Choice
The Joy of Earning

CHOICE EQUITY BROKING PVT. LTD

Consolidated ISMS Policies

Version Control

Action	Date	Revision Details	Prepared / Amended By	Approved By
Created On	17-Oct-16	1.0	Mahesh Tamhankar	Amit Jaokar
Reviewed On	21-Feb-17	1.1	Mahesh Tamhankar	Amit Jaokar
Reviewed On	13-Feb-18	1.2	Mahesh Tamhankar	Amit Jaokar
Reviewed On	20-Feb-18	1.3	Mahesh Tamhankar	Utpal Parekh
Reviewed On	10-Aug-19	1.4	Mahesh Tamhankar	Yogesh Jadhav
Reviewed On	11-Jan-20	1.5	Mahesh Tamhankar	Yogesh Jadhav
Reviewed On	15-July-21	1.6	Sunil Utekar	Yogesh Jadhav
Reviewed On	08-Jan-22	1.7	Sunil Utekar	Yogesh Jadhav
Reviewed On	09-Apr-23	2.0	Ashutosh Bhardwaj	Yogesh Jadhav
Reviewed On	31-Jan-24	2.1	Anil Ashok & Associates	Ashutosh Bhardwaj
Reviewed On	28-Mar-24	2.2	Babu Holeyara	Ashutosh Bhardwaj

Version Control Revised Format

Version	Activity	Date	Description	Person Responsible
2.3	Amendments	20th December, 2024	Amendments with respect to change management, segregation of duties, and aligning with SEBI CSCRF guidelines	Abhishek Vinayak, Associate Cybersecurity
2.3	Reviewed	23rd December, 2024	Reviewed and suggested additional changes	Shripad Mayekar, Manager Cybersecurity
2.3	Amendments	6th January, 2025	Amendments done and submitted for review regarding Identity Access Management & patch management	Abhishek Vinayak, Associate Cybersecurity
2.3	Reviewed	6th January, 2025	Reviewed the changes and recommended for CISO Approval	Shripad Mayekar, Manager Cybersecurity
2.3	Reviewed	6th January, 2025	Reviewed and considered amendments03-Jan-25 in the document under change management policy	Ashutosh Bhardwaj, CISO
2.3	Approved	8th January, 2025	Approved	Yogesh Jadhav, CTO
2.4	Reviewed	19th January, 2025	Reviewed and considered amendments in the document under change management policy	Shripad Mayekar Information Security Manager

2.4	Approved	20th February, 2025	Approved	Ashutosh Bhardwaj, CISO

Table of Contents

INFORMATION SECURITY ROLES AND RESPONSIBILITIES

1.0 Scope

The target audience of this document is all the employees of Choice Equity Broking Pvt. Ltd. and all the temporaries (vendors and users of Choice Equity Broking Pvt. Ltd.'s information assets, other than direct employees). The scope of this document is to make the target audience aware of their Information security roles and responsibilities.

2.0 Roles and Responsibilities

Information Security Management System Steering Committee

The Information Security Management System Steering Committee is responsible for the establishment, implementation, operation, monitoring, review, maintenance and improvement of Information Security Management System (ISMS) at Choice Equity Broking Pvt. Ltd. The responsibilities of the Information Security Management System Steering Committee include:

- Ensuring that Information security objectives and plans are established for ISMS.
- Communicating to the organization the importance of meeting information security objectives and conforming to the information security policy, its responsibilities under the organization's regulations and the need for continual improvement.
- Providing sufficient resources to develop, implement, operate and maintain the ISMS.
- Identifying the acceptable levels of risk for the Information Assets.
- Periodically reviewing the status of Choice Equity Broking Pvt. Ltd. Information Security Management System.
- Reviewing and monitoring remedial work related to Information security incidents.
- Approving new or modified information security policies and procedures.
- Approving major initiatives in enhancing Information security.
- Ensuring that an internal audit is carried out Annually or as and when required for client's requirements, and a third-party audit is carried out annually.
- Providing competent training and, if necessary, employing competent personnel to satisfy the security requirements of Choice Equity Broking Pvt. Ltd..
- If needed, reporting the security posture of Choice Equity Broking Pvt. Ltd.to the Management board and investors once in a year.
- The Information security Committee will compromise senior management C-Suite/SVP/director of different departments.

The Information Security Management System Steering Committee has to meet annually once to discuss and review the security program. This meeting shall be chaired by the Information Security Management System Steering Committee Chairman.

Authority :- The Steering Committee holds the authority to set strategic direction, approve policies, and oversee the implementation and effectiveness of the ISMS.

2.1 Responsibilities of Departments

Director / Vice President

The Director's / Vice President's responsibilities, with respect to ISMS, are as follows:

- Ensure that appropriate levels of security are applied to all information assets (whether retained in-house or under the control of contractors) and Oversee, define, plan, budget, and implement the information security program.
- Ensure that Choice Equity Broking Pvt. Ltd.has established ISMS program
- Allocate sufficient resources necessary for the protection of Choice Equity Broking Pvt. Ltd.'s information assets
- Hold Choice Equity Broking Pvt. Ltd.'s managers accountable for the security of the information assets under their control
- Ensure that staff, facilities, and IT processing assets with appropriate national security clearances are available in the Office of Choice Equity Broking Pvt. Ltd.

  Authority :- Senior leadership is authorized for providing necessary resources, and fostering a culture of security across their respective departments.

Chief Information Security Office (CISO)

The CISO responsibilities, with respect to ISMS, are as follows:

- Ensure that all information assets owned or operated by or for Choice Equity Broking Pvt. Ltd.'s are accredited and that all information assets are assigned to an information system
- Ensure that Choice Equity Broking Pvt. Ltd. has established ISMS program & Coordinate implementation of the information security program.
- Approve and issue information security program policy, procedures, and guidance.
- Ensure that information assets are developed and operated in full compliance with Department and Choice Equity Broking Pvt. Ltd.'s policies, as well as ISO 27001's information security- related directives.
- Ensure that positions with significant information security responsibilities are held by staff with sufficient training and education qualifications as well as by staff who have had appropriate background checks.

- Develop information security program policy, procedures, standards, and guidance consistent with Departmental and ISO 27001’s requirements.
- Implement and manage an information security awareness and training program
- Assist with the planning and budgeting of information security functions for Choice Equity Broking Pvt. Ltd.
- Establish and maintain an information security certification and accreditation program. This includes ensuring that all assets have completed and maintained security plans, risk assessments, contingency plans, and security self- assessments
- Ensure that IT system technical and operational security controls are being implemented and maintained according to the sensitivity level of the system and the data being processed
- Assist in the development and maintenance of required security documentation and related activities (e.g., system administration and operational procedures and manuals)
- Know which assets or parts of assets for which they are directly responsible (e.g., network equipment, servers, and LANs)
- Conduct Choice Equity Broking Pvt. Ltd.-wide intrusion detection and vulnerability monitoring and penetration testing.
- Maintain appropriate contact with special interest groups to receive advisories and threat notifications for current security incidents.

Authority :- The CISO is authorized for the development, implementation, and management of the ISMS and has the authority to approve ISMS policies.

<u>ISMS Manager (Information Security Manager)</u>

The ISMS Manager will perform the following:

- Coordinate implementation of the IT security program
- Develop IT security program policy, procedures, standards, and guidance consistent with Departmental and ISO 27001’s requirements
- Assist with the development of IT system specific policy, procedures, and safeguards
- Implement and manage an IT security awareness and training program
- Assist with the planning and budgeting of IT security functions for Choice Equity Broking Pvt. Ltd..
- Establish and maintain an IT security certification and accreditation program. This includes ensuring that all assets have completed and maintained security plans, risk assessments, contingency plans, and security self-assessments
- Ensure that an objective, independent review and approval process exists for both security plans and procurement requests to validate the adequacy of proposed security safeguards;
- Communicate security requirements to Choice Equity Broking Pvt. Ltd.’s management and staff and serve as a resource on effective IT security practices
- Create and maintain an incident response capability

Authority :- The ISMS Manager is authorized to enforce security policies, conduct risk assessments, propose and request resources including budget, tools, and personnel, to support ISMS-related activities, to initiate and enforce mandatory security awareness and training programs for employees.

Internal Auditor’s

- Provide an internal audit function capable of evaluating information security controls.

- Engage an outside consultant or auditors to perform the internal audit function.
- Or use a combination of both methods to ensure that the institution has received adequate information security audit coverage.

  Provide information, analyses, and counsel to assist in effectively and efficiently handling the ISMS project.
- Examines, evaluates and report on the adequacy and reliability of existing internal controls.
- Recommends, as necessary, actions to improve automated and manual systems of processing revenues and expenses, financial reporting, compliance with laws, regulations and internally developed policies and procedures and the safeguarding of assets.
- Internal Audit must cover, but are not limited to the following:

    - Inappropriate user access to information systems
    - Unauthorized disclosure of confidential information
    - Unreliable or costly implementation of IT solutions
    - Inadequate alignment between IT systems and ISMS objectives
    - Inadequate systems for monitoring information processing and transactions
    - Ineffective training programs for employees and temporaries
    - Insufficient due diligence in vendor selection
    - Inadequate segregation of duties
    - Incomplete or inadequate audit trails
    - Lack of controls for end-user systems
    - Ineffective or inadequate information security continuity plans
    - Financial losses and loss of reputation related to systems outages

Authority : - Internal Auditors have the authority to assess and evaluate the effectiveness of the ISMS, identify weakness and areas for improvement in the management system.

<u>Department Head’s Representatives/Working group (ISMS - SPOC)</u>

Department representatives are directly responsible for the security of the assets under their purview. Department representatives have the following responsibilities:

- Ensure that appropriate levels of security are applied to all the assets and that sufficient resources are planned and assigned to maintain the required level of security;
- Ensure all assets are developed and operated in full compliance with Department and policies (e.g., annual user training requirements) as well as ISO 27001’s information security-related directives and mandates;
- Account for IT security in capital investment plans which must include all information security resources (e.g., labour, hardware, software, maintenance) for procurement, maintenance, and replacement of all assets;
- Ensure that department positions with significant security responsibilities are held by staff with sufficient training and education qualifications as well as by staff who have had appropriate background checks;
- Assign ownership of information security resources such that all department resources are assigned to a particular system and such that all assets have a designated system owner;
- Perform business assets access rights review of the team members

  Authority :- Department representatives has the authority to enforce departmental adherence to security policies, represent their department or team in all ISMS-related matters, communication between the ISMS Manager and their department, request necessary resources, participate in internal audits, assessments, and compliance checks

<u>Authorized User’s (Employee’s)</u>

The success of IT security programs ultimately depends on the commitment of each user. Users are to:

- Operate IT assets in a secure and responsible manner
- Know and abide by all applicable policies and procedures. This includes reading and understanding system-specific rules of behaviour regarding inappropriate use or abuse of the company’s resources
- Participate in security awareness and training activities
  Know which assets or parts of assets for which they are directly responsible (e.g., printer, desktop, specific support service, etc.)
- Know the sensitivity of the data they handle and take appropriate measures to protect it as per the Information Labelling & Handling policy.
- Report incidents to the IT Team using the method devised.
- Follow acceptable usage policy.

Authority :-

Employees are authorized to access and use information and systems only as permitted by their role, to report security incidents, vulnerabilities, or potential threats to the appropriate teams without fear of retaliation.

1. LOGICAL ACCESS CONTROL POLICY

1.1. Purpose

Access to business information and data shall be controlled in order to restrict access to authorized users only. Logical access to information systems shall be controlled. Access control standards shall be clearly defined and implemented. These security measures are the minimum controls required to mitigate threats to information and information systems including unauthorized access, disclosure, duplication, modification, appropriation, destruction, loss, misuse, and denial of use.

1.2. Scope

This policy applies to all employees, contractors, consultants, and temporary staff etc. who have access to Choice Equity Broking Pvt. Ltd. (Choice) resources. These standards apply to all computer and data communication systems used by and/or administered by Choice Equity Broking Pvt. Ltd. (Choice). Similarly, these standards apply to all platforms (operating systems), all computer devices and all application systems (whether developed in-house or purchased from third parties, Internet Service Providers, or service bureaus).

1.3. Responsibility

The Head - Technology is responsible for the development, maintenance, implementation, operation and escalation of enforcement of this policy.

1.4. Policy

1.4.1. Managing User Access

1.4.1.1. User Access to Information, Data and Application

- Choice Equity Broking Pvt. Ltd. (Choice) users shall be granted access to information, data and applications strictly on a "need to know" basis.
- Any change in access privileges shall be carried out only after approved by appropriate personnel, by using a formal documented process.
- Segregation of duties shall exist between information access requestors, information access approvers and those implementing access changes. Each of these roles is limited to a pre-defined group and only those specifically given the responsibility shall be allowed to either request or approve access.
- All access changes shall be carried by the respective operations team specifically authorized to carry out such changes. Examples of access changes include: creation of new employee accounts, transfers, terminations, file folder permissions, etc.
- User access rights to applications and data shall be assigned based on the user role and permissions approved by the respective application administration team.
- Privilege escalation for any application and data shall be granted only by the application administrator (IT / Technical Team), on receipt of a documented approval from the LOB Head/ RA/ authorized approver of the person requesting access. All access requests shall include the purpose for request of access.
- In case the authentication and authorization for an application not being authenticated by the centralized active directory, then a separate application administrator shall manage the user management, password management, and privilege management for the application. The application owners shall be responsible

for defining and maintaining access control lists for applications and data. They shall ensure that the level of access granted is appropriate to the business requirements.

- If for any reason, a user's access rights need to be modified or revoked, the LOB Head shall send the request for the same in writing to the respective application's owner / Operations team. The team shall then accordingly modify/revoke the access rights.
- HR shall promptly report all changes (i.e. LOB transfers, termination, job duty changes) in end-user duties or employment status to application operations team and also to the Technology team handling the user IDs of the affected persons. Respective Operations Team and / or Technology team shall then accordingly modify/revoke the access rights.
- Users shall be required to re-authenticate themselves after a specific period of inactivity. All systems wherever possible shall use inactivity timeout for sensitive applications.
- All users shall be granted "read" access to all information classified as "public". Other rights to such information shall be strictly reserved with the owner of such information.
- Non-employee Internal System IDs – In addition to meeting the above requirements for internal system access, non-employees have additional constraints that must be adhered to by the non- employee. The leader responsible for the non-employee is accountable for all actions taken by the non-employee. All non-employee systems access should be limited to information necessary for specific business purposes and should be in accordance with the requirements set forth in the Non- Employee Access Standards and the contract governing the work.
- All Choice Equity Broking Pvt. Ltd. (Choice) information systems privileges shall be disabled within 24 hours of receipt of the termination request, unless otherwise it is stated to disable the access on the last day of the employment or any specific day of employment.

Access Logs

- Access logs for critical assets/ infrastructure shall be monitored and reviewed on near real time basis. In case of security breaches, Incident shall be reported to the Chief Information Security Officer (CISO) as well.

Managing User IDs

- User Ids shall follow a standard naming convention for all computer systems to facilitate user identification. Naming conventions shall cover all end users, contractors, consultants and vendors. Generic IDs shall not be used.
- Access to information services shall be controlled by using unique user Ids, wherever possible, which shall enable:
  - individual accountability
  - permit centralized identification of users
  - aids in timely control of potential threats
- The application / system administrators are responsible for identifying inactive accounts and disabling them. If a user account has been inactive for more than 30 days, the application / system administrator shall disable the account after confirmation from the respective LOB Heads. The application / system administrator

shall reactivate the account only after receiving a written request from the user and approval regarding the same from his LOB Head.

- "Guest" accounts and other default accounts shall be disabled on all servers.

Each user is personally responsible for the usage of his or her user ID and password.

Password Management

User authentication refers to the methods by which a user proves his or her identity. All users must be positively identified prior to using any computer or communication system resources. Traditional user authentication consists of a user ID/password.

The authentication process verifies the identity of a user attempting to access a system. The process uses one or more of three tests to determine if the user is the authorized user.

Passwords are confidential information and are the most commonly used security tool in company systems. Each user is responsible for maintaining and protecting the passwords, PINs, and tokens used for system access. As they become available, enhanced authentication methods may be used. A good password is the best defense against inadvertent or malicious damage to computer programs and company data. If passwords can be easily guessed or viewed, or if there are not sufficient integrity controls, a perpetrator can break into company systems and gain access to the business data. If a legitimate user ID/password is used to gain access, the breach can go undetected long enough for the perpetrator to do damage.
Organization would promote strong password controls and ensure the controls are updated from time to time as per security recommendations.

