Choice
The Joy of Earning

CHOICE EQUITY BROKING PVT. LTD

Supplier Relationship Policy

Version Control

Action	Date	Revision Details	Prepared / Amended By	Approved By
Created On	17-Oct-16	1.0	Mahesh Tamhankar	Amit Jaokar
Reviewed On	21-Feb-17	1.1	Mahesh Tamhankar	Amit Jaokar
Reviewed On	13-Feb-18	1.2	Mahesh Tamhankar	Amit Jaokar
Reviewed On	20-Feb-18	1.3	Mahesh Tamhankar	Utpal Parekh
Reviewed On	10-Aug-19	1.4	Mahesh Tamhankar	Yogesh Jadhav
Reviewed On	11-Jan-20	1.5	Mahesh Tamhankar	Yogesh Jadhav
Reviewed On	15-July-21	1.6	Sunil Utekar	Yogesh Jadhav
Reviewed On	08-Jan-22	1.7	Sunil Utekar	Yogesh Jadhav
Reviewed On	09-Apr-23	2.0	Ashutosh Bhardwaj	Yogesh Jadhav
Reviewed On	31-Jan-24	2.1	Anil Ashok & Associates	Ashutosh Bhardwaj
Reviewed On	20-Feb-25	2.2	Abhishek Vinayak	Shripad Mayekar
Approved On	20-Feb-25	2.2	Abhishek Vinayak	Ashutosh Bhardwaj

Version Control Revised Format

Version	Activity	Date	Description	Person Responsible
2.3	Amendments	05th April, 2025	Amendments done and submitted for review regarding the Changes done to align with SEBI CSCRF 2024	Abhishek Vinayak, Associate Information Security
2.3	Reviewed	07th April, 2025	Changes Reviewed	Shripad Mayekar, Manager Information Security
2.3	Approved	07th April, 2025	Changes Approved	Ashutosh Bhardwaj, CISO

Index

Contents

1 Introduction

1.1.1 Outsourcing involves commercial arrangements to transfer responsibility for various business activities to third parties. Outsourcers provide services to Choice Equity Broking Pvt. Ltd. (Choice) to a mutually agreed service level defined formally in a contract.

1.1.2 The providers of outsource services (outsourcers) are primarily business process and professional services specialists (e.g. IT, finance and HR services, consultants, telecommunications and networking services, cloud computing services), but may also include temporary staff and contractors or sub-contractors.

1.1.3 Many commercial benefits have been ascribed to outsourcing such as:

- Reducing the organization's costs (assuming the outsourcer can perform the services more efficiently and does not over-charge);
- Greater focus on core business by outsourcing non-core functions;
- Access to additional specialist skills and resources.

1.1.4 Despite the potential benefits, information security incidents such as inappropriate access to or disclosure of sensitive information, loss of intellectual property or the inability of the outsourcer to meet agreed service levels, would reduce the benefits and could jeopardize the customer's information security.

2 Objective

The purpose of this policy is to ensure that supplier relationships are managed effectively and that the information security risks associated with supplier products and services are properly mitigated.

3 Scope

The policy applies to all suppliers that provide products or services throughout Choice Equity Broking Pvt. Ltd. (Choice) that may affect the confidentiality, integrity, and availability of the organization's information.

4 Policy

4.1.1 The commercial benefits of outsourcing non-core business functions must be sufficient to offset the associated risks.

4.1.2 The risks associated with outsourcing must be mitigated to acceptable levels using appropriate administrative, physical and technical controls.

5 Policy Guidelines

5.1 Choosing an outsourcer

5.1.1 Criteria for selecting an outsourcer include the:

- Company's reputation and history;
- Quality of services provided to other customers;
- Number and competence of staff and managers;
- Financial stability of the company and commercial record;
- Retention rates of the company's employees;
- Quality assurance and security management standards currently followed by the company (e.g. certified conformity with ISO 9000 and ISO/IEC 27001), if applicable.

5.1.2 Further information security criteria may be defined as the result of supplier evaluation form.

5.2 Assessing outsourcing risks

5.2.1 Management should nominate a suitable Choice Equity Broking Pvt. Ltd. owner for each business function/process outsourced. The owner, with help from the Information Security Team, should identify, evaluate and decide how to treat the information risks before the function/process is outsourced, using Choice Equity Broking Pvt. Ltd.'s risk management process.

5.2.2 In relation to outsourcing, specifically, the risk assessment should take due account of the:

- Nature of logical and physical access to Choice Equity Broking Pvt. Ltd. information assets and facilities required by the outsourcer to fulfil the contract;
- Sensitivity, volume and value of any information assets involved;
- Commercial risks such as the possibility of the outsourcer's business failing completely, failing to meet agreed service levels, or providing services to Choice Equity Broking Pvt. Ltd.'s competitors where this might create conflicts of interest; and
- Security and commercial controls known to be currently employed by Choice Equity Broking Pvt. Ltd. and/or by the outsourcer.

