INFORMATION TECHNOLOGY GOVERNANCE

GLOSEC FINANCE PRIVATE LIMITED

Document Control

Document Name:	Information Technology Governance Policy
Version:	**1**
Key Areas	Framework for the use, governance, security, and resilience of all IT systems and data in connection with the Company's financial services business.
Reviewed and Approved By:	Board of Directors

Introduction

This Information Technology and Cyber Security Policy ("Policy") is established for Glosec Finance Private Limited ("the Company"), a Base Layer Non-Banking Financial Company (NBFC).

The Policy has been approved by the Board of Directors. This Policy lays down the framework for safeguarding the Company's information assets against various risks and threats, whether internal or external, deliberate or accidental. It aims to ensure the confidentiality, integrity, and availability of information and systems.

The Policy is designed in alignment with applicable regulatory expectations, including the guidelines issued by the Reserve Bank of India, and is proportionate to the size, scale, complexity, and risk profile of a Base Layer NBFC.

Objectives

The primary objective of this Policy is to establish a structured yet proportionate framework for managing Information Technology (IT) and cyber security risks within the Company, in line with the expectations of the Reserve Bank of India for Base Layer NBFCs.

The key objectives of this Policy are as follows:

1. Protection of Information Assets

To ensure that all information assets, including customer data, financial records, and internal information, are adequately protected against unauthorized access, alteration, disclosure, or destruction.

2. Ensuring Confidentiality, Integrity, and Availability (CIA)

To maintain

- Confidentiality of sensitive information
- Integrity of data and systems and
- Availability of IT systems for business operations

3. Cyber Security and Risk Management

To implement basic yet effective cyber security practices and controls to identify, assess, monitor, and mitigate IT and cyber risks, including threats arising from internal and external sources.

4. Adoption of Cyber Hygiene Practices

To promote standard cyber hygiene measures such as:

- Secure password practices
- Regular system updates and patching
- Anti-virus and endpoint protection
- Secure handling of emails and data

5. IT Governance and Board Oversight

To ensure that the Board of Directors and Senior Management:

- Exercise oversight over IT and cyber security risks
- Approve policies and review risk posture periodically
- Ensure implementation of appropriate and proportionate controls

6. Secure Use of IT Infrastructure

To regulate and monitor the use of IT systems, networks, devices, and applications by employees and authorized users to prevent misuse and security breaches.

7. Third-Party Risk Management

To ensure that risks arising from outsourcing and third-party service providers are identified and managed through appropriate due diligence and security controls.

8. Regulatory Compliance

To ensure compliance with applicable regulatory and statutory requirements, including guidelines issued by the Reserve Bank of India, as applicable to Base Layer NBFCs.

9. Incident Prevention and Response

To establish basic mechanisms for detecting, reporting, and responding to cyber security incidents in a timely and effective manner.

10. Business Continuity and Resilience

To ensure that critical IT systems and data are protected and can be recovered in the event of disruptions, ensuring continuity of operations.

Scope and Applicability

This Information Technology and Cyber Security Policy ("Policy") covers all information assets, IT infrastructure, systems, and processes of **Glosec Finance Private Limited** ("the Company").

The scope of this Policy includes:

- All hardware, software, applications, databases, servers, networks, and communication systems owned, leased, or used by the Company
- All data and information assets, whether in physical or electronic form, including customer information, financial data, and internal records
- All IT operations, including system administration, network management, data storage, and information processing activities
- Cloud services, outsourced IT services, and third-party systems handling or storing Company data
- All locations from which IT systems are accessed, including corporate office, remote locations, and work-from-home environments

This Policy also covers all activities related to access, processing, transmission, storage, and disposal of information within the Company.

This Policy is applicable to:

- All employees (permanent, contractual, and temporary) of the Company
- Directors and members of Senior Management
- Consultants, advisors, and interns engaged by the Company
- Third-party service providers, vendors, and outsourcing partners who have access to the Company's IT systems or data
- Any other individual or entity authorized to access the Company's information assets or IT infrastructure

All users covered under this Policy are required to:

- Comply with the IT and cyber security requirements prescribed herein

- Use IT resources only for authorized and legitimate business purposes
- Safeguard access credentials and sensitive information
- Immediately report any security incidents, breaches, or suspicious activities

Non-compliance with this Policy may result in disciplinary action, termination of services, and/or legal action, as deemed appropriate by the Company.