- An initial password shall be provided to the users in a secure manner during the user creation process and the system shall be configured to force the users to change the initial password immediately after the first logon.
- Passwords shall be conveyed to users in a secure manner. Passwords shall never be disclosed through third parties or through unprotected (clear text) electronic mails.
- Password constraints and account policy shall be enforced for all user and administrative accounts on operating systems, applications, databases and all other information protected by passwords controls. The controls enforced shall be:
    - Passwords shall be at least eight characters in length
    - Password shall be a mix of alphabets, numerals and special characters
    - Password shall not be a part or same as username or user Ids
    - New password shall not be same as of the previous 4 passwords (Password history)
    - Passwords shall not be transmitted over the network without encryption
- Minimum password age shall be 3 days. In Active Directory, at user level, password expiry shall be set to ‘Never Expiry’. Additionally, multi-factor authentication shall be enabled on available accounts. Non-AD integrated application specific password shall continue to have expiry period of 60 days.
- Users shall not choose passwords, which can be easily guessed such as the user’s name, car registration number, telephone number, birth date etc.
- Account shall be locked out after 3 consecutive failed access attempts. For unlocking the user account, user may choose the self-service option or contact Service Desk. Positive user identification is mandatory before any account is unlocked by Technology or by an automated system.

- In case the user has forgotten the password, the user needs to reset the password
- Password shall be changed immediately if a user suspects that the password is leaked or compromised.
- All vendor-supplied default passwords (or other alternative access mechanisms) shall be changed before any computer or communications system is used for any Choice Equity Broking Pvt. Ltd. (Choice) business activity beyond initial evaluation in a test environment. These standards apply to passwords associated with end-user user IDs, as well as passwords associated with systems administrator and other privileged user IDs.
- Locked account shall be automatically unlocked by the system after 30 minutes.
- Users shall not share their password with anyone, including their reporting supervisors or colleagues.
- Passwords should not be written down or left in a place where unauthorized persons might discover them.
- Passwords shall not be stored unencrypted format in system resources.
- Appropriate procedures shall be put in place for storing and management of administrative passwords for critical information systems.
- Due to system limitations or business necessity if any of the password or logical access control policy cannot be followed, associated risk should be brought the attention of the management, and exception shall be documented. Compensating controls shall be put in place to mitigate the associated risk.

Ensuring Logical Security on Laptops and Desktops

Securing Information on Laptops and Desktops

- The folders or disk drives in individual desktops or laptops shall not be shared unless appropriate access controls have been enabled on the folder or the disk drive. Sharing of any information classified as ‘confidential’ is not permitted unless authorized by concerned authority.
- Prior LOB Head approval shall be required to use any removable devices like floppy drives, CD Writer etc.

Controlling Privileged User IDs

Use of privileged user IDs

- User ids with high-level access privileges (administrators) shall only be used in the event of emergency.
- System Administrator shall logon using their normal user Id when performing regular work duties rather than logging in as the administrator. Use of Administrator profile shall be limited to administrative activities only.
- User id’s with privilege access shall be managed with PAM tool.
- All emergency actions, which bypass normal access control procedures, shall be logged and reported for immediate review by delegated authority.

Use of Generic IDs

- Local logon rights should be disabled for generic system ID’s
- Generic ID’s should not have system or security administration authority
- All interactive login methods (FTP, telnet, rexec, SSH, etc.) should be disabled for such user ID’s by either:
    - Denying access to the user rights: 'Access this computer from network' and 'Logon through Terminal Services' OR
    - Another method that disables interactive login methods for the given service or protocol
- If the password for such user ID is hardcoded in a file, the same needs to be encrypted and should not be in clear text.
- Id owner details should be established so ownership is documented for accountability

Use of Privileged utility programs

Sensitive system utilities are the utilities which give unrestricted access to the critical system resources. The sensitive system utilities include but not limited to Format, User addition / deletion / update, Change in Network Settings.

Restricting Use of System Utilities

- Access to system utilities shall be restricted to authorized personnel in accordance with their business functions and needs.
- All unnecessary sensitive utilities shall be removed / disabled from the system.
- The use of all system utilities shall be logged and regularly reviewed by the Technology team.
- It shall be ensured that normal users do not have access rights to use utilities. Any backend update to the data using SQL / similar utilities shall be done only after approval of credential request over email.
- System utilities shall be separated from application software.

1.5.0 Extended Authentication

When using an offsite remote/external connection to company systems or networks, there are different user authentication requirements based on the role used and the information desired.

A User ID and password is required when employees are accessing information about themselves in their role as a customer, providing access to information such as insurance mutual funds, demat account, etc. In order to access employee human resources application such as online pay stub, leaves, performance etc, a second User ID and password will be required.

1.6.0 Session Management and Data Movement

Session security controls are a combination controls used to limit access appropriately. Such controls may include:

- Individual user - Identification, Authentication
- Logical grouping - Authorization by membership in a group
- Perimeter - Managing user and system traffic between the public and the company’s restricted internal use network.

1.7.0 Unauthorized Access

- Accessing Information Systems - Users using corporate computer systems shall access or attempt to access only those information systems and networks for which they have been granted access to perform their job functions.

- Damaging Information Systems - Users using Choice Equity Broking Pvt. Ltd. (Choice) computer networks shall not engage in activities that damage, disrupt or interfere with the operations of multi-user information systems to which they are connected.

- Circumventing Access Control Mechanisms - Programmers and other users must refrain from installing trap doors that circumvent the authorized access control mechanisms found in operating systems and/or access control packages. Shortcuts bypassing systems security measures, as well as pranks and practical jokes involving the compromise of systems security measures are prohibited.

- Customer Requests to Compromise Security Mechanisms - Requests to compromise Choice Equity Broking Pvt. Ltd. (Choice) security mechanisms must NOT be satisfied unless (a) the Chief Operating Officer provides written approval in advance, or (b) Choice Equity Broking Pvt. Ltd. (Choice) is compelled to comply by law, or (c) is ordered in writing to do so by its General Counsel and CEO.

- Social Engineering - A social engineer is an unauthorized person who impersonates an authorized user. The social engineer will use personal charm, manipulation or inside knowledge to persuade the authorized person that he or she is legitimate. The social engineer asks an authorized company user to do something that should not be done for an unauthorized person. Employees must not give company confidential, restricted internal use, or non-restricted internal use data or access information to unidentified persons. Any actual or suspected Social Engineering attempt must be reported to Technology Team.

- Compromising Security Measures - Incidents involving system cracking (hacking), password cracking (guessing), file decryption, software copying, or similar unauthorized attempts to compromise security measures may be unlawful and will be considered serious violations of this policy.

2. INTERNET USAGE POLICY

1.0 Purpose

The purpose of policy is to define authorized use of the Internet using Choice Equity Broking Pvt. Ltd. (Choice) resources in order to minimize the risks arising from the use of the Internet.

2.0 Scope

This policy applies to the employees of Choice Equity Broking Pvt. Ltd. (Choice) and all personnel who use the Internet using Choice Equity Broking Pvt. Ltd. (Choice) resources. It also applies to those who represent themselves as being connected with Choice Equity Broking Pvt. Ltd. (Choice) Information Technology Network. This includes contractors, consultants, third-party associates and any temporary employees.

3.0 Policy

3.1 Internet Use

3.1.1 Access to Internet

3.1.1.1 Basic Access

- Choice Equity Broking Pvt. Ltd. (Choice) shall provide the employees with Internet access based on the organizational policy.
- Further there can be exceptions for specific line of business (LOB) or special user profiles
- Internet access to the employees shall be controlled through appropriate security measures like firewall and proxy server.
- All users shall use only approved internet browser for accessing the internet sites
- Users should be aware that Choice Equity Broking Pvt. Ltd. (Choice) accepts no liability for their exposure to offensive material that they may access via the Internet.
- The ability to connect to a specific website does not in itself imply that users are permitted to visit that site. Users are always expected to comply with this policy and not to access the internet in such a way such that it will be in noncompliance with the clauses mentioned in section '3.1.2 Unauthorized use of internet' within Internet Security Policy.
- Consistent & secure internet access shall be provided to users regardless of the location they connect from.
- The access to social media sites is monitored with history tracking using a firewall.
- The access to cloud based internet storage sites is monitored with history tracking using a firewall.

3.1.1.2 Additional Access

- Users may use additional outbound services like SSH instead of telnet/rlogin and SFTP instead of FTP. SSH is a powerful service that allows secure communication for users to establish remote connection with an external host. SFTP allows secure communication for users to retrieve and store files on external hosts.

- The facility to access additional outbound services (SSH or SFTP) must be provided to users only after the approval from respective LOB Head based on the valid business needs.

3.1.2 Unauthorized use of internet

- Activities carried out using Choice Equity Broking Pvt. Ltd. (Choice)computing facilities or equipment which may lead to abusive, unethical or “inappropriate” use of the internet shall be considered grounds for disciplinary, legal and/or punitive actions. Examples of prohibited internet use include, but are not limited to, the following:
    - Introduce material considered indecent, offensive, or is related to the production, use, storage, or transmission of sexually explicit or offensive items on Choice Equity Broking Pvt. Ltd. (Choice)’s network or systems, using Internet
    - Users accessing internet using computers of Choice Equity Broking Pvt. Ltd. (Choice)shall not access the same through sources other than authorized Choice Equity Broking Pvt. Ltd. (Choice)internet access gateways (e.g., dial-up modem connection to VSNL, MTNL, Satyam, or other third-party Internet service providers)
    - Conduct illegal activities, access or download pornographic material
    - Enter into contractual agreements via the internet, e.g. enter into binding contracts on behalf of Choice Equity Broking Pvt. Ltd. (Choice)over the internet unless approved by legal department and LOB Head in writing
    - Solicit for any purpose which is not expressly approved by company management
    - Use Choice Equity Broking Pvt. Ltd. (Choice) logos or Choice Equity Broking Pvt. Ltd. (Choice) materials in any webpage or internet posting unless it has been approved, in advance, by Choice Equity Broking Pvt. Ltd. (Choice) management. Reveal or publicize proprietary or confidential information. Represent personal opinions as those of Choice Equity Broking Pvt. Ltd. (Choice)
    - Use software files, images, or other information downloaded from the internet that has not been released for free public use
    - Upload, download or installation of any commercial software, shareware or freeware in violation of the product copyright or in violation of Choice Equity Broking Pvt. Ltd. (Choice) authorized software list
    - Make or post indecent remarks. E.g. malicious written attacks directed at someone or similar written attacks
    - Download any software or electronic files without reasonable updated virus protection measures in place, as approved by Technology team.
    - Intentionally interfere with the normal operation of any Choice Equity Broking Pvt. Ltd. (Choice) internet gateway
    - Attempt to gain illegal access to remote systems on the internet
    - Attempt to inappropriately telnet to or port scan remote systems on the internet
    - Use or possess internet scanning or security vulnerability assessment tools, such as Nessus, SATAN or ISS etc., without the explicit permission from CISO.
    - Establish Internet or other external network connections that could allow non-Choice Equity Broking Pvt. Ltd. (Choice)users to gain access into Choice Equity Broking Pvt. Ltd. (Choice)systems and information assets
    - Spoofing the identity of another user on the Internet or on any Choice Equity Broking Pvt. Ltd. (Choice)communications system is forbidden.

  - Prohibited use of online chatting, blogging and social networking sites except Choice Equity Broking Pvt. Ltd. (Choice)'s approved sites.

- Users should be aware that Choice Equity Broking Pvt. Ltd. (Choice)accepts no liability for their exposure to offensive material that they may access via the Internet.
- The ability to connect with a specific website does not in itself imply that users of Choice Equity Broking Pvt. Ltd. (Choice) systems are permitted to visit that site. Appropriate filtering should be enabled to block access to prohibited applications, sites etc. using methods such as blocking identified applications, known URLs, and their related IP addresses.
- All above cases shall be prosecuted as per the disciplinary policy described in the Personnel Security.

3.1.3 Downloading and Uploading of Software

- The users are not allowed to upload to Internet without prior approval from LOB Head or Head - Technology. Upload should be done only if there is some business requirement.
- The users can download from legitimate approved websites only.
- Trial versions of software must be deleted immediately after the expiry of trial period.

3.1.4 Internet Security Education

- Information security awareness sessions should include the awareness about internet security. The training must cover downloading of information and software, mobile code (Java, ActiveX), acceptable use of Internet, etc.

3.1.5 Website Blocking

- Proxy server shall be configured to block the users from accessing websites that are deemed inappropriate.

3.1.6 Auditing, Logging and Monitoring

- All access to Internet services must be logged.
- The log files should be periodically reviewed.

3. DATA BACKUP & RESTORATION POLICY

1.0 Purpose

Choice Equity Broking Pvt. Ltd. (Choice) and its subsidiaries, associates, and entities (collectively referred to as 'Choice')

This policy defines the backup strategy for the data hosted in the application and database servers whose backup needs to be taken. This policy is designed to protect data in the organization to ensure that it is not lost and can be recovered in the event of an equipment failure, intentional destruction of data, or disaster.

All necessary software and data shall be backed up regularly in order to ensure that each application and its data can be recovered in the event of systems failure, loss of service, or loss/corruption of data.

2.0 Scope

This policy applies to all employees, contractors, consultants, and temporary staff etc. who have access to Choice resources. All are expected to be familiar with and comply with this policy.

The scope of this policy also includes users' critical data, server data, application etc.

3.0 Policy

3.1 Responsibility

- Application / information owner or respective LOB Head shall identify the data which shall be backed up along with the frequency and the retention period. System administrator from Technology shall ensure that backups are taken as per the schedule. The primary responsibility of data backup process shall remain with the application owner and primary responsibility of execution shall lie with Technology. Similarly, the operating system files and database configuration files shall be identified by the respective system/database administrators.
- Application owner with the help from system administrators, database administrators and application owners shall decide appropriate backup plan for each type of data identified taking into consideration importance of data, legal requirements, technology available, application requirements, nature of transactions etc.
- The Head–Technology shall delegate the members of the team to perform regular backups. The delegated persons (backup team) shall develop a procedure for testing backups and test the ability to restore data from backups on sampling basis quarterly and whenever requested by business.
- Any changes done to system which affects regular backup shall be prior informed to backup team by application owner.
- Users are responsible for backing up any data stored on local file system. All the important data shall be either copied on departmental file server or SharePoint/ One-drive to ensure the backup.

3.2 Documentation and Records

- Backup procedures shall provide the following information:
  - Files and applications to be backed up

  - o Inventory of backup media including the location of their storage and contents

3.3 Backup Media and Storage

- Backup media shall be clearly and distinctly numbered. A master list of all the numbered backup media will define the content stored on them. A list shall be maintained of usage life of all backup media.
- All data stored on the backup media shall be classified. Removable media shall be treated with the same or greater security precaution warranted by the classification of data it holds.
- External labels of tapes / cartridges / floppies / CDs etc. shall mention the information like date and label etc.
- Backup media shall be selected depending on the quantum of data, type of application software package, speed of backup and restoration, life of storage of the data, reliability requirement, efficiency, available technology and the guidelines in force.
- The backup media shall not be kept for storage in the same place where original data resides. A backup copy of all data shall be maintained at an identified off-site location. Offsite backup shall be maintained in fire resistant cabinet and shall be provided with appropriate physical security.
- All movement of backup media to the onsite backup storage room or to the offsite backup storage area shall be controlled and logged for future reference.
- Access to backup media will be restricted on a ‘need to know’ basis. Access shall be provided only after approval from application / information owner.
- Storage media will be destroyed when not needed and evidence of destruction maintained. The media containing the backups shall be preserved and retained to a minimum period of as required under any relevant regulations.
- In case the backup media is to be changed with a new technology, the latest backup shall be converted to the new media in one copy. The backup software also shall be backed up into another media and kept or have compatibility with the new system.

3.4 Restoration Testing

- For all backup media, a restoration test shall be carried out on sampling basis quarterly and whenever requested by business
- The restoration test plan shall be documented. Records shall be maintained of the restore results. The restored data shall be removed from the test server.
- Recovery procedures as defined by application owners shall ensure the relevant files are restored in order to ensure full application functionality is restored.
- While restoring the files and directories, it shall be ensured that access permissions are not changed or corrected after restoration is complete.
- Logging of restore operation shall be enabled and logs screened to check errors during the restore operation and if the files have been completely restored.
- The restored data shall be removed from the test machine after the activity is concluded. All media with unsuccessful test shall be disposed appropriately. The application / information owner shall be informed of the same and fresh backup taken accordingly.

4.0 Exceptions

- Exceptions shall not be universal but shall be agreed on a case-by-case basis, upon official request made by the information owner. These may arise, for example, because of local circumstances, conditions or legal reason existing at any point of time.

- All exceptions during implementation shall be submitted by the concerned person responsible for implementation. These shall be submitted through the Exception Form and sign-off on the same shall be maintained as per the below grid.

Risk Acceptance Criteria

Action	**High/Medium**	**Low**
Reviewer	Level 1 – Business Unit CTO Level 2 – Business Unit Compliance Team	Business Unit CTO
Approver	Business Unit COO	

4. MOBILE DEVICE POLICY

1.0 Purpose

Choice Equity Broking Pvt. Ltd. (Choice) and its subsidiaries, associates, and entities (collectively referred to as 'Choice').

