure.

Review

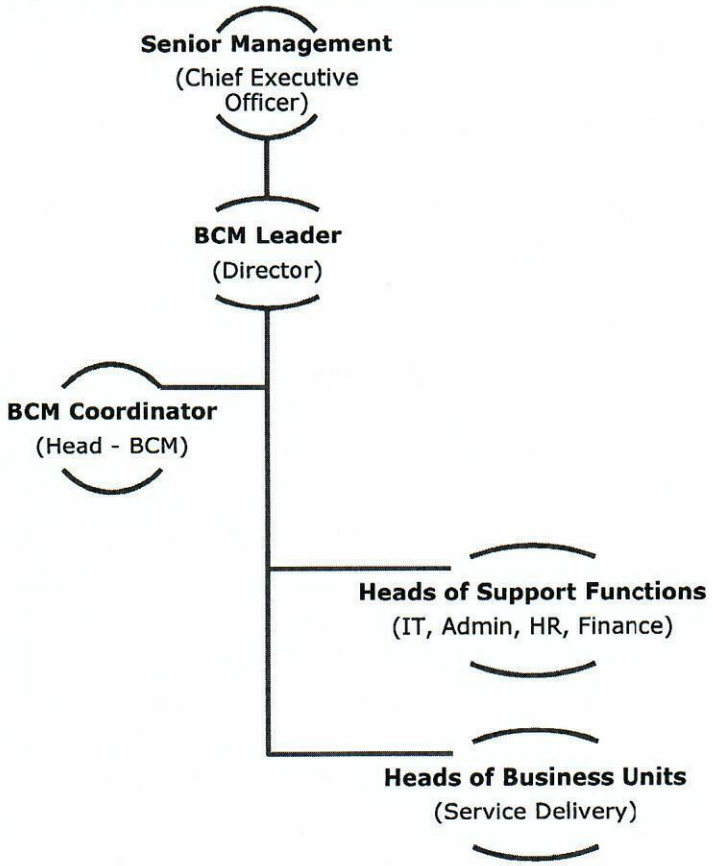
- Business Impact Analysis and Business Continuity plans must be reviewed at least annually and kept always updated.
- An interim review of Business Impact Analysis and Business Continuity plans should be undertaken whenever any of the following occurs:
  - Significant changes in the internal business process, systems, or infrastructure
  - Significant changes in the external business environment – such as market or regulatory change.

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

1.3.3 ORGANIZATION STRUCTURE

Governance Model

- Senior Management shall delegate executive responsibilities to the BCM committee.
- The BCM Committee is a core group comprised of representative from cross-functional areas covering key business units and support functions.
- The BCM Leader will lead activities of the BCM Committee.
- Each member within the BCM organization structure should have a nominated backup/alternate who can execute responsibilities in his absence.



1.3.4 ROLES AND RESPONSIBILITIES

Senior Management

- Assume responsibility for overall direction and coordination of BCM.
- Ensure that appropriate resources are provided to implement this Policy, and to ensure that it is properly communicated and understood throughout the organization.
- Establish communication with external stakeholders (investors, clients, media, etc.) during an emergency.
- Appoint the BCM Leader who will have the authority to take executive decisions before, during or after a disaster.
- Resolve any issues escalated from the BCM Committee.

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

BCM Leader

- Assume executive responsibilities for HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED BCM program.
- Report and be accountable to the Senior Management for effective management of the BCM program.
- Chair and supervise the activities of the BCM Committee.
- Trigger initiation of recovery procedures during an emergency/disaster scenario.
- Establish communication with internal stakeholders (employees, contractors, third-parties, etc.) during an emergency situation.
- Appoint other members of the BCM Committee.

BCM Committee

- Convene regularly to review the status of the BCM program.
- Ensure appropriate continuity plans are developed, implemented, and rehearsed across all operational teams, support functions, service partners and suppliers.
- Verify that essential business processes can be restored within required timescales by use of such plans.
- Focus on specific key corporate threats as appropriate (e.g. industrial action, pandemic).
- Review and evaluate the implications incidents and near misses on existing plans.
- Ensure appropriate communication and escalation arrangements are in place to ensure staff can be contacted in an emergency.
- Take part in BCM training and workshops.

BCM Coordinator

- Conduct business impact analysis and business continuity risk assessments.
- Lead and manage disaster-assessment efforts.
- Lead and coordinate the development of corporate and functional business continuity plans.
- Lead efforts to conduct review and audit of BCP at least once annually.
- Coordinate activities of the BCM Committee during a disaster scenario.
- Organize periodic trainings and workshops for the BCM Committee.

Heads of Business Units and Support Functions

- Represent their function on the BCM Committee.
- Support the BCM Committee by providing tactical response to an emergency or disaster.
- Identify and prioritize the critical business processes within their functions by performing a business impact analysis.
- Develop, review, test and maintain Business Continuity plans and procedures specific to their team.
- Identify and raise to the BCM Committee any continuity-related issues affecting their business units / functions.
- Ensure all employees in their team are aware of their individual responsibilities – and are trained and rehearsed to discharge them.

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

1.3.5 BCM PROCESS

The process includes the following stages:

- Form a Business Continuity Management Division & BCM Champions, working group & HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED Management Team.
- A Business Impact Analysis has already been conducted to ascertain the effects of a loss of product and services review its scope, assumptions, and findings.
- This recommendation will enable HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED Management team to set priority & finalize scope.
- Document the rationale behind excluding products, services, and locations from BCM.
- Provide HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED Management Team with the evaluation report to choose options.
- If Business Continuity is the chosen approach for a particular product or service, then it is necessary that suitable measures are put in place to ensure that the various activities supporting their delivery can be continued or recovered within the required timescales.
- For those products and services that are deemed out of scope, the business risk of loss or non-availability is not mitigated by HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED BCM. The choices available to HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED Management are:
    - **Acceptance** – accept that it is at risk of being disrupted
    - **Transfer** – transfer the risk of disruption to a third party
    - **Change, suspend or terminate** the product or service

Business Continuity management involves the following basic steps:

- Prioritising the businesses to be recovered by conducting a Business Impact Analysis (BIA)
- Performing a Risk Assessment (aka Risk Analysis) for each of the HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED Services to identify the assets, threats, vulnerabilities, and countermeasures for each service.
- Evaluating the options for recovery
- Producing the Contingency Plan
- Testing, reviewing, and revising the plan on a regular basis

Information security aspects of business continuity management

HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED Business Continuity Policy is based on its business needs and external requirements are established, documented, and periodically reviewed. HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED Business Continuity policy and associated controls shall take account of:

- Security issues for particular data systems, given business needs, anticipated threats and vulnerabilities
- All relevant legislative, regulatory and certificatory requirements
- Relevant contractual obligations or service level agreements
- other organizational policies for information access, use and disclosure
- consistency among such policies across HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED systems and networks

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

A managed process should be developed and maintained for business continuity throughout HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED that includes information security requirements needed for HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED business continuity.

These security considerations should be integrated with the testing of business continuity plan implementations.

Control includes:

- Identification of information assets involved in critical business processes
- A risk assessment that addresses likely causes and consequences of information system failures
- Identification and consideration of preventive and mitigating controls in light of these risks
- Identification of sufficient financial, technical, and human resources to address the preventive/mitigating control requirements
- Development and documentation of business continuity plans and processes, including assignment of responsibilities and incorporation into HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED general processes and structure
- Regular testing and updating of business continuity plans and processes

Business continuity and risk assessment

The objective of this control is to ensure that Events that can cause interruptions to HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED business processes shall be identified, along with the probability and impact of such interruptions and their consequences for information security.

Strategies should consider the different risk environment and the degree of risk mitigation necessary to protect the institution in the event the continuity plans must be implemented.

Control includes:

- Identification of all significant risk or risk categories, including the probability and probable impact on operations in terms of scale, likely damage, and recovery period
- Full involvement of owners of significant organizational assets in the assessment process
- Identification of acceptable and unacceptable losses and interruptions
- Formal documentation of the assessment's results, and a plan for regular updating to ensure completeness and currency

Developing and implementing continuity plans including information security

The objective of this control is to ensure business continuity plans should be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time, following interruptions to or failures of HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED business processes.

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

Control includes:

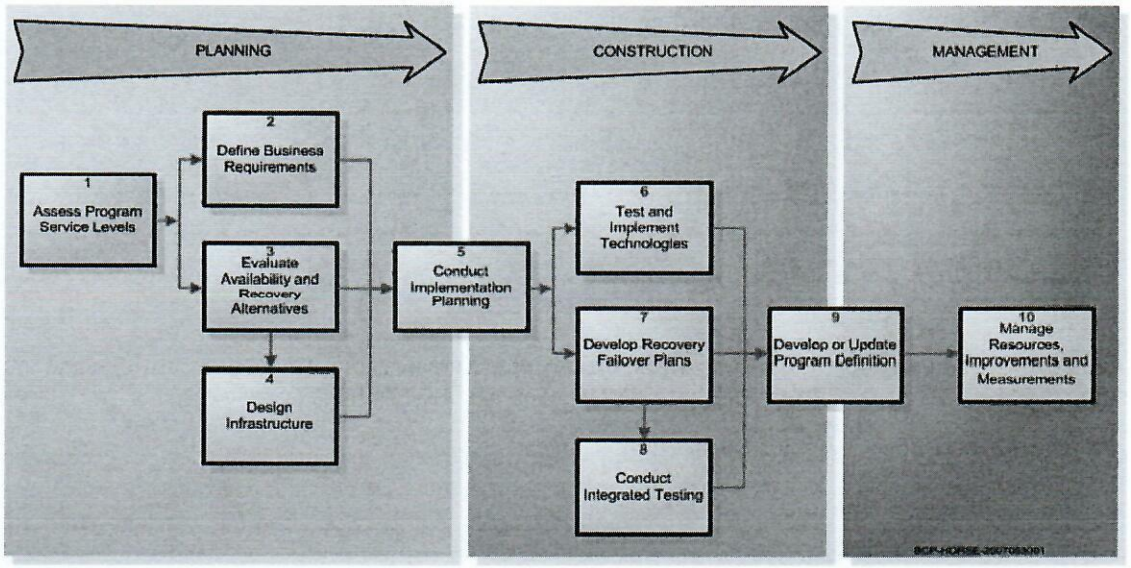
- Identification and agreement on all responsibilities and operational procedures
- Specification of the disaster recovery/business continuity procedures to effect recovery and restoration of business processes
- A data backup plan to ensure recovery of all data following process restoration, including the ability to replicate exact copies of data in its state prior to disruption of operations
- Specification of alternative operational procedures to follow pending completion of recovery and restoration, including methods for accessing all critical data
- Documentation of the above plan elements
- Appropriate education and awareness efforts for staff on the plan element
- Testing and updating of the plan

Business continuity planning framework

The objective of this control is to ensure a single framework of business continuity plans should be maintained at HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED to ensure that all plans are consistent, assess information security requirements, and to identify priorities for testing and maintenance.

Control includes:

- Specification of conditions and criteria for activating the plan
- Formal assignment of responsibilities for making assessments about plan activation, choices among emergency procedures and processes, resumption procedures, etc.
- Make informed choices that reveal the right cost benefit trade-offs for your business continuity program. Always analyse availability and recovery alternatives, recommend a business continuity strategy that meets the defined business requirements, and provide technical solutions identifying high level cost and benefits for each alternative.
- This diagram illustrates the basic decision process flow to successfully accomplish HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED business continuity program requirements.



H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

Testing, Maintaining and Re-assessing Business Continuity Plans

The objective of this control is to ensure that HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED business continuity plans shall be tested and updated regularly to ensure that they are up to date and effective.

Control includes:

- Testing that assures that all persons with significant responsibilities under the plan(s) are aware of and competent to perform them.
- A range and frequency of testing exercises, from table-top to complete rehearsals, performed as necessary to ensure awareness and competence
- Regular reviews and updating of the plan(s) considering testing results

FOR HARENDRA D. MEHTA SHARE & STOCK BROKER PVT. LTD.

DIRECTOR

Harendra D. Mehta Share & Stock Broker Pvt. Ltd.

MEMBER ➤ NSE Equity Segment ➤ BSE Equity Segment

Stock Exchange Rotunda Building, PG -12, Ground Floor, Mumbai Samachar Marg, Mumbai - 400 001.

Phone : 2272 2392 / 2272 2190 / 2272 2546 / 2272 2548 • E-mail : bhm264@gmail.com

CIN : U67120MH1997PTC110950 • **GSTIN :** 27AAACH2890J1ZE

BASELINING PROCEDURE DOCUMENT

HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED

15-04-2024

Author:	BAIJU HARENDRA MEHTA (DIRECTOR)
Owner:	BAIJU HARENDRA MEHTA
Organization:	HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED
Version No:	1.0
Date:	15-04-2024

Document Control

Document Title **Baselining Procedure Policy**

Version History

Version No.	Version Date	Author	Summary of Changes
1.0	15-04-2024	BAIJU HARENDRA MEHTA	NA

Approvals

Name	Title	Date of Approval	Version No
BAIJU HARENDRA MEHTA	Base-lining Procedure Document	15-04-2024	1.0

Distribution

Name	Title	Date of Issue	Version No
NA	NA	NA	NA

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

BASELINE PROCEDURE DOCUMENT

PURPOSE OF POLICY

Company assets should be hardened and configured securely. Systems should be configured with reference to CIS or NIST benchmarks. This document will cover assets like Windows, Linux and other devices.

