National Securities Depository Limited

NSDL
Technology, Trust & Reach

Outsourcing Policy

National Securities Depository Limited

Name of the Document	**Outsourcing Policy**
Document Number	**NSDL/Compliance/Outsourcing Policy/2025-26**
Department Name	**Legal & Compliance**
Maintained By	**Compliance Officer**

Revision History

Sr No.	Date of Revision	Ver	Document Owner	Remarks
1	June 21, 2012	1.0	Mr. S. Ganesh, SVP	
2	November 14, 2014	1.0	Mr. S. Ganesh, SVP	No change
3	October 29, 2015	1.0	Mr. S. Ganesh, SVP	No change
4	January 28, 2016	2.0	Mr. S. Ganesh, SVP	Outsourcing policy amended in terms of SEBI Circular on Outsourcing dated December 9, 2015
5	February 8, 2017	2.0	Mr. S. Ganesh, SVP	No change
6	August 9, 2018	2.1	Mr. S. Ganesh, SVP	Outsourcing policy amended
7	August 8, 2019	2.1	Mr. S. Ganesh, SVP	No change
8	August 14, 2020	2.1	Mr. S. Ganesh, SVP	No change
9	August 14, 2021	2.1	Mr. Malav Shah, VP	No change
10	November 4, 2022	2.2	Vice President, Legal & Compliance Officer	Change pursuant to annual review
11	November 01, 2023	2.3	Vice President, Legal & Compliance Officer	Change pursuant to annual review
12	November 12, 2024	2.3	Vice President, Legal & Compliance Officer	(No change)
13	January 28, 2026	3	Senior Vice President, Compliance Officer and Head Legal	Change pursuant to annual review

TABLE OF CONTENTS

1. Introduction

For the purposes of this Outsourcing Policy ("**Outsourcing Policy**"), "outsourcing" refers to the engagement of one or more entities (hereinafter, an outsourced "**Service Provider**"), whether within or outside the NSDL group, by NSDL to support its provision of services.

Upon engagement, Service Providers may support NSDL by performing one or more activities to enable its services, either for a specified period, or on a continuing basis.

NSDL is committed to ensuring, including through this policy, that such outsourcing arrangements do not compromise its ability to discharge its core and critical responsibilities as a SEBI registered depository, nor weaken regulatory oversight.

2. Need for an Outsourcing Policy

Outsourcing brings in its wake several risks such as Strategic Risk, Reputation Risk, Compliance Risk, Operational Risk, Legal Risk, Exit Strategy Risk, Counterparty Risk, Country Risk, Contractual Risk, Access Risk, Concentration Risk, and Systemic Risk.

The failure of a Service Provider to carry out a specific activity, meet services levels, obligations relating to security/confidentiality, or other legal or regulatory obligations, either of the Service Provider or NSDL, can lead to financial losses or loss of reputation for the organization, and could also lead to systemic risks.

This is especially true for depositories, since Service Providers may not be subject to the same level of regulatory oversight as NDSL, which heightens concerns, including regulatory concerns.

In order to address these concerns, SEBI has prescribed principles for outsourcing based on the IOSCO principles.

This Outsourcing Policy is designed to enable NSDL to make optimal use of outsourcing arrangements, while addressing regulatory concerns and other risks involved in outsourcing.

This Outsourcing Policy shall be read in conjunction with the following documents:

(i) SEBI Circular no. SEBI/HO/MRD/MRD-PoD-1/P/CIR/2024/168 dated

December 03, 2024, Master Circular for Depositories;

(ii) SEBI Circular CIR/MRD/DP/19/2015 dated December 09, 2015, Outsourcing by Depositories;

(iii) SEBI Circular no. IR/MIRSD/24/2011 dated December 15, 2011, Guidelines on Outsourcing of Activities by Intermediaries,

(collectively, "**SEBI's Outsourcing Circulars**").

(iv) Depositories Act, 1996 and SEBI (Depositories and Participants) Regulations, 2018;

(v) Circulars issued by SEBI from time to time or any amendments to the legislations and regulations referred to herein.

(vi) Procurement Policy, Risk Management Framework Policy and the Operations Manual.

3. Objectives

This Outsourcing Policy endeavors to achieve following objectives:

(i) **Mitigate risks:** Identify, monitor, and manage outsourcing risks including operational, legal, compliance, reputational, concentration, systemic, and information security risks.

(ii) **Ensure business continuity and resilience:** Establish safeguards so that outsourced activities support uninterrupted operations, strong business continuity, disaster recovery, and systemic stability.

(iii) **Preserve accountability:** Ensure that outsourcing does not reduce or dilute NSDL's obligations under SEBI's Outsourcing Circulars, or any other applicable regulatory requirements.

