GEECEE FINCAP LIMITED

FRAMEWORK ON INFORMATION TECHNOLOGY GOVERNANCE

Effective Date	**30.03.2024**
1st Review	**04.02.2025**

PREAMBLE:

Geecee FinCap Limited ("Company") has adopted this framework on Information Technology Governance & Information Security Audit as per the Master Direction issued by RBI dated 7th November, 2023 to incorporate, consolidate and update the guidelines, instructions and circulars on IT Governance, Risk, Controls, Assurance Practices and Business Continuity/ Disaster Recovery Management. The Company will use to administer these policies, with the correct procedure to follow. Therefore, from time to time it will be necessary to modify and amend some sections of the policies and procedures, or to add new procedures. All policies, procedures & assessment must be documented and made available to individuals responsible for their implementation and compliance. All activities identified by the policies and procedures must also be documented.

APPLICABILITY:

The Reserve Bank of India vide Master Direction – Reserve Bank of India (Non-Banking Financial Company – Scale Based Regulation) Directions, 2023 ('Scale Based Regulations') dated October 19, 2023 requires all the applicable Non-Banking Financial Company (NBFC) categorized as Middle Layer NBFC (NBFC-ML) to adopt a framework on Information Technology Governance & Information Security Audit.

DEFINITIONS:

- '*Cyber*' - Relating to, within, or through the medium of the interconnected information infrastructure of interactions among persons, processes, data, and information systems.
- ***'Cyber event'*** – Any observable occurrence in an information system. Cyber events sometimes provide indication that a cyber incident is occurring.
- ***'Cyber security'*** - Preservation of confidentiality, integrity and availability of information and/or information systems through the cyber medium. In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved.
- ***'Cyber incidents'*** shall mean a cyber event that adversely affects the cyber security of an information asset whether resulting from malicious activity or not.
- ***'Cyber-attack'*** - Malicious attempt(s) to exploit vulnerabilities through the cyber medium to damage, disrupt or gain unauthorized access to assets.
- ***'De-militarized Zone' or 'DMZ'*** is a perimeter network segment that is logically between internal and external networks.

- ***'Information Assets'*** - Any piece of data, device or other component of the environment that supports information-related activities. Information Assets include information system, data, hardware and software.

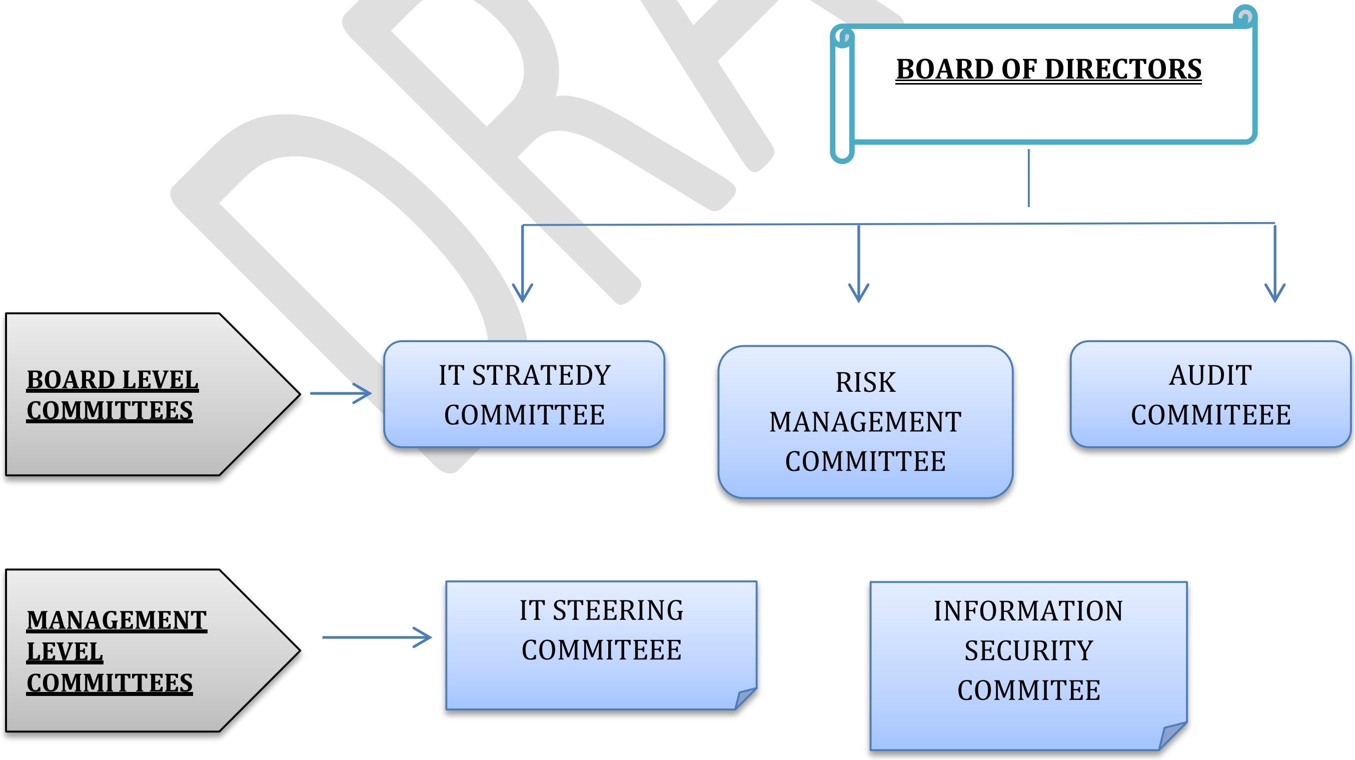
- ***'Information System'*** - Set of applications, services, information technology assets or other information-handling components, which includes the operating environment and networks.

