Choice
The Joy of Earning

CHOICE EQUITY BROKING PVT. LTD

Information Security Policy

Version Control

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

Version Control Revised Format

Version	Activity	Date	Description	Person Responsible
2.2	Amendments	03-Jan-25	Amendments with respect to grammatical mistakes aligning with SEBI CSCRF guidelines	Abhishek Vinayak, Associate, Cybersecurity
2.2	Reviewed	03-Jan-25	Reviewed and suggested additional changes	Shripad Mayekar, Manager Cybersecurity
2.2	Approved	8th January, 2025	Reviewed and Approved	Ashutosh Bhardwaj, CISO
2.2	Approved	8th January, 2025	Approved	Yogesh Jadhav, CTO

Table of Contents

1 Introduction

1.1 General

Choice Equity Broking Pvt. Ltd.(Choice) deals with critical customer data as part of its daily operations. It is imperative to protect and maintain the confidentiality, integrity and availability of the business-critical information stored, transmitted and managed by Choice. The Information Security Management System (ISMS) aims to identify all the risks that the organization faces from an information security perspective and methods to mitigate the identified risks. Furthermore, Choice has documented their IT policies and procedures that help establish management responsibilities towards the Information Security Management System (ISMS) and ensure that adequate and proportionate security controls are in place to protect the information assets and give confidence to all those entities interacting directly or indirectly with CHOICE

1.2 Normative References

The information security policies and procedures shall be developed in line with the following standards:

- ISO 27001:2022
- ISO 27002:2022
- Best practices in the information security domain

2 Objective of ISMS

Choice firmly believes that core values keep organizations stable and focused to its common goal. Choice core values have helped it to achieve the mission of bringing measurable benefits to its customers.

Choice realizes the importance of the information handled by them as part of their business operations. Choice's employees are aware of their responsibilities and perform them with the highest levels of trust, honesty and integrity of purpose and action.
Choice is highly committed to ensuring that all transactions performed through their service are secure, safe and confidential.

The objective of the information security program is to ensure that its core values of data security, privacy, confidentiality and integrity of process are consistently adhered to.

2.1 IS Objective Criteria

Choice shall define Information security objectives that fulfill the following criteria

- The objectives are clear, meaningful, and appropriate to the purpose of the organization.
- The objectives aim at Choice's success.
- The established objectives shall be reviewed at the end of the year.
- The established objectives shall be appropriate to the demands of the customer.

- The objectives shall aim at achieving a clear competitive edge in the market.
- Maintain or increase outstanding quality & safety standards towards information security and thus contribute towards safeguarding Choice information assets.
- The established objectives shall play a key role in the long-term development of Choice's information security posture.
- The established objectives shall be efficient and economical.
- Provides the framework for setting information security objectives.
- Includes a commitment to satisfy applicable requirements related to information security and
- Includes a commitment to continual improvement of the information security management system.

2.2 Information Security Objectives

Choice's objective is to protect and safeguard all critical information and information processing assets in order to ensure secure provision of services and business continuity. This includes (but is not limited to) electronic information on servers, workstations, laptops, networking and communication devices, tapes, USB devices, CDs and information printed or written on paper or transmitted by facsimile or any other medium.

- Critical information shall be protected from unauthorized access, use, disclosure, modification, and disposal, whether intentional or unintentional.
- The confidentiality, integrity and availability of critical information, whether acquired permanently or in transit, provided or created, shall be ensured at all times, as appropriate.
- Any security incidents and infringement of the Policy, actual or suspected, shall be reported, investigated by the designated Chief Information Security Officer (CISO) and appropriate corrective action initiated.
- Awareness programs on Information Security shall be available to all Employees and wherever applicable to third party viz. Subcontractors, Consultants, Vendors etc and regular training imparted to them.
- Business Continuity Plan /Disaster Recovery shall be maintained and tested.
- All Legal, Contractual, Regulatory and Statutory requirements with regard to information security shall be met wherever applicable.

2.3 IS Objectives Roadmap

Choice shall achieve its information security objectives in the below outlined manner:

- Establish a strong Information Security Governance structure.
- Monitor and proactively protect the infrastructure of all the departments under the scope
- Deploy security controls to protect resources from disruption, modification, and disclosure.
- Provide information security awareness and education programs for all the employees and, where relevant to contractors & suppliers.

- Create and maintain a security-conscious culture.
- Comply with Legal, Regulatory and Contractual requirements.
- Timely test and maintain business continuing plans and incident response plans for strategic IT and information services on a regular basis.
- Review of organization risks in a defined risk management context in which risks are identified and appropriate controls are implemented and documented.

All employees shall comply with the policies. Failure to comply with the policies shall entail appropriate action which may include disciplinary action.
Information is an important asset and as such, information and information processing resources shall be maintained in a manner that ensures information access on a need to know and need to access basis as well as protect it from unauthorized or improper use.

Chief Information Security Officer is directed to establish an information security program, consistent with the business practice.