5.2.3 If the risks involved are considerable and the commercial benefits are marginal (e.g. if the controls necessary to mitigate the risks are too costly), a function or process should not be outsourced.

5.3 Contracts and confidentiality agreements

5.3.1 A binding contract is required between Choice Equity Broking Pvt. Ltd. and the outsourcer to protect both parties.

5.3.2 The contract should clearly define the types of information exchanged and the purposes for doing so. If the information being exchanged is sensitive, the outsource contract should contain suitable confidentiality clauses or a separate non-disclosure agreement should be in place (quite likely before the outsourcing contract is executed).

5.3.3 Exchanged information shall be classified and controlled in accordance with Choice Equity Broking Pvt. Ltd. policy, as a minimum.

5.3.4 Upon termination of the contract, the confidentiality arrangements shall be revisited to determine whether confidentiality has to be extended beyond the tenure of the contract.

5.3.5 Draft contracts should be reviewed/updated and approved by Legal/Compliance before execution.

5.3.6 In addition to the commercial and legal formalities applicable to any contract (e.g. the full names of the parties, charges and payment terms, jurisdiction), outsourcing contracts should clearly specify each party's responsibilities toward the other (e.g. service levels and penalties or liabilities for non- performance).

5.3.7 According to the information risk assessment, specific information security controls may be required, such as:

- Legal, regulatory and contractual compliance obligations such as data protection/privacy laws, money laundering, tax etc.*;
- Information security obligations and controls such as:
  - Information security policies, procedures, standards and guidelines, normally within the context of an Information Security Management System such as that defined in ISO/IEC 27001;
  - Background checks on employees or third parties working on the contract (see section 5.4);
  - Access controls to restrict unauthorized disclosure, modification or destruction of information, including physical and logical access controls, procedures for granting, reviewing, updating and revoking access to systems, data and facilities etc. (see section 5.5);
  - Information security incident management procedures including prompt event and incident reporting (where 'prompt' means 'at the earliest practical opportunity' and 'event' includes early indications of possible security compromises and incidents ahead);

* In the case of "offshore" outsourcing, special consideration must be given to the ramifications of transferring information between countries or jurisdictions, particularly where privacy or other laws may conflict.

  - Return or destruction of all information assets by the outsourcer after the completion of the outsourced activity or whenever the asset is no longer required to support the outsourced activity;
  - Copyright, patents and similar protection for any intellectual property shared with the outsourcer or developed in the course of the contract;
  - Specification, design, development, testing, implementation, configuration, management, maintenance, support and use of security controls within or associated with IT systems, plus source code escrow;
  - Anti-malware, anti-spam, network and system security monitoring, logging and similar controls;
  - IT change and configuration management, including vulnerability management, patching and verification of system security controls prior to their connection to production networks;

- The right of Choice Equity Broking Pvt. Ltd. to monitor all access to and use of Choice Equity Broking Pvt. Ltd. facilities, networks, systems etc., and to audit the outsourcer's compliance with the contract, or to employ a mutually-agreed independent auditor for this purpose;
- Business continuity arrangements including crisis and incident management, resilience arrangements, backups, IT disaster recovery and contingency preparations.

5.3.8 Although outsourcers that are certified against ISO/IEC 27001 may have an effective Information Security Management System in place (depending on the scope and nature of certification),
Choice Equity Broking Pvt. Ltd. may require additional assurance that important information security controls adequately address Choice Equity Broking Pvt. Ltd.'s specific requirements, potentially both prior to and during the outsourcing (see section 5.6).

5.4 Hiring and training of employees

5.4.1 Outsource employees, contractors and consultants working on behalf of Choice Equity Broking Pvt. Ltd. should be subjected to background checks equivalent to those performed on Choice Equity Broking Pvt. Ltd. employees. Such screening shall take into consideration the level of trust and responsibility associated with the position and (where permitted by local laws):

- Proof of the person's identity (e.g. passport or similar official photo ID);
- Proof of their academic and professional qualifications (e.g. certificates);
- Proof of their work experience (e.g. résumé/CV and references);
- Criminal record check;

5.4.2 Companies providing contractors/consultants directly to Choice Equity Broking Pvt. Ltd. or to outsourcers used by Choice Equity Broking Pvt. Ltd. shall perform at least the same standard of background checks as those indicated above.

5.4.3 Regardless of who formally employs them, appropriate information security awareness and training is required for all workers, clarifying their responsibilities relating to Choice Equity Broking Pvt. Ltd. information security policies, standards, procedures and guidelines (e.g. privacy policy, acceptable use policy, procedure for reporting information security incidents etc.) and all relevant obligations defined in the contract.

5.5 Access controls

5.5.1 In order to prevent unauthorized access to Choice Equity Broking Pvt. Ltd.'s information assets by the outsourcer or sub-contractors, suitable security controls are required as outlined in this section. The details depend on the nature of the information assets and the associated risks, implying the need to assess the risks and design a suitable controls architecture.