Organizational Structure for IT Governance

Given the nature of operations, the Company is not required to implement complex IT governance structures; however, it shall ensure that responsibilities are clearly defined and risks are appropriately managed.

The framework shall ensure adequate oversight of IT systems and cyber security risks, protection of information assets and data integrity, implementation of basic cyber hygiene and security controls and alignment of IT systems with business objectives.

The IT governance structure of the Company shall broadly consist of:

Board of Directors

- Overall oversight of IT strategy, cyber security, and risk management

Senior Management

- Implementation of Board-approved IT and cyber security framework

Designated IT Function / Officer (Internal or Outsourced)

Day-to-day management of IT systems, cyber security controls, and incident handling

External Service Providers (if any)

- Managed service providers, cloud vendors, or IT support partners responsible for operational aspects under defined agreements

Roles and Responsibilities

a)	Board of Directors	The Board shall be responsible for ensuring effective IT governance and cyber security oversight. The key responsibilities include: • Approving the IT and Cyber Security Policy and any subsequent amendments • Ensuring that appropriate IT systems and security controls are in place • Overseeing cyber security risks and ensuring they are adequately managed • Ensuring allocation of adequate resources for IT infrastructure and security • Reviewing IT and cyber security posture periodically (at least annually or as required) • Ensuring compliance with regulatory guidelines issued by the Reserve Bank of India The Board may delegate operational responsibilities but shall retain overall accountability.
b)	Senior Management	Senior Management shall be responsible for implementing the IT governance framework approved by the Board. Key responsibilities include: • Implementing IT and cyber security policies, procedures, and controls • Ensuring that systems are secure, reliable, and aligned with business needs • Establishing basic risk management practices for IT and cyber security • Ensuring regular monitoring of systems,

		vulnerabilities, and threats • Putting in place appropriate access controls and user management practices • Ensuring timely reporting of IT incidents to the Board • Managing third-party IT risks, including vendor due diligence and oversight • Ensuring employee awareness on cyber security and safe IT practices
c)	Designated IT Function / Officer (Internal or Outsourced)	The Company shall designate an individual (internal staff or outsourced resource) responsible for IT operations and cyber security. Responsibilities include: • Managing IT infrastructure, systems, and applications • Implementing security controls such as antivirus, firewalls, and patch management • Monitoring system access and maintaining logs where feasible • Identifying and reporting vulnerabilities and incidents • Ensuring data backup and recovery mechanisms are in place • Coordinating with external vendors/service providers • Supporting audits and compliance requirements
d)	External Service Providers (if any)	To manage service providers, cloud vendors, or IT support partners responsible for operational aspects under defined agreements. Third-party vendors shall: • Comply with the Company's IT and cyber security requirements

		• Ensure confidentiality and protection of Company data • Implement adequate security controls as per contractual obligations • Report any security incidents impacting the Company.
e)	**Employees and Users**	All users of IT systems shall: • Use IT resources responsibly and only for authorized purposes • Maintain confidentiality of login credentials and sensitive data • Follow prescribed cyber hygiene practices • Report any suspicious activity, phishing attempts, or security incidents immediately

Access Control and User Management

The company shall ensure that access to the Company's IT systems, applications, and data is restricted to authorized users only and is based on business requirements.

a)	Access Control Principles	• Access shall be granted on a **need-to-know** and **least privilege** basis • User access shall be role-based and aligned with job responsibilities • Segregation of duties shall be maintained wherever feasible
b)	User Account Management	• Unique User IDs shall be assigned to each user • Sharing of user credentials is strictly prohibited • Default passwords must be changed upon first login • Strong password practices shall be enforced (minimum complexity and periodic change)

c)	Access Provisioning and De-provisioning	• Access shall be granted only upon proper authorization • Access rights shall be reviewed periodically (at least annually) • User access shall be revoked immediately upon: - Resignation/termination - Role change (as applicable)
d)	Privileged Access	• Administrative/privileged access shall be restricted to authorized personnel only • Such access shall be monitored and controlled
e)	Remote Access	• Remote access (including work-from-home) shall be allowed only through secure means • Appropriate safeguards such as secure networks and device protection shall be ensured

Cyber Security Controls

The Company shall implement the following baseline cyber security controls to ensure protection of its information assets, in line with the expectations of the Reserve Bank of India and proportionate to its size and risk profile.