3 Policy Statement

We at Choice, including but not limited to employees, associates, contract workers, shall follow Information Security Management System in all the processes and technology

- We are committed to secure information which is generated as part of business operations and include information shared with our interested parties.
- Provide information security awareness among team members and continual improvement in information security in all our processes through regular review of our information security management system.
- Protect Personal information in all its forms.
- Adopt a systematic approach to risk assessment and risk treatment.
- Comply with all Regulatory, Legal and Contractual requirements.
- Provide a comprehensive Business Continuity Plan encompassing the respective processes / departments.
- Information will be made available to authorized persons on a need-to-know basis.

3.1 Review of Information Security Policy

- The Information security policy shall be reviewed and approved by the management annually.
- The review shall include, but not limited to:
  - Feedback from business users;
  - Change in the business;
  - Change in the IT environment;
  - Trends related to threat and vulnerabilities; and
  - Reported security incidents.
- Records for the management review and approval shall be maintained.

- While any Major version upgrade will need Board/management approval, minor version upgrades need to be approved by the Head of Information Security.

4 Context of the Organization

A separate document detailing the context of the organization has been prepared.

4.1 Reference

- Context of the Organization in ISMS Scope document

5. Leadership

5.1 Leadership and commitment

Top management shall demonstrate leadership and commitment with respect to the information security management system by

- Ensure that the information security policy and the information security objectives are established.
- Ensure the integration of the information security management system requirements into Choice's processes.
- Ensure that the resources needed for the information security management system are available.
- Communicate the importance of effective information security management and conform to the information security management system requirements.
- Ensure that the information security management system achieves its intended outcome(s).
- Direct and support persons to contribute to the effectiveness of the information security management system.
- Promote continual improvement.

6. Organizational roles, responsibilities and authorities

Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated.

Top management shall assign the responsibility and authority to:

- Ensure that the information security management system conforms to the requirements of ISO27001:2022 and
- Report on the performance of the information security management system to top management.

6.1 Reference

- Organization of Information Security

7. Planning

7.1 Address risks and opportunities

7.1.1 General

When planning for the information security management system, Choice shall consider the issues, the organization context and determine the risks and opportunities that need to be addressed to:

- Ensure the information security management system can achieve its intended outcome(s)
- Prevent, or reduce, undesired effects
- Achieve continual improvement

The organization shall plan:

- Actions to address these risks and opportunities; and
- Methodology to
  - Integrate and implement the actions into its information security management system processes
  - Evaluate the effectiveness of these actions.

7.1.2 Information security risk assessment

Choice shall retain documented information about the information security risk assessment process. Choice s shall define and apply an information security risk assessment process that:

- Establishes and maintains information security risk criteria including
  - The risk acceptance criteria; and
  - Criteria for performing information security risk assessments
- Ensures that repeated information security risk assessments produce consistent, valid and comparable results;
- Identifies the information security risks:
  - Apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system and
  - Identify the risk owners;
- Analyses the information security risks:
  - Assess the potential consequences that would result if the identified risks were to materialize;
  - Assess the realistic likelihood of the occurrence of the identified risks and
  - Determine the levels of risk
- Evaluates the information security risks
  - Compare the results of risk analysis with the established risk criteria and
  - Prioritize the analyzed risks for risk treatment.

7.1.3 Reference

- Risk Assessment Methodology

7.1.4 Information security risk treatment

Choice shall retain documented information about the information security risk treatment process. Choice shall define and apply an information security risk treatment process to:

- Select appropriate information security risk treatment options, taking into account the risk assessment results.
- Determine all controls that are necessary to implement the chosen information security risk treatment options.
- Compare the controls determined above with those in Annex A and verify that no necessary controls have been omitted.
- Produce a Statement of Applicability that contains the necessary controls and justification
  - for inclusions, whether they are implemented or not, and
  - the justification for exclusions of controls from Annex A
- Formulate an information security risk treatment plan
- Obtain risk owners’ approval of the information security risk treatment plan and acceptance of the residual information security risks.

7.1.4.1 Reference

- Statement of Applicability

7.2 Information security objectives and planning

Choice shall establish information security objectives at relevant functions and levels. The information security objectives shall:

- Be consistent with the information security policy
- Be measurable (if practicable)
- Take into account applicable information security requirements, and results from risk assessment and risk treatment
- Be communicated and
- Be updated as appropriate

Choice shall retain documented information on the information security objectives. When planning how to achieve its information security objectives, Choice shall determine:

- What will be done
- What resources will be required
- Who will be responsible
- When it will be completed and
- How the results will be evaluated

8. Support

8.1 Resources

Choice shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the information security management system.

8.2 Competence

Choice shall:

- Determine the necessary competence of the person(s) doing work under its control that affects its information security performance.
- Ensure that these persons are competent based on appropriate education, training, or experience.
- Where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken and
- Retain appropriate documented information as evidence of competence.