(iv) **Build capability:** Enhance IT and non-IT capabilities through carefully governed outsourcing, enabling NSDL to deliver on expectations of its clients, investors, issuers, business partners, and SEBI.

(v) **Strengthen capacity:** Ensure NSDL maintains optimum access to quality resources, so that outsourcing arrangements augment its operations without diluting accountability or regulatory obligations.

(vi) **Cost effectiveness with prudence:** Achieve operational efficiencies and

rationalize costs, while ensuring financial considerations never override risk management, service quality, or protection of interests of investors, issuers, and market participants.

4. Definition

In this Outsourcing Policy, the following expressions including their grammatical variations and cognate expressions shall unless repugnant to the context or meaning thereof, have the meaning assigned to them respectively hereunder:

(i) "Board" means the Board of Directors of NSDL.

(ii) "Business Partner" means entities including but not limited to Depository Participants, Vault Managers, Issuers, Registrar and Share Transfer Agents, Professional Firms, Clearing Corporations and such other entities as may be empaneled by NSDL.

(iii) "Company" or "NSDL" means National Securities Depository Limited.

(iv) "Depositories Act" means the Depositories Act, 1996, as amended from time to time.

(v) "Outsourced Services" means services provided by a Service Provider under an outsourcing arrangement.

(vi) "Outsourcing" is defined as the use of one or more than one third party, either within or outside the group, by a registered intermediary to perform the activities associated with services which the intermediary offers.

(vii) "Outsourcing Policy" means this Outsourcing Policy of NSDL.

(viii) "SEBI" means Securities and Exchange Board of India.

(ix) "Service Provider" means an entity in business of providing goods, services or facilities under an Outsourcing arrangement.

Words and expressions not defined herein shall have the meaning assigned to them under the Risk Management Framework Policy or the Procurement Policy. In the event of any conflict or inconsistency between the definitions provided in this Outsourcing Policy and those in Risk Management Framework Policy or Procurement Policy, the definitions set out in the Risk Management Framework Policy or Procurement Policy as the case may be, shall prevail for the purposes of its interpretation and application, unless expressly stated otherwise.

If the conflict persists or cannot be resolved through this provision, the matter shall be referred to Legal Department for clarification and resolution.

5. Applicability

(i) This Outsourcing Policy applies to all arrangements wherein NSDL engages a Service Provider (whether a third-party service provider, affiliate, or independent party) to provide Outsourced Services.

(a) **In-Scope Activities**:

The activities or nature of activities that may be outsourced from time to time, and the selection of service providers to whom such activities may be outsourced, shall be undertaken in accordance with NSDL's Procurement Policy, subject to compliance with the overall framework of this Outsourcing Policy, specifically for service providers that fall within the category of Service Provider.

NSDL shall assess such arrangements case-by-case to ensure that these will fall within the scope of the Outsourced Services.

Further, in view of the changing business activities and complexities of various financial products, NSDL shall conduct self-assessment of its existing outsourcing arrangements on a continuous basis.

(b) **Core Activities**: Core activities as specified in Schedule-I of this Outsourcing Policy demand enhanced due diligence, risk assessment, and monitoring. The list of activities may be added, deleted amended or altered from time to time. Further, any activity shall not be outsourced if it would impair the management's right to assess, or its ability to supervise the business of NSDL.

Management shall periodically review the list of core activities and update it (with Board approval) if needed. If there is any doubt about whether an activity is core and cannot be Outsourced, the default approach is to seek clarification from the [Legal Department] before proceeding.

(c) **Related Parties**: NSDL may engage a service provider that is a related party, an associate or a group entity. This Outsourcing Policy continues to apply in such arrangements and the risk management practices while outsourcing to a related party shall be identical to those followed while outsourcing to an unrelated party. Further, additional

care shall be taken to maintain an arm's-length relationship in such cases to avoid conflicts of interest including, segregating infrastructure, personnel, decision-making, and records between NSDL and the related party service provider.

Necessary disclosures regarding the related party relationship shall be made as part of the contractual agreement between NSDL and the Service Provider.

6. Accountability

While Outsourcing any activity, the following points must be borne in mind:

(i) NSDL shall remain fully liable and accountable for all outsourced activities, to the same extent as if such activities were performed in-house. Outsourcing shall not dilute, transfer, or diminish NSDL's statutory obligations.

(ii) NSDL shall implement continuous monitoring systems including periodic reporting, audits, and technology-enabled oversight where feasible to track performance, risk, and compliance of all Service Providers.

(iii) Outsourcing arrangements shall not affect the rights of a Business Partner or investor against NSDL in any manner. NSDL shall be liable to the investors for the loss incurred by them due to the failure of the Service Provider and also be responsible for redressal of the grievances received from investors arising out of activities rendered by the Service Provider.