- ***'IT Risk'*** - The business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise.

- ***'Privileged user'*** refers to user who, by virtue of function, and/or role, has been allocated powers within an information system, which are significantly greater than those available to the majority of users.

GOVERNANCE STRUCTURE FOR INFORMATION TECHNOLOGY:

IT Governance entails number of activities for the Board and Senior Management, such as becoming aware of role and impact of IT on organization; assigning responsibilities, defining constraints within which to operate, measuring performance, managing risk and obtaining assurance. The IT organizational structure should be commensurate with the size, scale and nature of business activities carried out by the organization and the underlying support provided by information systems for the business functions.



ROLE OF THE BOARD OF DIRECTORS:

The Company will develop a wide spectrum of policies, codes, and procedures to facilitate that and established Board Committees for their implementation, well supported by people, process and technology.

The strategies and policies related to IT, Information Assets, Business Continuity, Information Security, and Cyber Security (including Incident Response and Recovery Management / Cyber Crisis Management) will be approved and periodically reviewed by the Board of Directors of the Company.

IT STRATEGY COMMITTEE OF THE BOARD:

The Company has constituted the Board Level and an independent IT Strategy Committee with technically competent and adequate number of directors as members, of the Committee as prescribed by RBI. The Committee meets at regular interval periods of time. The Committee of the Company will be governed by the terms of references as specified by RBI Circular issued from time to time;

- Ensure effective IT strategic planning process.
- Guide in the preparation of IT Strategy aligned with overall RE strategy.
- Validate IT Governance and Information Security Governance structure.
- Oversee IT and cybersecurity risk assessment and management processes.
- Review budgetary allocations for IT function and cybersecurity.
- Review the adequacy & effectiveness of Business Continuity Planning and Disaster Recovery Management.

SENIOR MANAGEMENT AND IT STEERING COMMITTEE:

The Company will constitute IT Steering Committee with representatives from the IT, HR, legal and business functions etc. The Committee meets at regular interval periods of time. Its role is to assist the Executive Management in implementing IT strategy that has been approved by the Board. It includes prioritization of IT-enabled investment, reviewing the status of projects (including, resource conflict), monitoring service levels and improvements, IT service delivery and projects. The committee will focus on implementation of the IT policy & framework and the responsibilities of the Committe Includes;

- Assist the ITSC in strategic IT planning, oversight of IT performance, and aligning IT activities with business needs;

- Oversee the processes put in place for business continuity and disaster recovery;

- Ensure implementation of a robust IT architecture meeting statutory and regulatory compliance; and

- Update ITSC and CEO periodically on the activities of IT Steering Committee.

HEAD OF THE IT FUNCTIONS:

The Company will appoint a sufficiently senior level, technically competent and experienced official in IT related aspects as Head of IT function to ensure effective assessment of IT Controls & IT risk.

The Head of IT Function will be responsible for the following.

- Ensuring that the execution of IT projects/ initiatives is aligned with the company's IT Policy and IT Strategy;

- Ensuring that there is an effective organisational structure to support IT functions in the company and

- Putting in place an effective disaster recovery setup and business continuity strategy/ plan.

IT SERVICES MANAGEMENT:

The Company will put in place a robust IT Service Management Framework for supporting their information systems and infrastructure to ensure the operational resilience of their entire IT environment (including DR sites).

A Service Level Management (SLM) process will be put in place to manage the IT operations while ensuring effective segregation of duties.

The Company will ensure identification and mapping of the security classification (in terms of Confidentiality, Integrity, and Availability) of information assets based on their criticality to the Company's operations.

The Company will avoid using outdated and unsupported hardware or software and will monitor software's end-of-support (EOS) date and Annual Maintenance Contract (AMC) dates of IT hardware on an ongoing basis and will develop a technology refresh plan for the replacement of hardware and software in a timely manner before they reach EOS.

THIRD-PARTY ARRANGEMENTS:

The Company will maintain proper vendor risk assessment process for systematic evaluation of the potential risks and vulnerabilities introduced into an organization's operations, systems, and processes through its interactions with external parties and controls proportionate to the assessed risk. The Company will ensures that contracts & agreements entered with vendors should address the Information Security requirements, as necessary and review the performance of vendors who are giving support to the operations of the Data Centre, Information Assets like Hardware, Applications, databases, Network Devices and Infrastructure devices like UPS, AC, Fire Extinguishers etc.