8.3 Awareness

Persons working with Choice shall be aware of:

- The information security policy
- Their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance; and
- The implications of not conforming to the information security management system requirements.

  Information security awareness shall be provided to all employees and contractors annually.

8.4 Communication

Choice shall determine the need for internal and external communications relevant to the information security management system including:

- On what to communicate
- When to communicate
- With whom to communicate
- Who shall communicate and
- The processes by which communication shall be affected.

8.5 Documented information

8.5.1 General

Choice information security management system shall include:

- Documented information required by this International Standard; and
- Documented information determined by the organization as being necessary for the

effectiveness of the information security management system.

8.5.2 Creating and updating

When creating and updating documented information Choice shall ensure appropriate:

- Identification and description (e.g. a title, date, author, or reference number)
- Format (e.g. language, software version, graphics) and media (e.g. paper, electronic) and
- Review and approval for suitability and adequacy

8.5.3 Control of documented information

Documented information required by the information security management system shall be controlled to ensure that

- It is available and suitable for use, where and when it is needed and
- It is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).

For the control of documented information, Choice shall address the following activities as applicable:

- Distribution, access, retrieval and use
- Storage and preservation, including the preservation of legibility
- Control of changes (e.g. version control) and
- Retention and disposition

Documented information of external origin, determined by the organization to be necessary for the planning and operation of the information security management system, shall be identified as appropriate, and controlled.

9. Operation

9.1 Operational planning and control

Choice shall

- Plan, implement and control the processes needed to meet information security requirements, and implement the actions determined in 6.1 above.
- Implement plans to achieve information security objectives determined in 2.2.
- Keep documented information to the extent necessary to have confidence that the processes have been carried out as planned.
- Control planned changes and reviews the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.
- Ensure that outsourced processes are determined and controlled.

9.2 Information security risk assessment

Choice shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur, taking into account the criteria established in 2.1. It shall retain documented information of the results of the information security risk assessments.

9.3 Information security risk treatment

Choice shall

- Implement the information security risk treatment plan.
- Shall retain documented information of the results of the information security risk treatment.

10. Performance evaluation

10.1 Monitoring, measurement, analysis and evaluation

Choice shall evaluate the information security performance and the effectiveness of the information security management system.

It shall determine:

- What needs to be monitored and measured, including information security processes and controls
- The methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results
- When the monitoring and measuring shall be performed
- Who shall monitor and measure
- When the results from monitoring and measurement shall be analyzed and evaluated and
- Who shall analyze and evaluate these results.

Choice shall retain appropriate documented information as evidence of the monitoring and measurement results.

10.2 Internal audit

Choice shall conduct internal audits at planned intervals to provide information on whether the information security management system

- Conforms to
  - the organization’s own requirements for its information security management system and
  - the requirements of ISO27001
- Is effectively implemented and maintained.

Choice shall

- Plan, establish, implement and maintain an audit program, including the frequency, methods, and responsibilities, planning requirements and reporting. The audit program shall take into consideration the importance of the processes concerned and the results of previous audits
- Define the audit criteria and scope for each audit
- Select auditors and conduct audits that ensure objectivity and the impartiality of the audit process
- Ensure that the results of the audits are reported to relevant management and

- Retain documented information as evidence of the audit program and the audit results

10.3 Management review

Top management shall review the organization’s information security management system at least annually to ensure its continuing suitability, adequacy and effectiveness. The management review shall include consideration of:

- The status of actions from previous management reviews
- Changes in external and internal issues that are relevant to the information security management system.
- Feedback on the information security performance, including trends in:
    - Nonconformities and corrective actions
    - Monitoring and measurement results
    - Audit results and
    - Fulfillment of information security objectives
- Feedback from interested parties.
- Results of risk assessment and status of risk treatment plan; and
- Opportunities for continual improvement.

The outputs of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system.
Choice shall retain documented information as evidence of the results of management reviews.

11. Improvement

11.1 Nonconformity and corrective action

In case of nonconformity, Choice shall

- React to the nonconformity, and as applicable:
    - Take action to control and correct it and
    - Deal with the consequences
- Evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by:
    - Review the nonconformity
    - Determine the causes of the nonconformity and
    - Determine if similar nonconformities exist, or could potentially occur
- Implement any action needed;
- Review the effectiveness of any corrective action taken; and
- Make changes to the information security management system, if necessary.

Corrective actions shall be appropriate to the effects of the nonconformities encountered.

Choice shall retain documented information as evidence of:

- The nature of the nonconformities and any subsequent actions taken, and
- The results of any corrective action.

11.2 Continual improvement

Choice shall continually improve the suitability, adequacy and effectiveness of the information security management system.

- **Exceptions to Information Security Policy**

  Any exceptions to the information security policy must be formally documented, reviewed, and approved by the CISO. The approval must include an assessment of potential risks and a plan for mitigating those risks. Exceptions must be regularly monitored and reassessed to ensure they do not compromise the organization's security posture.