Choice
The Joy of Earning

CHOICE EQUITY BROKING PVT. LTD

ISMS PROCEDURES

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
Approved On	08-Jan-25	2.2	Abhishek Vinayak	Yogesh Jadhav

Contents

I. Access Control Procedure

Purpose

The Access Control Procedure details the guidelines to be followed for the granting, modifying, reconciling and revoking physical and logical access to the information, information processing facilities, and premises of CHOICE EQUITY BROKING PVT. LTD referred to as CHOICE EQUITY BROKING PVT. LTD henceforth.

This procedure is applicable to all individuals who are provided with access to CHOICE EQUITY BROKING PVT. LTD Information processing facilities and information.

The objectives of this procedure are as follows:

- Ensure that the granting, modifying, reconciling and revoking of access to CHOICE EQUITY BROKING PVT. LTD Information and information processing facilities are performed based on the approval of authorized individuals;
- Ensure that the access rights provided to employees, contractor and third party users posted within the CHOICE EQUITY BROKING PVT. LTD Premises are reconciled on a periodic basis to identify and rectify any inadequate access rights;
- Ensure timely revocation of physical and logical access rights for terminated/transferred/absconding employees, contractors and third party users.

Scope

Access control procedure covers all aspects of the following –

- User Registration and Deregistration
- Review of User access rights
- Password Controls

Access Control Procedure

Business Requirement for Access Control

The steps for granting, modifying, reconciling, and revoking the access rights and privileges for the employees and third party personnel of CHOICE EQUITY BROKING PVT. LTD Shall follow the guidelines presented below:

Access shall be provided to information and various information processing facilities for the employees of CHOICE EQUITY BROKING PVT. LTD and third party personnel only on a need-to-know basis and upon completion of the access formalities. The information processing facilities include desktops, laptops, applications, servers, proprietary information, the CHOICE EQUITY BROKING PVT. LTD network and the CHOICE EQUITY BROKING PVT. LTD Premises and work areas.

External parties shall be provided with access to the aforementioned information processing facilities only if such a requirement is covered in the contract with CHOICE EQUITY BROKING PVT. LTD and the appropriate approvals are obtained by the personnel.

All visitors shall be escorted by an employee of CHOICE EQUITY BROKING PVT. LTD at all times within the CHOICE EQUITY BROKING PVT. LTD premises and shall not be provided with logical access rights. Any exceptions shall be approved by the CISO.

Access to enhanced privileges on any information systems shall be granted by conducting a comprehensive risk assessment & evaluating the necessary controls. Under no circumstances, generic shared IDs be used.

Access Management for Employees

Access Granting Procedures

Sr. No.	Activities	Mandatory (Y/N)	Responsibility
1.	HR team on-boards the new joiners on the first day	Y	HR
2.	During the on-boarding process, the new joiners are requested to fill the new joiner form	Y	HR and New Joiner
3.	New joiner form is to be approved by the appropriate authority	Y	HR
4.	The new joiner form is dispatched to the IT Team for the creation of physical access rights	Y	HR
5.	The new joiner form is dispatched to the IT Team for the creation of domain ID and e mail ID	Y	HR
6.	The IT Team also assigns a desktop or a laptop to the new joiner as indicated in the form	N	IT Staff member
7.	Access to applications/projects shall be provided to the new joiner based on approval of the respective access request mails by reporting manager.	N	IT Staff Member

Access Modification

Sr. No.	Activities	Mandatory (Y/N)	Responsibility
1.	Access Modification request to be made for an employee and appropriate approvals should be taken.	Y	Manager; CISO (if required)
2.	The access modification shall be effected by the relevant team.	Y	IT Staff Member

Revocation of Access Rights

Sr. No.	Activities	Mandatory (Y/N)	Responsibility
	Resigned/Terminated/Retired and Transferred Employees		
1.	The last working day of the employee is communicated to the employee, and the reporting manager of the employee	Y	HR
2.	The IT Team is informed regarding the last working day of the employee at least one day in advance	Y	HR
3.	Employee fills the termination checklist and that the termination checklist is signed off by the relevant personnel before the employee leaves the premises of CHOICE EQUITY BROKING PVT. LTD	Y	HR and employee
4.	Physical and logical access rights of the employee are revoked within one business working day from the last working day of the employee.	Y	IT
5.	In case the email ID of the employee is to be kept active for business reasons, the password of the email ID is changed with immediate effect	N	IT Staff Member
	Absconding Employees		
1.	The reporting manager informs the HR team regarding the uninformed absence of any employee for more than 5 business days	Y	Line Manager

Sr. No.	Activities	Mandatory (Y/N)	Responsibility
2.	The HR team contacts the IT team to temporarily disable the physical and logical access rights of the absconding employee	Y	HR
3.	A letter is sent by the HR team to the employee's residence on the sixth day of continued absence	Y	HR
4.	The CISO is informed in case the employee fails to respond to phone calls and the letter by the fifteenth day of continued absence	Y	HR
5.	The IT team and the security team to permanently revoke the logical and physical access rights of the employee on the sixteenth day The employee is treated as terminated as of the sixteenth day of continued absence	Y	IT Staff Member; CISO (to be informed)

Access Management for Third Party Users

Sr. No.	Activities	Mandatory (Y/N)	Responsibility
	Access Granting Procedures		
1.	Department responsible for the third party personnel informs the HR team	Y	Line Manager
2.	The HR team on-boards the new joiners on the first day	Y	HR
3.	During the on-boarding process, the new joiners are requested to fill the new joiner form	Y	HR and New Joiner
4.	The new joiner form is to be approved	Y	Line Manager
5.	The new joiner form is then dispatched to the Services Manager for the creation of physical access rights	Y	HR
6.	The new joiner form is also dispatched to the IT team for the creation of domain ID and e mail ID	N	IT Staff Member
7.	The IT team also assigns a desktop or a laptop to the new joiner as indicated in the form	N	IT Staff Member
8.	Access to applications shall be provided to the new joiner based on the approval of the respective access request mails by the reporting manager.	N	IT Staff Member

Sr. No.	Activities	Mandatory (Y/N)	Responsibility
	Access Modification		
9.	Access Modification request to be made for a contractor and appropriate approvals should be taken.	Y	Line Manager; CISO (if required)
10.	The access modification shall be effected by the relevant team.	Y	IT Staff Member
	Revocation of Access Rights Terminated Third Party Personnel		
11.	The HR is informed regarding the last working day of the third party personnel at least one day in advance	Y	Line Manager
12.	The HR team ensures that the third party personnel fills the termination checklist and that the termination checklist is signed off by the relevant personnel before the third party personnel leaves the premises of CHOICE EQUITY BROKING PVT. LTD	Y	HR
13.	Physical and logical access rights of the third party personnel are revoked within one business day of the last working day of the third party personnel	Y	IT Team
	Revocation of Access Rights Absconding Third Party Personnel		
14.	The HR is informed regarding the uninformed absence of any third party personnel for more than 5 business days	Y	Line Manager
15.	The HR team contacts the IT team to temporarily disable the physical and logical access rights of the absconding third party personnel	Y	HR
16.	The parent company of the third party personnel is contacted for a replacement	Y	HR

Verification Mechanism

Review of User Access Rights

Sr. No.	Activities	Mandatory (Y/N)	Responsibility
1.	● A review of the user access rights shall be conducted annually. ● The review shall cover the physical and logical access provided to the	Y	Physical – IT / Admin Logical – IT / CISO / Managers

Sr. No.	Activities	Mandatory (Y/N)	Responsibility
	CHOICE EQUITY BROKING PVT. LTD employees and external parties ● The logical rights review shall be conducted by the respective application owners and the results of the review shall be informed to the CISO		

- In addition to the above procedures, HR will provide the list of terminated employees and third party personnel to the CISO, who will then ensure that the physical and logical access rights are revoked for all the personnel mentioned in the list.
- The CISO shall take note of any non – conformities during the access right reconciliation and shall ensure that all unnecessary access rights are revoked by the relevant personnel on an immediate basis.