5.5.2 Technical access controls typically include:

- User identification and authentication;
- Authorization of access, generally through the assignment of users to defined user roles having appropriate logical access rights and controls;
- Data encryption and other Cryptographic controls as outlined in the Choice Equity Broking Pvt. Ltd.'s ISMS Consolidated Policy under Cryptographic Control section.

5.5.3 Procedural components of access controls shall be documented within procedures, guidelines and related documents and incorporated into awareness, training and educational activities. This includes:

- Choice of strong passwords and multi-factor authentication (especially for privileged accounts);
- Determining and configuring appropriate logical access rights;
- Reviewing and if necessary revising access controls to maintain compliance with requirements.

5.5.4 Physical access controls include:

- Layered controls covering perimeter and internal barriers;
- Strongly-constructed facilities;
- Access logging though the use of access cards, visitor registers etc.;

5.5.5 Choice Equity Broking Pvt. Ltd. shall ensure that all information assets handed over to the outsourcer during the course of the contract (plus any copies made thereafter, including

backups and archives) are duly retrieved or destroyed at the appropriate point on or before termination of the contract. In the case of highly classified information assets, this normally requires the use of a schedule or register and a process whereby the outsourcer formally accepts accountability for protecting the assets at the point of hand-over.

5.6 Ongoing Supplier Performance Monitoring

5.6.1 **Performance Monitoring:** The organization will monitor service levels and supplier performance to ensure that agreed-upon security and service delivery standards are maintained. This will include reviewing and holding regular progress meetings with suppliers to discuss performance and identify areas for improvement.

5.6.2 **Supplier Changes and Updates:** The organization will closely monitor any changes made by suppliers, including:

- Enhancements to existing services or offerings.
- Development of new applications, systems, or products.
- Introduction of new technologies or services

that may affect the organization's systems and data.

5.7 Supplier Incident Management

5.7.1 **Incident Reporting and Management:** Suppliers are required to report any information security incidents or operational problems. The organization will review these reports and ensure that proper incident management processes are followed. Any security events or incidents identified during supplier interactions will be investigated, and corrective actions will be implemented as necessary.

5.7.2 **Vulnerability Management:** The organization will work with suppliers to identify information security vulnerabilities in their products or services and manage the resolution of these vulnerabilities to prevent any potential impact on the organization's information security.

5.8 Service Continuity and Resilience

5.8.1 **Service Continuity:** Suppliers must maintain service continuity plans to ensure that information processing services remain available even in the event of a major failure or disaster. The organization will ensure that suppliers have adequate contingency and recovery measures in place to maintain service levels.

5.9 Termination of Supplier Relationships

5.9.1 **Secure Termination:** When the engagement with a supplier ends, the organization will ensure that:

- All access rights are de-provisioned.
- Intellectual property and data ownership are properly handled.
- Information security controls, including the return of assets, secure disposal of information, and management of records, are followed.
- Confidentiality requirements are maintained even after the termination of the supplier relationship.

5.10 Security audits

5.10.1 For outsourced functions involving critical systems or sensitive data, CHOICE may conduct periodic security reviews of the vendor to ensure compliance with agreed security practices.

5.10.2 These reviews may include (as applicable):

- Vulnerability Assessment & Penetration Testing (VAPT) for hosted applications or platforms;
- Cybersecurity posture assessments of the vendor's organization to evaluate basic controls and hygiene;
- Certifications or third-party audits, such as ISO/IEC 27001, if available;
- Review of incident handling, access control, and data protection measures.

5.10.3 The scope and frequency of the review will be defined by Choice management, based on the criticality of the service and inputs from the Information Security Team.

6 Responsibilities

6.1 Management

Management is responsible for:

- Designating suitable owners of business processes that are outsourced;
- Overseeing the outsourcing activities, ongoing supplier performance ensuring that this

policy and other applicable policies and procedures are followed;

- Mandating various controls to mitigate unacceptable risks relating to outsourcing.

6.2 Outsourced business process owners

Designated owners of outsourced business processes are responsible for assessing and managing the commercial and security risks associated with outsourcing, working in conjunction with Information Security, Legal and other functions as necessary.

6.3 Chief Information Security Officer

- Responsible for ensuring that security risks associated with suppliers are managed in accordance with this policy.
- The Information Security Manager will oversee information security related supplier audits , risk assessments, and incident management.

6.4 Internal Audit

Internal Audit is authorized by management to assess compliance with all corporate policies at any time. Internal Audit may assist with audits of outsourcing contracts including security compliance audits, and advise management on the risks and controls relating to outsourcing.

Reference Documents

- ISO 27001:2022
- SEBI/HO/ ITD-1/ITD_CSC_EXT/P/CIR/2024/113

A.5.19	Information security in supplier relationships
A.5.20	Addressing information security within supplier agreements
A.5.21	Managing information security in the information and communication technology (ICT) supply-chain
A.5.22	Monitoring, review and change management of supplier services