SCOPE OF POLICY

This policy applies to:

- All the company assets like Servers, Desktop, Network Devices in the organization.

BASE LINING PROCESS – WIDOWS SYSTEMS

- Software Installation
  - HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED maintains list of approved software.
  - New software installation should follow appropriate change management process along with all necessary business approvals.
  - System Administrator should review installed software on all desktop, laptops and servers at frequency of 6 months.
  - All unnecessary software should be removed from desktops, laptops and servers.
- Disable or Remove Unnecessary User-names
  - Default user accounts should be disabled.
  - If default user account is required to be used, user-name should be renamed.
  - Only necessary user should be part of Administrator group
- Strong Password Policy
  - Strong password policy should be followed for all user accounts:
    - Enforce Password History – 5 Passwords
    - Maximum Password Age – 60 Days
    - Minimum Password Age – 2 Days
    - Minimum Password Length – 8 Characters
    - Password must require complexity – Enabled
    - Account Lockout Threshold – 5 Invalid Attempts

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

- Disable or Remove Unnecessary Services
    - System Administrator should review all the services running on desktops, laptops and servers at frequency of 6 months.
    - All unnecessary services should be removed from desktops, laptops and servers
    - Run all services with low privilege user
- Install Security Patches
    - Install latest service pack for the server
    - Install all security patches regularly
        - Critical Risk Patch – within week
        - High Risk Patch – within month
        - Medium Risk Patch – within quarter
        - Low Risk Patch – within half year
- Install Anti-Virus and Anti-Malware
    - Install approved anti-virus on the desktop, laptops and servers.
    - Install all latest plugins and signatures released by anti-virus company.
- Auditing & Logging
    - Configure server with correct time zone settings.
    - Ensure that server is synchronized with centralized NTP server.
    - Ensure auditing is enabled and audit logs are pushed to centralized log server.
    - Configure strong permissions on log files
    - Configure Audit Logs as mentioned below:
        - Audit Account Logins Event – Success & Failure
        - Audit Logan Event – Success & Failure
        - Audit Policy Change – Success & Failure
        - Audit Privilege Use – Success & Failure
        - Audit Account Management – Failure
        - Audit Object Access – Failure
        - Audit Process Tracking – Failure
        - Audit System Event – Failure

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

- User Management
  - Shudo privilege should be given to limited users only
- System Access Management
  - Insecure services like telnet, ftp, rlogin, rsh, etc. should be disabled
  - Use secure remote administration protocols like SSH for server console access
  - Disable remote login for root user
- Strong password policy should be enforced
  - Pass Min Length – 8 Characters
  - Pass Max Days – 45 Days
  - Pass Min Days – 7 Days
  - Pass Warn – 14 Days
- Auditing & Logging
  - Enable auditing for all critical activities like user authentication, package installation, user addition, etc.
  - Configure strong permissions on log files
  - Server time should be synchronized with Centralized NTP server
  - Backup should be scheduled for all critical data with centralized log server
- Secure Permissions
  - Configure secure permissions on critical system files like password, shadow and group
  - Configure strong permissions on Cron and AT services to schedule jobs
  - U mask should be configured to 022
- Install Security Patches
  - Install all security patches regularly
    - Critical Risk Patch – within week
    - High Risk Patch – within month
    - Medium Risk Patch – within quarter
    - Low Risk Patch – within half year

BASE LINING POLICY STATEMENTS

H.O. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

- Only software that has been approved for use by the IT department may be installed on the organization's computing devices.
- Non-essential software applications and services will be uninstalled or disabled.
- Servers, desktops and laptops will be configured to prevent the execution of unauthorized software.
- Vulnerability scanning and inventory scanning software will be configured to automatically uninstall unauthorized software.
    - BIOS passwords will be implemented on all desktops and laptops to protect against unauthorized changes.
- The boot order of desktops and laptops will be configured to prevent unauthorized booting from alternative media.
- All desktops and laptops will be built from a standard image. Any change to the standard image must be supported by a business case.
- Access to the local administrator account will be restricted to members of IT Department to prevent the installation of unauthorized software and the modification of security software and controls.
- Default passwords will be changed following installation and before use in a production environment.
- All desktops and servers will be protected by anti-virus and anti-spy-ware software. The anti-virus and anti-spy-ware software will be configured to automatically download the latest threat databases.
- The use of removable media will be controlled. Removable media will be controlled by endpoint protection software.
- The headers on web servers and email servers will be changed.
- All server & new application must pass a vulnerability assessment prior to use. All network and operating system vulnerabilities will be rectified prior to use.

FOR HARENDRA D. MEHTA SHARE & STOCK BROKER PVT. LTD.

DIRECTOR

Harendra D. Mehta Share & Stock Broker Pvt. Ltd.

MEMBER > NSE Equity Segment > BSE Equity Segment

Stock Exchange Rotunda Building, PG -12, Ground Floor, Mumbai Samachar Marg, Mumbai - 400 001.

Phone : 2272 2392 / 2272 2190 / 2272 2546 / 2272 2548 • E-mail : bhm264@gmail.com

CIN : U67120MH1997PTC110950 • GSTIN : 27AAACH2890J1ZE

IT ACCESS CONTROL POLICY

HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED

15-04-2024

Author:	BAIJU HARENDRA MEHTA (DIRECTOR)
Owner:	BAIJU HARENDRA MEHTA
Organization:	HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED
Version No:	1.0
Date:	15-04-2024

Document Control

Document Title **IT Access Control Policy**

Version History

Version No.	Version Date	Author	Summary of Changes
1.0	15-04-2024	BAIJU HARENDRA MEHTA	NA

Approvals

Name	Title	Date of Approval	Version No
BAIJU HARENDRA MEHTA	IT Access Control Policy	15-04-2024	1.0

Distribution

Name	Title	Date of Issue	Version No
NA	NA	NA	NA

H. D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

1.0 IT ACCESS MANAGEMENT POLICY

1.1 PURPOSE

The purpose of this policy is to establish the framework and the rules for controlling logical access of HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED users to the information processing systems of HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED

1.2 SCOPE

This policy applies to all staff and non-employees and other individuals, entities or organizations responsible for administering and maintaining HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED 's IT infrastructure.

1.3 POLICY STATEMENT OF LOGICAL ACCESS

The Company shall control access to its information to help ensure its confidentiality and integrity.

1.3.1 ACCESS CONTROL

- Access shall be provided to meet following two principles of Role Based Access Control:
  - Need-to-know: granted access to the information you need to perform your tasks (different tasks/roles mean different need-to-know and hence different access profile)
  - Need-to-use: granted access to the information processing facilities
- There must be a formal user access provisioning and de-provisioning procedure for granting access to information, information processing systems and IT services.
- All users shall have controlled access (read, write, modify, execute, full control) to information processing systems, in accordance with the user's functional role and information security requirements.
- For Contract Employees, Interns and Consultants, the validation of the ID must be only for the period of contract and must be automatically De-activated thereafter. There must also be a periodic review of the same.
- A record of disabled accounts must be maintained by the Designated Officer & Technology Committee.
- All information processing systems shall be configured to enable audit logs.

H. D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

1.3.2 USER ID

- Unique user IDs shall be assigned to each user for the purpose of their job roles and responsibilities.
- HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED 's IT administrator is responsible for creation of all HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED 's User IDs.
- All User IDs shall follow a standard naming convention defined as a part of this policy:
  - For HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED employees (permanent and contractual basis) the naming convention is <First Name>Dot<<Last Name>
  - If the User ID already exists, <First Name>DOT<Last Name><Numeric Value> shall be considered.
- User-IDs and related passwords shall not be shared with any other individual.
- User-IDs must be disabled and deactivated when the user leaves HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED
- Anonymous user-ids (such as "Guest") must not be allowed.
- Common user-IDs must not be issued to multiple users. In situations where a common ID is required, written permission shall be taken from Senior Management and Designated Officer.
- Default user-IDs and passwords shipped with information processing systems and software applications must be disabled.
- User-ID that is inactive for a maximum period of 60 days shall be disabled after seeking the approval from the user's reporting manager and/or Designated Officer.

1.3.3 PRIVILEGE MANAGEMENT

- All privileges to the users shall be assigned through a formal access provisioning procedure
- Designated Officer shall ensure that no privileges are assigned before access request is approved by his/her reporting manager.
- Privileges that are temporarily granted shall be authorized and tracked. Such privileges shall be revoked as soon as they are deemed not required.
- Designated Officer shall maintain detailed records for all allocated privileges.

H. D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

1.3.4 REVIEW OF ACCESS RIGHTS

- Designated Officer in coordination with Technology Committee shall review all user access rights at least every 12 months.
- Designated Officer shall review access logs, security logs, etc., on a periodic basis (once in 6 months is recommended). Findings of such reviews shall be reported to senior management for their review and possible action.
- Privileged accounts shall be reviewed by the Designated Officer at least every 6 months, and changes to such accounts shall be logged for periodic review.

1.3.5 NETWORK ACCESS CONTROL

- Access to networks and network services shall be specifically requested by the user's reporting manager and reviewed by Designated Officer.
- Remote user access to HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED network shall be subjected to appropriate user authentication and Cryptographer controls, for example, use of VPN (virtual private network) connectivity and two factor authentication / security tokens.
- Wireless networks and publicly accessible systems shall be segregated from the rest of the internal network.
- Wireless networks shall be secured by binding each IT asset's physical address (MAC address binding) on wireless access point.
- Groups of information processing systems, services and users shall be segregated on networks based on their sensitivity and classification of information stored or processed, exposure to public networks/users and corresponding risk levels.
- Access between the segregated network segments shall be appropriately controlled.
- Use of Network services shall be continuously monitored.
- HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED shall formulate an internet access policy on content filtering proxy device to monitor and regulate the use of internet and internet-based services such as social media sites, cloud-based internet storage sites, etc. within their critical IT infrastructure.

H. D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

1.3.6 SECURE LOG-ON

Secure log-on shall be implemented for systems and applications, as follows:

- Information processing systems shall suspend the user account and prevent user access to the system when an incorrect user password has been entered for specific number of times
- All actions performed by an individual on system programs shall be logged.
- All systems shall be locked, or sessions terminated after a defined time of inactivity.

1.3.7 MEASURES FOR APPLICATION AUTHENTICATION SECURITY

- Any Application used by HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED containing sensitive, private, or critical data such as IBTs, SWSTs, Back office etc. referred to as "Application" over the Internet shall be password protected.
  - Strong password policy must be followed as per company's policy.
- Passwords, security PIN s etc. shall never be stored in plain text and shall be one-way hashed using strong cryptographer hash functions before being stored in database.
- For added security, multifactor e.g., two-factor authentication scheme shall be used. In case of IBTs and SWSTs, two-factor authentication is mandatory.
  - In case of Applications installed on mobile devices (such as smart-phones and tablets), a cryptographically secure bio-metric two-factor authentication mechanism shall be used.
- Post multiple failed lo gin attempts into Applications; the Customer's account should be locked out.
- HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED hall focus on strong multifactor authentication for security and educate Customers to choose strong pass-phrases.
  - Customers may be reminded within 60 days intervals to update their password.
- Logins attempts to system much be logged for both successful and failed attempts.
- CAPTCHAs can be implemented for limiting the brute force attack and enumeration attacks against logins.

FOR HARENDRA D. MEHTA SHARE & STOCK BROKER PVT. LTD.

DIRECTOR

Harendra D. Mehta Share & Stock Broker Pvt. Ltd.

MEMBER ➤ NSE Equity Segment ➤ BSE Equity Segment

Stock Exchange Rotunda Building, PG -12, Ground Floor, Mumbai Samachar Marg, Mumbai - 400 001.

Phone : 2272 2392 / 2272 2190 / 2272 2546 / 2272 2548 • E-mail : bhm264@gmail.com

CIN : U67120MH1997PTC110950 • GSTIN : 27AAACH2890J1ZE

IT ASSET MANAGEMENT POLICY

HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED

15-04-2024

Author:	BAIJU HARENDRA MEHTA (DIRECTOR)
Owner:	BAIJU HARENDRA MEHTA
Organization:	HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED
Version No:	1.0
Date:	15-04-2024

Document Control

Document Title **IT Asset Management Policy**

Version History

Version No.	Version Date	Author	Summary of Changes
1.0	15-04-2024	BAIJU HARENDRA MEHTA	NA

Approvals

Name	Title	Date of Approval	Version No
BAIJU HARENDRA MEHTA	IT Asset Management Policy	15-04-2024	1.0

Distribution

Name	Title	Date of Issue	Version No
NA	NA	NA	NA

H. D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

1.0 IT ASSET MANAGEMENT POLICY

1.1 PURPOSE

Purpose for defining this policy includes:

- Identify, categorize and classify Assets
- To educate users about the importance of protecting assets
- To identify procedures that shall be in place to protect the confidentiality, integrity and availability of the organization Information

1.2 SCOPE

This policy applies to:

All staff and non-employees, stakeholders of HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED and other individuals, entities or organizations that have access to and uses HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED's information processing systems to perform their daily job-related responsibilities.

