PRINCIPLES FOR OUTSOURCING FOR INTERMEDIARIES

1. **A merchant banker seeking to outsource activities shall have in place a comprehensive policy to guide the assessment of whether and how those activities can be appropriately outsourced. The Board of Directors (hereinafter referred to as the "the Board") of the merchant banker shall have the responsibility for the outsourcing policy and related overall responsibility for activities undertaken under that policy.**

   1.1. The policy shall cover activities or the nature of activities that can be outsourced, the authorities who can approve outsourcing of such activities, and the selection of third party to whom it can be outsourced. For example, an activity shall not be outsourced if it would impair the supervisory authority's right to assess, or its ability to supervise the business of the merchant banker. The policy shall be based on an evaluation of risk concentrations, limits on the acceptable overall level of outsourced activities, risks arising from outsourcing multiple activities to the same entity, etc.

   1.2. The Board shall mandate a regular review of outsourcing policy for such activities in the wake of changing business environment. It shall also have overall responsibility for ensuring that all ongoing outsourcing decisions taken by the merchant banker and the activities undertaken by the third party, are in keeping with its outsourcing policy.

2. **The merchant banker shall establish a comprehensive outsourcing risk management program to address the outsourced activities and the relationship with the third party.**

   2.1. A merchant banker shall make an assessment of outsourcing risk which depends on several factors, including the scope and materiality of the outsourced activity, etc. The factors that could help in considering materiality in a risk management program include-

      2.1.1. The impact of failure of a third party to adequately perform the activity on the financial, reputational and operational performance of the merchant banker and on the investors / clients;

2.1.2. Ability of the merchant banker to cope up with the work, in case of non-performance or failure by a third party by having suitable back-up arrangements;

2.1.3. Regulatory status of the third party, including its fitness and probity status;

2.1.4. Situations involving conflict of interest between the merchant banker and the third party and the measures put in place by the merchant banker to address such potential conflicts, etc.

2.2. While there shall not be any prohibition on a group entity / associate of the merchant banker to act as the third party, systems shall be put in place to have an arm's length distance between the merchant banker and the third party in terms of infrastructure, manpower, decision-making, record keeping, etc. for avoidance of potential conflict of interests. Necessary disclosures in this regard shall be made as part of the contractual agreement. It shall be kept in mind that the risk management practices expected to be adopted by a merchant banker while outsourcing to a related party or an associate would be identical to those followed while outsourcing to an unrelated party.

2.3. The records relating to all activities outsourced shall be preserved centrally so that the same is readily accessible for review by the Board of the merchant banker and / or its senior management, as and when needed. Such records shall be regularly updated and may also form part of the corporate governance review by the management of the merchant banker.

2.4. Regular reviews by internal or external auditors of the outsourcing policies, risk management system and requirements of the regulator shall be mandated by the Board wherever felt necessary. Merchant banker shall review the financial and operational capabilities of the third party in order to assess its ability to continue to meet its outsourcing obligations.

3. The merchant banker shall ensure that outsourcing arrangements neither diminish its ability to fulfill its obligations to customers and regulators, nor impede effective supervision by the regulators.

3.1. The merchant banker shall be fully liable and accountable for the activities that are being outsourced to the same extent as if the service were provided in-house.

3.2. Outsourcing arrangements shall not affect the rights of an investor or client against the merchant banker in any manner. The merchant banker shall be liable to the investors for the loss incurred by them due to the failure of the third party and also be

responsible for redressal of the grievances received from investors arising out of activities rendered by the third party.

3.3. The facilities / premises / data that are involved in carrying out the outsourced activity by the service provider shall be deemed to be those of the merchant banker. The merchant banker itself and regulator or the persons authorized by it shall have the right to access the same at any point of time.

3.4. Outsourcing arrangements shall not impair the ability of SEBI/SRO or auditors to exercise its regulatory responsibilities such as supervision/ inspection of the merchant banker.

4. The merchant banker shall conduct appropriate due diligence in selecting the third party and in monitoring of its performance.

4.1. It is important that the merchant banker exercise due care, skill, and diligence in the selection of the third party to ensure that the third party has the ability and capacity to undertake the provision of the service effectively.

4.2. The due diligence undertaken by a merchant banker shall include assessment of:

4.2.1. third party's resources and capabilities, including financial soundness, to perform the outsourcing work within the timelines fixed;

4.2.2. compatibility of the practices and systems of the third party with the intermediary's requirements and objectives;

4.2.3. market feedback of the prospective third party's business reputation and track record of their services rendered in the past;

4.2.4. level of concentration of the outsourced arrangements with a single third party; and

4.2.5. the environment of the foreign country where the third party is located.