User Password Management

The password complexity rules in the Windows operating system shall be enabled for all CHOICE EQUITY BROKING PVT. LTD workstations. The following rules shall be implemented:

Password Policy	
Enforce password history	10
Maximum password age	90 days
Minimum password age	1 day
Minimum password length	8 characters
Passwords must meet complexity requirements	Yes
Account Lockout Policy	
Account Lockout Duration	30 minutes
Account Lockout Threshold Reset Account Lockout counter after	5 invalid logon attempts 30 minutes

Administrator Password Management

All the administrator account details (OS, Networking devices etc.) shall be stored securely.

User Responsibilities

It is the responsibility of all employees of CHOICE EQUITY BROKING PVT. LTD to ensure that they follow these steps to minimize the risk of unauthorized user access and theft of information:

- Employees shall not share user IDs and passwords with anyone else;
- Employees shall choose complex passwords that cannot be easily guessed;
- Employees shall ensure that they log out of their computing devices, and the applications during periods of inactivity;
- Employees shall not leave their computing devices unattended when an active session is in progress.

Secure Log on Procedures

Employees of CHOICE EQUITY BROKING PVT. LTD shall follow secure log on procedures while logging into their computing devices and applications inclusive of the following:

- Employees shall ensure that there is nobody standing over their shoulders while logging in;
- Employees shall ensure that the passwords are masked for security;
- Employees shall ensure that their login credentials are not written down anywhere.

Use of System Utilities

The access to system utility programs such as registry editor, group policy editing shall be restricted only to the infrastructure team as they perform the role of system administrators. Other employees shall not have access to such programs.

Mobile Computing and Teleworking

Certain employees of CHOICE EQUITY BROKING PVT. LTD are provided with laptops and remote access in order to facilitate teleworking. The following guidelines shall be followed for teleworking:

- All employees who are assigned laptops shall be made aware of the risks involved in handling of laptops prior to allotting the device to the employee.
- The details of the laptop and the employee it is assigned to are updated in the asset register maintained by the IT team.
- All devices shall be password protected.
- The security team shall advice the employee and facilitates the reporting of the loss to the appropriate authorities.
- An employee shall be granted with remote access rights only upon obtaining the approval of the reporting manager and the CISO through the access modification process.
- Remote access shall be over a secure network connection to prevent unauthorized access.

Compliance

All users are requested to comply with this procedure. In case of breach/violate, the user would be subjected to disciplinary action. Violations shall be notified to *CISO.* Strict confidentiality shall be maintained on all notified violations.

Related Documents

ISMS_Logical Access Policy
ISMS_Remote Working Policy
ISMS_Supplier Management Policy

II. Antivirus Management

Purpose

The objective of this antivirus procedure is to provide a secure computing environment where the entire business data is processed. All machines at CHOICE EQUITY BROKING PVT. LTD shall be configured as per this procedure.

Scope

The information systems provide CHOICE EQUITY BROKING PVT. LTD with access to Business and confidential information. Deployment of servers is restricted to business purposes and System Administrators must be aware of and accept the terms and conditions of use especially the responsibility for the protection of the security of information held on such devices and processed using these devices.

The procedure is applicable to all employees of CHOICE EQUITY BROKING PVT. LTD and all third party personnel posted within the premises of CHOICE EQUITY BROKING PVT. LTD

Antivirus Procedure

Policy Enforcement

Installation for all Antivirus servers shall be done in the following manner.

- Groups should be created separately for desktops, laptops and servers.
- Should create separate policies for each group.
- Should create separate client packages for each group with specified policies.
- Should be up-to date with all product updates and virus definitions.
- Live update to be configured to fetch updates from internet every hour.
- All the clients connected to the management console should be monitored on a regular basis.

All Assets – Laptop, Desktop and Server

Policy for all desktop shall be configured in the following manner.

Antivirus and Antispyware policy

- o Administrative full scan should be scheduled once a week.
- o Auto protect should be configured in such a way that it cannot be disabled.
- o For auto protect as well as scheduled scan the first action on virus detection should be clean and the second action should be quarantined.
- o Displaying notification on the infected computer should be disabled.

Firewall Policy

- Firewall policy should be enabled for all machines.
- Firewall rules to be kept default unless for specific requirements
- NetBIOS protection, Allow token ring traffic, Reverse DNS, anti MAC spoofing should be enabled in the firewall policy.

Intrusion Prevention Policy

- Intrusion prevention should be enabled.
- Denial of service detection and port scan detection should be enabled under this policy.

Application and Device Control

- Application and device control policy should be enabled on all the computers.
- Editing of host files should be prevented using appropriate rule.
- Should block programs running from removable drives.
- Registry keys and client files should be protected
- Execution of Autorun should be disabled.

Live Update

- Live update of internal clients should use the default management server.
- Communication setting in the management server is to be configured in push mode so that at the same time when the server gets an update, it will push the update to all the clients connected.

Compliance

Violations may result in disciplinary action in accordance with company policy. Failure to observe these guidelines may result in disciplinary action by CHOICE EQUITY BROKING PVT. LTD depending upon the type and severity of the violation, whether it causes any liability or loss to CHOICE EQUITY BROKING PVT. LTD, and/or the presence of any repeated violation(s). Violations shall be notified to the *CISO.* Strict confidentiality shall be maintained on all notified violations.

Related Documents

ISMS_Network Security Policy

ISMS_Incident Management Policy

III. Asset Management

Purpose

The Asset Management Procedure contains the procedures for the identification, inventory, inventory verification, maintenance, and acceptable use of the information assets of CHOICE EQUITY BROKING PVT. LTD,, referred to as CHOICE EQUITY BROKING PVT. LTD henceforth. The Procedure also contains the information classification guidelines, information labelling and handling procedures.

The objectives of this procedure are as follows:

- Ensure that all information assets of CHOICE EQUITY BROKING PVT. LTD Are identified, inventoried, and assigned owners;
- Ensure that the rules for acceptable use of assets are implemented;
- Ensure that all information is handled by CHOICE EQUITY BROKING PVT. LTD It is classified based on the value, legal requirements, sensitivity and criticality to CHOICE EQUITY BROKING PVT. LTD;
- Ensure that appropriate handling procedures are implemented for the information categories.

Scope

This procedure will apply to all CHOICE EQUITY BROKING PVT. LTD Information assets and to all personnel responsible for these assets i.e.