1.3 POLICY STATEMENTS

HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED has the responsibility in protecting the information assets from unauthorized access, generation, modification, disclosure, transmission or destruction. In order to ensure the security, reliability, integrity, and availability of information, appropriate asset handling scheme for labels shall be adopted by HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED.

- Any asset acquisition or disposition should be performed only based on approvals from Technology Committee and Designated Officer
- All the assets shall be identified, and an inventory of these assets should be drawn up and maintained by Technology Committee.
- The inventory of assets shall minimum have the following details:
    - Asset Id – Unique id for tracking the asset
    - Asset Name and Description
    - Asset Location
    - Nominated Owner & Custodian of the asset
    - Asset Value (High, Medium and Low)

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

1.3.1 IT ASSETS OWNERSHIP

The asset owner shall:

- Ensure that assets are appropriately classified (High, Medium or Low on basis of Confidentiality, Integrity and Availability) and protected.
- Define and periodically review access restrictions and classifications to important assets, considering, applicable access control policies.
- The asset owner shall be responsible for approving access and the level of access permitted for information assets under his/her ownership.

1.3.2 IT ASSETS GROUPING

Assets for HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED shall be grouped under the following asset types:

- IT Infrastructure Assets - Network devices, security devices, servers, server racks, backup media, printers, bio-metric devices, desktops, laptops etc.
- Software Assets - Business applications, operating systems, database, executable files, etc.
- Electronic Information Assets – Internet links, MPLS links, E-mails, Contracts, Agreements, etc. in electronic format.
- Information classification must be reviewed at least once a year and signed off by the respective department heads.

H. D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

1.3.3 IT INFORMATION ASSETS CLASSIFICATION

All the information assets shall be categorized under one of the following four classification levels:

Classification Level	Description
Restricted	Data / Information that is very critical or sensitive in nature and needs to be available only to the identified members of top management. If this data is lost or disclosed to unauthorized persons could lead to significant adverse impact, financial loss, penalties. Examples include statutorily protected and sensitive information and information such as customer forms, strategic plans/ financial information, Merger and Acquisition information and investigation reports and findings.
Confidential	Data / Information which is of importance to department or teams within HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED and cannot be shared with non-members of the department or team. The unauthorized modification or destruction of this information can affect the confidentiality, integrity or adversely impact HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED or hamper the operations
Internal	Data / Information which must be confined only to HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED staff and not to be disclosed to outside parties / public, including clients. It includes, but is not limited to, routine correspondence, employee newsletters, internal phone directories, inter-office memoranda, non-person identifiable information, organization policies and procedures.
Public	Data / Information that is available to the general public and is intended for distribution outside HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED. Public Information includes, but is not limited to, various services, marketing brochures and promotional literature, advertising media and HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED web site.

1.3.4 IT ASSETS LABEL-LING

- All assets of HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED shall be prominently labeled to ensure that they are given the necessary protection in use, storage and transport.
- All information, data, documents shall be clearly labeled so that all the users are aware of the ownership and classification of the information.

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

1.3.5 IT ASSET INSPECTION, ACCEPTANCE, DISTRIBUTION & INSTALLATIONS

- Physical assets shall be received by Shipping/Receiving and forwarded to Tech Support.
- Tech Support shall inspect and test assets for performance and capability prior to acceptance.
- When a nonconforming asset is identified, Tech Support shall report the nonconformity to the Purchasing Officer.
- The Purchasing Officer shall contact the vendor for replacement of the nonconforming asset and dispose of the nonconforming asset in accordance with any purchase/lease agreement in place.
- Only Tech Support shall distribute and install Information Technology assets.
- On installing hardware, Tech Support shall give each item a unique asset identifier. And shall update IT Asset Inventory and IT Network Architecture Diagram after installing assets.

1.3.6 IT ASSET RECORDS RETENTION & STATUS VERIFICATION

- Records are information created, received, and maintained as evidence and information by an organization or person in pursuance of legal obligation/standard requirement or in the transaction of business.
- Retention period for all records shall be clearly identified by the owners and documented.
- The Designated Officer shall conduct a periodic assessment of Information Technology assets to verify their status (i.e., in use/not in use), and shall take corrective action.

1.3.7 MEDIA HANDLING

- Media should be disposed of securely when no longer required.
- Media containing information should be protected against unauthorized access, misuse or corruption during transportation.
- Upon disposal of said assets, Asset Management shall update IT Asset Inventory and IT Network Architecture Diagram.

FOR HARENDRA D. MEHTA SHARE & STOCK BROKER PVT. LTD.

DIRECTOR

Harendra D. Mehta Share & Stock Broker Pvt. Ltd.

MEMBER > NSE Equity Segment > BSE Equity Segment

Stock Exchange Rotunda Building, PG -12, Ground Floor, Mumbai Samachar Marg, Mumbai - 400 001.

Phone : 2272 2392 / 2272 2190 / 2272 2546 / 2272 2548 • E-mail : bhm264@gmail.com

CIN : U67120MH1997PTC110950 • GSTIN : 27AAACH2890J1ZE

IT COMPUTER MALWARE POLICY

HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED

15-04-2024

Author:	BAIJU HARENDRA MEHTA (DIRECTOR)
Owner:	BAIJU HARENDRA MEHTA
Organization:	HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED
Version No:	1.0
Date:	15-04-2024

Document Control

Document Title **IT Computer Malware Policy**

Version History

Version No.	Version Date	Author	Summary of Changes
1.0	15-04-2024	BAIJU HARENDRA MEHTA	NA

Approvals

Name	Title	Date of Approval	Version No
BAIJU HARENDRA MEHTA	IT Computer Malware Policy	15-04-2024	1.0

Distribution

Name	Title	Date of Issue	Version No
NA	NA	NA	NA

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

1.0 IT COMPUTER MALWARE POLICY

1.1 PURPOSE

Malicious codes such as viruses, worms, Trojans, spy ware, rootkits etc. represent a significant threat to the performance and security of HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED IT assets and services dependent on these assets.

1.2 SCOPE

All staff and non-employees (contractors, consultants, suppliers, vendors etc.) of HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED and other individuals, entities or organizations that have access to and use HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED IT systems and IT Services in order to perform their daily job-related responsibilities or meet their contractual obligations

1.3 POLICY STATEMENTS

All servers, desktops, laptops and hand-held devices of HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED must be protected against malicious code using enterprise level Anti-virus solution. The Anti-virus solution suite must ensure early detection, efficient containment and eradication of malicious code. Anti-virus software must be used on all systems commonly affected by malicious code to protect systems from current and evolving malicious software threats.

1.3.1 SELECTION OF ANTI-VIRUS

- Technology Committee shall identify suitable and reliable anti-virus software available.
- Selected anti-virus software shall be capable to detect, remove and protect against all known types of malicious software (for example viruses, Trojans, worms, spy ware, adware and root kits)
- The Anti-virus enterprise solution must support signature update rollback.

1.3.2 INSTALLATION & CONFIGURATION

- All servers, desktops, laptops and hand-held devices shall have anti-virus agent installed and configured before they are connected to the network.
- Anti-virus agent installation shall be password protected to ensure that end users cannot uninstall the agent or change any settings or to disable the agent.

H. D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

- Anti-virus agent shall be configured for full system scan the machine once in a week. The time of scanning can be either when the system boots up or during non-peak usage hours depending on load on various departments in HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED.
- Anti-virus agent shall be configured to do a real time scan of all the files when they are accessed, copied or moved. This will ensure that all viruses are detected before they get activated.
- Anti-virus agent shall be configured to scan all removable disks before use.
- Anti-virus agent shall be configured to quarantine virus infected files if they cannot be cleaned.
- Anti-virus administrator shall submit periodic reports (weekly & monthly) on the status of the Anti-virus protection to Designated Officer.
- The report shall include the following at a minimum:
  - Number of PC's / Servers / Laptops not updated with the latest signature patterns.
  - Top 10 viruses detected in the HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED network.
  - Number of viruses/worms/malicious programs detected.
  - Number of viruses/worms/malicious programs cleaned/quarantined.
  - Action taken to resolve the virus infection
  - Number of systems without the software installed
  - Number of systems without the latest signature patterns

1.3.3 ANTI-VIRUS SIGNATURE UPDATE

- The design of the Anti-virus application architecture shall ensure that all systems across the HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED are updated with latest signatures within 72 hours from the time of release
- All systems on the HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED network shall be configured to receive the signature updates from offline updates.

H. D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

1.3.4 EXTERNAL USERS

- External users (including consultants, vendors, customers and service providers) who bring laptops/desktops/servers into HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED premises shall not be allowed to connect to the HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED network without prior approval from the relevant Department Heads and Designated Officer.
- HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED Department shall verify whether vendor owned device has anti-virus installed and updated with latest signature pattern and that there are no active viruses.
- It shall also be checked whether all the necessary security patches have been installed. The device shall be allowed to connect only if all the above conditions have been met.

1.3.5 INCIDENT REPORTING

- In case of virus outbreak, anti-virus administrator shall take immediate steps to limit the extent of damage for recovering the systems with the help from the anti-virus solution vendor.
- Following steps shall be taken to ensure fast recovery:
  - Contact anti-virus vendor for assistance in formulating the action plan
  - Take necessary steps to limit the spread of virus including configuring access lists on firewalls
  - Take adequate steps to monitor the network for any traces of virus. This could include deployment of temporary intrusion detection systems or using vulnerability scanning tools.

FOR HARENDRA D. MEHTA SHARE & STOCK BROKER PVT. LTD.

DIRECTOR

Harendra D. Mehta Share & Stock Broker Pvt. Ltd.

MEMBER ➤ NSE Equity Segment ➤ BSE Equity Segment

Stock Exchange Rotunda Building, PG -12, Ground Floor, Mumbai Samachar Marg, Mumbai - 400 001.

Phone : 2272 2392 / 2272 2190 / 2272 2546 / 2272 2548 • E-mail : bhm264@gmail.com

CIN : U67120MH1997PTC110950 • **GSTIN :** 27AAACH2890J1ZE

IT INCIDENT HANDLING POLICY

HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED

15-04-2024

Author:	BAIJU HARENDRA MEHTA (DIRECTOR)
Owner:	BAIJU HARENDRA MEHTA
Organization:	HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED
Version No:	1.0
Date:	15-04-2024

Document Control

Document Title **IT Incident Management Policy**

Version History

Version No.	Version Date	Author	Summary of Changes
1.0	15-04-2024	BAIJU HARENDRA MEHTA	NA

Approvals

Name	Title	Date of Approval	Version No
BAIJU HARENDRA MEHTA	IT Incident Management Policy	15-04-2024	1.0

Distribution

Name	Title	Date of Issue	Version No
NA	NA	NA	NA

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

IT INCIDENT MANAGEMENT POLICY

1.1. PURPOSE

The purpose of this policy is to ensure timely and effective response to IT incidents by restoring service operations to agreed level as quickly as possible.

1.2. SCOPE

- All staff and non-employees and other individuals, entities or organizations responsible for administering and maintaining HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED Information processing systems.
- All Information assets involving data, applications, network, security devices, servers and other IT system.

1.3. POLICY STATEMENT

To promptly report, investigate, and resolve all incidents that are or may be a threat to secure and effective Information Technology operations and the network.

1.3.1 GENERAL STATEMENTS

- 'Incidents is a term related to exceptional situations or a situation that warrants intervention of specialist help or senior management. An incident is detected in day-to-day operations and management of the IT function. This may be result of unusual circumstances as well as the violations of existing policies and procedures of HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED
- All users and IT administrators shall be responsible for identifying incidents. Some examples are:
    - Abnormal system resource usage: If the CPU or memory utilization on a system is very high compared to the normal usage, the system could have been compromised. Compromised systems could be exploited by attackers for spreading viruses.
    - Abnormal, slow response of the application: Users could experience extremely slow response times if the application servers or the network has been compromised.
    - Data Corruption: If the user finds that data or files stored on the desktop/laptop has been either deleted or modified without their knowledge.

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

- Change in system: If your desktop/laptop configuration looks different in terms of the applications installed, screen savers or icons on the screen, or the system is misbehaving.
- Changes in password and user-id: Users shall report if they find their passwords have been changed or their account has been locked without their knowledge.
- Virus infection: Users shall report any virus or worm that infected one or more hosts. However, viruses or worms that are detected and cleaned by anti-virus software need not be reported; only those which are not getting cleaned and infecting the system needs to be reported.
- Changes in applications: If the applications accessed by user look different from its normal appearances.
- Security weakness detected: If any weakness in the applications accessed by user that can cause unauthorized access or modification or lead to any kind of compromise.
- Violation by others: Any instance of security violations committed by others like running of malicious tools, trying to break into system or committing IT frauds or thefts, copyright or license agreement violations, user shall report such instances.
- Denial of service or disruption to system activity - Such incidents include:
  - Distributed denial of service attack (D Dos) causing loss of external network connections through packet flooding
  - Causing system to crash
  - Causing system to partially or completely fail
- Changes to system software/firmware, hardware or environment without approval - Such incidents include:
  - Addition of software/hardware with malicious intent (e.g., keystroke logging or backdoor)
  - Unauthorized removal, addition or replacement of equipment
  - Installation of back door code without authorization
- Loss or physical damage to the systems
- Unauthorized activation of suspended / deleted user accounts

The importance of incident detection and analysis shall be propagated throughout the organization and users shall be made aware of the importance of the same and their responsibilities towards reporting of incidents and security weaknesses or any software malfunction.