The policy aims at providing guidelines to authorized users on usage of Choice supported Mobile devices for permitted corporate services.

2.0 Scope

This policy applies to users authorized to use corporate or personally owned (BYOD) mobile devices. Mobile devices currently scoped as part of this policy are limited to the following:

Apple iOS 11.0 and later
Apple iPad OS 13.0 and later
Mac OS X 10.14 and later
Android 5.0 and later (including Samsung KNOX Standard 2.4 and higher)

Corporate mobility services provisioned under corporate mobile devices policy are:

Email services
Outlook Contacts
Outlook Calendar
Business Applications
Corporate Collaboration Tools

Note: Above services shall only be provisioned via MDM (Mobile Device Management)/ MAM (Mobile Application Management). MDM/ MAM is security software that helps administer mobile device and protects corporate services/data published over mobile device with below controls:

- Protection against Jailbroken/Rooted device – MDM/ MAM detect and restrict installation of corporate application on rooted or jailbroken devices.
- Protection against unauthorized access - In case where a user does not implement screen lock, MDM/ MAM can use a policy in order to prevent data theft or unauthorized application usage.
- The corporate data is not accessible outside the MDM/ MAM container. It protects the data stored in the devices by access control policies
- Current/Updated app on all endpoints – Reduces pain of IT & user on installing updated app .Ensure all the endpoints with current/updated app.
- Data wipe – For resigned/unwanted employees or stolen devices.

3.0 Policy for Corporate Devices

3.1 Eligibility

- For existing employees, user will be required to raise a Logit ticket for corporate mobile device
- For new joiners, corporate mobile device may be allocated based on Logit raised by HR

3.2 Device Provisioning

- Users seeking corporate mobility service can avail the services on their personal device with appropriate versions of mobile device (as defined in scope – 2.0).
- The user's device should meet the pre-requisites and should not be rooted or-jail broken.
- A user can only have one device configured under this policy.

3.3 Device Configuring

- Corporate Devices
  - Technology Mobility team shall be responsible for configuring of corporate devices to eligible users.
  - Procurement/ Purchase/ Asset team hands over the corporate device to Technology Mobility team
  - Technology Mobility team configures the device as per corporate policy and hands over the device to user.

- Personal Devices
  - Users are required to download the company portal application and register the device
  - Users are expected to complete the configuration process by following on-screen instructions
  - User shall backup the data prior configuration. Technology Mobility team will not be responsible for any data loss that happens during the configuration of corporate mobile services.

3.4 Pre-requisites

- For personal device, please refer Section 2.0.
- Data services must be available on the device to allow Technology Mobility team to provision the corporate services.

3.5 Responsibilities

- Technology Mobility team shall be responsible for providing support for authorized corporate service devices only
- Technology Mobility team shall not be responsible for the accessories, service fees or charges incurred due to personal use of company-provided equipment or services, and any other related billing costs
- User shall be responsible and accountable for storing any personal or company's sensitive, proprietary or confidential information on the device under this policy.
- User shall be responsible for physical safeguarding of the mobile device.

3.6 Appropriate usage policy for corporate service device

- The user shall not use this mobile device for business activities that mandate certain safeguard / protocol to be followed in accordance with prevailing laws including but not limited to, call recording, logging, monitoring etc.

- User shall refrain from malicious downloads and storage on this device
- Users shall not install any unauthorized software (i.e hacking, cracking etc.) on the devices under this policy
- Users shall not leave the devices unattended anytime
- Users shall not share the device passwords with anyone
- When travelling devices would be kept within close view and shall not be left unattended at any point in time to avoid theft.
- In the event, if the device (company provided or personal) is lost or stolen, users are required to report the incident to Technology Mobility team immediately. These actions shall ensure that appropriate steps are taken to remotely wipe information residing on the device.
- The user shall not be allowed to create backup of the data on an unauthorized device.
- In case of violation, corporate services will be discontinued by the Technology Mobility team without any prior notice to the user.

3.7 Support Service Levels

- For corporate service mobile devices, Technology Mobility team would be responsible for supporting corporate applications/services only.

3.8 Exit User

- In cases where the user exits through the resignation or termination process, Technology Mobility team would remotely remove/wipe the MDM container. This activity would not impact the user’s personal data stored anywhere outside the MDM container.
- For all the Apple devices, it is mandatory for the users to support the Technology Mobility team to delete their Apple ID/Profile so that the devices can be used / accessible by the Technology Mobility team.

3.9 Violation

- Any Violation of the policy, or any of its tenets, could result in disciplinary action which may even lead to and include termination of employment and civil and/or criminal prosecution under local, state and federal laws.

4.0 Exceptions

- Exceptions shall not be universal but shall be agreed on a case-by-case basis, upon official request made by the information owner. These may arise, for example, because of local circumstances, conditions or legal reason existing at any point of time.

- All exceptions during implementation shall be submitted by the concerned person responsible for implementation. These shall be submitted through the Exception Form and sign-off on the same shall be maintained as per the below grid.

Risk Acceptance Criteria

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

5. REMOTE ACCESS POLICY

1. Purpose

The purpose of this policy is to define rules and requirements for connecting to Choice Equity Broking Pvt. Ltd.'s network from any host. These rules and requirements are designed to minimize the potential exposure to Choice Equity Broking Pvt. Ltd. from damages which may result from unauthorized use of Choice Equity Broking Pvt. Ltd. resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical Choice Equity Broking Pvt. Ltd. internal systems, and fines or other financial liabilities incurred as a result of those losses.

2. Scope

This policy applies to all Choice Equity Broking Pvt. Ltd. employees, contractors, vendors and agents with a Choice Equity Broking Pvt. Ltd.-owned or personally-owned computer or workstation used to connect to the Choice Equity Broking Pvt. Ltd. network. This policy applies to remote access connections used to do work on behalf of Choice Equity Broking Pvt. Ltd., including reading or sending email and viewing intranet web resources. This policy covers any and all technical implementations of remote access used to connect to Choice Equity Broking Pvt. Ltd. networks.

3. Policy

It is the responsibility of Choice Equity Broking Pvt. Ltd. employees, contractors, vendors and agents with remote access privileges to Choice Equity Broking Pvt. Ltd.'s corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Choice Equity Broking Pvt. Ltd..

General access to the Internet for recreational use through the Choice Equity Broking Pvt. Ltd. network is strictly limited to Choice Equity Broking Pvt. Ltd. employees, contractors, vendors and agents (hereafter referred to as “Authorized Users”). When accessing the Choice Equity Broking Pvt. Ltd. network from a personal computer, Authorized Users are responsible for preventing access to any Choice Equity Broking Pvt. Ltd. computer resources or data by non-Authorized Users. Performance of illegal activities through the Choice Equity Broking Pvt. Ltd. network by any user (Authorized or otherwise) is prohibited. The Authorized User bears responsibility for and consequences of misuse of the Authorized User’s access. For further information and definitions, see the *Acceptable Use Policy*.

Authorized Users will not use Choice Equity Broking Pvt. Ltd. networks to access the Internet for outside business interests.

4. Requirements

4.1 Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs)) and strong pass-phrases.

4.2 Authorized Users shall protect their login and password, even from family members.

4.3 While using a Choice Equity Broking Pvt. Ltd.-owned computer to remotely connect to Choice Equity Broking Pvt. Ltd.'s corporate network, Authorized Users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an Authorized User or Third Party.

4.1.1 Use of external resources to conduct Choice Equity Broking Pvt. Ltd. business must be approved in advance by InfoSec and the appropriate business unit manager.

4.1.2 All hosts that are connected to Choice Equity Broking Pvt. Ltd. internal networks via remote access technologies must use the most up-to-date anti-virus software, this includes personal computers. Third party connections must comply with requirements as stated in the *Third Party Agreement*.

4.1.3 Personal equipment used to connect to Choice Equity Broking Pvt. Ltd.'s networks must meet the requirements of Choice Equity Broking Pvt. Ltd.-owned equipment for remote access as stated in the *Hardware and Software Configuration Standards for Remote Access to Choice Equity Broking Pvt. Ltd. Networks*.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. BRING YOUR OWN DEVICE (BYOD) POLICY

1. Background

Choice Equity Broking Pvt. Ltd. and its subsidiaries, associates, and entities (collectively referred to as ‘Choice’)

This Bring Your Own Device Policy **(‘the Policy’)** is applicable to all individuals (hereinafter referred to as **Choice Users**) of Choice and its subsidiaries and associate entities in India and overseas (collectively referred to as **Choice**, at all levels and grades, whether regular, fixed term or temporary, without exception.

Choice grants the Choice Users the privilege of using their Personal Electronic Devices (‘PEDs’) for work related purposes, for their convenience. Choice reserves the right to revoke this privilege if Choice users do not abide by the procedures outlined in this policy. Choice users must agree to the terms and conditions set forth in this policy in order to be able to connect their PEDs to the Choice network.

This Policy is intended to protect the security and integrity of Choice data and technology infrastructure.

2. Scope

This Policy includes within its scope the following PEDs:

- Personal laptop/desktop to connect office desktop via Arcon
- Personal laptop/desktop to connect Azure Virtual desktop
- Personal laptop/desktop for accessing O365 and internal applications using Windows 10
- Above list is indicative and may be limited based on compatibility of technology.

3. Policy

3.1 Authorisation

Choice Users needs to seek the consent from LOB Head to use their PED for work purposes.
For new joinees, HR Relationship Manager shall take the required approval from LOB Head.

3.2 Acceptable Use

a) Acceptable business use is defined as activities that directly or indirectly support the business of Choice.

b) Acceptable personal use on Choice time is defined as reasonable and limited personal communication or recreation, such as reading or game playing.

c) While at work, Choice Users are expected to exercise the same discretion in using their PEDs as is expected for the use of company devices. Choice policies pertaining to anti harassment, anti discrimination, anti retaliation, protection of trade secrets, protection of confidential information and ethics apply to the use of PEDs for work-related activities.

d) PEDs with valid license operating system should only be used for BYOD

e) PEDs should not be used at any time to:
   a. Store or transmit illicit materials
   b. Store or transmit proprietary information belonging to another company
   c. Harass others
   d. Engage in outside business activities

f) Users may use their mobile PEDs to access the Choice-owned resources such as email, calendars, contacts, documents, etc.

3.3 IT Support

g) For personal owned laptop/desktop connectivity issues, operating system or hardware-related issues, Choice User should contact their own vendor for resolution.

h) Functionality issue of O365 and Choice' internal applications will be supported by Choice.

i) For issues with Choice' remote owned laptop/desktop or virtual machines, Choice User should contact Choice for technology support.

3.4 Security

j) In order to prevent unauthorized access, PEDs shall be password protected using the features of the PED and a strong password

k) Multi factor authentication shall be enabled

l) On PEDs, Windows 10 operating system should be install

m) Choice Users access to Choice' data shall be limited, based on user profiles defined by IT and automatically enforced.

n) For accessing O365, Windows Information protection (WIP) & Azure Information Protection (AIP) policy shall be enabled

3.5 Lost, stolen, hacked or damaged equipment

o) Choice Users are expected to protect PEDs used for work-related purposes from loss, damage or theft.

p) Choice will not be responsible for loss or damage of personal applications or data resulting from the loss of PED's. Choice Users must immediately notify management in the event their PED is lost, stolen or damaged.

q) In case of loss IT will wipe off the data remotely.

r) Choice Users may receive disciplinary action up to and including termination of employment for data leakage that is caused willfully.

- **Termination of employment**

Upon resignation or termination of employment, or at any time on request, the Choice User may be asked to produce the PED for inspection. All Choice data on PEDs will be removed by IT upon termination of employment.

3.6 Privacy/ Monitoring

s) No staff using the PED should expect any privacy requirements except that which is governed by law.

t) Choice has the right, at any time, to monitor and preserve any communication that uses the Choice' network in any way, including data, voice mail, telephone logs, Internet use and network traffic, to determine proper use.

u) Choice reserves the right to review or retain personal and Choice-related data on PEDs or to share the data with government agencies or third parties during an investigation or litigation. Choice may review the activity and analyse usage patterns and may choose to publicise this data to ensure that Choice' resources in these areas are being used in accordance with this Policy. Furthermore, no staff may knowingly disable any network software or system identified as a monitoring tool.

v) Choice reserves the right to disconnect any of the PEDs or disable any of the services without notification to the Choice User/s.

4. Review of Policy

This Policy shall be reviewed at least once in a year or earlier as may be required

5. Exception

Any deviation to this Policy should be properly documented and COO approval is needed on the same. Deviation will be there for a specific period of time.

7. PHYSICAL AND ENVIRONMENTAL SECURITY POLICY

1. Purpose

Physical and environmental security policy addresses measures for securing information processing facilities and information assets from unauthorized access, damage or interference or any natural calamities.

2. Scope

This policy and any other associated guidelines apply to the employees of Choice Equity Broking Pvt. Ltd. (Choice) and any person having access to physical assets of Choice Equity Broking Pvt. Ltd. (Choice). This could include contractors, consultants, third-party associates and any temporary employees and covers physical access to computing facilities, hardware, corporate data, application and systems software. These facilities include server rooms / data centers, network control centers and other related areas. Physical access scope is under Admin department and rest is with IT.

3. Policy

3.1 Physical Security

3.1.1 Physical Entry Controls by Admin

- Choice Equity Broking Pvt. Ltd. (Choice)shall have a well-defined and secure perimeter.
- All doors shall be locked, when unattended or beyond working hours.
- Security guards shall be placed at minimum, at entry points of the premises at all times.
- The date and time of entry and departure of visitors shall be recorded, and all visitors shall be supervised unless their access has been previously approved; they shall only be granted access for specific, authorized purposes. The identity of visitors shall be authenticated by appropriate means; Directories and internal books or layout plans identifying locations of organizational information processing facilities shall not be readily available or accessible to the public.
- A physical log book or electronic audit trail of all access shall be securely maintained and shall be reviewed as per the need.
- All employees, contractors and external parties shall be required to wear some form of visible identification and shall immediately notify security personnel if they encounter unescorted visitors and anyone not wearing visible identification.
- External party support service personnel shall be granted restricted access to secure areas or confidential information processing facilities only when required; this access shall be authorized and monitored.
- Access rights to secure areas shall be annually / Admin/ Admin reviewed and updated, and revoked when necessary.

3.1.2 Protocol during Pandemic

Office entry control & checks will be amended in line with Govt./equivalent authority’s guidelines.

3.1.3 Physical Entry Controls

Technology Team shall ensure access to areas where confidential information is processed or stored (e.g. Data Centers) shall be restricted to authorized individuals only by implementing appropriate access controls.

3.1.4 Security of Office and Facilities

- Admin shall ensure,
  - o Facilities to be set up to prevent confidential information or activities from being visible and audible from the outside-area
  - o The place where information-processing equipment is located shall be secured from theft, physical intrusion and environmental hazards.
  - o Incoming and outgoing mail (sealed documents/parcels) must be protected from unauthorized use during and outside normal working hours.
  - o A gate pass shall be issued for outgoing material. Security Personnel at the entry gate shall not allow any material outside without appropriate gate pass.

- Technology Team shall ensure
  - o Support functions and equipment's e.g. photocopiers, shall be sited appropriately within the secure area to restrict access, which could compromise information. Any equipment shall be taken outside only after an approval from the reporting authority of the asset owner and the Administration department. A written approval shall be obtained for the same and shall be produced to the security personnel on demand.

3.1.5 Security of Office and Facilities

- IT shall ensure
  - o Printer memory shall be cleared immediately after printing any documents classified as 'Confidential'.
  - o Details of movement of hardware equipment between offices shall be recorded to facilitate easy tracking of inventory and identification of hardware for disposal / buy back or write off.

3.1.6 Securing Access to Secure Areas (Server Rooms, Data Center)

- Technology Team shall ensure

o All critical servers and communications equipment shall be located in secure locked rooms (referred as secure areas) to prevent tampering and unauthorized usage.

o Additional controls (like access cards shall be in place to secure critical or sensitive information. Access to secure areas shall be strictly controlled e.g. access to server rooms shall be controlled and restricted to authorize personnel like server and database administrators who need to perform their duties.

o Signs indicating "Authorized Personnel Only" or a similar message shall be prominently posted at all entrances of secure areas.

o Knowledge or access to the "secure areas" [example: server room, UPS room, trading room etc.] shall be given to employees or third parties on a “need-to-know” basis.