- Asset Owners
- Asset Users

Entry Criteria

This procedure would be triggered by the following, but not limited to, activities –

- Acquisition of new information assets
- Maintenance of information assets
- Disposal of information assets
- Handling and classification of information assets

Asset Management Procedure

Asset Categories

The assets of CHOICE EQUITY BROKING PVT. LTD have been categorized into the following asset categories:

a) Physical Assets / IT Infrastructure
b) Information – Softcopy
c) Information - Hardcopy
d) Software
e) Services
f) Personnel

For list of all information assets at CHOICE EQUITY BROKING PVT. LTD, kindly refer *Asset Registers (in Tool).*

Key Activities

Sr. No.	Activities	Mandatory (Y/N)	Responsibility
	Physical / IT Infrastructure Asset		
8.	**Inventory of Assets** The owner of the Physical / IT Infrastructure assets is the IT Team along with the facilities team.	Y	Asset Owners
9.	The asset inventory will be updated by an identified IT team member whenever a new asset is procured by CHOICE EQUITY BROKING PVT. LTD, or an existing asset is decommissioned or disposed.	Y	IT Staff Member ; IT Manager
10.	A physical verification of the asset inventory shall be conducted on an annual basis by the IT team to ensure accuracy of the asset inventory. The results of the physical verification shall be reported to the IT Manager	Y	IT Staff Member ; IT Manager
11.	**Maintenance of Assets** Regular contact with the AMC service providers for the hardware assets and monitors the activities of the service providers to ensure that the hardware assets are maintained in proper working condition	Y	Asset Owner
12.	**Authorization for the Acquisition of Assets** The authorization process for the acquisition of assets shall follow the relevant change management procedure.	Y	Asset Owner
13.	**Disposal of Assets** The following procedures shall be followed for the disposal of assets: • All data existing on the hardware will be deleted by the infrastructure team through secure methods such as wiping the hard disks • The infrastructure team will format the hard drive of all laptops and desktops before disposal or re – assignment of the devices to a different employee	Y	Asset owner

Sr. No.	Activities	Mandatory (Y/N)	Responsibility
	• All application and configuration data shall be cleared from servers by the infrastructure team prior to disposal or movement of the devices outside CHOICE EQUITY BROKING PVT. LTD premises • All hard disks must be physically destroyed prior to disposal		
	Software Asset		
14.	**Inventory of Assets** An inventory of all the software assets is maintained. The respective application owners are responsible for providing the details regarding the software assets to the IT team member maintaining the inventory. Whenever new software is acquired by CHOICE EQUITY BROKING PVT. LTD, it is the responsibility of the application owner to inform the infrastructure team and ensure that the asset inventory is updated.	Y	Asset Owner
15.	**Maintenance of Assets** The following activities shall be carried out for the maintenance of software assets: • Ensure that the changes and customizations made to the software assets follow the relevant change management procedures • Ensure that the software licenses are acquired in adequate number, and are renewed when necessary • Ensure that a Vulnerability Assessment and a Penetration Test is carried out for the software asset on an annual basis, where applicable • Ensure that the necessary patches are tested by the application team, and installed on a timely basis for the software assets	Y	Asset Owner
16.	**Authorization for the Acquisition of Assets** The authorization process for the acquisition of assets shall follow the relevant change management procedure	Y	Asset Owner

Sr. No.	Activities	Mandatory (Y/N)	Responsibility
17.	**Disposal of Assets** This section is not applicable for the Software asset category.	Y	Asset Owner
	Service Assets		
18.	**Inventory of Assets** The network administrator and the security teams are responsible for maintaining the inventory for service assets. The inventory shall be maintained in the asset register. Any service asset acquired by CHOICE EQUITY BROKING PVT. LTD shall be updated in the asset inventory by an identified person within the administration team. A physical verification of the asset inventory shall be carried out on an annual basis to ensure accuracy of the asset inventory.	Y	Asset Owner
19.	**Maintenance of Assets** The administration team maintains regular contact with the AMC service providers for the service assets and monitors the activities of the service providers to ensure that the assets are maintained in proper working condition.	Y	Asset Owner
20.	**Authorization for the Acquisition of Assets** The authorization process for the acquisition of assets shall follow the relevant change management procedure.	Y	Asset Owner
21.	**Disposal of Assets** This section is not applicable for the Service assets.	-	-
	People Asset		
22.	The procedures relating to people asset management are outlined in the Human Resources Security Policy User Access Management Procedure	-	-
	Paper & Electronic Document Asset		
23.	It is essential to classify information according to its actual value and level of sensitivity in order to deploy the appropriate level of security. With the exception of information that is already in the public domain,	Y	Asset Owner

Sr. No.	Activities	Mandatory (Y/N)	Responsibility
	information should not be divulged to anyone who is not authorized to access it or is not specifically authorized by the information owner. Violations of the Information Classification guidelines should result in disciplinary proceedings against the individual.		

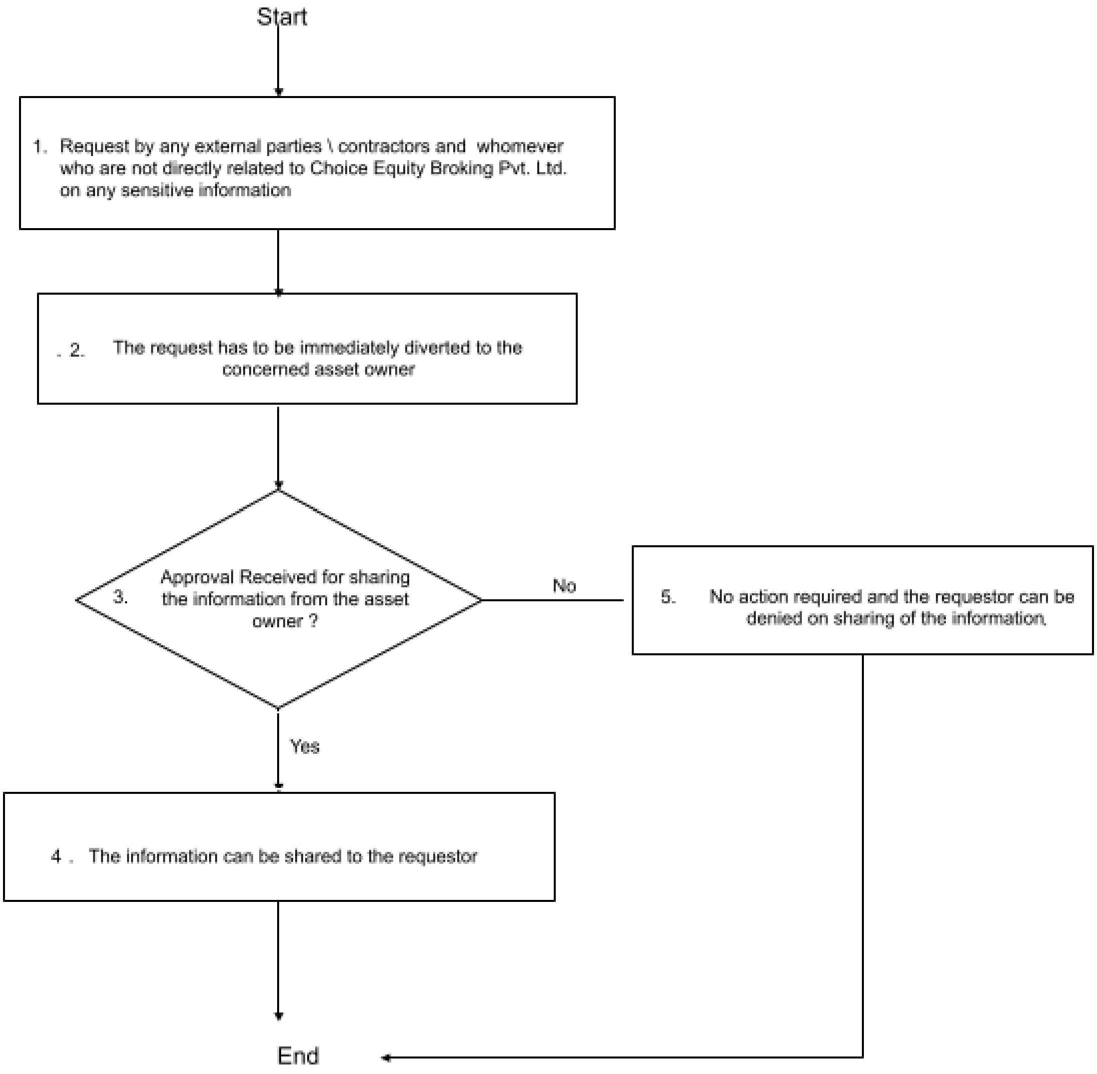
Sharing Sensitive Information

Key Activities

S.No	Input	Activities	Measurements/ Control measures	Output	Responsibility
1,2	Request by any external party whomsoever is not directly related to the CHOICE EQUITY BROKING PVT. LTD Operations	Any request from contractors, external parties and whomsoever not related to CHOICE EQUITY BROKING PVT. LTD directly has to be redirected to the concerned Asset owner for approval prior sharing the information	100% of all requests from external parties need to undergo this process flow	Request for demand of sensitive information by the external party is submitted for approval from the concerned Asset owner	Asset owner
3	Acknowledgement of approval by the asset owner	On analysis the Asset owner can decide on approving / disapproving the request	-	Approval/disapproval of the request	Asset owner