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

1.3.2 IT INCIDENT REPORTING AND RECORDING

- All employees of HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED shall be aware of their responsibility to promptly report any IT incidents.
- All IT related incidents shall be reported to the respective reporting manager, Designated Officer, Technology Committee or HR Head via phone or email.
- The Designated Officer shall evaluate the information, determine the potential for loss and the risk to the, and assign the incident to the Incident Response Handling Team or SOC Monitoring Team.
- The following details shall be recorded initially:
    - Details of the user(s) who reported the incident including contact details
    - Detailed description of the incident including time of incident
    - Asset / service affected
    - Details on how the incident was discovered / detected
    - Supporting evidence
    - Remedial steps taken, if any
    - Incident classification

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

1.3.3 IT INCIDENT PRIORITIZATION

Incident Management Priority Matrix	
Severity Level	**Description**
Severity 1 (Major Impact)	Direct threat or damage to image, reputation or credibility of HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED Multiple business functional units getting severely impacted.
Severity 2 (High Impact)	Severe outage affecting single business functional units, key services or location.
Severity 3 (Moderate Impact)	Moderate degradation to business functional units, locations, IT assets. Moderate to high impact to non-critical business units within organization.
Severity 4 (Minimal Impact)	Small issue with localized scope. Affecting few resources. Issue can be tolerated for a particular period of time.

All Incidents shall be prioritized based on the severity of the Incident.

1.3.4 IT INCIDENT HANDLING

- Employee should report suspicious incident or event to Designated Officer.
- Designated Officer will assign unique Incident ID
- Designated Officer shall evaluate the information contained on Incident ID to determine the potential for loss and the risk to the Company
- Designated Officer assigns the incident to the Incident Response Handling Team.
- The Incident Response Handling Team shall analyse the incident evidence, develop and test hypotheses regarding the incident, develop a set of findings and conclusions, and resolve the incident.
- The Incident Response Handling Team should perform a post-incident analysis, after an incident has been fully handled and all systems are restored to a normal mode of operation.
    - Analysing what has transpired and what was done to intervene
        - Did detection occur promptly or, if not, why not?
        - Was the incident sufficiently contained?

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

- Was communication adequate, or could it have been better?
- What practical difficulties were encountered?
- Was the incident caused due to negligence or malicious intent on part of an employee?

- Analysing the cost of the incident
  - How much is the associated monetary cost/ time?
  - How much did the incident disrupt ongoing operations?
  - Were any data irrecoverably lost, and, if so, what was the value of the data?
  - Was any hardware damaged?
- If any employee is suspected guilty, the HR should be informed for initiating disciplinary proceedings against the employee.

- The Incident Response Handling Team should discuss actions that were taken, and shall be recorded for future references
  - Workarounds and measures adopted to mitigate incident shall be updated in knowledge base.
  - Lessons learned, recommendations, and deficiencies should be presented to the Senior Management for discussion related security planning.
- The Team should report Incidents to respective exchange on quarterly basis.

FOR HARENDRA D. MEHTA SHARE & STOCK BROKER PVT. LTD.

DIRECTOR

Harendra D. Mehta Share & Stock Broker Pvt. Ltd.

MEMBER ➤ NSE Equity Segment ➤ BSE Equity Segment

Stock Exchange Rotunda Building, PG -12, Ground Floor, Mumbai Samachar Marg, Mumbai - 400 001.

Phone : 2272 2392 / 2272 2190 / 2272 2546 / 2272 2548 • E-mail : bhm264@gmail.com

CIN : U67120MH1997PTC110950 • GSTIN : 27AAACH2890J1ZE

IT OUTSOURCING POLICY

HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED

15-04-2024

Author:	BAIJU HARENDRA MEHTA (DIRECTOR)
Owner:	BAIJU HARENDRA MEHTA
Organization:	HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED
Version No:	1.0
Date:	15-04-2024

Document Control

Document Title **IT Outsourcing Policy**

Version History

Version No.	Version Date	Author	Summary of Changes
1.0	15-04-2024	BAIJU HARENDRA MEHTA	NA

Approvals

Name	Title	Date of Approval	Version No
BAIJU HARENDRA MEHTA	IT Outsourcing Policy	15-04-2024	1.0

Distribution

Name	Title	Date of Issue	Version No
NA	NA	NA	NA

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

1.0 IT OUTSOURCING POLICY

1.1 PURPOSE

To provide guidance with respect to managing outsourcing of Information Technology functions. To ensure that outsourcing affords the best overall solution to an Information Technology problem, satisfying customer requirements while controlling costs and conforming to the Company's strategic goals and objectives.

1.2 SCOPE

This procedure may apply to any Information Technology function or process.

1.3 POLICY STATEMENTS

To provide Information Technology services that satisfy Company requirements while controlling costs, maintaining flexibility, and providing special expertise as needed.

1.4 DEFINITION

Outsourcer – An outsourcing vendor; a business entity providing necessary services to the Company, allowing the Company to lower operating costs and gain flexibility while gaining special expertise on an as-needed basis.

Outsourcing – Seeking services (resources) outside the Company, typically to reduce costs, gain flexibility, and benefit from an outsourcer's expertise with respect to a given function or process.

Service Level Agreement (SLA) – A binding contract, formally specifying or quantifying a customer's expectations regarding solutions and tolerances.

1.4.1 IDENTIFYING A CANDIDATE FUNCTION FOR OUTSOURCING

- The Company may elect to outsource Information Technology functions in response to changing business conditions or requirements, including – but not limited to the following:
  - Need to control costs
  - Improving service to the Company's customer base
  - Temporarily requiring access to skilled experts that do not currently exist within the Company
  - Concentrating Company resources on core services; and/or
  - The function's relationship (relevance) to the Company's Strategic Plan.

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

1.4.2 RISK ASSESSMENT

- Before any contract is signed, a formal risk assessment of the contract shall be carried out and the results shall be presented to senior management for documentation of Acceptable Risk. The assessment shall consider the following:
  - Types of access needed
  - Value of the information/ system
  - Controls used by the third party
  - Implications of access on HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED information security
- The access approval notification shall include details on the following types of access:
  - Desktop/Laptop connectivity to HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED network
  - Email Accounts on the HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED mail system
  - Internet Access
  - Application/ Database access
  - VPN Connectivity to the HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED Network
  - Access to documents
  - Access to server rooms
  - Logical Access - Administrator login on servers and desktops

1.4.3 SELECTING AN OUTSOURCER

- All Third-party personnel/ organizations having access to HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED' classified information and information processing facilities shall adhere to HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED IT Security, IT Service Management, Business Continuity Policies.
- Any physical and logical access given to third party personnel shall be pre-approved, logged and monitored. The logs must be periodically reviewed by Technology Officer.
- The Identity cards given to the personnel shall be marked as Non-Transferable and Returnable on termination of contract.
- All third-party personnel who shall have access to HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED' information and information processing facilities shall sign a Non-Disclosure Agreement with HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED.

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

- Ensure controls are in place to determine loss or theft of data and to check the integrity of the data.

1.4.4 ACCESS PROVISIONING

- Access shall be provisioned by the respective owners. Authorization process followed for internal user creation shall be followed for third party users also.
  - Unique user ID shall be created if there are multiple people requiring access from the same external party.
  - Access shall be provided on the principle of "need to know" and the "need to have" basis.
  - Wherever technically feasible, create user accounts with specific end dates, so that it is automatically disabled after the pre-defined time interval.
  - For outsourced vendors, who may need to access HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED's systems for remote troubleshooting, access shall be provided using unique user-ID's and passwords.
- Respective Section Heads are responsible for disabling the access after the requested time.
- If the access requirements end before the date mentioned in the request form or if there is a need for extension, approval from the respective Business Head and Technology Officer needs to be taken as per user access provisioning process.
- If the third-party personnel are working at the critical areas, they shall always be accompanied by HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED official.
- If the third-party personnel are physically present in HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED premises, then all the procedure listed in the Physical and Environmental Policy applicable to third party shall be followed.
- Copy of acceptable usage policy shall be made available to third party personnel.

1.4.5 CONNECTING TO INTERNAL NETWORK

- If access is required to the internal network, the third-party user machine shall meet HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED's IT Security Policy.
- Third Party Access to the internal networks can be provided through either HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED desktop or laptop or the third party's laptop.
  - If it is a desktop or laptop provided by HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED, it shall be configured as per the Hardening guidelines.

H. D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

- It shall be ensured that only the software needed for the job is installed.

- Before connecting the third-party personnel's laptop to HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED network, it shall be scanned for viruses and worms.

1.4.6 NON-DISCLOSURE AGREEMENT

- Third party vendors shall sign non-disclosure agreements with HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED.
- The HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED shall make third party sign non-disclosure agreements to prohibit the third party and its agents from using or disclosing HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED information in any manner.

1.4.7 CONTRACTUAL REQUIREMENT

- Supplier agreements shall be established and documented to ensure that there is no misunderstanding between HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED IT Department and the supplier regarding both parties' obligations to fulfil relevant Information Security, IT Service Management, Business Continuity, and IT Service Quality requirements.
- Contracts between HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED IT Department and the vendor shall consider business requirements and key risk factors identified during the risk assessment.
- Contracts shall be clearly written and sufficiently detailed to provide assurances for performance, reliability, security, protection of Intellectual Property Rights and reporting.
- Scope of Service
  - The contract shall clearly describe the rights and responsibilities of parties to the contract including time frames and activities for implementation
  - Implementation provisions shall take into consideration other existing systems or interrelated systems to be developed by different vendors
  - The contracting parties' rights in modifying existing services performed under the contract
- Duration
  - HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED IT Department shall consider the type of technology and current state of the industry when negotiating the appropriate length of the contract and its renewal periods.
  - The contract shall address the vendor's responsibility for backup and record protection, including equipment, program, and data files.

H. D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

- HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED shall consider the appropriate length of time required to notify the vendor of HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED intent not to renew the contract prior to expiration
- The contract shall include provisions for addressing control over operations such as
  - Internal controls to be maintained by the vendor.
  - Compliance with applicable regulatory requirement.
  - Compliance with IPR (Intellectual Proprietary Rights) of software / modules used.
  - Records to be maintained by the vendor.
  - Insurance coverage to be maintained by the vendor.

- Audit
  - The contract may also specify rights to obtain documentation regarding the resolution of audit disclosed deficiencies and inspect the processing facilities and operating practices of the vendor.
  - HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED IT Department shall consider the degree to which internal audits completed by vendor audit staff can be used and the need for external audits and reviews.
  - Contract terms shall be added requiring periodic security audits to be performed by an in-house HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED team or by an independent party with enough expertise.
  - Contract terms shall be added requiring random or scheduled audits by RBI whenever required.
  - HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED IT Department shall receive sufficiently detailed reports on the findings of these on-going audits to adequately assess security without compromising the vendor's confidentiality.
- Cost
  - The contract shall fully describe fees and calculations for base services, including any development, conversion, and recurring services, as well as any charges based upon volume of activity and for special requests.
  - Cost and responsibility for purchase and maintenance of hardware and software may also need to be addressed.
  - Any cost to be incurred on termination or transitioning of service shall be identified.
  - If the cost cannot be quantified, a basis for arriving at the cost can be identified and agreed to in the contract.

H. D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

- Ownership and License
  - The contract shall address ownership and allowable use by the vendor of HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED data, equipment/hardware, system documentation, system and application software, and other Intellectual Property Rights.
  - Intellectual Property Rights may include HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED name and logo; its trademark or copyrighted material; domain names; web sites design; and other work products developed by the vendor for HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED.
- Performance
  - HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED IT Department shall include performance standards defining minimum service level agreements (SLA) and remedies for failure to meet standards in the contract.
  - HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED IT Department shall consider including in the contract a provision for a dispute resolution process that attempts to resolve problems in an expeditious manner.
- Limitation of Liability
  - Contract shall identify situations in which HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED may be liable for claims arising because of non-performance of vendor or resulting out of security breaches and specify indemnification of HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED by the vendor.
- Termination
  - The contract shall state termination and notification requirements with time frames to allow the orderly conversion to another vendor.
  - The contract must provide for return of HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED data, as well as other resources, in a timely manner and in proper format.

FOR HARENDRA D. MEHTA SHARE & STOCK BROKER PVT. LTD.

DIRECTOR

Harendra D. Mehta Share & Stock Broker Pvt. Ltd.

MEMBER > NSE Equity Segment > BSE Equity Segment

Stock Exchange Rotunda Building, PG -12, Ground Floor, Mumbai Samachar Marg, Mumbai - 400 001.