  - Secure areas shall not be visible or identifiable from the outside; i.e. there shall not be any directional signs providing access to such rooms.
  - Secure areas shall be equipped with CCTV systems. The tapes shall be retained for a period of one month.
  - Emergency lighting shall be installed in the server rooms and other such sensitive areas for use during power outages.
  - Visitors and suppliers shall be allowed entry to secure areas with visitor pass for authorized and specific purposes only. Visitors or third parties shall not be permitted unsupervised access to secure areas.
  - A separate register shall be maintained at the entry gate of the secure areas for recording the entry of the people (Employee, vendor, contractors etc.) who do not have regular access to the secure areas. Any such entry to the secure areas shall only be provided after making an appropriate entry in the register.
  - Unsupervised working in secure areas shall be avoided both for safety reasons and to prevent opportunities for malicious activities;
  - Vacant secure areas shall be physically locked and periodically reviewed;

Deliver and loading areas

Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access. The following guidelines shall be considered:

- Access to a delivery and loading area from outside of the building shall be restricted to identified and authorized personnel;
- The delivery and loading area shall be designed so that supplies can be loaded and unloaded without delivery personnel gaining access to other parts of the building;
- Incoming material shall be inspected and examined for explosives, chemicals or other hazardous materials, before it is moved from a delivery and loading area;
- Incoming material shall be registered in accordance with asset management procedures on entry to the site;
- Incoming and outgoing shipments shall be physically segregated, where possible;
- Security to inform the requesting dept. of incoming material which should be inspected by representative of requesting dept. for any evidence of tampering enroute.

3.1.7 Securing access to the Trading & Dealing rooms

- Admin shall ensure
  - Access to trading and dealing rooms shall be strictly controlled. E.g. access to trading room shall be controlled and restricted to authorize personnel like Choice Equity Broking Pvt. Ltd. (Choice)traders who need to perform their duties.
  - Signs indicating "Authorized Personnel Only" or a similar message shall be prominently posted at all entrances of trading and dealing rooms with the help of Admin
  - Knowledge or access of the trading / dealing rooms shall be given to employees or third party on a “need-to-know” basis.
- Technology Team shall ensure

  - Mobile phone usage shall be prohibited inside the trading and dealing rooms. Secure Storage space for mobile phones shall be provided where traders and dealers shall deposit their mobile phone before entering the trading / dealing areas.

3.1.8 Securing the Premises from Visitors and Suppliers

- Employees shall wear the Photo ID badge provided by Choice Equity Broking Pvt. Ltd. (Choice) during their stay on Choice Equity Broking Pvt. Ltd. (Choice) premises.
- Employees not carrying the Photo ID badges shall not be allowed inside the premise without getting a temporary access card issued to himself / herself. The access card shall be issued after verifying the employee. When the card is issued, an auto-generated email alert shall be sent to the employee's reporting authority. When exiting the premise for the day, the employee shall return the card to the Security Guard in charge, failing to which an auto-generated email alert shall be sent to the employee and escalation to the reporting authority the subsequent day onwards till the card is returned.
- Visitors shall be advised to provide the following details so that the relevant details can be captured for records:
  - Visitor name
  - Company
  - Date
  - Time in
  - Contact details
  - Purpose of visit
  - Whom to meet (Person to be met)
- A visitor badge shall be allotted to every visitor, except VVIP/VIP visitors, eg. Visitors/guests of Manco.
- Employees shall not be authorized to take any visitor near areas demarked as sensitive within the premise. Visitor's entry shall be restricted to the meeting / discussion rooms only.
- Choice Equity Broking Pvt. Ltd. (Choice) personnel may seek information by questioning all unescorted visitors

3.1.9 Securing Information Storage Media

- Technology Team shall ensure
  - All information storage media (e.g. hard disks, floppy disks, pen drives, magnetic tapes and CD-ROMs) containing sensitive or confidential data shall be physically secured, when not in use.
  - Information storage media shall not be taken outside the computer room or storage area, unless specifically authorized.
  - Physical access to magnetic tape, disk and documentation libraries shall be restricted to authorized personnel only.
  - Back-up media shall be stored in fire resistant safes or cabinets.
  - Employees are not permitted to bring any personal information storage media like cartridge tapes, DAT drives, CDs, pen drives, or floppy drives unless specifically approved by LOB Head.
  - Visitors and third parties shall not be allowed to connect external storage devices to Choice Equity Broking Pvt. Ltd. (Choice) Network, unless authorized by Choice Equity Broking Pvt. Ltd. (Choice) officials.

- Media containing sensitive corporate information shall be monitored with audit trails.

3.1.10 Securing Offsite Facilities [Disaster Recovery Site]

- Technology Team shall ensure
  - Fall back equipment and back-up media shall be stored at a safe distance (at an offsite location) to avoid damage from disaster at the main site
  - The physical and environmental safeguards available at the off-site location shall provide the same level of security, at a minimum, as at the primary site.

3.1.11 Security Inspections

- Admin shall
  - Perform random physical security inspections shall be done at all sites and locations.
  - The results of all inspections shall be documented & appropriate action shall be taken.

CCTV Monitoring and Incident Investigation

The organization shall implement CCTV surveillance systems in critical areas, including but not limited to entry/exit points, server rooms, and other sensitive areas, to ensure the security of the premises and assets. The CCTV footage will be used solely for the purpose of monitoring physical security and safeguarding the organization's property and personnel.

Purpose of CCTV Monitoring:

To monitor and detect unauthorized access to restricted areas.

To ensure the safety and security of employees, contractors, visitors, and assets.

To assist in investigating security incidents, breaches, or suspicious activities within the premises.

Retention and Access to Footage:

CCTV footage will be stored securely and retained for a period of   days, unless required for ongoing investigations or legal purposes.

Access to CCTV footage will be strictly controlled and limited to authorized personnel, such as admin team, the Information Security team, or law enforcement, in accordance with the organization's data access policies.

Use of Footage for Incident Investigation:

CCTV footage may be reviewed and utilized for investigating any security incidents, including unauthorized access, theft, vandalism, or any other event that could impact the safety, security, or integrity of the organization.

In the event of a security breach, suspected criminal activity, or policy violation, CCTV footage will be used as a part of the incident investigation process to identify the cause, assess the impact, and support corrective actions.

Privacy Considerations:

The use of CCTV surveillance will be conducted in compliance with relevant privacy and data protection regulations, ensuring that it does not infringe on individuals’ rights to privacy.

Employees and visitors will be notified about CCTV monitoring through appropriate signage and communication.

Footage Disposal:

After the retention period, CCTV footage will be securely deleted, ensuring that it cannot be accessed or recovered, unless required for legal or regulatory purposes.

3.2 Environmental Security

3.2.1 Ensuring Suitable Environmental Conditions in Data Centre

- Technology Team shall ensure
  - Temperature and humidity levels shall be monitored and maintained, especially in Server /UPS Room.
  - Smoking shall be strictly prohibited inside the office area.
  - Eating and drinking inside server and UPS rooms shall be strictly prohibited.

3.2.2 Securing Premises from Fire

- Admin shall ensure
  - All computer systems shall be housed in an environment equipped with fire extinguishers
  - The fire extinguishers shall be placed at all strategic and prominent locations within Choice Equity Broking Pvt. Ltd. (Choice) office so that they are easily accessible in all areas.
  - Smoke detectors shall be located within the office premises including Server Room.
  - Fire safety equipment shall be checked regularly in accordance with manufacturer's instructions. A maintenance sheet / note shall be attached with the equipment.
  - All fire exits shall be marked clearly and shall be easily accessible from work sections.
  - Hazardous and combustible materials shall be stored at a safe distance from the server rooms and other computer rooms. Computer supplies such as stationery shall not be stored in server rooms.
  - Fire and emergency instructions (via building escape plan) shall be displayed at prominent locations.
  - Functioning and operations of the fire safety devices / equipments installed by Choice Equity Broking Pvt. Ltd. (Choice) shall be explained to the security guards periodically during internal training programs. Some of the Choice Equity Broking Pvt. Ltd. (Choice) employees shall also be made part of such internal training programs.
  - Evacuation drills shall be conducted annually to ensure the effectiveness of the training and instructions to be followed in case of emergency.

3.2.3 Securing Premises from Floods and Water Damage-

- Technology Team shall ensure
  - Computer and communication rooms shall not be located in areas like basements which are susceptible to water seepage and flooding.

    - Computer and communication rooms shall be located on raised or elevated floors.
  - Admin shall ensure
    - Adequate drainage provision shall be provided to prevent water damage or flooding.
    - Water sprinklers shall not be installed in server rooms / storage rooms etc.
    - Electrical equipment, damaged due to water, shall be checked and dried before being returned to service.

3.2.4 Power Supplies

3.2.4.1 Power Supply Controls

- Technology Team shall ensure
  - Uninterrupted Power Supply (UPS) shall be installed to ensure continuous running of all critical computing and supporting equipment at all locations. UPS shall have the capability to continue the power supply to allow for an orderly shutdown of the system.
  - UPS equipment shall be maintained in accordance with the manufacturer’s recommendations to ensure that it is in working condition.
  - Backup generators may be installed for continuous running of information processing systems in case of prolonged power failures. The generator shall be maintained as per the manufacturer’s instructions and shall be checked regularly for sufficient fuel supply.
  - All buildings shall have proper earthing to prevent electric surges.
  - Voltage regulators shall be installed, wherever necessary, to guard against fluctuations in power. Circuit breakers of appropriate capacity shall be installed to protect the hardware against power fluctuations or short circuits.
  - Lightning protection filters shall be installed for the buildings.

3.2.4.2 Power off Switches

- Admin shall ensure
  - Emergency power off switches shall be installed at strategic locations in order to facilitate rapid power-off in case of an emergency such as a fire.
  - The power-off switches shall be clearly labeled, easily accessible but shielded to prevent accidental activation.

3.2.2 Cabling Security

- Technology Team shall ensure
  - Power and telecommunication cables that connect various information processing facilities are exposed to many environmental hazards like sand storms, floods, fire, lightning, cutting due to careless digging or damage by rats and rodents. Cables carrying data or supporting information services shall be protected from interception or damage to reduce the risk of power or communication failure.

3.3 Cabling Standards

- Technology shall ensure
  - Power and telecommunication lines used for information processing facilities shall be laid underground, where possible, or subject to adequate alternative protection.
  - Network cabling shall be protected from unauthorized interception or damage due to environmental hazards e.g. by using conduit or by avoiding routes through public areas.
  - Power cables shall be separated from communication cables to prevent interference.
  - For sensitive or critical systems further controls to consider include:
    - Use of electromagnetic shielding to protect the cables.
    - Controlled access to patch panels and cable rooms.

3.4 Clear Desk Policy and Clear screen policy

- Technology Team shall ensure a clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted. The clear desk and clear screen policy shall take into account the information classifications (Ref: Information classification). The following guidelines shall be considered:
- Sensitive or critical business information, e.g. on paper or on electronic storage media, shall be locked away (ideally in a safe or cabinet or other forms of security furniture) when not required, especially when the office is vacated.
- Computers and Terminals shall be left logged off or protected with a screen and keyboard locking mechanism controlled by a password, token or similar user authentication mechanism when unattended and shall be protected by key locks, passwords or other controls when not in use.
- Unauthorized use of photocopiers and other reproduction technology (e.g. scanners, digital cameras) shall be prevented.
- Sensitive (Confidential/Internal) information and storage media shall be locked (in a fire resistant safe or cabinet), when not required.

3.5 Equipment Security

3.5.1 Equipment sitting and protection

Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. The following guidelines shall be considered to protect equipment:

- Admin shall ensure
  - Storage facilities shall be secured to avoid unauthorized access.
  - Environmental conditions, such as temperature and humidity, shall be monitored for conditions which could adversely affect the operation of information processing facilities.
  - Lightning protection shall be applied to all buildings and lightning protection filters shall be fitted to all incoming power and communications lines.
- Technology Team shall ensure
  - Equipment shall be sited to minimize unnecessary access into work areas.

- o Items requiring special protection shall be safeguarded to reduce the general level of protection required.
- o Information processing facilities handling sensitive data shall be positioned carefully to reduce the risk of information being viewed by unauthorized persons during their use Equipment processing confidential information shall be protected to minimize the risk of information leakage due to electromagnetic emanation.
- o Guidelines for eating, drinking and smoking in proximity to information processing facilities shall be established.

3.5.2 Supporting utilities

Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities. Supporting utilities (e.g. Fax, telecommunications, water supply, sewage, ventilation and air conditioning) shall:

- Conform to equipment manufacturer’s specifications and local legal requirements.
- Be appraised regularly for their capacity to meet business growth and interactions with other supporting utilities.
- Be inspected and tested regularly to ensure their proper functioning.
- If necessary, be alarmed to detect malfunctions.
- If necessary, have multiple feeds with diverse physical routing.

Admin shall ensure

- Emergency lighting and communications shall be provided. Emergency switches and valves to cut off power, water, or other utilities shall be located near emergency exits or equipment rooms.

3.5.3 Physical Security of Laptops and Desktops

- Technology Team shall ensure
  - A complete and up-to-date inventory of all laptops/desktops issued by the organization shall be prepared and kept updated at all times with the TSG. Each laptop/desktops shall be marked with the asset code for easy identification.
  - Laptops / Workstations shall be traceable to individual users.
  - Laptops and desktops shall be physically secured at all times to prevent unauthorized access or theft. Each individual shall be accountable for the physical security of his / her laptop / workstation / handheld devices.
- All Employees to whom laptops / handheld devices are issued are responsible for the security of the data contained within the laptops / handheld devices.

3.5.4 Equipment Maintenance

- Technology Team shall ensure
  - o All equipment shall be maintained to ensure its continued availability and integrity in accordance with manufacturer's specifications.
  - o Only authorized maintenance personnel shall be allowed to service or perform repairs on equipment. A log shall be maintained of all repairs or service work.
  - o Records shall be kept of all suspected or actual faults, and of all preventive and

corrective maintenance.

- If equipment needs to be sent offsite for repairs, the confidentiality and integrity of the information, stored in the equipment, shall be ensured. The entire data available on the equipment shall be backed up on a backup device and securely wiped from the equipment.
- All maintenance requirements imposed by insurance policies shall be complied with.
- Before putting equipment back into operation after its maintenance, it shall be inspected to ensure that the equipment has not been tampered with and does not malfunction.

3.5.5 Removal of assets

- Technology Team shall ensure
  - Equipment, information or software shall not be taken off-site without prior authorization. The following guidelines shall be considered:
  - Employees and suppliers who have authority to permit off-site removal of assets shall be identified.
  - Time limits for asset removal shall be set and returns verified for compliance.
  - Where necessary and appropriate, assets shall be recorded as being removed off-site and recorded when returned.
  - The identity, role and affiliation of anyone who handles or uses assets shall be documented and this documentation returned with the equipment, information or software.

3.5.6 Security of Equipment off Premises

- Technology Team shall ensure
  - Security be applied to off-site assets taking into account the different risks of working outside the Choice Equity Broking Pvt. Ltd. (Choice)'s premises.
  - Equipment and media taken off premises shall not be left unattended in public places.
  - Controls for off-premises locations, such as home-working, teleworking and temporary sites shall be determined by a risk assessment and suitable controls applied as appropriate, e.g. lockable filing cabinets, clear desk policy, access controls for computers and secure communication with the office.
  - When off-premises equipment is transferred among different individuals or external parties, a log shall be maintained that defines the chain of custody for the equipment including at least names and organizations of those who are responsible for the equipment.
  - Risks, e.g. of damage, theft or eavesdropping, may vary considerably between locations and shall be taken into account in determining the most appropriate controls.
  - Any equipment can be taken outside office premises only after written permission from the LOB Head.
  - Any equipment or media taken outside the organization's premises shall be controlled, secured, protected and insured.
  - Employees or contractors shall not remove any Choice Equity Broking Pvt. Ltd. (Choice) property off premises, without prior authorization.
  - A returnable / non-returnable gate pass shall accompany all property movement outside

Choice Equity Broking Pvt. Ltd. (Choice).

3.5.7 Secure disposal or re-use of equipment

- Technology Team shall ensure
  - All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.
  - Equipment shall be verified to ensure whether or not storage media is contained prior to disposal or re-use.
  - Storage media containing confidential or copyrighted information shall be physically destroyed or the information shall be destroyed, deleted or overwritten using techniques to make the original information non-retrievable rather than using the standard delete or format function.

3.5.8 Unattended user equipment

- Technology Team shall ensure
  - Users shall ensure that unattended equipment has appropriate protection. All users shall be made aware of the security requirements and procedures for protecting unattended equipment, as well as their responsibilities for implementing such protection. Users shall be advised to:
  - Terminate active sessions when finished, unless they can be secured by an appropriate locking mechanism, e.g. a password protected screen saver.
  - Log-off from applications or network services when no longer needed.
  - Secure computers or mobile devices from unauthorized use by a key lock or an equivalent control, e.g. password access, when not in use.

Annexure/Supporting (Applicable During Pandemic):

office entry is restricted to users – All employees have to submit their health declaration in the prescribed format provided by the Organisation (Currently it is on PowerApps and also in an excel for those who cannot access PowerApps), wherein they must confirm they are without any ailments comorbidities such as common illnesses/diseases, which can be linked to upper-respiratory system, eg. diabetes, blood pressure or any of the family member having these or any of these illness/diseases or has a child less than 2 years of age. The address also needs to be validated of the user coming from Containment / Non-Containment zone as defined by Government of Maharashtra.