S.No	Input	Activities	Measurements/ Control measures	Output	Responsibility
4,5	Receipt of consent from the asset owner	On approval the information can be shared with the concerned parties On the Asset owner disapproving the request, the information shouldn't be shared strictly	100% of request need to pass through the consent of the asset owner	Dependent on the consent from the asset owner the sharing of information would take place	Asset owner

Process Flow


Start
1. Request by any external parties \ contractors and whomever who are not directly related to Choice Equity Broking Pvt. Ltd. on any sensitive information
. 2. The request has to be immediately diverted to the concerned asset owner
3. Approval Received for sharing the information from the asset owner ?
No
5. No action required and the requestor can be denied on sharing of the information.
Yes
4 . The information can be shared to the requestor
End

Compliance

All users shall comply with this process. In case of breach/violation to this process, the user shall be subjected to investigation and disciplinary action supervised by HR. HR disciplinary actions and procedures apply. Violations shall be notified directly to CISO

Strict confidentiality shall be maintained on all notified violations.

Related Documents

NA

Guidelines for Equipment Disposal by Third Party

- Where the destruction or disposal of IT equipment is carried out on behalf of CHOICE EQUITY BROKING PVT. LTD by a third party, there shall be a contract with that third party which appropriately evidences:
    - that third party's obligations to keep that data confidential and;
    - that third party's responsibility for the secure disposal of the data.
- In any case where IT equipment is to be passed on by CHOICE EQUITY BROKING PVT. LTD for reuse, those staff involved in the sale or transfer of the equipment shall ensure that any information on the equipment has been irretrievably destroyed and that any other appropriate issues, including, but not limited to, the safety of the equipment are satisfactorily addressed

IV. ISMS Internal Audit Procedure

Scope of the Audit

All Data Center processes across all the locations within the scope of the ISMS (Ref: ISMS_ISD_DOC) must be audited periodically to ensure compliance to the Information Security policies, controls and procedures defined and implemented.

Audit Methodology

Audit Requirements

In preparation for an audit the following topics should be adequately addressed

- Scope of the audit
- Audit criteria
- Focus area(s) of audit
- Resources required for execution

The auditors shall have a thorough understanding of the ISO/IEC 27001:2022 standards and its requirements before the audit. They shall review the existing security policies, procedures, guidelines and documents for adequacy against the requirements and also if they address the business risks.

The audits should be carried out by individuals independent of the area under review; an auditor should never have to audit his / her own work. The audit must also take into consideration the status and importance of the audit area, its functions and sensitivity. Auditor selection must ensure the impartiality of the activity.

The audit shall maintain objectivity and probe for compliance to controls as opposed to non-conformities. The audit should be initiated and driven by the Information Security Management Forum.

The audits must also consider and review the results of previous audits and verify that resolved NC's have indeed been closed and been effective.

Audit Schedule

This must be at minimum once a year for effectively identifying and resolving the non-conformities and areas for improvement. The audit schedule and individual plans must be drawn up and communicated to all relevant personnel beforehand to ensure adequate participation and effectiveness.

Procedure for Internal Audit

Planning the Internal Audit

- Internal communication amongst interested parties, including employees of the organization.
- External communication with customers, partner's entities, local community and other interested parties including media.
- The internal audit team or ISMS audit team will be responsible to conduct the internal ISO 27001 audit in accordance with the guidelines given in ISO/IEC 27001:2022 standard, for scope defined in the ISMS scope document.
- The audit team shall prepare an annual ISO 27001 internal audit plan post consultation with the Information Security Management Forum (ISMF).
- The audit team shall incorporate the changes suggested by ISMF and the audit plan shall be finalized.
- The audit team in coordination with the Information Security Officer henceforth referred to as ISO shall conduct a pre audit meeting at least a week in advance with the Information Security Representatives to inform them about the internal audit and to discuss areas of concerns that need to be addressed.
- ISMS audits will be conducted twice in a year to assess the efficiency of Security System and to determine the controls and procedures of ISMS are effectively implemented, maintained and conform to relevant legislations, standard and security requirements and perform as expected. Information Security Management Forum will prepare an Internal Audit Plan.

Appointment of Internal Auditor

- The members of Information Security Management Forum shall appoint the Lead Auditor, for the carrying out the internal audit as per the schedule.
- The appointed Lead Audit shall be independent of the area to be audited and must have at least undergone an ISO 27001:2022 Lead Auditor training.
- The Lead Auditor would conduct the ISO 27001 internal audit as per the audit plan with the assistance of the ISO.

Internal Audit Process

- The Lead Auditor shall conduct an opening meeting to inform the purpose, scope of the audit, the audit methodology and address any questions in regards to the internal audit.
- The Lead Auditor shall conduct a detailed documentation review of the ISMS mandatory documents, DC policies, procedures, prior audit reports and corrective action reports.

- Post completion of the documentation review, the auditor shall conduct the onsite audit by means of interviews with the auditee, assessing the practical implementation of controls, which, may include investigation of associated records and testing the effectiveness of controls satisfying the requirements of the ISMS or the Choice Equity Broking Pvt. LTD's policies, procedures and guidelines.
- The Lead Auditor shall make use of the audit work papers to note audit findings and to collect sample evidences as required.
- The Lead Auditor shall provide a detailed ISO 27001 internal audit report to the internal audit team post completion of the audit as per the format attached in Appendix at the end of this document.

Note: In view of the COVID-19 pandemic situation due to the travel restrictions the internal/ external audits were conducted remotely over secured WebEx sessions. ISMS forum has been apprised during the management review meetings.

The internal audit report findings shall be classified as –

- Major non-conformity – The absence of, or the repeated failure to implement and maintain, one or more required ISO 27001 management system elements, or a situation which would, on the basis of objective evidence raise significant doubt as to the capability of the ISMS to achieve the Information Security Policy and Objectives of the organization.
- Minor non-conformity – The failure to implement and maintain, one or more required management system elements, or a situation which would, on the basis of objective evidence raise doubt as to the capability of the ISMS to achieve the Information Security Policy and objectives of the organization.
- Observation and opportunity for improvement (OFI) – Any recommendations or opportunities for improvement that are not classified as a Major or Minor, which may be based on subjective elements and industry good practice seen elsewhere which assist in improvement of the Choice's ISMS.
- The internal audit team shall present the internal audit report to the ISMF for review.

- The report shall further be provided to the ISO for development and implementation of the corrective actions.