Phone : 2272 2392 / 2272 2190 / 2272 2546 / 2272 2548 • E-mail : bhm264@gmail.com

CIN : U67120MH1997PTC110950 • GSTIN : 27AAACH2890J1ZE

IT THREAT-RISK ASSESSMENT POLICY

HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED

15-04-2024

Author:	BAIJU HARENDRA MEHTA (DIRECTOR)
Owner:	BAIJU HARENDRA MEHTA
Organization:	HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED
Version No:	1.0
Date:	15-04-2024

Document Control

Document Title **IT Threat-Risk Assessment Policy**

Version History

Version No.	Version Date	Author	Summary of Changes
1.0	15-04-2024	BAIJU HARENDRA MEHTA	NA

Approvals

Name	Title	Date of Approval	Version No
BAIJU HARENDRA MEHTA	IT Threat-Risk Assessment Policy	15-04-2024	1.0

Distribution

Name	Title	Date of Issue	Version No
NA	NA	NA	NA

H. D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

3. IT THREAT-RISK ASSESSMENT POLICY

1.1 PURPOSE

All information assets need not be equally important for HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED's operations for achieving its vision and mission. Some assets are more important and need close attention and enhanced level of protection to ensure that mission critical systems are on and functioning.

The primary purpose of risk management is to make judicious use of the resources and provide the best possible protection at an acceptable cost. Information Risk Assessment consists of under noted components:

- Risk profiling - Identification of risk on the backdrop of perceived threats to information asset and vulnerability associated with information asset
- Assessing the risk
- Selecting the most effective controls to reduce the risk to an acceptable level

1.2 SCOPE

This policy applies to:

- All the company assets like IT infrastructure, Information stored in the organization.
- All staff (permanent & on contractual basis) and non-employees (contractors, consultants, suppliers, vendors etc.)

1.3 POLICY STATEMENTS

1.3.1 PROCESS

Information Risk Assessment Framework is a sequence of steps used to identify, understand and mitigate the risks to the confidentiality, integrity and availability of organisation information to the acceptable level.

A risk assessment is a pre-requisite to the formation of mitigation strategies, and this guides the organisation as it develops, implements, tests, and maintains its information systems security posture. This is an ongoing part of the information security management program.

1.3.2 ASSET & RISK MANAGEMET METHODOLOGY

The initial asset inventory & risk assessment and reviews are performed by the Asset Owner in consultation with Technology Officer. Risk assessment is reviewed once in every twelve months.

Further, risk assessment is also performed in the following circumstances,

- When new systems are implemented, or applications are developed or acquired.

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

- When critical business processes & procedures are changed & which may impact on information security.
- When major changes are made to IT infrastructure.

Methodology:

The Risk Assessment Methodology defines the methodology used by HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED to assess risks to the confidentiality, integrity and availability of information assets. The risk assessment needs to be carried out for important assets identified by the asset management processes and functions in HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED.

The Risk Assessment Evaluation:

- Consider IT Asset Classification from IT Asset Management Policy to identify valuation of IT Assets.
- Identified threats and vulnerabilities for a particular asset group are evaluated independent of existing controls.
- Control strengths that HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED already has in place are then mapped to evaluate the risks.
- On completing the Risk Assessment, each asset group will have multiple risk values based on threat/vulnerability pairs mapped to existing control strengths.
- Necessary controls are used towards a Risk Treatment plan.
- Any residual risks above baseline levels after Risk Treatment need to be formally accepted by the HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED senior management.

1.4 IDENTIFICATION & VALUATION OF ASSETS

1.4.1 ASSET IDENTIFICATION

Assets encompass all those items which contribute to the provision of information required by HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED to conduct its business. An asset may be a component or part of a total system to which HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED will assign a value and arrange for protection according to value. Following are the various categories of assets accordance with asset management process.

- All IT assets shall be identified by HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED, and an asset inventory shall be maintained by IT Security.
- IT assets shall be organized under categories mentioned in IT Asset Management policy.
- All IT assets shall be mapped with specific owners at different level of management in HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED.

H. D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

- IT Assets can be grouped for conducting IT risk assessments. It may not be practical or useful to perform IT risk assessment for individual assets in all cases.
- IT risk assessment shall attempt to optimize effort by using a combination of baseline approach for asset groups and detailed IT risk analysis for critical assets.
- Grouping of assets for the purpose of IT risk assessment shall use the following criteria:
  - Grouped assets shall have the same asset value in terms of criticality and sensitivity
  - Grouped assets shall have similar threat profiles. This means that similar threats, vulnerabilities and controls are applicable
  - The overall functionality of the grouped assets is similar
  - Grouped assets shall belong to same asset owners.

The asset valuation methodology is as below:

The value of an asset is based on the impact to HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED if the asset suffers from loss of confidentiality, integrity, or availability. Six dimensions shall be considered to evaluate the potential impact on HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED, and thus derive the value of the asset:

- Customers affected
- Critical systems affected
- Financial loss
- Brand and reputation
- Proprietary information
- Regulatory implication

For each asset, "What is the extent of damage along these six dimensions if the asset is compromised in Confidentiality, Integrity, or Availability?" is to be determined.

1.4.2 ASSET CLASSIFICATION

- All IT assets of HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED shall be classified by the Asset Owners as per Asset Management Policy based on their sensitivity and impact to business operations. HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED classifies assets as one of the following:
  - High – impact that may stall the business
  - Medium – impact that may affect the business
  - Low – impact that has no significant effect on the business

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

- All assets of HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED shall be valued by the Asset Owners based on the business impact on the loss of Confidentiality (C), Integrity (I) and Availability (A) in terms of High, Medium and Low.
  - Confidentiality – business impact as a result of disclosure of the asset
  - Integrity – business impact as a result of modification of the asset
  - Availability – business impact as a result of failure of the asset
- The designated asset owner shall review and revise the classification given to an asset based on changes in business requirements.
- Asset register for IT risk assessment along with valuation shall be maintained by the Technology Officer.

1.4.3 LIKELIHOOD OR PROBABLITY OF THREAT OCCURANCE

While determining the probability, the threat frequency in terms of how often it might occur, based on experience and statistics shall be considered. The likelihood of threat occurrence is valued using the following scale.

Unlikely	=	1
Could happen	=	2
Very Likely	=	3

1.4.4 IMPACT OF THE THREAT ON CIA OF THE ASSET GROUP

Once the likelihood of threats is valued, identify the affected aspect (C, I and A) and assess the impact on the asset if the threat were to materialize. Impact of threat on asset (CIA) is valued using the following scale:

Low	=	1
Medium	=	2
High	=	3
Very High	=	4

H. D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

1.4.5 IDENTIFICATION & VALUATION OF VULNERABILITIES

Vulnerabilities are weaknesses associated with an organization's assets. These weaknesses may be exploited by a threat causing unwanted incidents that may result in loss, damage or harm to these assets.

The vulnerability identification should identify the weaknesses related to the assets by considering the following:

- Physical environment
- Personnel and administration procedures and controls
- Hardware, software or communication equipment and facilities

Vulnerabilities are categorized into Low (1), Medium (2), High (3), and Very High (4) based on the levels of vulnerability in the assets

- Low - The possibility of the vulnerability being exploited is very less
- Medium - The vulnerability might be exploited
- High - The vulnerability can be easily exploited
- Very High - The vulnerability can be very easily exploited

1.4.6 IDENTIFICATION & VALUATION OF CONTROL STRENGTH

After identification and valuation of threats and vulnerabilities, the existing processes and control in the HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED environment to minimize the threat and vulnerabilities are identified. For each control, a control strength value is calculated. The "Control Strength" is calculated from "Nature of Control" and "Type of Implementation".

A numerical value is assigned to the Type of Implementation:

Manual	=	1
Automated	=	2

A numerical value is assigned to the Nature of Control:

Awareness	=	1
Recovery	=	2
Detection/Deterrent	=	3
Preventive	=	4

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

The control strength value is calculated using the following formula:

Control Strength = Type of Implementation x Nature of Control

If there is more than one control; all control strengths are added to arrive at the final strength.

1.4.7 CALCULATION OF RISK VALUES & IDENTIFYING RISK OWNER

All the threats and vulnerabilities a particular asset may be exposed are identified and the existing controls are implemented in the organization are listed and the control strengths are calculated.

The Risk Score is calculated using the following formula:

Risk Score = Asset Value x Threat Value x Vulnerability Value

The Risk Value is calculated using the following formulas based on the existing controls availability:

- Risk Value = Risk Score / Control strength - If existing controls are available.
- Risk Value = Risk Score / (1 + Control strength) - If there are no existing controls.

Risk Ownership

Overall ownership of risk shall remain with Asset owners shall,

- Assume ownership of risk pertaining to their asset.
- Be accountable to ensure that appropriate controls, commensurate with the security classification level are maintained and the risks associated with the assets are managed.

1.4.8 INITIAL BASE LEVEL FOR ACCEPTABLE RISK VALUES & PRIORITIZATION OF RISK

Risk Treatment requires a baseline for prioritizing and treating risks. The baseline level indicates the acceptable values of risk. Risk values within the baseline level may be accepted. Risk values above this level require treatment based on the priority.

Risk values above baseline should be prioritized for risk treatment based on the subjective analysis of risk values, risk exposure, likelihood of occurrence, and likelihood of detection, severity of impact and resource requirements.

Priority of risk would be defined as following:

H. D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

Threat Value	Low				Medium				High				Very High			
Vulnerability Value	L	M	H	VH	L	M	H	VH	L	M	H	VH	L	M	H	VH
Low	1	2	3	4	2	4	6	8	3	6	9	12	4	8	12	16
Medium	2	4	6	8	4	8	12	16	6	12	18	24	8	16	24	32
High	3	6	9	12	6	12	18	24	9	18	27	36	12	24	36	48
Very High	4	8	12	16	8	16	24	32	12	24	36	48	16	32	48	64

Some risk values may remain above this baseline level because they cannot be immediately treated due to various factors such as lack of resources, mitigation cost exceeds benefit, etc. These need to be separately accepted at their higher risk values and signed off by the Technology Officer.

Management reviews the acceptable risk values based on available resources and budget for risk treatment. The Technology Officer has formally accepted an initial HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED- baseline level=8.

1	2	3	4	6	8	9	12	16	18	24	27	32	36	48	64
Acceptable Risks						Non-Acceptable Risks									

The above shows the 8 as the baseline level. Risk values above this level are by default non-acceptable unless formally accepted by management.

Justification for choosing a Baseline level of 8

To calculate the baseline value:

- The maximum risk score is 64.
- An acceptable baseline level of 10% would ensure that 90% of the identified risks are put on a treatment plan.
- Thus, the baseline level of 8 is chosen above which the risks shall be treated, and exceptions need to be formally signed off.
- The Technology Officer may decide to further decrease the baseline level in subsequent management reviews.

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

1.4.9 RISK TREATMENT / RISK ACCEPTANCE

Risk Treatment requires a baseline for prioritizing and treating risks. Risk values within the baseline level may be accepted. Risk Assessment Risk Treatment would be conducted annually. It would be schedule and informed to the key stakeholders one week prior to the start date.

It is seldom possible to eliminate risks to information in terms of confidentiality, integrity, or availability. Identification of the appropriate security controls as per the ISO27001 is necessary before the implementation.

- Any of the following IT risk treatment strategies or a suitable combination can be adopted to mitigate the IT risk:
    - Transfer Risk
    - Tolerate (Accept) Risk
    - Treat the Risk
    - Terminate the Risk

When evaluating the levels of acceptable risk in managing a specific risk, the Technology Officer should consider the following issues:

- Location – The location determines the probable risks from accidental damage, e.g. from fire, contamination or floods.
- Existing Security – Physical, logical and personnel security measures already in place.
- Awareness on information security across organization.
- Number of security weaknesses – The higher the number of security weaknesses, the higher the risk of exposure/penetration.
- Facilities available – The more sophisticated the facilities available to a malicious user, the higher are the probability of exploiting the security weaknesses.
- Business continuity planning – The ability of existing business continuity measures to deal with an event.

The risks are managed to the level of acceptable risk through policies that avoid the risk, transfer the risk, reduce the vulnerabilities, reduce the threats, reduce the possible impacts, detect unwanted events, or employ a combination of the above.

Where action is required to manage a risk, the management decisions are documented in the management team meeting minutes and communicated to the appropriate member(s) of staff for implementation of the control/countermeasure. Such decisions may require a new policy statement or the amendment of an existing policy.

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

Where a risk is identified, but controls/countermeasures is not implemented because of financial, environmental, technological, cultural, timescale or other reasons, then risk is accepted, and business exception is taken for the same. These points should be reviewed on a regular basis to ensure the decision remains valid.

Management reviews of the Risk Management shall periodically review the acceptable risk values based on available resources and budget for risk treatment.

1.4.10 MONITORING AND REVIEW

- Having identified the risks and determined a plan of remedial action, it is essential that assurance regarding the effectiveness of the action is obtained.
- All responsible risk owners will provide periodical updates, to the Technology Officer regarding the progress made in reducing/removing risks. This information will be used to update the Risk Register.

1.4.11 RESPONSIBILITIES

The responsibility for the upkeep of the asset identification and perceived valuation remains with the Technology Officer who review the situation regularly, and especially when any significant changes are made to the departments.

