QRG Investments and Holdings Limited

IT Governance Policy

Version 2.0

Document Control

S. No.	Type of Information	Document Data
1.	Document Title	QRG Investments and Holdings Limited IT Governance Policy
2.	Document Code	QRGIHLITGP
3.	Date of Release	October 22, 2022
4.	Document Superseded	Information Technology Policy
5.	Document Approvers	Board of Directors

Document Change Approvals

Version No	Revision Date	Nature of Change	Date Approved
1.0	NA	Initial Version	October 22, 2022
1.0	NA	No Change	October 04, 2023
2.0	February 06, 2024	As per RBI Master Directions, Nov,23.	February 06, 2024

Table of Contents

1. Introduction

The Reserve Bank of India (RBI) had issued the guidelines on Information Technology Framework for Non-Banking Finance Companies (NBFCs) in Master Direction DNBS.PPD.No.04/66.15.001/2016-17 (as and when amended) to enhance safety, security, efficiency in processes leading to benefits for NBFCs and their customers are enclosed.

NBFCs are required to formulate a Board approved IT policy, in line with the following objectives:

a) An IT organizational structure commensurate with the size, scale and nature of business activities carried out by the NBFC;
b) NBFCs may designate a senior executive as the Chief Information Officer (CIO) or in-Charge of IT operations whose responsibility is to ensure implementation of IT Policy to the operational level involving IT strategy, value delivery, risk management and IT resource management.
c) To ensure technical competence at senior/middle level management of NBFC, periodic assessment of the IT training requirements should be formulated to ensure that sufficient, competent and capable human resources are available.
d) The NBFCs which are currently not using IPv6 platform should migrate to the same as per National Telecom Policy issued by the Government of India in 2012. (As per Circular DNBS(Inf.).CC.No 309/24.01.022/2012-13 November 08, 2012)

In accordance with the above regulations Board of QRGIHL has approved this IT and Cyber Security Policy

2. IT Governance

IT Governance is an integral part of corporate governance. It involves leadership support, organizational structure and processes to ensure that the QRGIHL's IT sustains and extends business strategies and objectives. Effective IT Governance is the responsibility of the Board of Directors and Executive Management.

Well-defined roles and responsibilities of Board and Senior Management are critical, while implementing IT Governance. Clearly-defined roles enable effective project control. People, when they are aware of others' expectations from them, are able to complete work on time, within budget and to the expected level of quality. IT Governance Stakeholders include: Board of Directors, IT Strategy and Steering Committee, Business Executives, Chief Information Officer (CIO), Chief Technology Officer (CTO), and Risk Committees.

The basic principles of value delivery, IT Risk Management, IT resource management and performance management must form the basis of governance framework. IT Governance has a continuous life-cycle. It's a process in which IT strategy drives the processes, using resources necessary to execute responsibilities. Given the criticality of the IT, QRGIHL follows relevant aspects of such prudential governance standards that have found acceptability in the finance industry.

3. IT Strategy and Steering Committee

The composition of the committee is:

Shri Sunil Behari Mathur- Chairman
Shri Surender Kumar Tuteja
Shri Anil Rai Gupta
Shri Ramesh Kumar Sharma

The IT Strategy and steering Committee should meet at an appropriate frequency atleast quarterly. The Committee shall work in partnership with other Board committees and Senior Management to provide input to them. It will also carry out review and amend the IT strategies in line with the corporate strategies, Board Policy reviews, cyber security arrangements and any other matter related to IT Governance. Its deliberations may be placed before the Board.

4. Roles and Responsibilities of IT Strategy and Steering Committee

Some of the roles and responsibilities include:

- The constitution of the Information Security Committee (ISC), with Chief Information Security Officer (CISO) and other representatives from business and IT functions, etc., shall be decided by the IT Strategy and Steering Committee.
- Approving IT strategy and policy documents and ensuring that the management has put an effective strategic planning process in place;
- Ascertaining that management has implemented processes and practices that ensure that the IT delivers value to the business;
- Ensuring IT investments represent a balance of risks and benefits and that budgets are acceptable;
- Monitoring the method that management uses to determine the IT resources needed to achieve strategic goals and provide high-level direction for sourcing and use of IT resources;
- Ensuring proper balance of IT investments for sustaining the Company's growth and becoming aware about exposure towards IT risks and controls.
- For Steering Committee: Monitoring of the progress of the project, including deliverables to be realized at each phase of the project and milestones to be reached according to the project timetable.
- CISO should be a permanent invitee of IT Strategy and Steering Committee.
- The CISO shall directly report to the Executive Director or equivalent executive overseeing the risk management function.
- Ensure that the company has put an effective IT strategic planning process in place;
- Guide in preparation of IT Strategy and ensure that the IT Strategy aligns with the overall strategy of the company towards accomplishment of its business objectives;
- Satisfy itself that the IT Governance and Information Security Governance structure fosters accountability, is effective and efficient, has adequate skilled resources, well defined objectives and unambiguous responsibilities for each level in the organisation;
- Ensure that the company has put in place processes for assessing and managing IT and cybersecurity risks;