Corrective Action Follow up

- The Lead Auditor shall make a follow-up audit to check the implementation of corrective action as stated on the Corrective Action report, if deemed necessary by the ISMF.
- Post receiving the satisfactory report for the corrective action implementation from the Lead Auditor, the non-conformity shall be considered to be closed.
- If follow-up audit is not conducted, the lead auditor shall review the corrective action reports during the next internal audit.

Reporting and Follow up

Reporting Structure

The audit function should ideally be an independent function with direct reporting to the Information Security Management Forum, but where this is not feasible a cross functional auditing team may be formalized factoring the independence required in the audit.

The audit team must submit the audit report and findings directly to the Information Security Management Forum to avoid any undue influence from the implementation team or auditees.

Non Conformance Closure / Verification

The audit team shall also play a part in verification of resolution of reported non conformities and subsequently reporting back to the ISMF.

For identified deviations from normal operations or Non Conformities (NCs) Corrective action reports shall be prepared stating the actions taken to close the NCs and those taken to prevent recurrence of the same deviation in the future.

The audit records along with the corrective actions must be maintained as records for a specified period of time.

Refer ISMS_IA_FOR for the Audit report format.

Audit Team

Competence and Skill

The appointed Lead Audit shall be independent of the area to be audited and must have at least undergone an ISO 27001:2022 Lead Auditor training.

Where required external specialist organizations may also be considered for a completely independent review.

Annexure A – Audit Plan Template

Sr. No.	Function/Department	Key Auditee(s)	Auditor(s)	Date of Audit	Time of Audit	Location
J. B. Nagar						
Marol						

V. Corrective Actions Procedure

Purpose

The process of reacting to an existing non conformity, fixing it and ensuring it does not reoccur is called corrective action.

Identified and reported non conformities must be closed within an agreed timeframe. It is important to analyze and where feasible carry out a root cause analysis to determine the cause for the deviation from the standard requirements or policy requirements.

Upon determining the cause, it is imperative that immediate corrective or remedial action be taken to contain the incident. This Corrective action must be documented for review and approval by the ISMF. The next step in ISMS improvement is to identify steps to verify the effectiveness of the corrective action. Once this has been confirmed, an analysis on whether similar vulnerabilities or weaknesses exist in similar processes needs to be identified and the corrective action to be applied across the ISMS.

Procedure

Adequate mechanisms to investigate reported non conformities and arrive at corrective actions to prevent occurrence/ recurrence shall be implemented to ensure continued improvement of the ISMS.

Seven step handling methodology has been established to deal with the identified or suspected non conformances. The following steps are to be considered for all issues:

1. Identification of the problem (Audit reports, staff observations, service requests, process monitoring, risk analysis, incident reports, etc.)
2. Evaluation of the magnitude of impact and the level of action required
3. Investigation – This involves identifying the resources involved, the objectives of the investigation, assignment of responsibilities.
4. Analysis of the findings to determine every possible cause and to further identify the root cause. This is essential and critical to corrective actions.
5. Summarizing the tasks required to resolve the issue into an action plan detailing specific changes to be made, responsibilities and timelines – Corrective Action Report.
6. Implementation of the devised action plan and monitoring procedures after due authorization.
7. Follow up i.e.; evaluating the actions taken in terms of completion of identified tasks, appropriateness and effectiveness of the action taken.

Corrective Action report must be documented for every non-conformance raised during the audit. However, documenting the corrective action report including root cause of the observation and learning from the observation raised during is not mandatory and also for the following –

- Major IS incidents, concerns raised etc.
- Inputs or observations from internal or external audits.
- Feedback from interested parties and stakeholders.
- Information security breaches / incidents.
- Violations in implementation of ISMS.

The objective of this procedure is to identify the cause of the problem and to take suitable action to eliminate the cause to prevent occurrence/recurrence as the case may be.

All corrective actions should be approved by the ISMF before implementation.

Note: The corrective actions taken for identified Non Conformities shall be recorded in the Non Compliance Corrective Actions (NCCA) Tracker.

Annexure A – Non Compliance Corrective Actions (NCCA) Tracker Template

- NCCA Tracker Template

VI. Human Resources Security Procedure

Introduction

The objective of this procedure is to ensure that Choice Equity Broking Pvt. LTD employees, contractors and external party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risks of human error, theft, fraud or misuse of facilities.

Scope

This policy applies to all Choice Equity Broking Pvt. LTD employees and third party personnel providing various services to Choice Equity Broking Pvt. LTD

General

Choice Equity Broking Pvt. LTD shall lay down security roles and responsibilities, and document them wherever appropriate. These responsibilities shall include any general responsibilities for implementing or maintaining security policy (Ref A.5.1 ISMS Policy ISO/IEC 27001:2022) as well as any specific responsibilities for the protection of particular assets or for the execution of particular security processes or activities.

All employees, third party personnel working at Choice Equity Broking Pvt. LTD premises must be trained on information security policies and procedures. Adequate information security awareness shall also be imparted to prevent occurrence of any incidents.

Prior to accessing Choice Equity Broking Pvt. LTD Information processing facilities

Choice Equity Broking Pvt. LTD shall ensure that background checks are done for employees and contractors/contingent workers prior to the commencement of work especially for sensitive jobs.

Background verification checks should include but not limited to :-

- Address Verification
- Previous Employment Check
- Educational Qualification

Choice Equity Broking Pvt. LTD shall identify requirements for confidentiality or non-disclosure agreements for employees and external parties reflecting the organization’s need for the protection of information and shall regularly review these agreements.

During the course of work/ engagement

Choice Equity Broking Pvt. LTD shall provide appropriate awareness trainings and regular updates in organizational policies and procedure to all employees of the Choice Equity Broking Pvt. LTD and where relevant to contractors and external party users as relevant for their job function.

Choice Equity Broking Pvt. LTD shall follow a formal disciplinary process for employees who have violated any of the organizations policies.

Termination/Change of work/ engagement

Choice Equity Broking Pvt. LTD shall follow a termination / change of role process to include the return/review of all previously issued information and information processing assets.

Choice Equity Broking Pvt. LTD shall ensure that the access rights of all employees, contractors and third-party users to information and information processing facilities is removed upon termination of their employment, contract or agreement or adjusted upon change.

VII. Patch Management Procedure

Purpose

The purpose of this procedure is to ensure that software patches are applied on the information systems in accordance with the approved business and technical requirements.

Scope

This procedure applies to all CHOICE EQUITY BROKING PVT. LTD employees, contractors, consultants and temporary staff hereafter referred to as “users”.

Patch Management

Step. No.	Input	Activities	Measurements/ Control measures	Output	Responsibility
1	Patches released by the vendors. This includes but not restricted to the below: **Server -** OS SP, Hotfixes, Security patches,Exchange Patches, Software Application Patches (Office applications),Blackberry Patches,SAN Patches, SQL Server patches **Security -** ISA, Symantec,RSA, Firewall management servers, RFA, Firewall Management Patches, SMS Server related patches.	The security and the server team need to identify the new patches whichever is released under their respective domain	100% of all the applicable patches need to be identified	Identified patches are run through the test bed for further proceedings	IT Team
2,3	Identified patches from the respective vendors would be the input for this process step	*Risk assessment conducted for the need of implementation of patches and implementation scheduled for the patches required * Testing of the patches required carried out in the test environment	All the patches required to be implemented need to be tested in the test bed	Output of the test bed along with rollback plan need to be captured and submitted to the IT Manager for acknowledgement .	IT Team
Step. No.	**Input**	**Activities**	**Measurements/ Control measures**	**Output**	**Responsibility**

6	Approval from CHOICE EQUITY BROKING PVT. LTD based on the test results for implementation of the patches	The engineer need to raise a Change Request through Assyst for applying the Patch/Hotfixes mentioning the Time of Execution, Duration required, Impact.	All Patches/ Hotfixes implemented need to pass through the Change Request available in Assyst	Change to be approved as per the change approval matrix	IT Team & CISO
7,8,9	Updated change request in Assyst	IT Team need to check for the approval/Dismissal of the Change Request	-	For the approved changes, the IT team needs to proceed with the implementation	IT Team & CISO
10	Implementation of Patch/Hotfixes	Check for any impact post implementation	-	Information to CHOICE EQUITY BROKING PVT. LTD on the closure of the change request.	IT Team

Compliance

All users are requested to comply with this procedure. In case of breach/violation, the user would be subjected to disciplinary action. Violations shall be notified to *CISO.* Strict confidentiality shall be maintained on all notified violations.