OUTSOURCING OF IT SERVICES:

IT outsourcing is the use of external service providers to effectively deliver IT-enabled business process, application service and infrastructure solutions for business outcomes. Whenever the Company intending to outsource any of its IT activities will put in place a comprehensive Board approved IT outsourcing policy.

CAPACITY MANAGEMENT:

The Company will identify the IT assets either owned by it or used by the group companies. Also, the Company will formalize documents for the usage of IT assets of its group companies. Currently, the Company has adequate capacity of IT resources for meeting current as well as future requirements. The head of the IT functions will be responsible for calculating the capacity requirements for various information assets like Hardware Infrastructure, Server Operating Systems, Application Systems, Database Systems, Network devices and Network Infrastructure (Bandwidth and redundancies) and the supporting Data Centre Infrastructure like UPS, Power Generator, Air Conditioners, Fire Extinguishers etc.

The assessment of IT capacity requirements and measures taken to address the issues will be reviewed by the IT Strategy Committee.

PROJECT MANAGEMENT:

The Company will follow the management approach for the adoption of new technologies & new software applications with agreements. The IT personnel will ensures the top management of projected risks involved for adopting new technologies and the progress thereon. The Company will maintain enterprise data dictionary to enable the sharing of data among applications and information systems and promote a common understanding of data.

CHANGE AND PATCH MANAGEMENT:

The Company will put in place documented policy (ies) and procedures for change and patch management to ensure the following:

- the business impact of implementing patches/ changes (or not implementing a particular patch/ change request) are assessed;

- the patches/ changes are applied/ implemented and reviewed in a secure and timely manner with necessary approvals;

- any changes to an application system or data are justified by genuine business needs and approvals supported by documentation and subjected to a robust change management process.

POLICY ON DATA MIGRATION:

The Company will have a documented data migration policy specifying a systematic process for data migration, ensuring data integrity, completeness and consistency. The policy will inter alia, contain provisions pertaining to signoffs from business users and application owners at each stage of migration, maintenance of audit trails, etc.

AUDIT TRAIL:

The Company will put in place an audit trail to ensure;

- Every IT application which can access or affect critical or sensitive informations will have necessary audit and system logging capability and should provide audit trails.

- The audit trails will satisfy company's business requirements apart from regulatory and legal requirements. The audit trails must be detailed enough to facilitate the conduct of audit, serve as forensic evidence when required and assist in dispute resolution, including for non-repudiation purposes.

- The Company will put in place a system for regularly monitoring the audit trails and system logs to detect any unauthorized activity.

CRYPTOGRAPHIC CONTROLS:

The Company will adopt internationally accepted and published standards that are not deprecated/ demonstrated to be insecure/ vulnerable and the configurations involved in implementing such controls and will be compliant with extant laws and regulatory instructions.

STRAIGHT THROUGH PROCESSING:

The Company will ensure that there is no manual intervention or manual modification in data while it is being transferred from one process to another or from one application to another, in respect of critical applications. Data transfer mechanism between processes or applications properly tested, securely automated with necessary checks and balances, and properly integrated through ***"Straight Through Processing"*** methodology with appropriate authentication mechanism and audit trails.

PHYSICAL AND ENVIRONMENTAL CONTROLS:

The Company will implement the suitable controls in Data Centre and Data Recovery sites for protecting the information and technology resources from physical and environmental threats and reduce the risk of loss, theft, damage, or unauthorized access. The DC and DR sites should be geographically well separated so that both the sites are not affected by a similar threat associated to their location. The Company will ensure that their DC and DR sites are subjected to necessary e-surveillance mechanism.

CONTROL ON TELEWORKING:

The Company inter alia, will:

- Ensure that the systems used and the remote access from alternate work location to the environment hosting company's information assets are secure;
- Implement multi-factor authentication for enterprise access (logical) to critical systems;
- Put in place a mechanism to identify all remote-access devices attached/ connected to the company's systems; and
- Ensure that data/ information shared/ presented in teleworking is secured appropriately**.**

INFORMATION TECHNOLOGY (IT) ACCESS CONTROL:

- The Company will have a documented standards and procedures, which are approved by the ITSC and kept up to date for administering need-based access to an information system.

- Personnel with elevated system access entitlements will be closely supervised with all their systems activities logged and periodically reviewed.

- The Company will adopt multi-factor authentication for privileged users of
  - ❖ critical information systems and
  - ❖ for critical activities, basis the company's risk assessment.

METRICS:

The Company will define suitable metrics for system performance, recovery and business resumption, including Recovery Point Objective (RPO) and Recovery Time Objective (RTO), for all critical information systems. (b) For non-critical information systems, the Company will adopt a risk-based approach to define suitable metrics. (c) The Company also implement suitable scorecard/ metrics/ methodology to measure IT performance and IT maturity level.

****