- Ensure that the budgetary allocations for the IT function (including for IT security), cyber security are commensurate with the Company IT maturity, digital depth, threat environment and industry standards and are utilized in a manner intended for meeting the stated objectives; and
- Review, at least on annual basis, the adequacy and effectiveness of the Business Continuity Planning and Disaster Recovery Management of the Company.
- 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 IT Strategy and Steering Committee and CEO periodically on the activities of IT Steering Committee.
- Execution of the IT Strategy approved by the Board;

5. Information Security Committee (ISC)

Major responsibilities of the ISC, inter alia, shall include:

- Development of information/ cyber security policies, implementation of policies, standards and procedures to ensure that all identified risks are managed within risk appetite;
- Approving and monitoring information security projects and security awareness initiatives;
- Reviewing cyber incidents, information systems audit observations, monitoring and mitigation activities; and
- Updating key activities of Information Security to IT Strategy and Steering Committee periodically.
- Assist the IT Strategy and Steering Committee in strategic IT planning, oversight of IT performance, and aligning IT activities with business needs;
- IT/ IS and their support infrastructure are functioning effectively and efficiently;
- Necessary IT risk management processes are in place and create a culture of IT risk awareness and cyber hygiene practices in the company;
- Cyber security posture of the company is robust; and
- Overall, IT contributes to productivity, effectiveness and efficiency in business operations.

6. Roles and Responsibilities of CISO

The responsibilities of Chief Information Security Officer (CISO) are listed below, but not limited to:

- Accountability for oversight of the management of Information Security including the review and approval including assisting in the implementation of QRGIHL' information security management system policies;
- Decide and approve the scope of Information Security Management System (ISMS) in consultation with IT Strategy and Steering Committee;
- Ensure that QRGIHL' processes integrate information security management systems requirements through a set of policies and procedures;
- Ensure the resources needed for ISMS are available;
- Periodically communicate the importance of ISMS and its conformance to employees;
- Monitor through periodic meetings & reviews that the intended outcomes of ISMS are achieved;
- Promote continual improvement of information security controls;

- Identify emerging trends in the industry vertical (within which the organization is currently poised), in relation to information safety and security measures;
- Point of contact to the department heads on information security implementation and non-compliances and to ensure that an effective process for implementing and maintaining the information security controls is in place;
- Ensure that the information security requirements for new information processing facilities have been identified and approved;
- Review and monitor major incident reports together with the results of any investigation carried out;
- Ensure that the policy is regularly reviewed and any recommendations to the same shall be reviewed with Information Security Committee;
- Encourage the participation of the managers, auditors, legal department, and the employees from various departments, who can contribute to compliance with information security practices;
- Coordinate any incident response procedures undertaken in response to potential information security breaches; and
- Ensure that adequate information security training is provided to various end users and Information Security Awareness programs are conducted regularly
- The CISO shall be responsible for driving cyber security strategy and ensuring compliance to the extant regulatory/ statutory requirements.
- The CISO's Office shall manage and monitor Security Operations Centre (SOC), Cyber Security Incident Management and drive related projects.
- The CISO's office shall ensure the effectiveness of the implemented information security solutions deployed.
- CISO shall place a review of cyber security risks/ arrangements/ preparedness of the Company before the Board/ IT Strategy and Steering Committee atleast on a quarterly basis.

7. Detailed IT and Cyber Security Framework

In continuation to this overall IT and Cyber Security Policy the Board has also approved various other IT and Information security related sub policies to provide a comprehensive IT and Cyber Security framework for QRGIHL.

8. Document Management

- Any amendment to this policy/ procedure or issue of any guidance or circular etc. under this policy/ procedure has to be incorporated in the policy on an ongoing basis by the Management.
- This policy will be reviewed atleast every year by Board/ Committee.
- This procedure replaces any other procedure issued earlier by the Company to the extent specifically covered here. This policy should be followed both in letter and spirit.
- The Company is committed to continuously reviewing and updating policies and procedures-based on the Company's risk assessment and incorporating any regulatory requirement as maybe required.
- Any amendment to this procedure or issue of any guidance or circular etc. under this procedure has to be approved in writing by the approving authority.

****