- *Upon receipt of confirmation from the Incident Room to employee, Security, Facilities Team of respective office, clearing the entry protocol, the employee or visitor is allowed to enter in the premise to operate from office.*
- *Every employee is expected to follow the protocol of wearing a mask, wash hands frequently/sanitize hands, maintain social distance , so as to keep themselves and others safe whilst in the premise.*

8. PATCH MANAGEMENT POLICY

1.0 Purpose

To ensure that the patches are rolled out on the network in a controlled and secure manner.

2.0 Scope

All operating systems / applications / servers / desktops / network equipment identified in the Asset Register.

3.0 Responsibility

The Head – Technology for execution of this policy

Information Security team for auditing the policy

4.0 Policy

The minimum baseline security standards shall be reviewed from the point of view of various technical vulnerabilities and vendor’s recommendations for additional security patches and updated at least once in year or need basis.

4.1 Guidelines for implementation

- ISG shall document the baseline configuration of all IT assets identified in the asset inventory. The baseline is the minimum patch level required on the network. The baseline shall be based on Industry best practices and fine tuned to Choice Equity Broking Pvt. Ltd. (Choice) landscape.
- The baseline configuration shall be reviewed at least once in a year
- Once a baseline has been established, Technology team shall conduct a patch analysis. The analysis shall involve determining:
    - If all machines on the network meet the minimum baseline established
    - All available patches for the network and
    - Whether the patches are installed or missing on all machine
- Vulnerability assessment on the network shall also be carried out at least once in year. Technology team shall analyze the severity of vulnerabilities found and prioritize and schedule the patch rollouts required on the basis of the severity found.
- The regular updates received directly from the supplier shall also be maintained centrally and updated.
- Every patch to be deployed shall be tested before being rolled out onto the production environment on need basis. Technology team shall maintain a test plan with acceptance criterion and also develop a roll back strategy for the same. For applications, the roll back strategy will be provided by the internal / external vendor.
- Once successfully tested, the patch shall be deployed in the production environment during the maintenance window period. Technology team shall also ensure that the roll back plan is in place.
- Once the patch has been deployed, the team shall verify and confirm the successful application of the patch by logging on the system.

9. INFORMATION CLASSIFICATION POLICY

1.0 Purpose

To ensure that integrity and confidentiality of information is maintained, an information classification scheme has been designed for Choice Equity Broking Pvt. Ltd. (Choice). The level of security to be afforded to the information / data of Choice Equity Broking Pvt. Ltd. (Choice) is dependent directly on the classification of the information. All employees are expected to familiarize themselves with this information classification scheme, to consistently use it in their business activities.

2.0 Scope

This information classification scheme is applicable to all information including intellectual property (IP), whether stored or transmitted, which is in the possession or under the control of Choice Equity Broking Pvt. Ltd. (Choice). For example, confidential information entrusted to Choice Equity Broking Pvt. Ltd. (Choice) by its customers, suppliers, business partners, and others shall be protected with this information classification scheme. Similarly, the employees, contractors & service providers of Choice Equity Broking Pvt. Ltd. (Choice) are expected to protect third party information with the same care that they protect information belonging to Choice Equity Broking Pvt. Ltd. (Choice).

3.0 Policy

3.1 Information

Information is an asset which, like other business assets, has value to the organization and consecutively, needs to be protected. Information can be of any form as mentioned below:

- Printed or written on paper
- Stored electronically
- Transmitted by emails or any other electronic means
- Shown on corporate videos
- Spoken in conversation

3.2 Personal Information:

- Personally Identifiable Information (PII) is data that can be traced back to an individual and that, if disclosed, could result in harm to that person. Such information includes biometric data, medical information, personally identifiable financial information (PIFI) and unique identifiers such as passport or Social Security numbers.

- Information containing PII data shall be considered as confidential information and shall be protected using minimum baseline controls mention in Information classification policy.

- Personal information received / stored / sent by employees without any business reason will not be treated as confidential information. Safeguarding personal information stored on corporate systems shall be user responsibility. Any such personal information stored on corporate infra shall be accessed by Choice Equity Broking Pvt. Ltd. (Choice) only post management approval. e.g. Employees share personal data with HR to complete the HR formalities and forget to delete these records like PAN card, Salary slip from the corporate systems. Choice Equity Broking Pvt. Ltd. (Choice) shall not be liable to safeguard this data.

3.3 Business information:

Sensitive business information includes anything that poses a risk to the company in question of discovered by a competitor or the general public. Such information includes trade secrets, acquisition plans, financial data and supplier and customer information, among other possibilities.

- Information pertains to business is further classified to restrict the use or access the information based on its level of sensitivity (for example, confidential, internal and public). Information is generally classified to protect such information from unauthorized use.

Any information classified as confidential and internal shall be protected with minimum baseline controls as mentioned in information classification policy. Access / sharing of such information shall not be conducted without any business reason and appropriate approval. Information classified as public will have no control and restriction on disclosure and storage.

3.4 Intellectual Property (IP):

Choice Equity Broking Pvt. Ltd. (Choice) Intellectual Property includes anything that poses a risk to organization if discovered by a competitor or the general public. Such information includes trade secrets, algorithmic trading source codes / products, acquisition plans, financial data and supplier and customer information, among other possibilities. Such IP may be created by Choice Equity Broking Pvt. Ltd. (Choice) employees or contractors or consultants.

To protect intellectual property, maintain appropriate asset registers giving details of asset ownership and controls implemented for each asset. Ownership of each Intellectual property need to be assigned and reviewed on quarterly basis.

Detailed authority matrix needs to be developed by respective Business Heads to grant appropriate access to Business specific IP. Respective Business Head is overall owner for all the IPs developed and managed by business unit. Different Controls need to be implemented to protect the IP.

Intellectual Property need to be classified as “Confidential” by default.

3.5 Classification Responsibilities

The respective Information owners / business owner are responsible for execution of the policy on Information Classification. Unclassified information shall always be deemed as sensitive information.

3.6 Need to Know

One of the fundamental principles of information security is "need to know." This principle holds that information shall be disclosed only to those people who have a legitimate business need for the information. The following information classification scheme has been designed for Choice Equity Broking Pvt. Ltd. (Choice)to support the need-to-know principle so that information will be protected from unauthorized disclosure, use, modification, and deletion.

3.7 Inventory of assets

The information of Choice Equity Broking Pvt. Ltd. (Choice)shall be consistently protected throughout its life cycle, from its origination to its destruction. Information shall be protected in a manner commensurate with its sensitivity; no matter where it resides, what form it takes, what technology is used to handle it, and what purpose it serves. Although this Information Classification scheme provides overall guidance to achieve consistent information protection, employees of Choice

Equity Broking Pvt. Ltd. (Choice) need to apply and extend these concepts to fit the needs of day-to-day operations.

Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.

The lifecycle of information shall include creation, processing, storage, transmission, deletion and destruction. Documentation shall be maintained in dedicated or existing inventories as appropriate. The asset inventory shall be accurate, up to date, and consistent and aligned with other inventories.

3.7.1 Information Asset Owner

The information asset owner is the individual who oversees the implementation and is responsible for the availability of the information. The information asset owner is responsible to define the access matrix for policy implementation. Information Owner shall coordinate with the information asset custodian to ensure the access privileges as defined on “need to know” basis is implemented.

Any individual creating any official document related to the company, he/she becomes an information owner for those set of documents created by him. There shall be an information owner for every information asset. The information owners shall be responsible for assigning / maintaining appropriate information classifications for the critical information under their custody as defined below.

- Ensure that assets are inventoried.
- All files / e-mails created by individuals shall be owned and classified by them.
- The information classification process shall be completed for existing critical information and shall be undertaken for any new avenues that can create new form /instance of the information like new software application
- Same information stored in several media formats (either hard copy or electronic) shall have the same level of classification.
- Define and periodically review access restrictions and classifications to important assets, considering applicable access control policies.
- Ensure proper handling when the asset is deleted or destroyed.

3.7.2 Acceptable use of information assets

- The Choice Equity Broking Pvt. Ltd. (Choice) information assets shall be used only for business purpose
- The responsibility of ensuring the security of the asset shall lie with the asset owner (information owner)
- However, the user shall exercise Due Diligence and Due Care towards the information asset assigned to him
- Any misuse, abuse of Information asset shall be considered as a policy violation
- Information assets shall not be shared with unauthorized individual
- Users must not engage in activities that could compromise the security of information or assets, such as unauthorized access, sharing, copying, or downloading data, or using personal devices without security controls.
- Employees, contractors, and third parties must ensure that confidential information is protected and not disclosed to unauthorized individuals or external parties.
- Only licensed, authorized, and secure software is permitted for use on organizational systems. Unauthorized software, including pirated or unapproved applications, is prohibited.

- Minimal or no personal use of organizational information and assets is permitted. Any personal use must not interfere with work responsibilities or compromise security.
- The organization reserves the right to monitor the use of information and assets to ensure compliance with security policies, detect suspicious activities, and maintain an audit trail for accountability.
- Violation of acceptable usage policies will result in disciplinary action, which may include termination of employment, legal action, and reimbursement for damages if any.

3.7.3 Return of assets

- All employees and external party users shall return all the Choice Equity Broking Pvt. Ltd. (Choice) assets in their possession upon termination of their employment, contract or agreement.
- The termination process shall be formalized to include the return of all previously issued physical and electronic assets owned by or entrusted to the Choice Equity Broking Pvt. Ltd. (Choice).
- In cases where an employee or external party user purchases the Choice Equity Broking Pvt. Ltd. (Choice)'s equipment or uses their own personal equipment, procedures shall be followed to ensure that all relevant information is transferred to the organization and securely erased from the equipment.
- In cases where an employee or external party user has knowledge that is important to ongoing operations, that information shall be documented and transferred to the Choice Equity Broking Pvt. Ltd. (Choice).
- During the notice period of termination, the Choice Equity Broking Pvt. Ltd. (Choice)shall control unauthorized copying of relevant information (e.g. intellectual property) by terminated employees and contractors.

3.8 Information Classification Matrix

Information owners of Choice Equity Broking Pvt. Ltd. (Choice)shall use the following matrix to classify information assets in a manner that balances the risk of compromise with the needs of normal business operations.

Table No. 1

Classification Level	Definition	Examples (includes but not limited to)
Confidential (Level III)	This classification applies to the most sensitive business information, which is intended strictly for use within Choice Equity Broking Pvt. Ltd. (Choice). Its unauthorized disclosure could seriously and adversely impact Choice Equity Broking Pvt. Ltd. (Choice), its stockholders, its business partners, and/or its customers leading to legal and financial repercussions and adverse public opinion. Information that some people would consider to be private is included in this classification.	Investment plans, trading positions, trading strategies (long / short), Algorithm Trading (source codes / developed products), merger and acquisition plans, customer Information, information security data, Strategy Documents. Employee performance evaluations, internal audit reports, short-term marketing plans, analysis of competitive products / services and intellectual capital of Choice Equity Broking Pvt. Ltd. (Choice)which comprises the collective experience, knowledge, skill, and information of Choice Equity Broking Pvt. Ltd. (Choice)and its people. Sensitive personal information and information that can come under data protection act / legislation.
Internal (Level II)	This classification applies to all other information, which does not clearly fit into any of the other two classifications. While its unauthorized disclosure is against policy, it is not expected to seriously or adversely impacts Choice Equity Broking Pvt. Ltd. (Choice), its employees, its stockholders, its business partners, and/or its customers.	Choice Equity Broking Pvt. Ltd. (Choice)internal telephone directory, training materials, and policy documents
Public (Level I)	This classification applies to information, which has been explicitly approved by Choice Equity Broking Pvt. Ltd. (Choice)management for release to the public. By definition, there is no such thing as unauthorized disclosure of this information and it may be freely disseminated without potential harm.	Published research reports, Published annual/quarterly published reports Web site content, Service brochures, advertisements, job opening announcements, and press releases

3.8.1 Cumulative Classification

The information classification levels represent cumulative information sensitivity. As the levels of sensitivity increase, the access and modification controls become more rigorous and comprehensive. For example, confidential information is a restricted subset of internal information and requires additional security controls.

3.8.2 Minimum Baseline Security Control Matrix

The requirements in the following table outline the minimum baseline security control (MBSC) mechanisms that shall be used for each information classification.

Security Objective	Public	Internal	Confidential
Identification and Authentication	None	User IDs and Passwords	User IDs and Passwords, Strong Authentication (2 Factor)
Authorization and Access Control	Access Control for Modification	Authorization for granting access by LOB Head, access control as per functions, or directory level access control	Access control
Confidentiality	None	Encryption over public communications facilities (Internet, dial-up)	Encrypted communications and encrypted files on storage media
Integrity	Access / change control	Minimal audit trail (e.g., document history), data integrity checks	Detailed audit trail (e.g., system-level file history), “maker-checker”, Field-level change history
Non-repudiation	Access / change control	Minimal audit trail (e.g., document history)	Detailed audit trail (e.g., system-level file history), Field-level change history, digital signatures
Auditing	Modification, events	User activities, access denials	All events
Availability	Virus scanning, backup / restore	Virus scanning, backup/restore	Virus scanning, strong change control over system configuration, backup/restore

3.8.3 Consistent Classification Labeling

All confidential information in physical format shall be labeled accordingly, from the time it is created until the time it is destroyed or re-labeled. Such markings shall appear on all manifestations of the information (hard copies, floppy disks, CD-ROMs, etc.).

3.8.4 Handling of assets

The handling of sensitive material shall be guided by:

- Access restrictions supporting the protection requirements for each level of classification
- Storage of IT assets in accordance with manufacturers’ specifications.
- Labeling material to reflect its sensitivity and security classification
- Minimizing distribution of sensitive material
- Recording authorized recipients, marking information with the recipient’s identity, confirming

receipt of transmitted data and periodically reviewing records of authorized recipients

- Checking completeness of sensitive material (e.g. by ensuring all information is Input / processed and there is proper accounting for all computer media)
- Sensitive documents and data storage media shall be stored in physically secure locations (e.g. locked, fireproof cabinets etc.)

3.9 Media handling

3.9.1 Management of removal media

Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the Choice Equity Broking Pvt. Ltd. (Choice). The following guidelines for the management of removable media shall be considered:

- If no longer required, the contents of any re-usable media that are to be removed from the Choice Equity Broking Pvt. Ltd. (Choice)shall be made unrecoverable by destroying the media
- Where necessary and practical, authorization shall be required for media removed from the Choice Equity Broking Pvt. Ltd. (Choice)and a record of such removals shall be kept in order to maintain an audit trail.
- All media shall be stored in a safe, secure environment, in accordance with manufacturers' specifications.
- If data confidentiality or integrity is important considerations, cryptographic techniques shall be used to protect data on removable media.
- To mitigate the risk of media degrading while stored data are still needed, the data shall be transferred to fresh media before the media is rendered unreadable.
- Multiple copies of valuable data shall be stored on separate media to further reduce the risk of coincidental data damage or loss.
- Removable media drives shall only be enabled if there is a business reason for doing so.
- Where there is a need to use removable media the transfer of information to such media shall be monitored.

3.9.2 Disposal of media

The disposal of sensitive documents and data storage media shall be guided by:

- Using secure means of disposal
- Recording its disposal
- Checking that embedded data storage media has been erased prior to disposal

3.9.3 Physical media transfer

Media containing information shall be protected against unauthorized access, misuse or corruption during transportation. The following guidelines shall be considered to protect media containing information being transported:

- Reliable transport or couriers shall be used.
- A list of authorized couriers shall be agreed with management.
- Procedures to verify the identification of couriers shall be developed.
- Packaging shall be enough to protect the contents from any physical damage likely to arise

during transit and in accordance with any manufacturers' specifications, for example protecting against any environmental factors that may reduce the media's restoration effectiveness such as exposure to heat, moisture or electromagnetic fields.

- Logs shall be kept, identifying the content of the media, the protection applied as well as recording the times of transfer to the transit custodians and receipt at the destination.

When information is exchanged between two parties with the use of information exchange equipments like mobile, answering machine, fax machine, electronic mail, Internet etc., following controls shall be considered:

- While using a mobile phone in a public place, ensure that the information is not overheard by others
- Inform the receiver before sending a fax.
- Follow the controls on exchange of information or software using electronic mail and Internet as described in the "Electronic Mail Security Policy" and "Internet Security Policy" respectively
- Users shall ensure that any internal or confidential information is not left as a message on answering machines

3.10 Responsibility of Information Custodian and Information Users

3.10.1 Information Custodian

The information custodian is the individual or team managing the infrastructure needs of the system. The information custodian is responsible for providing a secure infrastructure in support of the data, including, but not limited to, providing physical security, backup and recovery processes, granting access privileges to system users as authorized by information owners or their designees, and implementing and administering controls over the information.