(iv) The facilities / premises / data that are involved in carrying out the outsourced activity by the Service Provider shall be deemed to be those of NSDL.

(v) NSDL itself, SEBI and any other regulator/ statutory authority or the persons authorised by it shall have the right to access the facilities / premises / data of the Service Provider at any point of time.

(vi) Outsourcing arrangements shall not impair the ability of SEBI, self-regulatory organizations, auditors, or NSDL's own oversight functions to carry out supervision, inspection, audit, or enforcement.

7. Governance and Approval Process

(i) **Board Oversight**: The Board shall have oversight over all outsourced activities, including ensuring that all ongoing outsourcing decisions taken

by NSDL and the activities undertaken by the Service Provider, are in line with this Outsourcing Policy. The Board shall approve this Outsourcing Policy and any material amendments to it. It shall also review a report on NSDL's outsourced activities annually to ensure that outsourcing decisions remain in line with this Outsourcing Policy and risk appetite of NSDL.

(ii) **Management Committees**: Business heads proposing to outsource a function must present a clear case including risk analysis and due diligence on the chosen vendor (see Section 10 (*Due Diligence*)). The internal committee will vet the proposal to ensure it falls within the permissible scope of outsourcing and complies with all policy requirements. NSDL's [Procurement Committee, Compliance Committee or similar management committee] shall thereafter evaluate and approve outsourcing proposals in accordance with this Outsourcing Policy.

(iii) **Approval Levels**: Certain critical or large-scale outsourcing arrangements may require Audit Committee or Management approval on a case-by-case basis. Any proposal to outsource a function that could materially impact NSDL's operations or carries significant risk shall be escalated to the Audit Committee and/or Management for prior approval. Routine or low-risk outsourcing (of non-core activities) shall be approved by the designated senior executives responsible for such business function, provided it remains within the framework of this Outsourcing Policy. All approvals shall be documented.]

(iv) **Policy Communication**: This Outsourcing Policy (and any updates hereunder) shall be disseminated to all relevant NSDL personnel as appropriate. Service Providers engaging with NSDL shall also be made aware of the policy requirements so they understand NSDL's compliance expectations.

8. Service Provider Evaluation

(i) NSDL shall conduct appropriate due diligence as set out in Section 10 (*Due Diligence*) in selecting the Service Provider to whom activity is proposed to be outsourced and ensure only reputed entities having proven high delivery standards are selected. Key principles guiding the decision shall include:

(a) Conflict of interest check;

(b) Risk materiality assessment and mitigation strategies;

(c) Continuity and contingency evaluation; and

(d) Review of technical and organisational measures for data protection and cyber security followed by the Service Provider.

9. Risk Assessment and Mitigation Strategies

(i) At the time of onboarding, an assessment of the Service Provider shall be carried out by the respective Head of Department and shall be reviewed by Risk Department in the manner as prescribed in the 'Operations Manual for Vendor Evaluation under NSDL Outsourcing Policy' (hereinafter referred to as "**Operations Manual**"). further, each Service Provider shall be subject to annual evaluation as per the procedure prescribed in *the Operations Manual*.

(ii) The risk assessment shall include the following:

(a) The impact of failure of the Service Provider to perform the Outsourced Services in accordance with the Outsourcing arrangement, on NSDL's financial, reputational, operational, and systemic obligations;

(b) The ability of NSDL to continue services in case of non-performance or failure by the Service Provider, including existence of back-up arrangements;

(c) Fitness and probity status of the Service Provider, its compliance history, and potential for breach of SEBI/Depositories Act obligations;

(d) Assessment of situations where conflicts may arise between NSDL and the Service Provider, including intra-group outsourcing;

(e) Assessment of adequacy of systems to prevent misuse of confidential information, including cyber resilience and access controls;

(f) The potential for market or investor confidence to be undermined due to failures, misconduct, or deficiencies in outsourced services;

(g) Impact of excessive reliance on a single service provider or geographic region, including systemic concentration across the market;

(h) Legal, regulatory, political, and data protection environments in the host jurisdiction (for cross-border outsourcing), and enforceability of SEBI's oversight rights;

(i) Impact of occurrence of coercion and undue influence on any employees of NSDL and non-compliance with code of conduct, anti-bribery and anti-corruption policies of NSDL, that may be applicable;

(j) Impact on NSDL's understanding of how the Outsourced Service is performed, with a consequential loss of control over that Outsourced Service;

(k) Potential risks to the regulatory objectives of maintaining fair, orderly, and transparent markets;

(l) Impact on price formulation;

(m) Whether NSDL would be unable to deliver core services to its clients without the relevant Outsourced Service; and

(n) Impact of deterioration of the quality of services provided by the Service Provider on NSDL's clients.