Control Area	Key Requirements	Explanation / Purpose
a) Endpoint Security	Installation of antivirus/anti-malware software on all systems; Regular updates and patching of operating systems and applications	Ensures that end-user devices (laptops, desktops) are protected from malware, ransomware, and other cyber threats. Regular updates reduce exposure to known vulnerabilities.
b) Network Security	Use of firewall/router-level protection (where applicable); Secure configuration of Wi-Fi (password protection, encryption); Avoid use of	Protects the Company's network from unauthorized access and external attacks. Securing Wi-Fi and avoiding public networks reduces risk

	public/unsecured networks for official work	of data interception and hacking.
c) Data Protection	Protection of sensitive data from unauthorized access; Data sharing strictly on need-to-know basis; Restriction/control over use of external storage devices (USB, hard drives)	Ensures confidentiality and integrity of business and customer data. Minimizes risk of data leakage, theft, or misuse, especially through removable media.
d) Email & Phishing Security	Users to exercise caution while handling emails; Awareness on phishing and social engineering attacks; Avoid opening unknown links or attachments	Email is a primary attack vector. These controls help prevent fraud, malware infections, and credential theft through phishing or malicious emails.
e) Patch & Vulnerability Management	Regular updating of systems and software; Timely identification and fixing of known vulnerabilities	Keeps systems secure by addressing weaknesses that attackers may exploit. Regular patching is one of the most critical cyber hygiene practices.
f) Logging & Monitoring	Maintenance of basic logs of user/system activity (where feasible); Periodic review of logs for suspicious activity	Enables detection of unauthorized access or abnormal behavior. Logs act as evidence for investigation and help in early identification of security incidents.
g) Incident Management	Immediate reporting of cyber incidents; Recording and tracking of incidents; Timely resolution and escalation of significant incidents to Senior Management	Ensures quick response to cyber incidents to minimize damage. Proper reporting and escalation improve accountability and strengthen overall security posture.

Information Systems (IS) Audit

The objective of the Information Systems (IS) Audit is to evaluate the adequacy, effectiveness, and reliability of the Company's IT systems, cyber security controls, and processes. The audit aims to ensure that information assets are protected and that systems operate in a secure and efficient manner in line with the expectations of the Reserve Bank of India.

a)	**Scope of IS Audit**	The IS Audit shall cover, at a minimum: • IT infrastructure, systems, and applications • User access management and access controls • Cyber security practices and baseline controls • Data protection, backup, and recovery mechanisms • Network and endpoint security • IT operations and system maintenance practices • Third-party IT service providers and outsourced activities (if any)
b)	**Periodicity of Audit**	IS Audit shall be conducted periodically, preferably once in one to two years, based on the Company's risk profile and operational requirements Additional audits may be conducted in case of: • Significant system changes • Cyber security incidents • Introduction of new IT systems or applications
c)	**Auditor**	The IS Audit may be conducted by: • Internal auditor (if suitably qualified), or • External independent IT / IS auditor The auditor shall possess adequate knowledge and experience in information systems and cyber security.

d)	**Reporting and Review**	The audit report shall be submitted to Senior Management for review Key findings, risks, and corrective actions shall be placed before the Board of Directors Significant observations shall be tracked for closure.

Policy Review and Disclosure

a)	This Policy shall be reviewed by the Board of Directors annually to ensure its continued relevance and alignment with the regulatory framework, business environment, and the Company's strategic objectives. The Policy shall also be reviewed as and when there are any changes in the applicable laws, regulations, or guidelines issued by the Reserve Bank of India, the Ministry of Corporate Affairs, or any other statutory authority.
b)	Any amendments, modifications, or revisions to this Policy shall be subject to approval of the Board of Directors. The Board may also delegate authority to a committee or designated officials to recommend changes to the Policy.
c)	**Disclosure** This Policy shall be: • Communicated to all employees and relevant stakeholders • Made available internally through appropriate channels (such as internal systems or shared repositories) • A summary or key features of the Policy may be disclosed externally, if required, in accordance with applicable regulatory requirements. • The Company shall ensure that sensitive information contained in the Policy is not disclosed publicly.