3.10.2 Information User

Information users are individuals who need and use Choice Equity Broking Pvt. Ltd. (Choice)data as part of their assigned duties or in fulfillment of assigned roles or functions within Choice Equity Broking Pvt. Ltd. (Choice). Individuals who are given access to sensitive information have a position of special trust and as such are responsible for protecting the security and integrity of that information.

3.11 Declassification / Downgrading

- The designated information owner may, at any time, upgrade or downgrade (declassify) the classification level of information. To achieve this, the owner shall change the classification label appearing on the original document and notify all known recipients / users. Any change in the Information classification level shall be authorized by the LOB Head / COO. Proper justification should be provided during label downgrade.
- If known, the date that the confidential information shall no longer be sensitive shall be recorded.
- The designated information owner's LOB head may, at any time prior to scheduled declassification or downgrading, extend the period that information is to remain at a certain classification level.
- To determine whether sensitive information may be declassified or downgraded, it is recommended, at least once a year, information owners shall review the sensitivity classifications assigned to information for which they are responsible.

10. CAPACITY PLANNING POLICY

1. Managing Capacity for Information Processing Facilities

- Capacity planning process ensures that adequate capacity is available and that best and optimal use is made of it to meet performance needs. Capacity planning process shall cover all critical IT resources including the following:
    - Server resources
    - Network resources
    - Application software
    - Critical PCs/ Laptops
- Capacity of information processing facilities shall be monitored continuously, and the data gathered shall be used for projecting future capacity requirements and identifying potential bottlenecks.
- Items to monitor, include but are not limited to the following:
    - Processors
    - Primary memory (RAM)
    - Secondary memory (Hard disk)
    - Backup media
    - Printers and other output devices
    - Communication systems

11. LOG AND MONITORING

1. **Monitoring**

   Systems shall be monitored, and information security events shall be recorded. Administrator/Operator logs and event logging shall be used to ensure information system problems are identified. System monitoring shall be used to check the effectiveness of controls adopted and to verify conformity to logical access controls applied across the various systems in Choice.

2. **Audit Logging**

   Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring. System administrators shall not have permission to erase or de-activate logs of their own activities.

3. **Monitoring System Use**

   Monitoring use of information processing facilities shall be established and the results of the monitoring activities reviewed regularly. Usage monitoring procedures are necessary to ensure that users are only performing activities that have been explicitly authorized.

4. **Protection of Log Information**

   Logging facilities and log information shall be protected against tampering and unauthorized access. Changes to log information and operational problems with the logging facility including:

   - Log files being edited or deleted.
   - Storage capacity of the log file media being exceeded, resulting in either the failure to record events or over-writing of past recorded events.

5. **Administrator and Operator Logs**

   - System administrator and system operator activities shall be logged.
   - System administrator and operator logs shall be reviewed on a regular basis.

6. **Event Logging**

   - Events shall be logged, analyzed, and appropriate action shall be taken
   - Technology team shall be utilized to manage all logging activities.

7. **Network Time Protocol (NTP):**

- Implement NTP to synchronize the clocks of all computers, servers, and network devices to a trusted time source (such as a public or internal NTP server).
- Ensure that devices are synchronized within an acceptable margin (e.g., within 1-2 minutes) to maintain consistency across systems logs.

12. CHANGE MANAGEMENT POLICY

1.0 Purpose

Changes to Choice Equity Broking Pvt. Ltd. (Choice) Information Technology facilities and systems shall be controlled in order to ensure that changes made to a production component are applied in a controlled and consistent manner.

2.0 Scope

This policy applies to all employees, contractors, consultants, and temporary staff etc. using Choice's computing resources. All are expected to be familiar with and comply with this policy.
The change management policy applies to the changes in the following areas:

- Changes to operating systems, which shall include application of patches and service packs, configuration changes, and version upgrades.
- Changes to networks and network devices like routers, switches, firewall (access control list), etc. This shall include changes to router and switch configurations, firewall policy changes, network layout/traffic changes and changes to intrusion detection systems.
- Changes to IT hardware of servers such as change of RAM, addition / removal of disk drives (HDD, FDD, and CD/DVD Drive) etc.
- Changes in source code
- Changes to ISMS
- Additions of new location / new application / new hardware to the existing setup
- Changes to code in the application software being carried out by using proper version controls or special version control software

3.0 Policy

3.1 Change Management

- The change management process shall involve documenting and managing the change requests.
- The documentation shall provide a brief description of the change requested, the date on which the request was made, priority of the request, and a unique number for each request.
- All changes shall be planned, scheduled and all the affected parties shall be informed in advance of the change.
- All the change requests shall accompany rollback procedures along with them and all changes have to be reviewed after the roll out.

3.2 Change Approval

- Any change request shall be approved by the concerned LOB approver / Application Owner / Project Manager / Technology team and Information Security Team based on business requirements or rejected and more clarifications shall be asked from the end user. This request shall be forwarded or acted upon by the relevant team.
- An assessment of the proposed system changes shall be performed to assess its potential impact on Choice's computing systems before its approval.

3.3 Testing of Changes and Backup

- All critical and complex changes shall be tested before being carried out in the live/production environment.
- A quality assurance test (i.e. including Business Requirement Specification Sign off, Application team Sign off Process, UAT Sign Off, Information Security team Sign off) of the changes shall be performed in a test environment prior to implementation in the production environment.
- A backup of the system impacted by the change shall be made prior to its being updated.
- In case of unsuccessful changes the rollback and recovery procedures shall be followed.

3.4 Unscheduled/Emergency Changes

- Unscheduled / emergency changes shall be carried out only in case there are critical production issues, which require the change to be carried out and shall be marked as an exception.
- Any unscheduled changes shall not be done without proper approval by the concerned LOB Head, Application Owner and Tech Owner.
- An audit trail of the emergency activity shall also be generated which logs all activity, including but not limited to:
  - The user-ID making the change
  - Time and date
  - The commands executed
  - The program and data files affected
- After unscheduled changes are carried out, normal change procedures shall be expedited.

3.5 User ID and Access Changes

- User ID creation, modification and deletion shall be managed by the Identity and Access Management Team.
- Any changes to user id including changes to the authorization levels shall be done by following the procedure defined in Logical Access Control Policy by the approval from the team.
- The change shall involve raising a request, followed by risk assessment by the Information Security Team and approval of the same by LOB Head / Application owner.

3.6 Hardware Changes

- Any changes to hardware shall be done by following the change management process which includes raising a change request, approval by the appropriate person and documentation of the same.
- The custodian of the hardware shall conduct all the hardware changes after due approval of the change.
- Changes done to the hardware shall be updated in the hardware/asset inventory after the change is done.
- Changes done to the hardware shall be monitored after the change to ensure that there is no negative effect due to the change.

3.7 Operation System Changes

- Any change to the operating system shall be strictly controlled by the use of the change management process, which will include raising a change request, testing, approval and documentation of the same.
- Changes to the operating system shall be done by following the steps mentioned in the documented operating procedures, wherever applicable.
- All changes shall be documented, and a trail must be maintained by means of preserving the change requests.
- Any change that involves downtime or disruption of services shall be done after giving an appropriate notification to the affected users by email.
- A technical review shall be carried out with standard test cases after any changes are done on the operating system.

3.8 Application Changes

- For application related change management, please refer to the **SDLC Policy**.

3.9 Changes to ISMS

All changes to the ISMS must be thoroughly documented, including:

- **Change Request Forms**: Detailed records of the change request, including the justification for the change, approval, and assessment of security risks.
- **Risk Assessment Reports**: Documentation of the risks identified, the impact assessment, and any mitigation measures.
- **Implementation Logs**: Step-by-step documentation of the change process, including the date, time, and responsible parties.
- **Post-Change Reviews**: A summary of the post-implementation review, including any corrective actions taken to address security issues.
- Changes to the ISMS must be authorized by designated individuals, typically including information security management, senior management, and relevant department heads.
- A change advisory board (CAB) may be formed to oversee significant changes, especially those with a large impact on information security, legal compliance, or business operations.
- **Impact on Information Security:-**

  Changes to the ISMS must consider the potential impact on information security controls, processes, and compliance with relevant laws and regulations. The following areas should be assessed:

  - **Confidentiality, Integrity, and Availability:** Changes should not compromise the organization's ability to maintain confidentiality, integrity, and availability of sensitive data.
  - **Compliance Requirements:** Changes must adhere to relevant legal, regulatory, and contractual obligations (e.g., SEBI regulations).
  - **Security Controls:** Changes must align with the established security controls in the ISMS, and any deviations must be carefully justified and monitored.
  - **Business Continuity:** Ensure that changes do not negatively affect the organization’s ability to continue operations or respond to potential disruptions.

3.10 Patch and Service Pack Management

- Application of patches shall be done in a controlled manner.
- A patch or service pack shall be applied only when it is a critical patch or there is a requirement for the application of the same.
- Only tested versions of the patch or service pack shall be considered for application, wherever needed.
- The patch or service pack shall be obtained directly from the vendor or downloaded from the vendor site only.
- A test bed shall be prepared whenever possible to simulate the actual production environment and the patch or service pack shall be installed in the test environment. The test environment shall be monitored for performance and other issues.
- On successful testing by the functional users on a UAT / non production server, the patch shall be applied on the Production DR Server first and then the Production Primary Server after verification from the DR Server about the relevant functionality and their compatibility.
- Patching and auto-update process for desktops/laptops has been omitted from the change management process considering the low/negligible business impact. Changes in production environment
- Addition, removal of any hardware, software or IT resource from the production environment shall be controlled and approved and shall be maintained to ensure non-disruption of the production environment.

13. CRYPTOGRAPHIC CONTROL POLICY

1.0 Purpose

The Cryptographic Controls Policy defines the standards and controls that will be followed in order to maintain a minimum level of protection for information assets.

2.0 Scope

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

3.0 Policy

- Information assets shall be secured from unauthorized access, damage or interference. Cryptographic controls shall be implemented to ensure the confidentiality, authenticity or integrity of information assets located within Choice Equity Broking Pvt. Ltd. (Choice).
- The management approach towards the use of cryptographic controls across Choice Equity Broking Pvt. Ltd. (Choice), including the general principles under which business information shall be protected
- Encryption type and other implementation details shall be decided based on the relevant legislations and the level of protection required for the information. A regular review shall be carried out to determine the level of protection required by the information.
- Industry standard strong algorithm (e.g. RSA, AES etc) shall be used wherever encryption is implemented
- The use of proprietary/closed encryption algorithms shall not be allowed for any purpose, unless reviewed by qualified experts independently of the vendor in question.
- The various needs for encryption of information involved in business transactions shall be derived from
    a) Risk assessment
    b) Customer requirement(s)
    c) Regulation/Law/Standards compliance requirement(s)
    d) Information exchange using mobile or removable media devices or across communication lines
- Based on the above requirements, data shall be stored and encrypted if necessary.
- Depending on the business requirements, the information owner and Technology shall decide a mutually acceptable encryption methodology for protecting identified critical and sensitive business information.
- Import, export and use of encryption methodologies shall follow applicable laws and regulations.
- Encryption options available within Choice Equity Broking Pvt. Ltd. (Choice) mailing solution shall be used for sharing restricted / confidential information with external parties via email.

4.0 Good practices

4.1 Encryption

- Encryption is a cryptographic technique that can be used to protect the confidentiality of information. Appropriate levels of encryption shall be considered for the protection of sensitive or critical information.

- Choice Equity Broking Pvt. Ltd. (Choice) shall consider use of cryptographic controls for protection of some of the information. The following shall be implemented:
  - The use of at least TLS V1.2 certificate issued by a reliable and well-known certification authority shall be used for securing browser to web server communications for Internet based transaction-oriented websites.
  - Transport security needs to be implemented for intranet sites as well with a minimum TLS V1.2 certificate
  - Industry standard strong algorithm (e.g. AES) shall be used for encryption of data at rest.

- The following shall be considered when a decision on implementation of cryptographic control is taken:
  - Regulations and national restrictions that might apply to the use of cryptographic techniques.
  - The required level of protection shall be identified based on a risk assessment, considering the type and quality of the encryption algorithm used.

14. ELECTRONIC MESSAGING POLICY

1. Introduction

Electronic messaging has now become a vital business tool for communicating both internally and with customers and suppliers. However, because of its flexibility and general availability, the use of electronic messaging carries with it several significant risks and all users must remain vigilant and adopt good practice when sending and receiving messages.

Electronic messaging covers email and various forms of instant and store-and-forward messaging such as SMS texts, messaging apps, web chats and messaging facilities within social media platforms.

This policy document tells you how you may use the provided Choice Equity Broking Pvt. Ltd. electronic messaging facilities, including what you must and must not do. It applies to all use of these facilities whatever the means or location of access e.g. via mobile devices or outside of the office.

If you do not understand the implications of this policy or how it may apply to you, you should approach your line manager in the first instance.

This control applies to all systems, people and processes that constitute the organization's information systems, including board members, directors, employees, suppliers and other third parties who have access to Choice Equity Broking Pvt. Ltd.

The following policies and procedures are relevant to this document:

- *Internet Usage Policy*

1 Electronic messaging policy

1.1 Sending and receiving electronic messages

The organization-provided electronic messaging facilities must always be used when communicating with others on official business. You must not use a personal account for this purpose. Guidelines on the sending of classified information via electronic messaging must always be observed. These are set out in document Asset Handling Procedure.

All messages sent from an organization account remain the property of Choice Equity Broking Pvt. Ltd. and are considered to be part of the corporate record. All organization messages should be considered to be official communications from the organization and treated accordingly.

The organization maintains its legal right to monitor and audit the use of electronic messaging by authorised users to assess compliance to this policy. This will be done in accordance with the provisions of relevant legislation.

Deletion of a message from an individual account does not necessarily mean that it has been permanently removed from the organization's IT systems and such messages may still, be subject to audit and review.

Users should remain aware that it cannot be guaranteed that a message will be received or read by a recipient and that messages can be interpreted in different ways according to the culture, role and even prevailing mood of the individual reading it. You should therefore always consider whether the use electronic messaging is an appropriate means of conveying the information involved and whether an alternative such as the telephone would be preferable, particularly if the message is urgent or complex.

Particular care must be taken when addressing messages that include classified information to prevent accidental

transmission to unauthorised recipients. Beware of the auto-completion feature of some text and email clients where the system suggests recipients based on the characters typed in so far.
Users must avoid sending unnecessary messages to distribution lists, particularly those with wide circulation such as the "global list" of all employees. Where required, such messages should be sent via the organization's communications department.
Messages from an organization address should be considered in the same way as other more formal methods of communication. Nothing must be sent externally which might affect the organization's reputation or affect its relationships with suppliers, customers or other stakeholders.
In particular, users must not send messages containing material, which is defamatory, obscene, does not comply with the organization's equality and diversity policy or which a recipient might otherwise reasonably consider inappropriate. If you are not sure whether your intended message falls into this category, please consult your line manager before sending.
Official organization electronic messaging facilities must not be used:

- For the distribution of unsolicited commercial or advertising material, chain letters, or other junk-mail of any kind, to other organizations
- To send material that infringes the copyright or intellectual property rights of another person or organization
- For activities that corrupt or destroy other users' data or otherwise disrupt the work of other users
- To distribute any offensive, obscene or indecent images, data, or other material, or any data capable of being resolved into obscene or indecent images or material
- To send anything which is designed or likely to cause annoyance, inconvenience or needless anxiety to others
- To convey abusive, threatening or bullying messages to others
- To transmit material that either discriminates or encourages discrimination on the grounds of race, gender, sexual orientation, marital status, disability, political or religious beliefs
- For the transmission of defamatory material or false claims of a deceptive nature
- For activities that violate the privacy of other users
- To send anonymous messages - i.e. without clear identification of the sender
- For any other activities which bring, or may bring, the organization into disrepute

If you receive unsolicited junk messages or spam, it is advised that you delete them without reading them. Do not reply to the message as this can confirm the existence of a valid address to the sender, resulting in further unwanted communications.

1.2 Monitoring of electronic messaging facilities

Electronic messaging usage within the organization system is monitored and recorded centrally in order to:

- Plan and manage its resource capacity effectively
- Assess compliance with policies and procedures
- Ensure that standards are maintained
- Prevent and detect crime
- Investigate unauthorised use

Monitoring will be undertaken by staff specifically authorised for that purpose. Consistent monitoring procedures will be applied to all users and may include checking the contents of messages.

If a manager suspects that the electronic messaging facilities are being abused by a user, they must contact a Director. All such reports will be investigated according to documented procedures and where appropriate, evidence provided. There is also a requirement to provide such information to regulatory or legislative bodies in accordance with the law.

Users must not access another user’s electronic messaging account unless they have obtained permission from the owner of the account or their line manager. In such cases this must be for legitimate business reasons and only messages which may reasonably be judged to be relevant to the question in hand should be opened.

1.3 Use of email

In addition to the policy statements in other sections of this document, the following applies specifically to the use of email.