(iii) NSDL shall consider the totality of all factors relevant to an outsourced task. The combination of a number of factors, which are minimal in isolation may determine that the outsourced task to which they are related is material or critical when they are considered in aggregate.

(iv) NSDL shall employ mechanisms to mitigate risks, these mechanisms may include:

(a) In case a Service Provider is engaged, then it shall be ensured that the services of the Service Provider are supervised by an employee of NSDL. The supervision shall be documented (monitoring reports, periodic review meetings).

(b) Framing and implementation of a whistleblower policy with a clear and defined mechanism.

(c) Framing policies on retention, archival and deletion of data and information, in line with statutory requirement.

(d) In instances, where the Service Provider acts as an outsourcing agent for multiple companies (Intermediaries), NSDL and the Service Provider shall ensure that strong safeguards are put in place so that there is no co-mingling of information/documents, records and assets.

(e) Ensuring that appropriate risk mitigation measures like

backup/restoration system are in place.

(f) Risk assessments shall not be a one-time exercise but will be periodically reviewed throughout the outsourcing lifecycle, including upon any material change in ownership, operations, or scope of the Service Provider.

(g) Outsourcing arrangements assessed as "material" shall be subject to enhanced governance, with risk evaluation and mitigation status reported to the Board at defined intervals.

(h) NSDL shall also periodically assess whether its internal controls are adequate to oversee the Outsourced Activities, including the fulfilment of all contractual terms by the Outsourced Entities.

(v) The concerned department shall provide copy of the documents and information of any new outsourcing arrangements to the Compliance Officer as and when it enters into such arrangement but not later than fifteen (15) days of signing the agreement or any material change thereof. Every concerned department as a part of the quarterly compliance report shall submit status of compliance with this Outsourcing Policy to the Compliance Officer. Status of compliance of Outsourcing Policy will form part of the compliance report submitted by the Compliance Officer to the Governing Board.

10. Due diligence in selecting the Service Provider and in monitoring of its performance

(i) Before entering into or renewing any outsourcing arrangement, NSDL shall conduct comprehensive due diligence on the proposed Service Provider, ensuring compliance with SEBI Circulars and internal governance requirements. The goal is to ensure that only reputable, capable, and dependable service partners are entrusted with NSDL's functions, consistent with SEBI's expectation that "only reputed entities having proven high delivery standards are selected".

(ii) The due diligence shall cover both qualitative and quantitative parameters, including:

(a) **<u>Quantitative Parameters</u>**

- **Stability**: Review the financial stability and solvency of the Service Provider to ensure it can sustain operations for the duration of the outsourcing arrangement. NSDL shall avoid engaging vendors who

are financially weak or facing bankruptcy/insolvency proceedings, as they pose a continuity risk. Risk Department shall review and evaluate from the details available in public domain regarding any insolvency, bankruptcy, or similar proceedings, which may affect the going-concern of the Service Provider.

- **Capability and Capacity Assessment:** Evaluate the prospective service provider's resources and technical capabilities to perform the intended functions efficiently and on fixed timelines. This covers financial soundness, skilled personnel, expertise, any specific licenses or certifications required.

- **Infrastructure and Systems Compatibility**: Assess whether the Service Provider's technology systems, security standards, and operating processes are compatible with NSDL's requirements and policies, including SEBI's Cybersecurity and Cyber Resilience Framework. For IT or data-related outsourcing, NSDL's IT team will review the provider's system architecture, cybersecurity measures, and data protection controls. Cybersecurity due diligence is especially important, as the vendor must be capable of meeting NSDL's criteria under SEBI's Cybersecurity and Cyber Resilience Framework.

- **Conflict of Interest Check**: NSDL will evaluate potential conflicts of interest between NSDL and the Service Provider. If an outsourcing arrangement could create a conflict (such as the Service Provider has competing obligations or insider access) that cannot be adequately mitigated, NSDL shall avoid such outsourcing.

- **Cyber Security Measures**: The Service Provider shall have appropriate cybersecurity measures, consistent with applicable regulatory guidelines, to ensure the confidentiality, integrity, and availability of data and systems.

- **Cost-Effectiveness**: Evaluation of whether the proposed arrangement is rational and proportionate in terms of cost versus benefit, without compromising regulatory or investor protection standards.

- **Service-Levels**: Evaluate performance indicators such as response time, resolution timelines, and escalation procedures.

- **Service Uptime**: The Service Provider's ability to ensure continuous, uninterrupted service delivery, supported by evidence of redundancy,

business continuity planning, and disaster recovery arrangements.

- **Key Performance Indicators (KPIs)**: Pre-defined KPIs shall be tracked to monitor the Service Provider's performance against contractual benchmarks.

- **Reviews/ Reports**: Review results from audits and compliance reports of the Service Provider.