Related Documents

VIII. Procedure for Control of ISMS Documents and Records

Purpose

The purpose of this procedure is to:

- Establish effective control over the preparation, authorization, issue, distribution, maintenance, integrity and subsequent change (if any) of documents required by the ISMS, in all process areas.
- Establish effective control over the ISMS records for identification, storage protection, retrieval, retention time and disposition of records.

Scope

This procedure is applicable to all ISMS documents such as policy and procedures. This procedures is also applicable to ISMS records including, but not limited to, records of incident management, change management, minutes of steering committee meetings, equipment maintenance records etc.

Control of Documents

All new issues of ISMS documents as well as revised versions owing to changing practices are initiated, reviewed, approved and issued through the following method.

Structure of ISMS Documents

All ISMS documents contain the following document control information:

a) The first page shall contain organization name, document name and version

b) The information given in Header and Footer are organization name and logo, Classification of document, and organization website.

To record the revision history, the following details would be captured:

a) Version number

b) Author

c) Date of the revision

d) Details about the changes made to the document

The revisions would be approved and the following details would be captured:

a) Name of the approver

b) Signature

c) Date of review and approval

All ISMS related documents shall follow the naming convention detailed below:

CHOICE_ISMS_<Name of Document>VXX.Y

The version number shall be included in the name of all the ISMS documents. The version number is indicated by VXX.Y where V is the short form for version, XX indicates major version number, and Y indicates the minor version number.

Preparation of the Documents

All ISMS system documentation that includes ISMS policy and other relevant policies and procedures shall be prepared by the concerned process owner. The details shall be entered in the applicable standard formats. Any new documents that need to be generated shall be identified by the concerned department in consultation with the CISO and the activities mentioned above will be executed.

All major changes to the documents would be controlled by the change management. A major change to the document would be an update that modifies the outcome of the process and affects the operations and service.

Minor updates or amendments to the documents would be agreed upon between the department and CISO.

Review and Approval of Documents

ISMS documentation shall be reviewed for adequacy of contents, clarity and also approved before distribution. All documents shall be reviewed by the corresponding process owner(s), CISO and approved by the IT Director.

Distribution and Control of Documents

The original - approved documents shall be maintained by the CISO

A soft copy of the documents shall be uploaded on the intranet portal. This will enable all employees to access the ISMS documentation.

“Read-Only” access will be provided for the documents uploaded on the intranet. This will ensure that the documents on the intranet are not tampered / changed by anyone.

At any given moment, the ISMS documents on the intranet will be considered as a “Controlled Copy”. Any print out or downloaded version of the document available on any desktop / server (apart from the one on the intranet) will be considered as “Uncontrolled Copy”.

The original document of the superseded versions will be stamped as “obsolete”.

When the documents undergo revision, the revised versions will be verified for completeness and accuracy before distribution; the CISO will ensure that the obsolete versions are simultaneously withdrawn from use. The obsolete versions are to be retained for three years.

When there is a requirement to distribute certain ISMS documents to an outside agency the issue will be made after prior approval from the IT Director. The copies so issued, will be stamped as “Uncontrolled Copy”.

Master list of Documents

A Master List of ISMS documents shall be maintained by the CISO. The following details should be captured:

a) Latest Version Number
b) Document Title
c) Approval Date
d) Document Storage (Link to the document on the intranet)

A review and approval of ISMS documentation will be conducted every year or as and when a change is requested. The Master list will also be updated accordingly.

Changes to Documents

A review and approval of ISMS documentation will be conducted every year or as and when a change is requested. The Master list will also be updated accordingly.

Any department / team requiring a change in the ISMS documents will initiate the change via discussion with the CISO. Depending on the type of update required a Change Request will be raised. All changes will be subject to the same review and approval process given above. The changes will be captured in the version history of each document.

Control of Records

General Guidelines

Records shall be created and maintained to provide evidence of conformity to requirements and the effective operation of the ISMS. They shall be controlled. Records shall be legible, readily identifiable and retrievable. The controls needed for the identification, storage, protection, retrieval, retention time and disposition of records shall be documented.

Various records that are to be maintained are provided within the ISMS procedures

Records will be collected, filed, stored and maintained by the concerned departments / teams in such a way that deterioration, loss or damage is prevented and they can be easily retrieved. They will also be written / entered in a legible manner.

Access to the records should be on a need-to-know basis.

The files containing records will be stored under lock and key in filing cabinets / cupboards and will be periodically checked for any deterioration and / or damage. The respective process owner will be responsible for key security.

These records (e.g. Training Records, test protocols, etc.) are not controlled by change management, they are the objective proof for performance of demanded actions.

Retention of Records

The records are required to be kept for one year. At the end of one year, Management shall decide on the retention requirements of the records.

Compliance

All users are requested to comply with this policy. In case of breach/violate, the user would be subjected to disciplinary action. Violations shall be notified to soc@choiceindia.com. Strict confidentiality shall be maintained on all notified violations.

Related Documents

- Document Change Request Template

DOCUMENT CHANGE REQUEST NOTE					
From: Name of the Employee/Auditor/Copy Holder			To: Department Head		
DETAILS OF DOCUMENT TO BE REVISED					
Document		Issue		Revision	
Title	Number	Number	Date	Number	Date
Current text of the document to be changed (Give Accurate details of the Page No./Exhibit/Note to be Changed)					
Nature of Revision & Reason for Revision					
FOR USE OF APPROVING AUTHORITY (ISO / ISMF)					
Request Approved / Not Approved					
Remarks (IF Any):					
Signature			Date		

Approving Authority					
FOR USE OF ISO					
Request Approved / Not Approved					
Remarks (IF Any)					
Signature ISO				Date	
DETAILS OF DOCUMENT AFTER REVISION (ISO)					
Document		Issue		Revision	
Title	Number	Number	Date	Number	Date

VIII. Backup and Restoration Procedure

Purpose

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

The primary use of this document is to implement the controls for data backup as specified within Data Backup Policy. The document serves:

- As the process document for the process owners
- To define various templates for data backup process

Scope

The scope of this document is to provide detailed procedures and templates for implementation of Data Backup Policy of Choice.

Responsibility and Authority

Refer to the Roles and Responsibilities document.

Definition

- Backup - The saving of files / database onto magnetic tape or other offline mass storage media i.e. USB hard drive for the purpose of preventing loss of data in the event of equipment failure or destruction.
- Archive - The saving of old or unused files / database onto magnetic tape or other offline mass storage media for the purpose of releasing on-line storage room.
- Restore - The process of bringing off line storage data back from the offline media and putting it on an online storage system.

Procedure

Creation of backup schedule

- Application / information n owners will create the backup schedule for all critical systems being used by Choice
- The backup schedule for On-Premises and Cloud will mention the frequency and the data that is going to be backed up
- Backup team will follow the schedule and take backups accordingly.

Backup Timing

Full backups for On-Premises and Cloud are performed on all trading day evening as per schedule.

