Nalwa Sons Investments Limited
CIN: L65993DL1970PLC146414
Corporate Office: Jindal Centre, 12, Bhikaiji Cama Place, New Delhi – 110066
Registered Office: 28, Najafgarh Road, Moti Nagar Industrial Area, New Delhi-110028
Phone No.: (011) 45021854, 45021812, Fax No. (011) 45021812
Branch Office: O.P. Jindal Marg, Hisar – 125 005 (Haryana)
E-mail: investorcare@nalwasons.com, Website: www.nalwasons.com

IT Governance Framework

Document Control Sheet	
Document Name	IT Governance Framework
Name of Company	Nalwa Sons Investments Limited
Policy Authorization by	Board of Directors
Review of the policy	annual
Board Approval date	November 30, 2023

NSIL has established this IT Governance Framework in accordance with the Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices issued by the Reserve Bank of India vide notification no. RBI/2023-24/107 DoS.CO.CSITEG/SEC.7/31.01.015/2023-24 dated November 7, 2023. This Framework sets out the principles, structure, and processes to ensure effective governance of Information Technology within the Company.

1) PURPOSE

The purpose of this IT Governance Framework and Information Security Governance framework is to establish a robust structure for managing information and IT resources in line with industry best practices, legal regulations, and the specific requirements set forth by the Reserve Bank of India (RBI) for Non-Banking Financial Companies (NBFC).

2) SCOPE

This framework and policy apply to all IT and Information Security operations, activities, personnel, and third-party service providers associated with NSIL.

3) OBJECTIVE

- Alignment of IT strategy with business goals.
- Information Security and Privacy Risk management is integrated into business processes.
- Effective and efficient use of IT resources. Compliance with applicable laws, standards, and regulatory requirements

4) IT GOVERNANCE PRINCIPLES

- Strategic Alignment: Align IT strategy with organizational goals and business processes.
- Value Delivery: Ensure that IT delivers the expected benefits against the strategy, concentrating on optimizing costs and proving the intrinsic value of IT.
- Risk Management: Recognize the applicability and significance of risks, and ensure they are adequately managed.
- Resource Management: Use IT resources, including infrastructure, applications, information, and people, responsibly and efficiently.
- Performance Measurement: Monitor the strategic implementation and delivery of IT services through a set of defined metrics.

5) INFORMATION SECURITY GOVERNANCE PRINCIPLES

- Security Policy: Establish a written information security policy that provides direction and support for security in accordance with business requirements and relevant laws and regulations.
- Organization of Information Security: Maintain a security organization structure with defined roles and responsibilities that does not have any conflict of interest.
- Asset Management: Identify, classify, and manage IT and information assets.
- Human Resource Security: Ensure that employees, contractors, and third-party users are aware of and fulfill all their information security responsibilities.
- Physical and Environmental Security: Secure physical and electronic areas, prevent unauthorized physical access, damage, and interference.
- Access Control: Limit access to information and IT assets to only those who need access to

perform their roles.

6) STANDARDS AND REGULATIONS

- Data Protection and Digital Privacy (DPDP) Act - To ensure personal data is handled with respect for privacy and security.
- COBIT - For developing, implementing, monitoring, and improving IT governance and management practices

Additionally, NSIL will strictly adhere to all rules, circulars, and guidelines released by the RBI for NBFCs.

7) RISK MANAGEMENT FRAMEWORK

NSIL shall define a risk control framework covering all areas defined under risk management areas. Then the next steps of risk management shall take place as follows:

Risk Identification:
This shall happen in multiple ways like audit, assessment, incident etc. Once the risk is identified it is documented.

Risk Assessment:
Once the risk is identified, impact assessment is conducted, and appropriate ranking is given to the risk as key/non-key. All fraud risks and any other risk which can create financial /reputational impact are categorized as key risk.

Risk Treatment:
The identified and assessed risk shall be mitigated (by applying appropriate controls), transferred (to a third party), avoided (by identifying alternatives), accepted (only if within limits).

Monitor results:

Once a decision has been made on the identified risks, the implementation is done and the same is monitored for effectiveness and maintenance of the same within the acceptable limit.

8) ROLES AND RESPONSIBILITIES

- Board of Directors: Ensure that IT and Information Security Governance aligns with business needs.

- Chief Technology Officer (CTO) / Head of IT function: It ensures that IT strategies align with business objectives, oversees technology infrastructure and security, manages IT risks and compliance, and promotes innovation while optimizing technology resources and performance.

- Chief Information Security Officer (CISO)/ Chief information Officer (CIO): It supports IT governance by providing secure networking solutions, cybersecurity tools, cloud infrastructure, and compliance management systems. It helps organizations improve risk management, ensure data protection, maintain operational efficiency, and align IT operations with business objectives and regulatory requirements

  Steering Committee:

- Assist the ITSC in strategic IT planning, oversight of IT performance, and alignment of IT activities with business needs.
- Assist in execution and monitoring of IT projects/initiatives in line with the approved IT strategy.
- Oversee implementation of IT systems, governance framework, and organisational structure supporting IT functions.
- Oversee business continuity planning, disaster recovery setup, and cyber security arrangements.
- Ensure implementation of a robust IT architecture in compliance with applicable statutory and regulatory requirements.
- Monitor IT project progress, timelines, and performance.
- Ensure compliance with applicable regulatory requirements, IT policies, and governance standards.
- Report and update the IT Strategy Committee and the Whole Time Director (WTD) periodically on the activities of the Committee.
- Any other matter related to IT governance as may be assigned from time to time

- Strategy Committee:

- To approve IT strategy, policies, and related governance documents and ensure that management has established and implemented an effective IT strategic planning process.
- To ascertain that management has implemented appropriate processes and practices to ensure that information technology delivers value to the business and supports the Company's strategic objectives.
- To ensure that IT investments represent an appropriate balance between risks and benefits and that the related budgets and expenditures are reasonable and aligned with business requirements.
- To monitor the methodology adopted by management for determining the IT resources required to achieve strategic goals and to provide high-level direction regarding the sourcing, deployment, and utilization of IT resources.
- To ensure an appropriate balance of IT investments for sustaining the Company's growth and to oversee the Company's exposure to IT risks, cyber security risks, and the adequacy of related controls.

- All Employees: Comply with all IT and information security policies, procedures, and standards.