- **Geo-political Risk**: If the Service Provider is located outside India, NSDL will assess country risk factors, including the stability of the jurisdiction, legal protections for data, and the relationship of that country with Indian authorities. Cross-border outsourcing will only be undertaken if equivalent safeguards and regulatory access can be ensured in the foreign location.

- **Continuity and Contingency**: Evaluate how the work will continue if the Service Provider fails or the arrangement is terminated, including consideration of exit strategies and contingency plans (bringing the function back in-house or transitioning to an alternate provider) to address potential service disruption.

(b) **Qualitative Parameters**

- **Track Record and Reputation**: Gather market feedback and check the business reputation and track record of the Service Provider. Past performance with other clients and any history of regulatory or legal violations will be examined. Preference is given to Service Providers who have a strong compliance culture and positive references in the industry.

- **Compliance and Regulatory Status**: Verify the regulatory status of the Service Provider, if applicable. Conduct background checks including fitness and propriety of key personnel, to ensure the provider can be trusted with sensitive tasks.

- **Competence**: Compatibility of the practices and systems of the Service Provider with NSDL's requirements and objectives.

- **Level of Concentration**: Consider how much dependency NSDL would have on a single Service Provider. If the same Service Provider handles multiple outsourced functions for NSDL or is a common provider for many market entities, NSDL shall evaluate concentration risks such as:

- If the Service Provider suddenly and unexpectedly becomes unable to perform services that are material or critical to the business of a significant number of regulated entities, each entity will be similarly disabled;
- A latent flaw in the design of a product or service that multiple regulated entities rely upon may affect all the users;
- A vulnerability in application software that multiple regulated entities rely upon may permit an intruder to disable or corrupt the systems or data of some or all users; or
- If multiple regulated entities depend upon the same provider of business continuity services, a disruption that affects a large number of those entities may reduce the capacity of the business continuity service.

Each of these scenarios may have an adverse effect on other sectors or on public confidence in markets. Over-reliance on one Service Provider shall be avoided to prevent a single point of failure. Diversification of outsourced services across vendors may be pursued where prudent.

(iii) Basis the above-mentioned parameters, the concerned Department Heads shall carry out the evaluation of a Service Provider on a set of risk matrix laid down in the Operations Manual before on-boarding. This matrix can be amended or added or deleted as per the discretion of the Risk Department/ team. An indicative list of parameters in the risk matrix and key risk mitigation strategies is set out in **Schedule II** of the Outsourcing Policy.

(iv) The due diligence findings shall be documented in a standardized format (template/checklist) and maintained centrally by the Compliance/Risk Department for regulatory and audit review.

(v) NSDL's Risk or Compliance Department may maintain an approved panel or whitelist of vendors that have passed initial due diligence. Final selection of a service provider will also factor in commercial considerations (cost, service quality, etc.).

11. Outsourcing Agreement

(i) Outsourcing arrangements shall be governed by a clearly defined and legally binding written contract between the Company and each of the Service Provider, the nature and detail of which shall be appropriate to the

materiality of the outsourced activity in relation to the ongoing business of the Company. A contract would mean an agreement, purchase order or terms and conditions agreed upon in writing between the Company and Service Provider. Care shall be taken to ensure that the outsourcing agreement:

(a) **Scope of Services and Performance Standards:** The contract explicitly defines the activities or services being outsourced, including detailed service level agreements or performance metrics expected from the Service Provider. Deliverables and timelines should be clear.

(b) **Roles, Obligations, and Liability**: Mutual rights and obligations of NSDL and the Service Provider are laid down. The contract provides for the liability of the Service Provider to the Company for unsatisfactory performance/other breach of the contract. It defines of 'material event' and includes indemnification clauses (along with the extent of liability) where the Service Provider indemnifies NSDL for losses or third-party claims arising from the Service Provider's acts.

(c) **Control and Intervention Rights**: NSDL retains sufficient control over the outsourced process via contract terms. The contract should provide that any necessary corrective measures can be taken up immediately, i.e., the contract shall enable NSDL to retain an appropriate level of control over the Service Provider and the right to intervene (including NSDL's right to intervene) with appropriate measures to meet legal and regulatory obligations.

(d) **Sub-contracting Restrictions:** The contract prohibits the Service Provider from sub-contracting any part of the Outsourced Services to another entity without NSDL's prior approval. If sub-contracting is permitted, conditions of sub-contracting by the Service Provider shall be identical such that the contract shall enable NSDL to maintain a similar control over the risks when a Service Provider outsources to further third parties as in the original direct outsourcing.

(e) **Confidentiality and Data Protection**: The contract has unambiguous confidentiality clauses as detailed in Section 13 (*Protection of Confidential* Information) to ensure protection of proprietary, investor and other confidential data in accordance with privacy laws and NSDL's data protection and data sharing practices and cyber security policies, including SEBI's Cybersecurity and Cyber Resilience

Framework.