Changes in HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED organizational structure may result in changes to process ownership. Handover of responsibilities includes acceptance of the risk assessment procedure and understanding of the risk in the process or function.

The new and emerging risk will be identified in the following manner:

1. Based on inputs and feedback obtained by the Technology Officer from the process personnel or through other means
2. During the internal or external audits
3. Based on inputs from the management

The identified risks need to be added to the risk assessment sheet.

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

1.4.12 RESIDUAL RISK APPROVAL & TREATMENT PROCESS

Identified risks from the Risk Assessment should be extracted and condensed to form a unique list of residual risks that when addressed would bring down the risk levels to acceptable values.

The minutes of the meeting should be recorded to serve as evidence for management approval and acceptance of the proposed treatment activities. The Residual Risk Tracker should serve as a dynamic document that details treatment items for all current risks above acceptable baseline levels and their status updates.

FOR HARENDRA D. MEHTA SHARE & STOCK BROKER PVT. LTD.

DIRECTOR

Harendra D. Mehta Share & Stock Broker Pvt. Ltd.

MEMBER > NSE Equity Segment > BSE Equity Segment

Stock Exchange Rotunda Building, PG -12, Ground Floor, Mumbai Samachar Marg, Mumbai - 400 001.

Phone : 2272 2392 / 2272 2190 / 2272 2546 / 2272 2548 • E-mail : bhm264@gmail.com

CIN : U67120MH1997PTC110950 • GSTIN : 27AAACH2890J1ZE

IT VENDOR SELECTION POLICY

HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED

15-04-2024

Author:	BAIJU HARENDRA MEHTA (DIRECTOR)
Owner:	BAIJU HARENDRA MEHTA
Organization:	HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED
Version No:	1.0
Date:	15-04-2024

Document Control

Document Title **IT Vendor Selection Policy**

Version History

Version No.	Version Date	Author	Summary of Changes
1.0	15-04-2024	BAIJU HARENDRA MEHTA	NA

Approvals

Name	Title	Date of Approval	Version No
BAIJU HARENDRA MEHTA	IT Vendor Selection Policy	15-04-2024	1.0

Distribution

Name	Title	Date of Issue	Version No
NA	NA	NA	NA

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

1.0 IT VENDOR SELECTION POLICY

1.1 PURPOSE

IT Vendor selection policy is required for initial Information Technology vendor identification and collecting information regarding potential vendors. IT Vendor selection policy is also required for maintaining vendor performance data for ongoing evaluations.

1.2 SCOPE

This procedure applies to all potential and current vendors of Information Technology products and services. Information Technology Managers are responsible for final review and approval of new Information Technology vendors, as well as maintaining a file on current vendors.

1.3 DEFINITONS

Service Level Agreement (SLA) – Contract between a service provider and an end user, stipulating and committing the provider to a required level of service. An SLA typically includes such features as support options, enforcement or penalty provisions for services not rendered, guaranteed system performance levels related to up-time/downtime, specific levels of customer support.

1.4 POLICY STATEMENTS

To ensure vendor performance capabilities are sufficient to meet Information Technology requirements.

1.4.1 IT VENDOR EVALUATION

- The Designated Officer shall select Information Technology Vendors for all IT Products, IT Services and IT Consultants in the following manner:
  - Conduct vendor's market reviews.
  - Request a full profile from the vendor, which should include:
    - The vendor's history with firms like the Company in nature of business, size, and scope.
    - The vendor's capabilities with regard to the Company's needs.
    - Sales and marketing information.

H.D. MEHTA SECRETARIAL BUREAU PVT. LTD. MUMBAI

- Obtain customer referrals – survey the vendor's current clients to determine their degree of satisfaction with the vendor and the product/service desired by the Company.
- For critical assets, or for asset purchases where the Company wishes to rely on the quality assurance of the vendor, vendor inspection shall be performed and approved.
  - Check the vendor's certifications – ISO, Microsoft, Oracle, etc. – especially those that apply to the product or service under consideration.
  - Conduct a security background check, to confirm the vendor's compliance with applicable legal and regulatory requirements.

- Designated Officer shall evaluate the vendor profile from the cyber security perspective also.
- HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED shall execute an agreement with MIIs (Market Infrastructure Institutions) where applications offered to HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED over the internet by MIIs, for e.g., NSE's NOW, BSE's BEST etc.
- MII shall be solely responsible for ensuring Cyber Resilience on those applications reside with the MIIs and not with HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED.
- HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED is exempted from applying the guidelines to such systems offered by MIIs such as NOW, BEST, etc.

1.4.2 VENDOR SELECTION

- The Designated Officer shall evaluate vendor proposals by the due date, recommendations, and forward proposals to Management and Finance team.
- Finance and Management team shall evaluate vendor information and the accompanying recommendations, weigh all factors appropriately, and indicate their recommendation and approval of a vendor or vendors.
- Management team shall review the results of the security check and determine the level of vendor access to sensitive information.

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

1.4.3 VENDOR REVIEW

- Technology Committee shall periodically re-evaluate Information Technology vendors, according to the vendor performance criteria.
- If a vendor is found to be out of compliance, Technology Committee shall submit a Corrective Action Request.
  - If a vendor does not respond to a Corrective Action Request or is unable to correct problems within a reasonable time frame, it may be disqualified.
    - Technology Committee shall maintain a list of disqualified vendors.
  - If the vendor opts to take corrective action, Technology Committee shall follow up with the vendor immediately and again within three months to verify that:
    - The corrective action has been taken; and
    - The corrective action continues to produce the desired results.

FOR HARENDRA D. MEHTA SHARE & STOCK BROKER PVT. LTD.

DIRECTOR

Harendra D. Mehta Share & Stock Broker Pvt. Ltd.

MEMBER ➤ NSE Equity Segment ➤ BSE Equity Segment

Stock Exchange Rotunda Building, PG -12, Ground Floor, Mumbai Samachar Marg, Mumbai - 400 001.

Phone : 2272 2392 / 2272 2190 / 2272 2546 / 2272 2548 • E-mail : bhm264@gmail.com

CIN : U67120MH1997PTC110950 • GSTIN : 27AAACH2890J1ZE

LOGGING AND MONITORING POLICY

HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED

15-04-2024

Author:	BAIJU HARENDRA MEHTA (DIRECTOR)
Owner:	BAIJU HARENDRA MEHTA
Organization:	HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED
Version No:	1.0
Date:	15-04-2024

Document Control

Document Title Logging and Monitoring Policy

Version History

Version No.	Version Date	Author	Summary of Changes
1.0	15-04-2024	BAIJU HARENDRA MEHTA	NA

Approvals

Name	Title	Date of Approval	Version No
BAIJU HARENDRA MEHTA	Logging and Monitoring Policy	15-04-2024	1.0

Distribution

Name	Title	Date of Issue	Version No
NA	NA	NA	NA

H. D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

1.0 LOGGING AND MONITORING POLICY

1.1 PURPOSE

- IT infrastructure components forms a crucial part of HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED operations. IT assets are constantly under threat from malicious users and as a result, needs to be monitored effectively on a continuous basis for any abnormal activities. This policy aims to establish effective system to centrally log and monitor information security controls.

1.2 SCOPE

This policy applies to:

- All staff and non-employees, stakeholders (interns, contractors, consultants, suppliers, vendors etc.) of HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED and other individuals, entities or organizations that have access to and use HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED information processing systems and card holder data environment to perform their daily job-related responsibilities or meet their contractual obligations.
- All Information assets involving data, applications, network, security devices, servers and other IT system

1.3 POLICY STATEMENTS

Logging shall be enabled on all information processing assets. All access to critical applications and HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED' network shall be logged and monitored for suspicious activities or security breaches and adequate response mechanism shall be setup for controlling security breaches.

1.3.1 LOG MONITORING

- Logging shall be enabled for all the critical devices including application servers, network devices and security devices.
- The logs of the applications shall be monitored periodically to ensure proper functioning and policy compliance.
- Some of the following activities and parameters shall be logged and monitored, but not limited to:
  - Access to all audit trails
  - Initialization of audit logs
  - Stopping or pausing of audit logs
  - Remote access activities of vendors
  - All individual access to cardholder data
  - Actions taken by any individual with root or administrative privileges

H. D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

- Invalid logical access attempt
- Identification and authentication mechanisms
- Creation and deletion of system level objects

- Parameters related to audit trails:
  - Ensure user identification is included in log entries
  - Ensure type of event is included in log entries
  - Ensure date and time stamp is included in log entries
  - Ensure success or failure indication is included in log entries
  - Ensure that audit trails are enabled and active for system components
  - Ensure ONLY individuals who have a job-related need, can view audit trail files. Access to audit trail files shall be monitored regularly
  - Ensure current audit trail files are promptly backed up to a centralized server or media that is difficult to alter
- The logs shall be analyzed for the following:
  - Unauthorized access
  - Configuration changes
  - Abnormalities in mail routing events
  - Failed logins
  - Denial of service attempts

1.3.2 INCIDENT REPORTING

- Any incident shall immediately initiate the IT Incident Management Process as per the IT Incident Management Policy.
- Designated Officer shall prepare the "Log Analysis Report", post any event identified.

1.3.3 BACKUP

- Logs in the centralized server shall be backed up on a periodic basis.
- The backup logs shall be protected from unauthorized access.
- The Retention period of the logs shall be decided by the Designated Officer. Though all logs shall be maintained for minimum period of 1 year.

FOR HARENDRA D. MEHTA SHARE & STOCK BROKER PVT. LTD.

DIRECTOR

Harendra D. Mehta Share & Stock Broker Pvt. Ltd.

MEMBER > NSE Equity Segment > BSE Equity Segment

Stock Exchange Rotunda Building, PG -12, Ground Floor, Mumbai Samachar Marg, Mumbai - 400 001.

Phone : 2272 2392 / 2272 2190 / 2272 2546 / 2272 2548 • E-mail : bhm264@gmail.com

CIN : U67120MH1997PTC110950 • GSTIN : 27AAACH2890J1ZE

NETWORK SECURITY POLICY

HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED

15-04-2024

Author:	BAIJU HARENDRA MEHTA (DIRECTOR)
Owner:	BAIJU HARENDRA MEHTA
Organization:	HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED
Version No:	1.0
Date:	15-04-2024

Document Control

Document Title **Network Security Policy**

Version History

Version No.	Version Date	Author	Summary of Changes
1.0	15-04-2024	BAIJU HARENDRA MEHTA	NA

Approvals

Name	Title	Date of Approval	Version No
BAIJU HARENDRA MEHTA	Network Security Policy	15-04-2024	1.0

Distribution

Name	Title	Date of Issue	Version No
NA	NA	NA	NA

H.D. MEHTA SH. & ST. BR. PVT. LTD. * MUMBAI

1. NETWORK SECURITY POLICY

1.1 PURPOSE

The purpose of this policy is to ensure authorized and secure access to HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED network infrastructure internally and from external networks and establish effective management/assured Network services quality and service continuity.

1.2 SCOPE

This policy applies to:

- LAN and WAN network infrastructure at Primary site deployed and maintained by HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED
- Relevant third-party personnel responsible for administering and maintaining HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED IT infrastructure
- All Infrastructure Coordinators and Infrastructure Specialists, Section Heads, administering and maintaining the network infrastructure viz. LAN and WAN
- All IT assets used to build the network viz. network devices, communication links and assets that use the network viz. servers, desktops, smart devices owned by HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED

1.3 POLICY STATEMENTS

- HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED network infrastructure shall be adequately designed, managed and controlled in order to strengthen security, continuity and quality of its IT assets and services.
- All connections to external networks including Internet, outsourced vendors and partners will be authorized and provided in a secure and controlled manner.
- Any kind of remote access to HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED network must be first approved based on valid business justification and initial risk assessment done by Head of Information Security.
- Network shall be designed and maintained for high availability to meet the Business Continuity requirements.

1.3.1 NETWORK ACCESS

- All user accesses to the network resources shall be approved and authenticated.

H.D. MEHTA & SH. BR. PVT. LTD. MUMBAI

- Administrative access and privileges on servers, network devices and other HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED' IT systems shall be granted only after necessary approvals from Head of Information Security.
- Prior approval shall be taken from Head of Information Security to connect desktop, laptop, smart phone or any network endpoint to HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED network (wired or wireless), including the guest wireless access for third party officials working within the wired/wireless network coverage.
- Before porting a new application on HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED network, Head of Information Security shall study the network usage of application, it's impact to existing infrastructure and provide the report which shall minimum contain the following details:
    - Whether the existing network infrastructure can accommodate the new application without affecting the existing applications
    - Whether there is need to modify the existing network infrastructure in order to accommodate the new application.
    - If there is need for modification, provide the estimated expense involved and the estimated time required for implementing the modification
- Open ports on networks and systems which are not in use or that can be potentially used for exploitation of data shall be blocked and measures taken to secure them.