- Full backups for On-Premises and Cloud are performed every day evening as per defined schedule.
- Weekly Full backups for On-Premises and Cloud are performed as per defined schedule
- Monthly backup for On-Premises and Cloud is performed as per defined schedule.
- Backup for UAT On-Prem servers shall be taken as per requirement of the Application Owners

Backup Procedure

- During the regular backup routine, the Backup team will take the backup as per the Backup Schedule.
- The backup activity for On-Premises and Cloud will be closely monitored and logged. Application / information owner will be informed incase of any undesirable event. Application / information owner will verify the facts and any non-compliance would be reported to the LOB Head.
- The backup tapes will be rotated after the completion of the backup cycle

Tape Labeling

- All backup stored on media / storage must be appropriately labeled and the label should be noted down in the Backup Register.
- The backup on tapes /storage would always be kept offsite / different Availability Zones for any disaster management.

Backup Restoration Testing

- Backup team will conduct restoration testing on the backed-up tapes/Storage. The activity should be scheduled in a round robin way, so that each application tapes should be tested on a sampling basis at least once in three months.
- Backup team will locate the backup tape/Storage path and will try to restore the same on an identified system (can be a test machine).

- Backup team will maintain evidence of back up restoration success / failure
- Users that need files restored must submit a request to the Technology team. Include information about the file creation date, the name of the file, the last time it was changed, and the date and time it was deleted or destroyed.
- Backup Storage Locations:
  - Tapes used for backup shall be stored in a safe locker and also in other office premises.
  - Backup taken on Cloud Storage shall be stored in three different availability zones

Backup Operations

- Backup Storage
  - There should be a separate or set of tapes for each backup day including Monday, Tuesday, Wednesday, and Thursday.
  - Backups performed Monday through Thursday shall be kept for one week and used again the following appropriate day of the week.
  - At least one full backup set should be stored offsite. All backups should be stored at secure locations with controlled environment. At least one set should be kept in a safe locker/Storage.
  - A comprehensive record of storage should be maintained. Offsite storage should be carefully planned considering physical access, transportation procedures etc.
- Tape Cleaning

Tape shall be cleaned and the cleaning tape shall be changed as per usage and manufacturer specification.

- Logging
  - Detailed logging of the backup operation should be enabled. Once the operation is completed, the log-file must be checked whether all the relevant data was really backed up and if any faults occurred during the back up.
- Retention
  - All monthly backup tapes will be retained for at least 7 years
  - Emails will be retained for at least 7 years
- Data Backed Up
  - Data to be backed up include but not limited to the following information:
    - Production web server
    - Production database server
    - Production Trading Server
    - UAT Servers

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	

IX. Communication Procedure

1. Purpose

The purpose of this document is to define the communication procedure for ensuring the security of information related to the Equity Broking business in compliance with the **regulatory requirements** and the requirements of the **Information Security Management System (ISMS)** framework. This document aims to ensure that all communication related to information security, data protection, and compliance is managed effectively, securely, and in line with the company’s ISMS policy.

2. Scope

This communication procedure applies to all employees, contractors, third-party vendors, and other stakeholders who have access to the organization's information systems, and it covers all forms of communication including:

- **Internal communications** within the company
- **External communications** with clients, regulatory bodies (SEBI), vendors, and other third parties
- **Incident reporting and escalation**
- **Confidentiality and security in communication**

3. Objectives

- Ensure that communication regarding information security (IS) and data protection is managed effectively and securely.
- Establish clear and consistent channels for information security-related messages.
- Ensure compliance with regulatory requirements and ISMS standards.
- Protect sensitive and confidential information during internal and external communications.
- Establish communication guidelines for incident reporting, risk management, and compliance reporting.

4. Roles and Responsibilities

- **Chief Information Security Officer (CISO):** Responsible for overseeing the implementation and management of the ISMS and ensuring compliance with communication standards related to information security.
- **Legal and Compliance Officer:** Ensures compliance with regulatory requirements, including reporting of critical incidents and handling sensitive communications with regulatory bodies.
- **IT Department:** Ensures that technical measures are in place for secure communication and that systems used for communication are compliant with ISMS policies.
- **Employees and Contractors:** Responsible for adhering to the communication procedures and ensuring security and confidentiality in all communication related to their role.
- **Third-Party Vendors:** Responsible for ensuring secure communication practices when handling the company's sensitive information or systems.

5. Communication Channels

- **Internal Communication Channels:**
  - **Email:** All sensitive communications must be encrypted and password-protected if necessary.
  - **Intranet/Collaboration Tools:** Secure internal systems must be used for internal discussions and sharing of sensitive information.
  - **Instant Messaging/Voice Calls:** Should be secured using approved encryption technologies and should not be used for sharing confidential client information.
  - **Document Management Systems:** Use secure, authorized systems for sharing and storing information related to equity broking activities.
- **External Communication Channels:**
  - **Official Email:** Use encrypted emails (with appropriate firewalls and anti-malware tools) for communication with clients, vendors, or regulatory bodies such as SEBI.
  - **Secure Web Portals:** Communications with external partners should occur through secure channels.
  - **SMS & Voice Calls:** These should be avoided for sharing sensitive or confidential information unless encrypted or protected by other security mechanisms.
- **Incident Communication:**
  - **Incident Reporting Tool:** A dedicated platform or tool for reporting incidents (such as data breaches, system failures) securely.
  - **Escalation Path:** A defined and immediate escalation path to senior management and security teams for critical incidents that require quick response or action. Refer Incident Management Procedure.

6. Key Communication Procedures

6.1. Internal Communication on Information Security:

- All employees must follow the company's **Information Security Awareness Program**. Any internal communication regarding information security, policy changes, or threats must be conducted via secure channels.
- **Confidentiality:** Employees must use secure email systems, encrypted messages, and VPNs when accessing or transmitting sensitive information, especially regarding client trades, portfolios, or financial details.
- **Training and Awareness:** Regular training must be provided to all staff on secure communication practices, SEBI regulations, and incident reporting.

6.2. External Communication:

- All external communication, including messages to clients, vendors, and regulatory bodies like SEBI, must be formal, clear, and secure.
- **Data Protection:** Ensure that personally identifiable information (PII), trading data, and other confidential client information is protected. Use encrypted email, secure portals, or authorized encryption technologies for transmitting such data.

- **Third-Party Communication:** All third-party communications must comply with contractual agreements, which include confidentiality clauses, and security measures should be in place to prevent data leakage.

6.3. Communication During Security Incidents:

- **Incident Identification:** Employees must report any suspected security breaches or vulnerabilities immediately to the designated incident response team using the approved incident reporting tool.
- **Escalation:** A defined escalation path should be followed, with appropriate urgency depending on the severity of the incident. Critical incidents must be communicated directly to senior management, the ISO, and SEBI (if required).
- **Incident Reporting to SEBI:** According to SEBI regulations, any data breach or security incident that affects trading data or client information must be reported to SEBI immediately following the internal investigation.
- **Public Communication:** In the event of a security breach with public ramifications, a formal communication plan with stakeholders (including clients, vendors, regulators) must be executed, ensuring that the message is consistent, clear, and compliant with relevant laws.

6.4. Compliance and Regulatory Reporting:

- **SEBI Reporting Requirements:** All reports related to compliance, risk management, and incident reports must be provided to SEBI in accordance with SEBI guidelines. These include but are not limited to:
  - Breaches of trading data security
  - Vulnerabilities that may affect client funds or market integrity
  - Annual security audits and assessments
- **Audit Trails:** Communication records must be maintained in line with SEBI's record-keeping guidelines for audit purposes.