(f) **Security and Resilience Obligations**: The Service Provider agrees to implement appropriate IT security measures business continuity plans as detailed in Section 12 (*Contingency Plans*), insurance cover and force majeure clause commensurate with the outsourced activity. The contract should detail expectations around data encryption, access controls, incident reporting, disaster recovery infrastructure, and compliance with standards like SEBI's Cybersecurity and Cyber Resilience Framework.

(g) **Inspection, Audit and Access Rights**: The contract grants NSDL, its auditors, and regulators (such as SEBI) and the authorized representatives of the regulators the right to inspect the vendor's operations, facilities, systems, records and data pertaining to activities related to the outsourced service as detailed in Section 14 (*Audit*).

(h) **Regulatory Compliance**: States that the outsourcing arrangement shall not prevents nor impedes NSDL from complying with its regulatory obligations, nor regulators from exercising their authority. If any regulatory requirements change, the vendor must accommodate those changes contractually. The contract will also require the vendor to comply with all applicable laws and regulations (for example, the laws on data protection and privacy) in performing the services.

(i) **Intellectual Property**: Provides for ownership of Intellectual Property Rights in any tangible or intangible asset as may be created, developed, designed, procured, built for NSDL under the outsourced services.

(j) **Disclosures to Avoid Conflict of Interest**: Have terms around infrastructure, manpower, decision-making, record keeping, etc. In case the arrangement is between related parties, the contract should include arm's-length clauses.

(k) **Termination and Exit Strategy**: Includes clear terms for termination, including NSDL's right to terminate the contract for convenience or for cause, such as material breach, insolvency of the vendor, or persistent poor performance, with defined notice periods and transition assistance obligations. Further an exit management plan, detailing how data, assets, or processes will be handed back to NSDL or transferred to a new provider upon termination, to ensure business continuity.

(l) **Dispute Resolution and Jurisdiction**: Includes dispute resolution mechanism and specify governing law. For any outsourcing involving an overseas vendor, choice-of-law and jurisdiction clauses will be carefully set so that NSDL's interests are protected, and enforcement is feasible.

(m) **Periodic Review and Updates**: Provides for the continuous monitoring and assessment by NSDL of the service. Long-term contracts should include provisions for periodic performance reviews and the ability to renegotiate terms if external circumstances (like regulatory changes) require it.

(n) **Additional Protection for Foreign Outsourced Entities**: The contract should address additional issues arising from country risks and potential obstacles in exercising oversight and management of the arrangements when Company outsources its activities to foreign Service Provider.

(o) **SLAs and Contractual Safeguards**: All contracts shall embed clear SLAs specifying minimum service levels, contingency response timelines, escalation triggers, and penalties for breach. SLAs shall expressly cover: (a) disaster recovery performance; (b) incident notification and reporting obligations; (c) regulatory access and cooperation requirements; and (d) step-in rights for NSDL in case of critical failure.

12. Contingency Plans

(i) **Contingency Plans**: NSDL shall ensure that comprehensive contingency plans are established and maintained covering: (a) contingency plans at the Service Provider's end; (b) coordination of contingency plans between the Company and the Service Provider; and (c) contingency plans of the Company in the event of non-performance by the Service Provider.

(ii) **Principle of Continuity and Control**: NSDL shall ensure that outsourcing of any activitydoes not impair its ability to discharge regulatory obligations or its accountability to SEBI, investors, or market participants.

(iii) **Business Continuity and Disaster Recovery**: Every outsourcing arrangement that is identified as 'critical' shall be supported by a documented Business Continuity Plan ("**BCP**") and Disaster Recovery ("**DR**") Plan, covering operational disruption, IT or cyber incidents, natural disasters, and force majeure events. The BCP/DR shall:

(a) define recovery time objectives and recovery point objectives consistent with the criticality of the function;

(b) provide for alternate infrastructure and data recovery mechanisms, including geographically separate backup sites; and

(c) ensure uninterrupted access to critical data, systems, and records of NSDL.

(iv) NSDL shall conduct periodic testing of BCP/DR arrangements with each critical Service Provider, document the results, and report material gaps to senior management and the Board.

(v) Appropriate steps must be taken to assess and address the potential consequence of a business disruption or other problems at the Service Provider level.

13. Protection of Confidential Information

(i) **Confidentiality Obligations in Contracts**: All outsourcing agreements shall contain clear and unambiguous confidentiality provisions requiring the Service Provider to: (a) maintain confidential information of both NSDL and its customers from intentional or inadvertent disclosure to unauthorized persons; (b) protect proprietary and customer data during and after the term of the contract; and (c) use NSDL data solely for the performance of the contracted service, with no right of secondary use.