1.3.2 SEGREGATING SERVER AND USER SEGMENTS

- A list of mission critical servers or servers processing sensitive information shall be prepared.
- List of critical servers shall be periodically reviewed and updated. All critical servers shall be separated from LAN users by creating dedicated server segments on firewalls.
- The user segment and the server segments must be distinct and access between them must be controlled.
- Server's segments shall be segregated and secured from user LAN by firewalls and continuously monitored by Head of Information Security for any malicious or abnormal traffic.
- In addition to firewall rules, all critical servers shall have restrictive access control policies configured on them which provide access to users on "Need to know" and "Need to Access" basis only.
- Internet facing servers and servers accessed by external parties like the Extranet shall be hosted on a separate segment De-Militarized Zone – DMZ Segment.

H.D. MEHTA & ST. BR. PVT. LTD. MUMBAI

- Utility servers like AV, Active Directory, Proxy, etc. shall be on a separate segment – Server Segment
- Application and database servers shall be protected by placing them on separate protected segment. This segment shall be accessible to authorized users only.
- Intrusion Prevention System (IPS) shall be strategically installed at network segments to monitor the traffic flowing, to and from critical servers.

1.3.3 SEGREGATION OF DEVELOPMENT & PRODUCTION FACILITIES

- Production systems shall be segregated from development and testing systems to mitigate unwanted modifications to live systems.
- Development and testing personnel shall not have direct access to production systems. If required, such access shall be through strict authorization and access control.
- Development, UAT and Production environment shall be segregated from each other with adequate access rights.
- Demilitarized Zone (DMZ)
- A list of DMZ servers (servers which are going to face Internet or process external requests) and ports / services to be opened for external users shall be prepared by respective administrators and submitted to Management Representative - Information Security Officer (MR-ISO).
- Request to open service or ports shall be supported by valid business justification from respective administrators.
- MR-ISO shall approve the request after adequate review and forward the approved request to Infrastructure Team.
- List of DMZ servers and open services shall be periodically reviewed and updated by the Infrastructure Specialist.
- Demilitarized Zone (DMZ) segment shall be created on firewall for Internet facing servers that hosts services that an organization needs to make available to the general public (such as web server, Mail server, Internet Banking Server etc.)
- DMZ shall be segregated from the internal server segments and LAN users through a firewall.
- Both Incoming and Outgoing traffic shall be continuously monitored for any malicious content.
- All channels connecting to DMZ resources shall preferably be encrypted. (SSL using valid certificates, VPN Tunnels with strong encryptions etc.)
- Event logging shall be enabled for all DMZ resources to send logs to a centralized log server.
- Internal IP address of DMZ servers shall be properly NAT-ed with Public IP address on firewalls.

H.D. MEHTA & CO. ST. BR. PVT. LTD. MUMBAI

- Internal IP addresses (Private IP Addresses) shall not be allowed to pass from the internet into the DMZ.(Configure Anti spoofing Rules)

1.3.4 VPN CONNECTIVITY

- Any approval for Remote access via Internet to HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED IT systems shall be granted by Head of Information Security.
- Remote access to network resources must be done using the SSL / IPsec VPN infrastructure provided by HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED. SSL must always be used for remote desktop protocol or SSH.
- Head of Information Security shall conduct quarterly audit of the VPN users.
- The use of remote access to HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED IT systems is strictly prohibited without a reasonable and documented business reason illustrating the necessity to complete job responsibilities.
- The VPN system shall automatically disconnect sessions upon reaching an idle time of 15 minutes.
- Remote access for vendors shall be enabled to the test and development environment upon receiving a written request, with adequate business justification and approved by Head of Information Security
- It is prohibited to copy, move, or store HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED data into local hard drives and removable media while using remote access to HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED IT systems.

1.3.5 NETWORK DEVICES – ROUTERS & SWITCHES

- Network devices like routers; switches; etc. shall be configured securely as per the Secure Configuration Document (SCD).
- Each Router & Layer -3 devices shall have the following statement as a banner in clear view:
  - "UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device are logged, and violations of this policy shall result in disciplinary action and will be reported to law enforcement."

1.3.6 NETWORK DEVICES – FIREWALL

Access to the Firewall

- The firewall shall be hardened and secured as per the Secure Configuration Document
- The firewall shall not have any additional services that can be accessed remotely

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

- The firewall shall be placed in a controlled environment with access only to authorized personnel
- Any unused physical interface shall be disabled/de-activated on the firewall

Firewall Rule Base

- Firewall rule-base shall only allow access to required ports and services on the target machine.
- Access requests for all the opened ports and services with valid business justification shall be documented and maintained
- Rule addition must be approved by Head of Information Security Officer prior to deployment
- All connections from the internal network to external networks shall be approved by the Head of Information Security. All connections to approved external networks shall pass through firewalls
- The rule base shall have a Stealth Rule which is a rule to deny all access requests that are not explicitly allowed
- The placement of this rule in the rule base is critical and shall be placed after all VPN and administrative and access rules to the firewall
- Firewall rule base shall deny all the ICMP Traffic
- Firewall rule base shall deny all the IP spoofing by enforcing egress filtering

Firewall Administration

- Default device password of the firewall shall be changed before deploying the device into the production and follow the Password Security Guideline.
- Unique usernames shall be used by each firewall administrator

Firewall up gradation and Patches

- Firewall shall be updated with latest stable firmware upgrades and patches released by the firewall vendor and follow the Patch Management Policy and Procedure
- Infrastructure Team shall evaluate new version release of firewall, test and verify if the upgrade is required or not before applying it in production
- After any upgrade, firewall shall be tested to verify all functionalities are working as desired

Firewall redundancy

- Redundant firewall in HA (High availability) mode shall be configured so that in case of a firewall failure, the backup firewall shall be switched in order to maintain the security level

Change Control

- Appropriate change control procedures shall be followed when making changes to the firewall system, including but not limited to -

H.D. MEHTA SR. & ST. BR. PVT. LTD. MUMBAI

- Upgrades or modification of the firewall application
- Addition of new firewall system hardware
- Physical movement of firewall system components
- All new user access requests shall be accompanied with business requirement and access details such as the IP address and the corresponding port numbers
- All changes to the firewall application shall be approved by the Head of Information Security

- Firewall rule base reviews needs to be done on periodic intervals (yearly once).

1.3.7 WIRELESS NETWORKS

- External auditor can perform wireless audit to detect unauthorized access points, at frequency of once a year.
- For any unauthorized access point detected Information Security Specialist should check for existence of any suspicious network. If such access points exist, such access points should be disconnected immediately.
- All unauthorized networks that are detected should be discussed with HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED senior management and it should be documented in MOM.

1.3.8 CLOCK SYNCHRONIZATION

- Network Time Protocol (NTP) shall be used to ensure synchronization.
- Clocks of all the systems throughout the organization shall be synchronized with NTP server.
- Any changes to time settings on critical systems shall be logged, monitored, and reviewed.

1.3.9 NETWORK LOGGING

- Adequate levels of information to be logged shall be clearly defined and configured.
- Type of log category and log information shall include the following:
  - Users - Login/logout information: location and time of failed attempts, attempted logins to privileged accounts; changes in authentication status such as different privileges etc.
  - Networks - Service initiation requests: name of the user/host requesting the service; network traffic; new connections.
  - Applications - Applications and services specific information: mail logs, ftp logs, web server logs, modem logs, firewall logs, router logs.
  - File Systems - Changes to access control lists and file protections; file accesses (opening, creating, executing, deleting).

- The log files shall be protected from being accessed, modified or deleted by unauthorized users and shall be stored in centralized log repository with restricted access.

1.3.10 RESTRICTION ON FILE TRANSFER PROTOCOL (FTP) SERVICE

- The use of File Transfer Protocol (FTP) shall be restricted on production systems
- The IT administrators for all servers shall ensure that anonymous file transfers (anonymous FTP) into the company system are disallowed
- If needed, then use of SFTP (Secured File Transfer Protocol) shall be encouraged, instead of FTP service
- No inbound FTP shall be allowed from the Internet to the firewall or internal network unless approved
- All files that are downloaded via SFTP shall undergo malware scan

1.3.11 NETWORK ARCHITECTURE DIAGRAM

- Network Architecture diagram shall be kept confidential and shall be made available only on need-to-know basis after the approval of Head of Information Security.
- Network Architecture diagram shall be updated as and when changes are done, latest network diagram shall be aligned with Business Continuity Plan/Disaster Recovery Plan.
- There shall be strict version control for Network Architecture Diagrams, and they will be stored in a centralized configuration register under the custodian of the Head of IT Infrastructure.
- Network Architecture diagram shall be:
  - Reviewed and updated at least annually
  - Shall clearly indicate wireless networks which are used in HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED
  - Shall clearly indicate the author, approver, date created, date reviewed & version number
  - Shall include all internal and external network devices, endpoint devices, server segments, logical and physical inter connections, WAN locations, LAN, internet and connection to service providers.

FOR HARENDRA D. MEHTA SHARE & STOCK BROKER PVT. LTD.

DIRECTOR

Harendra D. Mehta Share & Stock Broker Pvt. Ltd.

MEMBER ➤ NSE Equity Segment ➤ BSE Equity Segment

Stock Exchange Rotunda Building, PG -12, Ground Floor, Mumbai Samachar Marg, Mumbai - 400 001.

Phone : 2272 2392 / 2272 2190 / 2272 2546 / 2272 2548 • E-mail : bhm264@gmail.com

CIN : U67120MH1997PTC110950 • GSTIN : 27AAACH2890J1ZE

PASSWORD POLICY

HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED

15-04-2024

Author:	BAIJU HARENDRA MEHTA (DIRECTOR)
Owner:	BAIJU HARENDRA MEHTA
Organization:	HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED
Version No:	1.0
Date:	15-04-2024

Document Control

Document Title **Password Policy**

Version History

Version No.	Version Date	Author	Summary of Changes
1.0	15-04-2024	BAIJU HARENDRA MEHTA	NA

Approvals

Name	Title	Date of Approval	Version No
BAIJU HARENDRA MEHTA	Password Policy	15-04-2024	1.0

Distribution

Name	Title	Date of Issue	Version No
NA	NA	NA	NA

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

1. PASSWORD POLICY

1.1 PURPOSE

The purpose of this policy is to provide best practices for creating strong passwords.

1.2 SCOPE

This guideline applies to employees, interns, contractors, consultants, temporary and other workers, including all personnel affiliated with third parties. This guideline applies to all passwords including but not limited to user-level accounts, system-level accounts, web accounts, e-mail accounts, screen saver protection, voicemail, and local router logins.

1.3 POLICY STATEMENTS

PASSWORD CONSTRUCTION GUIDELINES

- Have minimum length of eight characters
- Must contain of alphanumeric characters
- Contain both upper- and lower-case alphabets
- Contain at least one numeric character (for example, 0-9)
- Contain at least one special character (for example,$%^&*()_+|~-=\`{}[]:";'<>?,/)
- Password should not be same as user ID
- Should not contain dictionary-based words or proper names, including foreign language, or exist in a language slang, dialect, or jargon
- Should not contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters
- Should not contain characters in sequential patterns such as aaabbb, qwerty, zyxwvuts, or 123321
- Should expire within maximum of 60 days
- Should maintain password history of last 10 passwords to restrict reuse of older passwords
- Should not be transmitted in clear or plain text
- Should not be written down in book, sticky notes or saved in notepad or excel files
- Interactive logon: Should prompt user to change password before expiration to five days. When their password expiration date is five or fewer days away, users will see a dialog box each time that they log on to the domain.

H. D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

PASSWORD DELETION GUIDELINES

All user accounts and passwords that are no longer needed, must be deleted or disabled immediately. This includes, but not limited to:

- User retires, quits or dismissed from his service
- Default password should be changed immediately on all systems
- Contractor's account should be disabled immediately after their service is no longer needed

PASSWORD PROTECTION GUIDELINES

- Do not use your user ID as password
- Do not share your password with anyone, including your manager, administrative assistant, or secretary
- Do not share your password over phone to anyone
- Do not reveal password in an email message
- Do not talk about password in front of others
- Do not hint at format of password (e.g., "My Pet Name")
- Do not share your password with colleague while on vacation
- Do not use "Remember Password" feature of browsers or any other applications

If someone demands to share password, refer them to this document or ask them to call IT Security Head.

If an account or password is suspected to be compromised, report this incident to Head of Department, Head of IT or Head of IT Security & Governance.

FOR HARENDRA D. MEHTA SHARE & STOCK BROKER PVT. LTD.

DIRECTOR

Harendra D. Mehta Share & Stock Broker Pvt. Ltd.

MEMBER > NSE Equity Segment > BSE Equity Segment

Stock Exchange Rotunda Building, PG -12, Ground Floor, Mumbai Samachar Marg, Mumbai - 400 001.

Phone : 2272 2392 / 2272 2190 / 2272 2546 / 2272 2548 • E-mail : bhm264@gmail.com

CIN : U67120MH1997PTC110950 • **GSTIN :** 27AAACH2890J1ZE

PHYSICAL SECURITY POLICY

HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED

15-04-2024

Author:	BAIJU HARENDRA MEHTA (DIRECTOR)
Owner:	BAIJU HARENDRA MEHTA
Organization:	HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED
Version No:	1.0
Date:	15-04-2024

Document Control

Document Title **Physical Security Policy**

Version History

Version No.	Version Date	Author	Summary of Changes
1.0	15-04-2024	BAIJU HARENDRA MEHTA	NA

Approvals

Name	Title	Date of Approval	Version No
BAIJU HARENDRA MEHTA	Physical Security Policy	15-04-2024	1.0

Distribution

Name	Title	Date of Issue	Version No
NA	NA	NA	NA

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

1.0 PHYSICAL SECURITY POLICY

1.1 PURPOSE

Physical and environmental protection of office facilities is of prime importance to HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED

The purpose of this policy is to build a secure environment that will protect against unauthorized physical access and environmental threats to HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED facility.