All e-mails sent from organization addresses to recipients outside of the organization will automatically carry the following disclaimer:
“The information contained in this message is intended for the addressee only and may contain classified information. If you are not the addressee, please delete this message and notify the sender; you should not copy or distribute this message or disclose its contents to anyone. Any views or opinions expressed in this message are those of the individual(s) and not necessarily of the organization. No reliance may be placed on this message without written confirmation from an authorised representative of its contents. No guarantee is implied that this message or any attachment is virus free or has not been intercepted and amended.”

Do not use auto-forwarding on emails e.g. whilst on holiday, if there is a possibility that this may result in classified information being forwarded to a recipient that does not have sufficient security clearance for the level of information involved.

Your mailbox will be set up with a limitation on its size. This is in order to prevent the available storage capacity from being exceeded and to ensure the cost-effective use of email.

You must manage your email account(s) to remain within the mailbox size limit, making use of the archiving facility included in most email clients where possible. If your mailbox has filled up, contact the [IT Service Desk] for advice in the first instance.

Where possible, make use of links to files within email messages rather than attaching a copy of the file, particularly if the email message has a wide distribution. This will prevent other user’s mailboxes filling up and so avoid consequent disruption.

There is a system-wide size limit to emails which is 50Mb. If you need to send a larger email for legitimate business purposes, then please contact the Service Desk for advice.

Computer viruses, adware and other malware are small programs that can have a negative effect on your computer and your use of the internet and can expose the organization’s information to extreme risk. Such viruses can be inadvertently downloaded and installed via emails received into your inbox. The organization provides anti-virus software which runs on every computer that has access to the network and is intended to detect any viruses before they have been installed.

If you believe you may have a virus or you have been sent an email that may contain one, please report this to the Service Desk immediately. Do not open any attachments you believe may contain a virus.
In addition, you must not:

- Transmit by email any file attachments which you know to be infected with a virus

- Download data or programs of any nature from unknown sources
- Disable or reconfigure the installed anti-virus system operating on a computer used to access email facilities
- Forward virus warnings other than to the Service Desk

If a computer virus is deliberately or accidentally sent to another organization, Choice Equity Broking Pvt. Ltd. could be held liable if the transmission could be considered negligent.

15. CLOUD COMPUTING POLICY

1 Introduction

The purpose of this document is to set out the organization’s policy in the area of cloud computing.

Choice Equity Broking Pvt. Ltd. makes extensive use of cloud computing services in the delivery of its core business systems. The nature of these services is such that data is stored outside of the Choice Equity Broking Pvt. Ltd. internal network and is subject to access and management by a third party. Furthermore, many cloud services are offered on a multi-tenanted basis in which the infrastructure is shared across multiple customers of the Cloud Service Provider (CSP), making effective and secure segregation a key requirement.

It is therefore essential that rules are established for the selection and management of cloud computing services so that data is appropriately protected according to its business value and classification.

Cloud computing is generally accepted to consist of the following types of services:

- **Software-as-a-Service (SaaS):** The provision of a hosted application for use as part of a business process. Hosting usually includes all supporting components for the application such as hardware, operating software, databases etc.

- **Platform-as-a-Service (PaaS):** Hardware and supporting software such as operating system, database, development platform, web server etc. are provided but no business applications

- **Infrastructure-as-a-Service (IaaS):** Only physical or virtual hardware components are provided

This policy applies to the use of all types of cloud computing services and is particularly relevant where personal data is stored.

2 Policy

It is Choice Equity Broking Pvt. Ltd. policy in the area of cloud computing that:

Data belonging to Choice Equity Broking Pvt. Ltd. will only be stored within cloud services with the prior permission of the Choice Equity Broking Pvt. Ltd., Directors.

Appropriate risk assessment must be carried out regarding proposed or continued use of cloud services, including a full understanding of the information security controls implemented by the CSP.

Due diligence must be conducted prior to sign-up to a cloud service provider to ensure that appropriate controls will be in place to protect data. Preference will be given to suppliers who are certified to the ISO/IEC 27001 international standard and who comply to the principles of the ISO/IEC 27017 and ISO/IEC 27018 codes of practice for cloud services.

Service level agreements and contracts with cloud service providers must be reviewed, understood, and accepted before sign-up to the service.

Contracts involving personal data must be checked to ensure that they comply with applicable data protection legislation. If not, a separate data processing agreement may be required.

Roles and responsibilities for activities such as backups, patching, log management, malware protection and incident management must be agreed and documented prior to the commencement of the cloud service.

Procedures must be established to ensure that activities that are irreversible in the cloud environment (e.g. deletion of virtual servers, terminating a cloud service or restoration from backups) are subject to appropriate controls to avoid error. Supervision by a second, suitably qualified person must be a stated part of such procedures.

The location of the data stored with the CSP must be understood and the applicable legal basis established, such as the country whose law applies to the contract.

Where available, multi factor authentication must be used to access all cloud services.

Sufficient audit logging must be available to allow Choice Equity Broking Pvt. Ltd. to understand the ways in which its data is being accessed and to identify whether any unauthorized access has occurred.

Confidential data stored in cloud services must be encrypted at rest and in transit using acceptable technologies and techniques. Where possible encryption keys will be held by Choice Equity Broking Pvt. Ltd. rather than the supplier.

Choice Equity Broking Pvt. Ltd. policies for the creation and management of user accounts will apply to cloud services.

Backups must be taken of all data stored in the cloud. This may be performed either directly by Choice Equity Broking Pvt. Ltd. or under contract by the cloud service provider.

All Choice Equity Broking Pvt. Ltd. data must be removed from cloud services in the event of a contract coming to an end for whatever reason. Data must not be stored in the cloud for longer than is necessary to deliver business processes.

16. DATA DISPOSAL AND RETENTION POLICY

1. Scope

The aim of Data Disposable and Retention Policy is to set out practices to be followed for ensuring the information that is supposed to be disposed is not stolen or misused and maintained securely. This is applicable to all the Employees of Choice Equity Broking Pvt. Ltd. who have access to data.

2. Purpose

The purpose of the policy is to ensure that data is handled in a manner that the confidentiality, integrity and availability of the data are not compromised. It also ensures that data is adequately protected and maintained and to ensure that data is no longer needed or have no value are destroyed at the appropriate time.

3. Procedure

Data is “information created, received, and maintained as evidence and information by any individual in the organization, in pursuance of legal/statutory/contractual obligations or in the transaction of business.

3.1 Data Maintenance

- Data shall be maintained for the client audits as a part of compliance requirement and deemed necessary by virtue of a legal or a statuary requirement.
- Data shall be maintained in a protective environment, safeguarding them against deterioration, damage by environmental or deliberate threats.
- Electronic storage media shall be ensured for the ability to read data throughout the retention period and safeguarded against loss of readability due to technology change.
- Choice Equity Broking Pvt. Ltd. shall establish and maintain procedures for identifying, maintaining, retaining and disposal of data.
- Data should be kept securely and made available to authorized persons when required.

3.2 Data Retention Period

- For customer specific application data, the retention period will be defined in the Choice Equity Broking Pvt. Ltd. applications and share drives as a part of client SLA.
- For Choice Equity Broking Pvt. Ltd. owned data, the length of the retention period is based on the likelihood that the evidence will be needed at some point in the future.
- Evidences and Audit Reports that will serve no further purpose (as determined by the length of their retention period) will be destroyed. As in documents, records which are in soft copy format, shall be reviewed and deleted post authorization.

3.3 Data Disposal

- Choice Equity Broking Pvt. Ltd. shall identify data to be disposed.
- Data shall be disposed in a protective environment and under the supervision of authorized person with prior approvals.

3.3.1 Paper Records

- Paper record to be disposed of are to be segregated from the paper documents that are going to be used.
- Employees of Choice Equity Broking Pvt. Ltd. must make sure that they don’t dispose documents that are required.
- Wherever required shredder OR pulping method is to be used to shred/pulp the unwanted paper documents.

3.3.2 Equipment

- IT team must ensure equipment productivity after its depreciation period. If the equipment is not functioning to meet the business requirements of Choice Equity Broking Pvt. Ltd., then IT team of Choice Equity Broking Pvt. Ltd. can take a call to scrap/donate/sell the equipment.
- The equipment’s memory elements have to be damaged beyond repair and other parts can be disposed-off by destroying them or sending them for recycling.
- In case of donating/selling the equipment, it has to be ensured that the memory elements of the equipment are formatted thoroughly and tested to see if data can be still retrieved.
- If it is possible to retrieve data, the equipment’s memory elements should be removed, and the rest of the equipment can be donated.

17. MALWARE PROTECTION POLICY

1. Scope

This policy applies to Choice Equity Broking Pvt. Ltd.’s information processing and communication facilities. It includes all employees of Choice Equity Broking Pvt. Ltd. and third-party users who in any form use IT infrastructure of Choice Equity Broking Pvt. Ltd.

2. Purpose

Purpose of this policy is to provide the directions for enforcement of procedural and prevention of Virus Attacks related security controls in the day to day working across software platforms of Choice Equity Broking Pvt. Ltd.

- The purpose of the anti-virus policy is divided into the following ways
- To prevent unexpected and unauthorized access attempted on Choice Equity Broking Pvt. Ltd. IT infrastructure which are external threats.
- To ensure customers’ and organization’s information assets like data, computer application systems and IT equipment are adequately and consistently protected from unauthorized use or access, data damage, inappropriate data alteration or data loss. The level of protection should be commensurate to the level of information services required by the company to conduct its business.
- To strive for minimum downtime thus make information and information systems available to authorized users as per the business needs to promote Choice Equity Broking Pvt. Ltd.’s IT Security mission.
- To meet all audit requirements pertaining to information collection, storage, processing, transmittal and disclosure those are applicable to the company.
- To create within the company a level of awareness on information security as part of the day to day operations of the company and to ensure that all employees understand their responsibilities for maintaining information security.
- To establish detailed information security processes based on this policy and ensure compliance against such processes

3. Policy Statement

This policy states security awareness, prevention, and detection controls should be utilized to protect information systems and services against malicious software.

4. Procedure

General Clauses

- All Choice Equity Broking Pvt. Ltd. Laptops and Desktops must have Choice Equity Broking Pvt. Ltd.'s standard, supported anti-virus software installed and scheduled to run at regular intervals.
- Choice Equity Broking Pvt. Ltd.’s in-house Antivirus server is in sync with the global server that allows automatic update of file at Choice Equity Broking Pvt. Ltd. end.
- Virus-infected computers must be removed from the network until they are verified as virus-free.
- Any activity with the intention to create and/or distribute malicious programs into Choice Equity Broking Pvt. Ltd.'s networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) is prohibited.

Antivirus Management (Users)

- Choice Equity Broking Pvt. Ltd.'s systems must have Antivirus software installed and enabled at all times.
- The systems facing internet should have antivirus software installed Automatic updates are to be scheduled to ensure maximum protection against malicious software.
- Scanning the physical storage media and external storage devices should be done automatically or are to be scheduled such that Choice Equity Broking Pvt. Ltd. business or user's performance is not affected.
- Reports should be generated and reviewed periodically to ensure correct working of the antivirus software and analyse Choice Equity Broking Pvt. Ltd.'s security posture against various malware threats.

Control against Malicious Software

Unless proper control precautions are taken, information systems are vulnerable to the introduction of malicious software such as computer viruses, network worms, Trojan horses, logic bombs and spyware / adware code. Protection from malicious software shall be based on awareness, and system access controls, such as the following:

- All antivirus software on servers, desktops and laptops should be configured to protect the system on real time basis (Each file accessed should be first scanned by antivirus software). Users should not be allowed to change these settings.
- Users should be made aware through mail about the new virus outbreaks and necessary precautions to be taken.
- Users should be made aware about the precautions to take and to operate antivirus software.

18. VULNERABILITY ASSESSMENT & PENETRATION TESTING POLICY & PROCEDURE

1. Purpose

The standard is designed to minimize potential exposure to CHOICE EQUITY BROKING PVT. LTD. from damages which may result from unauthorized use of CHOICE EQUITY BROKING PVT. LTD. resources. Damages include the loss of sensitive or confidential data, intellectual property, damage to public image and damage to critical Information Technology systems.

2. Scope

This standard is applicable to information processing systems of Choice Equity Broking Pvt. Ltd. .

3. VAPT

- IT Team owners shall identify and appoint a CERT-In empanelled consultant for managing vulnerabilities/security updates related to CHOICE EQUITY BROKING PVT. LTD. Infrastructure.
- IT Team should identify the information processing systems to be covered as part of periodic Vulnerability Assessment and Penetration Testing (VAPT).
- Vulnerability assessment and network penetration testing shall be undertaken at least on a yearly basis.The final report on said VAPT shall be submitted to the Stock Exchanges / Depositories after approval from Technology Committee within 1 month of completion of VAPT activity. Frequency of VA/PT to be carried out for each information processing system shall be determined by the IT team based on the criticality of the system and regulatory requirements.
- Vulnerability assessment and Penetration Testing shall also be done for off-the-shelf products (used for core business) or applications provided by exchange empaneled vendors and the report will be submitted to the vendors and exchange in a timely manner.
- The testing schedule shall be informed at least one week in advance to the respective departments to ensure no business priorities are affected. In case any business group’s deliverable is getting affected due to schedule then dates shall be redefined accordingly.
- VA/PT should not be done during business/trading hours for production systems.
- Vulnerability scanning should be performed in authenticated mode.
- Penetrations testing of public facing systems are to be carried out by professionally qualified teams.
- Penetration testing should include all the real time modules of the successful penetration like reconnaissance, scanning and profiling, gaining access, maintaining access, covering tracks etc.
- The consultant identified by IT team shall identify and document all technical vulnerabilities of information systems and evaluate the exposure to such vulnerabilities.
- The observation / vulnerabilities identified during the testing will be prioritized and appropriate corrective actions (Patch updating, Configuration change, Disabling insecure services and protocols etc.)

shall be taken to mitigate the associated risk.

- A time frame will be devised for addressing the identified vulnerabilities. All the critical and high rated vulnerabilities shall be closed within 2 weeks of its reporting. All the medium rated vulnerabilities shall be closed within 3 weeks of its reporting and all the low rated shall be closed within 4 weeks of its reporting.
- IT Team shall ensure that all vulnerabilities within their area of operations are addressed.
- Respective IT teams shall be responsible for ensuring deployment of patches in a controlled and timely manner within their area of operation. For this purpose, a governing patch management procedure shall be established and shall be strictly adhered to.
- Formal change management procedure should be followed for all corrective actions.
- Open Findings of VA & PT shall be tracked separately in an open point's tracker and the follow up actions necessitated should be monitored closely by the CISO as well as Cyber Security Committee.
- Wherever testing environments are non-prevalent, corrective action such as patches shall first be implemented at DR site to ensure minimal impact in case the implementation is unsuccessful.
- IT team must confirm closure for the gaps identified during penetration testing. Closure reports pertaining to penetration testing shall be documented and reported to management.
- Vulnerability scanning and conduct penetration testing should be conducted prior to the commissioning of a new system which offers internet accessibility and open network interfaces.
- Results of vulnerability scans should be reviewed to verify that vulnerabilities were addressed either by patching, implementing a compensating control, or by documenting and accepting a reasonable business risk.
- In case if any
- Acceptance of risks for existing vulnerabilities should be periodically reviewed to determine if newer compensating controls or subsequent patches can address vulnerabilities that were previously accepted, or if conditions have changed increasing the risk.

19. COMPLIANCE POLICY

1. Objective

To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements as defined by the organization's policy, procedure, standard or guideline.

2. Compliance with Legal Requirements

Identification of applicable legislation and contractual requirements:

- All relevant statutory, regulatory and contractual requirements shall be defined explicitly and documented for all information processing facilities. The Head of Information Security shall be accountable for compliance. (Refer with compliance register)

2.1 Intellectual property rights (IPR)

- Choice Equity Broking Pvt. Ltd. shall be the legal owner of all business information stored on or passing through its systems, except the information clearly owned by third parties.
- All intellectual property, such as patents, copyrights, inventions, etc., developed by a user while employed by Choice Equity Broking Pvt. Ltd., shall be the property of Choice Equity Broking Pvt. Ltd..
- At the time of termination of their relationship with the Choice Equity Broking Pvt. Ltd., all employees shall return any intellectual property provided or developed during the period of the person’s employment.
- All Choice Equity Broking Pvt. Ltd. intellectual property shall be classified as per the Choice Equity Broking Pvt. Ltds.’ data classification policy and labelled and handled as per Choice Equity Broking Pvt. Ltd. policies
- Software and hardware shall be used in compliance with all legal, statutory, regulatory and contractual compliance and after due authorization
- Software, licensed to the Choice Equity Broking Pvt. Ltd., shall only be deployed and used on Choice Equity Broking Pvt. Ltd. owned information processing facilities.
- Unless otherwise provided in the applicable license, notice, or agreement, copyrighted software shall not be duplicated, except for back-up and archival purposes.
- The IT Manager shall be the custodian of the original copies of all Choice Equity Broking Pvt. Ltd. hardware and software licenses.
- Any software that is acquired illegally or does not have a valid license shall not be deployed or used on Choice Equity Broking Pvt. Ltd. information processing facilities.
- Internal Audit department shall conduct audit for license compliance every 12 months.