(ii) **Access Control and Data Minimisation**: Access to NSDL data by Service Provider personnel shall be limited to a "need-to-know" and "least-privilege" basis. Additional measures shall be taken shall as, access credentials on role-based, logged, monitored, and revoked promptly on cessation of engagement and multi-factor authentication and other strong access protocols shall be mandated for sensitive systems.

(iii) **Data Security Standards**: The Service Provider shall maintain information security measures at least equivalent to NSDL's own standards, including: (a) encryption of sensitive and personal data at rest and in transit; (b) implementation of firewalls, intrusion prevention, and data loss prevention tools; and regular vulnerability assessments, penetration testing, and remediation of high-severity vulnerabilities within regulatory timelines.

(iv) **Data Preservation and Storage**: NSDL shall ensure that the Service Provider preserves documents and data in compliance with SEBI record-keeping

requirements. Data shall only be stored in jurisdictions permitted under applicable law. On termination of the contract, all NSDL data shall be returned or securely destroyed, with certification of destruction provided.

(v) **Prevention of Co-Mingling**: Where an Service Provider services multiple intermediaries, robust safeguards shall be imposed to ensure strict segregation of NSDL's data, documents, systems, and assets, both logically and physically.

(vi) **Incident Reporting and Response**: The Service Provider shall report any data breach, cyber incident, or unauthorized disclosure to NSDL as soon as the occurrence or being aware of the incident. NSDL shall notify SEBI and other competent statutory authorities of incidents within the regulatory timelines and ensure prompt remediation. Joint investigation and corrective action plans shall be implemented with the Service Provider, where necessary.

(vii) **AI/ML-Linked Data Processing**: Where a Service Provider deploys AI/ML tools to process NSDL's information, the entity shall remain contractually responsible for ensuring the privacy, security, and integrity of all investor data, regardless of whether such tools are internally developed or third-party solutions. Further, such deployment shall be in compliance with the applicable laws.

14. Audit

(i) The Outsourcing Policy document shall act as a reference for audit of the outsourced activity. Audit of implementation of risk assessment and mitigation measures listed in the Outsourcing Policy document and outsourcing agreement/service level agreements pertaining to IT systems shall be part of System Audit.

(ii) To ensure the outsourcing framework remains effective and up-to-date, NSDL will implement the following review and audit mechanisms:

(a) **Internal Audit**: NSDL's internal audit team will include outsourcing arrangements in their audit plan. Audits will check for compliance with this Outsourcing Policy, effectiveness of vendor oversight, accuracy of records, and whether risk mitigation measures are functioning as intended.

(b) **System and Compliance Audits**: In line with SEBI requirements,

NSDL's System Audit shall cover the outsourced IT systems and related service-level compliance. Auditors will verify that the vendor's controls and NSDL's monitoring of those controls are adequate. Additionally, any SEBI-mandated audit (such as cybersecurity audits under SEBI's Cybersecurity and Cyber Resilience Framework) that applies to NSDL will also extend to relevant third-party arrangements. The audit reports might need to comment on third-party risk management, NSDL shall ensure auditors get access to Service Provider's security posture as required.

(c) **Outsourcing Policy Audit**: The Outsourcing Policy itself acts as a reference point for audits. Auditors will check that NSDL's practices align with the stated policy If there are deviations or the policy is not being effectively implemented in any area, those will be flagged and corrected. The audit findings might also recommend updates to the policy in response to new threats or regulatory changes.

Further, the records relating to all activities outsourced shall be preserved by the Management Committees who has outsourced its activity and in addition centrally by the Procurement Department so that the same is readily accessible for review by the Board and Management, as and when needed.

(d) **Regulatory Feedback**: NSDL will also take into account any observations from SEBI inspections or communications regarding outsourcing. If the regulator highlights any concerns, NSDL's Management and Board ha;; address the issue and strengthen controls.

(iii) All review and audit results related to outsourcing will be documented. Significant findings or recommendations are reported to senior management and the Board, and corrective action plans are tracked to completion. This continuous improvement loop ensures that NSDL's outsourcing practices remain industry-leading and fully compliant. By regularly auditing itself against best practices, NSDL can demonstrate to regulators and stakeholders that its outsourcing arrangements are sound and effectively managed.

15. Review of the Outsourcing Policy

(i) The Outsourcing Policy shall be approved by the Governing Board of NSDL and any amendment to the Outsourcing Policy can be made with the approval of the Governing Board.

(ii) The Outsourcing Policy shall be reviewed as and when required and in any case on an annual basis by the Board.

(iii) Any new regulation circular issued by SEBI shall be tracked by the Legal and Compliance teams and shall deemed to have been included in the Outsourcing Policy upon their issuance, without waiting for formal approval of the Board. The provisions in the Outsourcing Policy are in addition to, and not in derogation of, other applicable laws.

