GEECEE FINCAP LIMITED

INFORMATION SECURITY AUDIT POLICY

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

SCOPE:

The objective of the IS Audit is to provide an insight on the effectiveness of controls that are in place to ensure confidentiality, integrity and availability of the organization's IT infrastructure. IS Audit will identify risks and methods to mitigate risk arising out of IT infrastructure such as server architecture, local and wide area networks, physical and information security, telecommunications etc.

OBJECTIVE:

The objective of the Information System and Security audit is to identify risks that an organization is exposed to in the computerized environment. IS audit evaluates the adequacy of the security controls and informs the management with suitable conclusions and recommendations. IS audit is an independent subset of the normal audit exercise. Information systems audit is an ongoing process of evaluating controls; suggesting security measures for the purpose of safeguarding assets/resources, maintaining data integrity, improve system effectiveness and system efficiency for the purpose of attaining organization goals.

MANDATE:

IS audit is required for protection of Information systems assets of the organization such as hardware, software, facilities, people, data, technology, system documentation and supplies. This is because hardware can be damaged maliciously, software and data files may be stolen, deleted or altered and the same can be used for unauthorized purposes. Regarding the protection of information assets, one purpose of an IS audit is to review and evaluate an organization's information system's availability, confidentiality and integrity.

AUTHORITY AND ACCESS CONTROL*:*

Hierarchical pattern: A senior manager will have the authority to decide what data can be shared and with whom. The policy should outline the level of authority over data and IT systems for each organizational role.

Network security policy: Users are only able to access company networks and servers via unique logins that demand authentication, including passwords, biometrics, ID cards, or tokens.

ACCOUNTABILITY OF AUDIT:

The Audit Committee of the Board will be responsible for exercising oversight of IS Audit of the Company. The Company will establish a separate IS Audit function or resources who possess required professional skills and competence within the Internal Audit function. The Company may use external resources for conducting IS audit in areas where skills are lacking within the Company, the responsibility and accountability for such external IS audits would continue to remain with the competent authority within Internal Audit function.

The Information systems audit will evaluates the adequacy of the security controls and informs the management with suitable conclusions and recommendations. IS audit is an independent subset of the normal audit exercise. Information systems audit is an ongoing process of evaluating controls; suggesting security measures for the purpose of safeguarding assets/resources, maintaining data integrity, improve system effectiveness and system efficiency for the purpose of attaining organization goals.

The objective of the IS Audit is to provide an insight on the effectiveness of controls that are in place to ensure confidentiality, integrity and availability of the organization's IT infrastructure. IS Audit will identify risks and methods to mitigate risk arising out of IT infrastructure such as server architecture, local and wide area networks, physical and information security, telecommunications.

PERIODIC REVIEW

The policy will be reviewed periodically or at the time of any major change in existing IT environment affecting policy and procedures and placed to the Board for approval. This policy will remain in force until next review / revision.