5. Outsourcing relationships shall be governed by written contracts / agreements / terms and conditions (as deemed appropriate) {hereinafter referred to as "contract"} that clearly describe all material aspects of the outsourcing arrangement, including the rights, responsibilities and expectations of the parties to the contract, client confidentiality issues, termination procedures, etc.

5.1. Outsourcing arrangements shall be governed by a clearly defined and legally binding written contract between the intermediary and each of the third parties, the nature and detail of which shall be appropriate to the materiality of the outsourced activity in relation to the ongoing business of the intermediary.

5.2. Care shall be taken to ensure that the outsourcing contract:

5.2.1. clearly defines what activities are going to be outsourced, including appropriate service and performance levels;

5.2.2. provides for mutual rights, obligations and responsibilities of the intermediary and the third party, including indemnity by the parties;

5.2.3. provides for the liability of the third party to the intermediary for unsatisfactory performance/other breach of the contract

5.2.4. provides for the continuous monitoring and assessment by the intermediary of the third party so that any necessary corrective measures can be taken up immediately, i.e., the contract shall enable the intermediary to retain an appropriate level of control over the outsourcing and the right to intervene with appropriate measures to meet legal and regulatory obligations;

5.2.5. includes, where necessary, conditions of sub-contracting by the third-party, i.e. the contract shall enable intermediary to maintain a similar control over the risks when a third party outsources to further third parties as in the original direct outsourcing;

5.2.6. has unambiguous confidentiality clauses to ensure protection of proprietary and customer data during the tenure of the contract and also after the expiry of the contract;

5.2.7. specifies the responsibilities of the third party with respect to the IT security and contingency plans, insurance cover, business continuity and disaster recovery plans, force majeure clause, etc.;

5.2.8. provides for preservation of the documents and data by third party;

5.2.9. provides for the mechanisms to resolve disputes arising from implementation of the outsourcing contract;

5.2.10. provides for termination of the contract, termination rights, transfer of information and exit strategies;

5.2.11. addresses additional issues arising from country risks and potential obstacles in exercising oversight and management of the arrangements when intermediary outsources its activities to foreign third party. For example, the contract shall include choice-of-law provisions and agreement covenants and jurisdictional covenants that provide for adjudication of disputes between the parties under the laws of a specific jurisdiction;

5.2.12. neither prevents nor impedes the intermediary from meeting its respective regulatory obligations, nor the regulator from exercising its regulatory powers; and

5.2.13. provides for the intermediary and /or the regulator or the persons authorized by it to have the ability to inspect, access all books, records and information relevant to the outsourced activity with the third party.

6. The merchant banker and its third parties shall establish and maintain contingency plans, including a plan for disaster recovery and periodic testing of backup facilities.

6.1. Specific contingency plans shall be separately developed for each outsourcing arrangement, as is done in individual business lines.

6.2. A merchant banker shall take appropriate steps to assess and address the potential consequence of a business disruption or other problems at the third party level. Notably, it shall consider contingency plans at the third party; co-ordination of contingency plans at both the merchant banker and the third party; and contingency plans of the merchant banker in the event of non-performance by the third party.

6.3. To ensure business continuity, robust information technology security is a necessity. A breakdown in the IT capacity may impair the ability of the merchant banker to fulfill its obligations to other market participants/clients/regulators and could undermine the privacy interests of its customers, harm the merchant banker's reputation, and may ultimately impact on its overall operational risk profile. Merchant banker shall, therefore, seek to ensure that third party maintains appropriate IT security and robust disaster recovery capabilities.

6.4. Periodic tests of the critical security procedures and systems and review of the backup facilities shall be undertaken by the merchant banker to confirm the adequacy of the third party's systems.

7. The merchant banker shall take appropriate steps to require that third parties protect confidential information of both the merchant banker and its customers from intentional or inadvertent disclosure to unauthorized persons.

7.1. A merchant banker that engages in outsourcing is expected to take appropriate steps to protect its proprietary and confidential customer information and ensure that it is not misused or misappropriated.

7.2. The merchant banker shall prevail upon the third party to ensure that the employees of the third party have limited access to the data handled and only on a "need to know" basis and the third party shall have adequate checks and balances to ensure the same.

7.3. In cases where the third party is providing similar services to multiple entities, the merchant banker shall ensure that adequate care is taken by the third party to build safeguards for data security and confidentiality.

8. **Potential risks posed where the outsourced activities of multiple merchant bankers are concentrated with a limited number of third parties.**

In instances, where the third party acts as an outsourcing agent for multiple merchant bankers, it is the duty of the third party and the merchant banker to ensure that strong safeguards are put in place so that there is no co-mingling of information /documents, records and assets.