Schedule I

1. **Participant/Issuer Admission and facilitating Issuers/RTAs to execute Corporate Actions**: Processing applications for admission/registration of Depository Participants (DPs), issuers, Registrar & Transfer Agents (RTAs), Vault managers or any similar entities in NSDL's ecosystem and facilitating them to execute corporate actions.

2. **ISIN Allocation**: Allotting International Securities Identification Numbers (ISINs) for securities.

3. **Safekeeping of Beneficial Owner (BO) Data**: Maintaining the central depository records and ensuring the integrity and safekeeping of BO account data.

4. **Settlement Operations**: Execution of settlement activities for securities pay-in and pay-out, along with associated incidental tasks.

5. **Securities Transfers and Other Core Transactions**: Execution of transfers of securities between accounts and processing of other transactions like pledges, lien marking, freezes/unfreezes, etc.

6. **DP and RTA Inspections:** Conducting inspections and compliance audits of Depository Participants and registrar/transfer agents connected to NSDL.

7. **Investor Grievance Monitoring and Redressal**: Monitoring investor complaints/grievances related to depository services and ensuring their resolution. However, the activity of making entry of Audit/Inspection Reports received from the DPs in NSDL back-office system i.e. maker level activity may be outsourced who will perform the job under the supervision of employees of NSDL.

8. **Surveillance, Risk Management and Compliance Functions**: All surveillance activities and risk management functions (market monitoring related to depository operations). This includes compliance with KYC/AML requirements and reporting obligations to the Financial Intelligence Unit (FIU)

or any other statutory or competent authority.

9. **Continuous Connectivity and System Integrity**: Ensuring continuous connectivity with DPs, RTAs, clearing corporations, other depositories.

10. **Investor-facing Online Services**: Provision of internet-based facilities for investors such as online **access** to demat accounts, electronic delivery instructions submission.

Schedule II

Risk Category	Description and Mitigation Strategies
Operational and Systemic Risk	**Description:** Risks of service failure, delays, or inability to perform critical functions, which can affect the entire market system. **Mitigation:** Clear service level agreements, robust business continuity plans, and diversification of vendors.
Financial Risk	**Description:** Risks related to the financial stability of the outsourced provider and potential for unforeseen costs. **Mitigation:** Thorough due diligence on the financial health of the vendor and clear terms on payment and pricing.
Compliance and Legal Risk	**Description:** Risks of failing to meet regulatory requirements, which can lead to penalties and legal action. **Mitigation:** Ensuring the vendor is fully compliant with all relevant regulations, with specific clauses in the contract detailing responsibilities and audit rights.
Reputational Risk	**Description:** Damage to the depository's reputation due to failures or misconduct by the Service Provider. **Mitigation:** Careful selection of vendors with a good track record and establishing clear communication channels to address any negative publicity quickly.
Cyber Security Risk	**Description:** Risks of data breaches, cyberattacks, and other malicious activities compromising sensitive information.

	Mitigation: Requiring the vendor to have strong cybersecurity measures in place and conducting regular security audits.
Contractual Risk	**Description:** Risks arising from poorly drafted or incomplete contracts. **Mitigation:** Ensuring contracts are comprehensive, legally sound, and clearly define all aspects of the outsourcing arrangement, including responsibilities, liability, and exit strategies.
Technological Risk	**Description:** Risks associated with outdated or unreliable technology, system integration issues, and technology failures. **Mitigation:** Selecting vendors with robust and up-to-date technology, with clear plans for system upgrades and maintenance.
Human Resource Risk	**Description:** Risks related to the outsourced provider's employees, including lack of experience, high turnover, or unethical behavior. **Mitigation:** Due diligence on the vendor's HR practices, ensuring proper training and a clear code of conduct for their employees.
Concentration Risk	**Description:** Over-reliance on a single vendor, which can create significant risk if that vendor fails. **Mitigation:** Diversifying outsourced activities across multiple vendors where possible and having a clear exit strategy to transfer functions to an alternative provider if needed.
Country Risk	**Description:** The risk associated with outsourcing to a service provider in a different country, including political instability, economic fluctuations, and differing legal and regulatory environments. **Mitigation:** Perform country-specific due diligence, assessing the legal, political, and economic stability of the foreign country. Diversify outsourcing locations to avoid over-reliance on a single country.
Exit-Strategy Risk	**Description:** The risk that the depository cannot successfully transition its outsourced functions back in-house or to another vendor when the contract ends, leading to business disruption, data

	loss, or increased costs. **Mitigation:** Include a detailed exit plan in the contract, outlining a clear transition process. Ensure the vendor cooperates with the transition and provides necessary documentation and training to the in-house team or new vendor.