7. Security Measures for Communication

- **Encryption:** All sensitive communications, both internal and external, must be encrypted using industry-standard encryption techniques.
- **Authentication:** Use multi-factor authentication (MFA) for systems that handle communication involving sensitive information.
- **Access Control:** Limit access to communication systems based on job roles and responsibilities, ensuring that only authorized individuals can send/receive confidential information.

8. Monitoring and Enforcement

- **Auditing:** All communication channels should be audited regularly to ensure compliance with ISMS policies and regulatory requirements. Logs of communication should be stored securely and made available for audit.
- **Policy Violations:** Any violation of the communication procedure, such as unauthorized disclosure of sensitive information, will be addressed according to the company's disciplinary procedures, which could include penalties or legal actions.

9. Review and Updates

This communication procedure should be reviewed annually, or more frequently if required, to ensure continued compliance with regulatory requirements, evolving information security threats, and organizational changes. The ISMS team will be responsible for ensuring the procedure remains up to date.

X. Performance Monitoring Procedure

1. Purpose

The purpose of this document is to define the performance monitoring procedure for ensuring the effectiveness of the **Information Security Management System (ISMS)**. This procedure will help monitor, measure, and improve the performance of information security processes within the equity broking company to ensure the protection of sensitive financial data and compliance with regulatory requirements.

2. Scope

This procedure applies to the monitoring of the information security performance related to the company's IT infrastructure, data protection practices, and risk management. It covers all components of the ISMS, including:

- **System and Network Performance Monitoring**
- **Security Incident and Event Management**
- **Compliance Monitoring and Reporting**
- **Continuous Improvement of Security Controls**

3. Objectives

- Ensure the effectiveness and continuous improvement of the ISMS.
- Monitor the performance of information security controls and systems.
- Identify and mitigate risks to information security.
- Ensure compliance with regulations and other relevant legal requirements.
- Maintain the confidentiality, integrity, and availability of financial and trading data.

4. Roles and Responsibilities

- **Chief Information Security Officer (CISO):** Responsible for overseeing the performance monitoring of ISMS and ensuring it aligns with regulatory compliance. The ISO is also responsible for reporting on security performance to senior management and regulatory authorities.
- **Legal and Compliance Officer:** Responsible for monitoring compliance with regulations and ensuring the timely submission of reports and audits.
- **IT Department:** Responsible for maintaining the technical monitoring systems, ensuring their proper operation, and addressing any performance issues related to information security infrastructure.
- **Risk Management Team:** Responsible for identifying and analyzing security risks and vulnerabilities, providing recommendations for risk mitigation, and monitoring the risk control processes.
- **Employees:** Responsible for adhering to security protocols and reporting any issues related to information security performance or system anomalies.
- **Third-Party Vendors:** Responsible for ensuring their services are continuously monitored for compliance with agreed-upon security measures.

5. Performance Monitoring Framework

5.1. Key Performance Indicators (KPIs) for ISMS

To effectively measure the performance of ISMS, the company will monitor the following key KPIs:

- Security incidents(High/Medium) are closed timely
- Information security policies and procedures to be reviewed Annually
- Information Security assessments to be conducted for Information Assets
- External VAPT for all critical systems
- Security awareness should be conducted for employees and contractors annually
- Internal Audit is conducted for ISMS
- DR Testing to be conducted annually for critical applications.

5.2. Tools and Technologies Used for Monitoring

The following tools and technologies will be used to monitor the performance of ISMS:

- **Ticketing Tool for incident tracking:** For centralized logging of security incidents.
- **Network Monitoring Tools:** For monitoring the performance of networks and detecting potential security threats, such as unauthorized access or unusual traffic patterns.
- **Vulnerability Management Tools:** For conducting regular vulnerability scans to identify and address security risks across systems and applications.
- **Intrusion Detection Systems (IDS):** For monitoring and detecting any potential intrusions or malicious activity within the organization's network or systems.

5.3. Monitoring Frequency

- **Real-Time Monitoring:** Continuous monitoring of critical systems (e.g., trading platforms, financial transactions) to ensure they are functioning securely and with minimal downtime.
- **Quarterly and Annual Reviews:** Review of ISMS performance in totality, including audits of internal systems, third-party vendors, and compliance with regulations. A formal security audit will be conducted quarterly and annually.

6. Incident and Performance Reporting

6.1. Incident Reporting and Escalation

In the event of a security incident or performance issue, the following steps will be followed:

- **Incident Detection:** All security events, including abnormal network traffic, unauthorized access, or system malfunctions, will be detected through monitoring tools.
- **Incident Reporting:** Employees must report any security incidents or performance issues immediately through the designated reporting tool or communication channels.
- **Incident Escalation:** If the incident cannot be resolved by the IT or Security teams within a specified time, it will be escalated to senior management for further investigation.

- **Regulatory Reporting:** Any serious incidents (e.g., data breaches, trading disruptions) that affect client data or market integrity must be reported to as per their requirements. This includes reporting the incident's nature, impact, and remedial actions taken.

6.2. Performance Review and Reporting

- **Annual Reports:** A comprehensive review of the ISMS will be submitted to senior management, outlining the effectiveness of security controls, risks, compliance with regulations, and any issues encountered during the year. This report will also include an action plan for the next year.

7. Corrective and Preventive Actions (CAPA)

7.1. Corrective Actions

- Any identified performance issues, whether from incidents or routine monitoring, must be corrected immediately. The corrective action may include system patches, updates, or reconfiguration of security settings.
- An investigation will be carried out to identify the root cause of performance issues, and necessary adjustments will be made to the ISMS processes, systems, or controls.

7.2. Preventive Actions

- Based on performance monitoring outcomes, preventive measures will be taken to avoid recurrence of issues. This may involve:
  - Enhancing security controls or system configurations.
  - Conducting additional training or awareness programs for employees.
  - Revising procedures to improve compliance with regulations.

8. Review and Continuous Improvement

- **Ongoing Monitoring:** The performance monitoring process will be continually reviewed for effectiveness and improvements. This includes evaluating the appropriateness of the selected KPIs, tools, and monitoring frequencies.
- **Annual Review:** A full review of the ISMS performance monitoring procedure will be conducted annually to ensure alignment with changing regulations, emerging threats, and best practices in information security.

XI. Skill Development Procedure

1. Purpose

To establish a procedure for skill development related to the **Information Security Management System (ISMS)**, ensuring employees have the necessary skills to safeguard sensitive data and comply with regulatory requirements.

2. Scope

Applies to all employees, contractors, and third-party vendors handling the company's information systems, financial data, and client information.

3. Objectives

- Equip employees with essential information security skills.
- Ensure compliance with relevant regulatory requirements.
- Foster continuous improvement in security practices.

4. Roles and Responsibilities

- **CISO:** Oversees skill development and ensures alignment with ISMS.
- **HR:** Coordinates training logistics.
- **Employees:** Participate actively in training and apply learned practices.
- **Legal and Compliance Officer:** Ensures training meets regulatory standards.

5. Training Programs

- **Mandatory Training:**
    - Information security awareness training (data protection, phishing, incident reporting) to be conducted annually.
- **Methods:** Online modules, classroom sessions, workshops, and simulations.

6. Monitoring and Evaluation

- **Post-Training Assessments** to ensure understanding.
- **Performance Monitoring** through periodic evaluations and feedback.
- **Annual Audits** to assess overall training effectiveness.

7. Documentation

- Maintain records of all training sessions, assessments, and compliance reports for audits.

8. Continuous Improvement

- Annual reviews of the training program and updates based on emerging threats and regulatory changes.