1.2 SCOPE

This policy applies to:

- All staff and stake holders, non-employees of HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED and other individuals, entities or organizations that have access to HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED information systems
- All Information assets involving data, applications, network, security devices, servers and other IT system that needs to be appropriately protected from physical and environmental threats

1.3 PHYSICAL SECURITY POLICY STATEMENTS

Information processing facilities must be secured from unauthorized access, damage or interference. Physical security measures must be in place to ensure the security and integrity of information processing facilities and the information assets.

1.3.1 SECURING THE OFFICE PREMISES

- The main entry to HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED office must be secured with appropriate controls like Access Cards / CCTV Camera
- All offices entry points shall be locked, when unattended, beyond working hours
- Movement of IT Assets must be recorded with appropriate information to track its movement

1.3.2 SECURING PREMISES FROM THIRD PARTY AND VISITORS

- The date, time of entry and departure and the purpose of visit must be recorded during office hours or outside office hours in a visitor's log maintained at reception.

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

- If separate area for loading or delivery of goods is not available, it shall be done at reception of the office.
- In Visitor's Register, all visitors shall be made to declare their personal belongings. Example: Laptops / Tablets / Camera Phones / Storage Devices.
- Strict access control measures shall be put in place to lockdown unused network points. Network Access to visitors or guests shall be granted upon prior approval by Designated Officer or Technology Committee.

1.3.3 SECURING INFORMATION STORAGE MEDIA

- All information storage media containing sensitive or confidential data shall be physically secured and access must be restricted to authorized personnel only.
- Back-up media shall be stored in fire resistant safes or cabinets and a copy of all backup media shall be maintained at an off-site location.
- Employees, Visitors and third parties shall not be allowed to bring along their personal laptops or any other external storage devices, unless authorized by Designated Officer or Technology Committee.

1.3.4 PHYSICAL SECURITY OF PORTABLE COMPUTING DEVICES

- Official Portable computing devices (Laptops, phones etc.) shall not be left on desk unattended for extended period or any other visible location overnight.
- In the event of a portable computing device being stolen, the concerned employee shall notify Designated Officer or Technology Committee about the theft immediately.
- Access to such portable and physical medias shall be controlled by encryption mechanism necessary to warrant loss of confidential information

H.O. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

1.3.5 CLEAR DESK AND CLEAR SCREEN

- Computer terminals when unattended shall be locked out or password protected.
- Controls like Automatic screen lockout or screen-saver passwords shall be enabled if left unattended for more than ten minutes.
- Files and other papers that contain sensitive information shall be protected from unauthorized access.
- Users shall not leave papers unattended on printer trays, photocopiers or their desks.
- Information classified as 'Restricted (in paper format or storage media like CD's, DVD or Tapes) shall be locked in a fire-resistant safe or cabinet, when not required.

1.3.6 EQUIPMENT SECURITY

- Eating, Drinking or smoking shall be restricted in secure areas where information processing equipment is placed.
- Combustible materials shall not be stored in secure areas where information processing equipment is placed.
- Only authorized maintenance personnel must be allowed to service or perform repairs on equipment.
- The confidentiality and integrity of all information shall be ensured prior sending any information processing equipment for repairs or maintenance.

1.3.7 SECURE DISPOSAL OR RE-USE OF EQUIPMENT

- All items of equipment containing storage media shall be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.
- Devices containing sensitive information shall be physically destroyed or the information shall be deleted or overwritten using adequate format techniques such that the original information remains non-retrievable in any manner.

H. D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

1.4 ENVIRONMENTAL SECURITY POLICY STATEMENTS

Adequate environmental security measures must be implemented to reduce exposure to environmental threats.

1.4.1 ENSURING SUITABLE ENVIRONMENTAL CONDITIONS

- The air-conditioning and humidity levels must be monitored.
- Smoking is strictly prohibited inside the office area. It may be permitted in the open designated areas only.

1.4.2 SECURING PREMISES FROM FIRE

- All computer systems must be housed in an environment equipped with fire extinguishers.
- The fire extinguishers must be placed in such a way so that they are easily accessible in all areas.
- Fire safety equipment must be checked regularly in accordance with manufacturer's instructions. A maintenance records must be maintained with the equipment.
- Comprehensive fire and emergency instructions must be displayed in prominent locations.
- Functioning and operations of the fire safety devices / equipment installed by HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED must be explained to employees and security guards periodically during Internal Training Programs.
- Regular mock drills shall be conducted to ensure effectiveness of the training and instructions to be followed.

FOR HARENDRA D. MEHTA SHARE & STOCK BROKER PVT. LTD.

DIRECTOR

Harendra D. Mehta Share & Stock Broker Pvt. Ltd.

MEMBER > NSE Equity Segment > BSE Equity Segment

Stock Exchange Rotunda Building, PG -12, Ground Floor, Mumbai Samachar Marg, Mumbai - 400 001.

Phone : 2272 2392 / 2272 2190 / 2272 2546 / 2272 2548 • E-mail : bhm264@gmail.com

CIN : U67120MH1997PTC110950 • **GSTIN :** 27AAACH2890J1ZE

TECHNICAL GLITCH POLICY

HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED

15-04-2024

Author:	BAIJU HARENDRA MEHTA (DIRECTOR)
Owner:	BAIJU HARENDRA MEHTA
Organization:	HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED
Version No:	1.0
Date:	15-04-2024

Document Control

Document Title **Technical Glitch Policy**

Version History

Version No.	Version Date	Author	Summary of Changes
1.0	15-04-2024	BAIJU HARENDRA MEHTA	NA

Approvals

Name	Title	Date of Approval	Version No
BAIJU HARENDRA MEHTA	Technical Glitch Policy	15-04-2024	1.0

Distribution

Name	Title	Date of Issue	Version No
NA	NA	NA	NA

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

TABLE OF CONTENT

Overview:- 4

Purpose:- 4

Scope:- ..... **Error! Bookmark not defined.**

Definition:- 5

Preventive Measures:- 6

Incident Information:- 7

Incident Escalation Matrix:- 8

Roles and Responsibilities:- 8

Incident Response Form: 9

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

1.0TECHNICAL GLITCH

1.1 OVERVIEW

- A Technical Glitch is any observable occurrence in a system or network.
- Events include a user connecting to a file share, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt.
- Adverse events are events with a negative consequence, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data.
- This guide addresses only adverse events that are computer security related, not those caused by natural disasters, power failures, etc.

1.2 PURPOSE

- The Purpose of this policy is to resolve any Technical Glitch as per the NSE Circular Ref. No: 108/2021 read with other relevant circulars of the respective exchanges
- The objective of this guideline is to outline the technology infrastructure and system requirements that a member should put in place to prevent any incident of business disruption resulting from technical glitches. These guidelines also prescribe the Standard Operating Procedures (SOP) for reporting of technical glitches, handling business disruption, management of such business disruption, including declaration of disaster and framing of provisions for disciplinary action in case of non-compliance in reporting/inadequate management of business disruption.

1.3 SCOPE

This policy applies to:

- All staff (permanent & on contractual basis) and non-employees / stakeholders (interns, contractors, consultants, suppliers, vendors etc.) of HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED and other individuals, entities or organizations that have access to and use HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED' information systems environment.
- HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED staff, who are responsible for administering and maintaining HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED' IT infrastructure.

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

1.4 DEFINATION

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.
Technical Glitch	Technical Glitch shall mean any malfunction of the systems including malfunction in hardware or software or any products/services provided, whether on account of any inadequacy or non-availability of infrastructure/network/ other systems or otherwise, which may lead to business disruption.
Business Disruption	Business Disruption shall mean either stoppage or variance in the normal functions /operations of systems HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED, due to a technical glitch, for a continuous period of more than 15 minutes
Business Continuity	Strategic and tactical capability of the organization to plan for and respond to incidents and business disruptions in order to continue business operations at an accepted predefined level.
Disaster Recovery	Disaster recovery involves a set of procedures to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster.

H.D. MEHTA SH. BR. PVT. LTD. MUMBAI

2.0PREVENTIVE MEASURES

- HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED shall put in place robust systems and technical infrastructure in place in order to provide essential facilities, perform systemically critical functions relating to securities market and provide seamless service to their clients. HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED shall deploy resiliency/redundancy measures to ensure continuity of their business operations as per guidelines issues by SEBI from time to time. HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED also adopt the various redundancy options provided by Exchange. However, HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED shall ensure due compliance while deploying the resiliency/redundancy measures.
- HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED shall comply with the system requirements prescribed under the PMS System Audit Framework as well as the framework for Cyber Security & Cyber Resilience prescribed by SEBI vide its Circular CIR/MRD/DMS/34/2013 and SEBI/HO/MIRSD/CIR/PB/2018/147 respectively and any other circulars/regulations & guidelines issued by SEBI/Exchange in this regard from time to time.
- HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED shall maintain enough capacity links to perform BAU operation including, Trading applications, BackOffice, customer support operations& connectivity to all exchange terminals with sufficient level of redundancy. Trading applications is primary working on Primary network if any disruption happens then the maximum time taken to restore and Recovery Time Objective (RTO) is 10 sec to 15 sec it switches automatically to Secondary network
- There shall be monitoring tools to monitor the data traffic within the organization network and from the organization network.
- The response and recovery plan of HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED shall have plans for the timely restoration of systems affected by incidents of technical glitch. HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED should based in their internal policy, define the Recovery Time Objective (RTO) and the Recovery Point Objective (RPO). The same shall be informed to the clients by the HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED.

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

3.0INCIDENT INFORMATION

3.1 INCIDENT INFORMATION

- If the disruption continues for more than 15 minutes, it shall be announced as an incident
- The CTO shall declare the incident
- Post declaring the incident, BCP & DR to be invoked as per BCP / DR plan
- All client communication should be completed within 30 minutes from the time of disruption. Technical glitches, resulting in business disruption needs to be reported to the exchange over common email ID: infotechglitch@nse.co.in
- _HARENDRA D MEHTA SHARE & STOCK BROKER PRIVATE LIMITED shall intimate the Exchange about the incident within 2 hours from the start of the glitch.
- 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.
- Root Cause Analysis (RCA) of the issue in the format as enclosed in Incident Management Procedure, to be submitted within 21 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.
- All incidents will be reported to Compliance, Risk Management committee and IT Steering committee.
- All communications with the media, other broadcasting channels and agencies shall be directed through the Communications team, in consultation with the CISO and CTO.
- All communications regarding business disruption with clients shall be done by the Customer Support Team the response can be vetted through Compliance/Business/Corporate Communication team & Risk team. There shall be an alternate means of communication including channel for communication for communicating with the clients in case of any Patch Scheduling & Prioritization

H.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

4.0INCIDENT ESCALATION MATRIX

4.1 INCIDENT 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	Crisis Management	Not resolved within 3 to 5 mins
Second Level	CRO-Chief Risk Officer/ BISO-Business Information Security Officer	Not resolved within 5 to 10mins
Third Level	CTO - Chief Technology officer / CISO – Chief Information Security Officer	Services are not up within 10 minutes

4.1.1 ROLES AND RESPONSIBILITIES

Crisis Management team, post resolution of crisis, shall update the Crisis Response Plan based on the Learning's. Business Information Security (BISO) along with the Chief Risk Officer (CRO) & Chief Technology Officer (CTO) shall review the Crisis Response Plan at least once in year and shall be responsible to assess the incident, oversee the implementation of the corrective and preventive actions and ensure the implementation of the aforementioned procedures. The plan shall be tested.

- System Audit:
  The infrastructure specified herein above shall be subject to System Audit.
- MIS
  A quarterly MIS shall be put up to the Board on incident reported, the corrective action taken and the future plan of actions including delay in deployment of corrective measures.
- Annual Review:
  This policy to be reviewed on Annual Basis

M.D. MEHTA SH. & ST. BR. PVT. LTD. MUMBAI

5.0INCIDENT RESPONSE FORM

All the incidents occurred will be maintained in the Incident response form given below:

Incident Reporting Form/RCA	
1. Letter/ Report Subject -	Name of the Member- Member Code -
2. Designated Officer (Reporting Officer details)	Name: Email: Mobile:
3. Date & Time of Incident & Incident duration	
4. Incident Description & chronology of events (please use additional sheets)	Brief information on the incident observed
5. Business Impact	
6. Immediate action taken (please give full details) (Please use additional sheets if necessary)	
7. Date & Time of Recovery	
8. Root Cause Summary (Pl attach the detailed Report separately)	
9. Back up measures available	
10. Details of long-term action (please give full details) (please use additional sheets if necessary)	
Note: In case of technical disruption due to Network issues, Architecture Diagram also needs to be annexed	

FOR HARENDRA D. MEHTA SHARE & STOCK BROKER PVT. LTD.

DIRECTOR