- Users shall not copy, or reproduce in any way, copyrighted material from the Internet on information systems.

2.2 Protection of organizational records

- Choice Equity Broking Pvt. Ltd. shall manage the lifecycle of all records created or received by it in pursuance of legal obligations or transactions of business.
- All Choice Equity Broking Pvt. Ltd. records and information, such as personnel details, legal documents, shall be retained and disposed only in accordance with the retention periods as per the applicable laws.
- All restricted and confidential information shall be destroyed in a secure manner.
- Provide read only access to audit tools, logs, and data only to authorized personnel.
- Ensure audit logs are tamper-evident and cannot be altered or deleted during the audit.
- Provide temporary and read only access to audit tools or systems needed for testing, and ensure privileges are revoked immediately after testing is complete.

2.3 Privacy and protection of personally identifiable information

- Choice Equity Broking Pvt. Ltd. shall implement controls for collecting, processing, and disseminating personal information. Employee personal data maintained on information systems shall be secured through implementation of appropriate security controls.Personal data shall be processed in accordance with lawful grounds and legitimate business processing.
- Only select authorized personnel shall have access to such information. The security controls shall address:
  - Mechanisms for ensuring that information is obtained and processed fairly, lawfully and properly.
  - Ensuring that information is accurate, complete and up-to-date, adequate and relevant.
  - Appropriate feeding and deletion of information.
  - Compliance with individual rights, such as subject access.
  - Compliance with the relevant data protection/ privacy regulations. Legal team shall be responsible for identifying and marinating a list of applicable data protection/ privacy regulations and the same shall be communicated to the Head

of Information Security on a continuous basis.

    - Contracts with third parties handling personal information shall include clauses on right to audit.

- Choice Equity Broking Pvt. Ltd. may log, review, and utilize any personal information stored on or passing through its systems.
- Choice Equity Broking Pvt. Ltd. shall, at its discretion, monitor usage of its information assets as per applicable laws and terms and conditions of employment agreed upon by the Choice Equity Broking Pvt. Ltd. and the employee. This may include logging and reviewing of user activity such as telephone numbers dialed, web sites visited from Choice Equity Broking Pvt. Ltd. owned assets, electronic communications exchanged through Choice Equity Broking Pvt. Ltd. information processing facilities etc.
- Ensure data masking of personal data wherever possible for data protection.
- In case of any issues regarding the privacy / personal data, reach out to soc@choiceindia.com .

2.4 Prevention of misuse of information processing facilities

- Choice Equity Broking Pvt. Ltd. information systems shall be used only after authorization from management and for business purposes only.
- Choice Equity Broking Pvt. Ltd. shall not be responsible for the safe keeping of any personal data on its systems.
- Users of Choice Equity Broking Pvt. Ltd. assets shall not acquire, possess, trade, or use hardware or software tools that could be employed to evaluate or compromise information systems security, unless specifically authorized by the IS department.

3. Information Security Reviews

3.1 Independent review of Information security

- Choice Equity Broking Pvt. Ltd. top management shall initiate an independent review of the information security arrangements. Such an independent review is necessary to ensure the continuing suitability, adequacy and effectiveness of the organization’s approach to managing information security.
- The review should include assessing opportunities for improvement and the need for changes to the approach to security, including the policy and control objectives. Such a review should be carried out by individuals independent of the area under review,

e.g. the internal audit function, an independent manager or an external party organization specializing in such reviews.

- The individuals carrying out these reviews shall have the appropriate skills and experience. The results of the independent review shall be recorded and reported to the management who initiated the review. These records should be maintained.
- If the independent review identifies that the organization’s approach and implementation to managing information security is inadequate, e.g. documented objectives and requirements are not met or not compliant with the direction for information security stated in the information security policies (see 5.1.1), management shall consider corrective actions.
- The Head of Information Security shall ensure that all security procedures within her/his area of responsibility are carried out correctly and within the Information Security Management Structure framework. In support of the review, all areas should be considered for regular review to ensure compliance with security policies and standards.

3.2 Compliance with security policies and standards

Respective Departmental Heads shall ensure compliance with this information security policies and issue specific policies.

The Head of Information Security is authorized to perform compliance checks against security policy. The frequency of such compliance checks shall be performed according to the size of the facility or prior audit results and If any non-compliance is found as a result of the review, management shall:

- Determine the causes of the non-compliance.
- Evaluate the need for actions to avoid recurrence of the same.
- Determine and implement appropriate corrective action. and
- Review the corrective action taken

Results of reviews and corrective actions carried out shall be recorded and these records shall be maintained.

3.3 Technical compliance review

- Internal Audit management must perform an annual review and random tests of production computer system backup processes.

- Technical compliance checks shall be regularly carried out, which involves examination of operational systems to ensure that hardware and software controls have been correctly implemented.
- Information Security Team shall develop and execute compliance review plan based on risk assessment. The plan shall define scope and frequency of review based on the business impact of the system.
- In addition to regular updates, information systems security risk assessments for critical information systems and critical production applications shall be reviewed at least once every year, and all major enhancements, upgrades, conversions, and related changes associated with these systems or applications shall be preceded by a risk assessment.

20. CONFIGURATION MANAGEMENT POLICY

1. Introduction

Configuration Management ensures effective control of all the CHOICE EQUITY BROKING PVT. LTD. Service Assets and Configuration Items.

1.1 Objectives

The objective is to track and control accurate information about all CI's including their attributes, status and relationships with services and other configuration items throughout the lifecycle.

1.2 Scope

The scope includes all Configuration Items within CHOICE EQUITY BROKING PVT. LTD. as covered by the Configuration Management Process.

2. Configuration Management Policy

CHOICE EQUITY BROKING PVT. LTD. has determined that Configuration Management forms as an essential element of the IT Service Delivery. The following are the policies for Configuration Management

1. A member of CHOICE EQUITY BROKING PVT. LTD. shall be assigned as the Configuration Manager.
2. The Configuration Manager is responsible for recording, maintaining and verifying CMDB contents related to configuration, items, support resources, vendors, and service contracts.
3. Additions or changes to catalogue, inventory or configuration items shall be accurately recorded on the Configuration Management Database (CMDB) with a lag time that does not exceed 10 working days from the delivery of a new item or the change to an existing item.
4. Additions or changes to other CMDB record types (vendor, support resources, service contract) shall be accurately recorded in the CMDB with a lag time that does not exceed 2 working days from the occurrence of the change.
5. An integrated tool shall be implemented to enable effective access to CMDB information for all dependent processes and staff.
6. Appropriate controls shall be implemented to prevent unauthorized access and unauthorized changes to the CMDB records.
7. CMDB access privileges shall be granted in accordance with the role-based CMDB Access Control List.
8. A CMDB specifications sheet shall be established and maintained to define:
   - The standard categories used for the classification of items.
   - The standard attributes (mandatory and optional) for each item type and category.
   - The supported item relationships and status options.
   - The CMDB schema and data entry standards.
9. The Configuration Manager must always comply with the data entry standards defined by the CMDB policy, the specification sheet and with the generally acceptable rules of high-quality data entry.
10. If an CHOICE EQUITY BROKING PVT. LTD. staff member discovers errors or discrepancies in the CMDB data, he or she must immediately report those errors to the Configuration Manager. The CMDB Officer must immediately take the actions necessary to rectify those errors.
11. The CMDB system must be capable of tracking the history of record changes and must have the ability to report a complete audit trail for any item throughout its lifecycle.

12. Configuration status shall be defined. Item status shall be changed to “Archived” when the item is no more part of the production environment, but “Scraped” status shall be assigned only following the completion of a formal disposal of the CI.
13. On a routine basis, all the scrap items shall be moved to the archive database and retained for any further reference if required.
14. All configurations shall be labelled with the Configuration ID. If the configuration consists of multiple inventory items then all component items shall also be labelled with the sXXXXe Configuration ID.

21. Installation of Approved Software

1. Purpose

The purpose of this policy is to ensure that the installation of software on operational systems is conducted securely, with integrity, and in compliance with established security protocols. The policy aims to prevent the exploitation of technical vulnerabilities, safeguard organizational data, and maintain the security of operational systems by regulating the installation and updating of software.

2. Scope

This policy applies to all employees, contractors, and third-party vendors involved in the installation, updating, and maintenance of software on the organization's operational systems. This includes software provided by vendors, open-source software, and any internally developed or customized software.

3. Policy Guidelines

3.1 Authorized Software Installation

- **Approved Software Only:** Only approved software, which has been tested and authorized by the Department Heads and CISO, shall be installed on operational systems. The installation of development code, compilers, or any unapproved executable code is prohibited.

- **Software Authorization:** All software to be installed must be approved by respective department heads and CISO. Software installation requests must be submitted through the IT support desk, which will initiate a security assessment.

3.2 Software Installation Process

- **Testing Prior to Installation:** All software must undergo extensive and successful testing in a controlled environment before being installed on any operational system. This testing should include validation of security functionality and the absence of known vulnerabilities.

- **Change Control:** The installation of software must be managed under a formal change control process to ensure that any changes are documented, assessed, and approved before implementation. The process should also include risk assessments related to the installation.

- **Rollback Strategy:** A defined rollback strategy must be established and tested before the installation of any software updates or patches. This ensures that if any issues arise during or after the installation, the system can be reverted to its previous stable state.

3.3 Configuration and Version Control

- **Configuration Control System:** A configuration control system must be used to track and manage all software versions installed on operational systems. This system should maintain records of software configurations, installation details, and version history.

3.4 Software Update Management

- **Maintaining Supported Software Versions:** Vendor-supplied software must be kept at a version that is supported by the vendor. Outdated or unsupported versions should be updated or replaced as soon as practical. This also applies to open-source software, which should be updated to the latest stable and secure release.

- **Monitoring External Software Components:** If the software relies on externally supplied modules or packages (e.g., hosted software), these components should be monitored and controlled to prevent unauthorized modifications or vulnerabilities.

3.5 Vendor-Supplied Software Installation

- **Supplier Access:** If third-party vendors are involved in the installation or updating of software, their access will be restricted to the minimum necessary level, and access will only be granted upon appropriate authorization. Supplier activities must be monitored to ensure that the software installation is secure and compliant with organizational policies.

3.6 User Privileges and Installation Control

- **Principle of Least Privilege:** The principle of least privilege must be applied to software installation rights. Users will only be permitted to install software relevant to their job functions and based on their roles. Personal or non-approved software installations are strictly prohibited.

- **Types of Allowed Installations:** Only software related to the organization's business needs, including approved updates, security patches, and necessary applications, may be installed. Any software unrelated to business operations or with unverified sources (e.g., potentially malicious software) is prohibited.

3.7 Monitoring and Logging

- **Audit Logging:** An audit log must be maintained for all software installations and updates. This log will include details such as the software name, version, installer, installation date, system affected, and authorization details. Audit logs must be stored securely and reviewed periodically to ensure compliance with this policy.

- **Incident Investigation:** In case of a security incident or software-related vulnerability, the installation logs and any relevant data will be used to investigate the issue and identify the root cause.

4. Roles and Responsibilities

- **IT Team:** Responsible for evaluating, approving, and testing all software before installation, as well as ensuring that security standards are met.

- **System Administrators:** Responsible for performing software installations and updates, following the approved process, and ensuring that software is installed in compliance with organizational security policies.

- **Department Head:** Responsible for authorizing software installations and updates, ensuring that the proper procedures are followed and that security considerations are prioritized.

- **End Users:** Responsible for adhering to software installation restrictions and only using authorized software within their roles.

22. Security of Off-Site Assets

1. Purpose

The purpose of this policy is to ensure the protection of off-site assets, preventing loss, damage, theft, or compromise of devices and media that store or process information outside the organization's premises. This includes ensuring uninterrupted operations and maintaining the security of client data, assets, and the organization’s reputation.

2. Scope

This policy applies to all employees, contractors, vendors, and any other personnel who use, manage, or access off-site assets, whether owned by the organization or personally owned and used on behalf of the organization. Off-site assets include mobile devices, laptops, external storage media, and any other equipment that stores or processes organizational information.

3. Policy Guidelines

3.1 Authorization and Accountability

- All devices that will store or process organizational data outside of the company premises must be authorized by department head / IT before use.
- Employees and authorized personnel must adhere to this policy to request, track, and record off-site asset usage.

3.2 Off-Site Asset Security and Management

- **Physical Security:** Off-site assets must never be left unattended in public or unsecured locations (e.g., public transport, cafes, etc.). In cases where assets must be temporarily left unattended, they must be secured in a locked, tamper-proof container or similar secure storage solution.
- **Asset Transfer and Chain of Custody:** When assets are transferred among individuals, a clear chain of custody must be maintained using manage engine tool. The chain of custody should be recorded in a secure, auditable log that includes at least the names, organizations, and dates of the individuals handling the asset. Any information on the device that is not necessary for the transfer must be securely deleted before transferring the asset.
- **Environment Protection:** Employees must follow IT do’s and don’t s instructions for equipment protection, ensuring devices are safeguarded from exposure to harmful conditions such as electromagnetic fields, water, heat, humidity, and dust.

3.3 Remote Asset Management and Tracking

- **Remote Wipe and Location Tracking:** Devices that store or process sensitive information must be configured to enable remote wiping capabilities wherever feasible. This ensures that in the event of a loss or theft, the device can be remotely wiped to protect sensitive information.
- **Remote Monitoring:** The organization will implement monitoring tools to track device location and usage. In the event of an unauthorized device removal or suspicious activity, immediate corrective action will be taken.

3.4 Protection Against Information Exposure

- **Screen Privacy:** Employees must take measures to protect against unauthorized viewing (shoulder surfing) when accessing information on off-site devices in public spaces. For instance, using privacy filters, adjusting device screen brightness, or ensuring information is not visible to others in close proximity.
- **Data Encryption:** All data stored on off-site devices must be encrypted, using strong encryption algorithms, both at rest and in transit, to ensure data confidentiality and integrity.

4. Compliance and Auditing

- **Regular Audits:** Regular audits will be conducted to verify compliance with the off-site asset security policy. This will include random checks, and review of asset inventories, **Enforcement and Consequences:** Any employee or contractor found in violation of the off-site asset security policy may face disciplinary actions, including revocation of privileges to remove assets from premises, suspension, or termination of employment, depending on the severity of the violation.

5. Roles and Responsibilities

- **ISMS Steering Committee:** The ISMS Steering Committee will ensure that this policy is communicated, enforced, and reviewed regularly. They will provide the necessary resources for implementation and security measures for off-site assets.
- **IT Security Team:** The IT security team is responsible for implementing the technical controls for encryption, remote wipe, and location tracking, as well as maintaining an inventory of authorized off-site assets.
- **Employees and Contractors:** Employees and contractors are responsible for complying with the policy, ensuring proper protection of off-site assets, and reporting any incidents of theft, loss, or compromise immediately.

Enforcement

Necessary disciplinary action will be taken against any employee not following the policies and procedures laid down by the Choice Equity Broking Pvt. Ltd.'s code of conduct. Similarly, action will be taken against those employees encouraging/observing such an activity and not reporting the same to the concerned authority. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment as per Choice Equity Broking Pvt. Ltd. code of conduct.

Review and Continuous Improvement

This policy will be reviewed annually or in response to significant changes, including new technological advancements or changes in the regulatory landscape. Regular reviews will ensure that the policy remains relevant and effective in securing the installation of software on operational systems.

Reference Documents

- ISO 27001:2022

ISO 27001 CONTROL NUMBERS	CONTROL TITLE
8.24	Use of cryptographic controls
5.20	Addressing information security within supplier agreements
5.9	Inventory of information and other associated assets
5.10	Acceptable use of information and other associated assets
5.12	Classification of information
5.13	Labeling of information
7.10	Storage media
5.14	Information transfer
8.1	User endpoint devices
6.7	Remote working
7.1	Physical security perimeter
7.2	Physical entry
7.3	Securing offices, rooms and facilities
7.5	Protecting against external, physical and environmental threats
7.6	Working in secure areas
7.8	Equipment siting and protection
7.11	Supporting utilities
7.12	Cabling security
7.13	Equipment maintenance
7.9	Security of assets off-premises

7.14	Secure disposal or re-use of equipment
7.7	Clear desk and clear screen policy
5.18	Access Rights
	Compliance with legal and contractual requirements
8.8	Management of technical vulnerabilities
5.9	Inventory of information and other associated assets
5.10	Acceptable use of information and other associated assets
5.4	Management Responsibilities
5.13	Labelling of information
7.14	Secure Disposal or re-use of equipment
5.15	Access control
8.32	Change management
8.8	Management of technical vulnerabilities
8.15	Logging
8.13	Information backup