

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

INFORMATION SYSTEM AUDIT POLICY

Document Control Sheet	
Document Name	Information System Audit Policy
Name of Company	Nalwa Sons Investments Limited
Policy Authorization by	Board of Directors
Review of the policy	Bi-annual
Board Approval date	November 30,2023

- 1) This policy may be known as "NSIL – Information System Audit Policy" hereinafter referred to as the "Information System Audit Policy".
- 2) This Policy on Information System Audit Policy has been made pursuant to Relevant Notifications and Master Direction – Reserve Bank of India (Non-Banking Financial Company –Scale Based Regulation) Directions, 2023 as amended from time to time.
- 3) The Board of Directors has approved and adopted this 'Information System Audit Policy' on 30th November, 2023.

4) **Company's Profile**

Nalwa Sons Investments Limited (NSIL) is a Non-Banking Financial Company (NBFC) registered with the Reserve Bank of India (RBI). In accordance with the Master Direction-Non-Banking Financial Company – Scale Based Regulations - (Reserve Bank) Directions, 2023 (hereinafter referred to as "the RBI Directions") issued by the RBI, the Board of Directors of an applicable NBFC is required to frame and approve an Information System Audit Policy.

5) **Objectives**

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 shall 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.

6) **Scope**

IS Audit shall cover effectiveness of policy and oversight of IT systems, evaluating adequacy of processes and internal controls, recommend corrective action to address deficiencies and follow-up. IS Audit shall also evaluate the effectiveness of business continuity planning, disaster recovery set up and ensure that BCP is effectively implemented in the organization. During the process of IS Audit, due importance shall be given to compliance of all the applicable legal and statutory requirements.

7) **Definitions**

For the purpose of this Investment Policy –

- a) "Act" means the Reserve Bank of India Act, 1934;
- b) "Board of Directors" means the Board of Directors of Nalwa Sons Investments Limited.
- c) "Body corporate" means a body corporate as defined under Section 2 of the Companies Act, 2013;
- d) "Company" or "NSIL" means Nalwa Sons Investments Limited;
- e) "Companies Act" means the Companies Act, 2013 or any statutory modifications or re-enactment thereof for the time being in force.

Other terms not defined hereinabove shall have same meaning as defined in "Master Direction – Reserve Bank of India (Non-Banking Financial Company – Scale Based Regulation) Directions, 2023" and as amended from time to time.

8) Information System Audit Process:

The information System Audit Process has defined the comprehensive approach to fulfill the need of the organisation. The details of audit approach are as follows:

Approach

The purpose of audit approach is to enable the development of a strategic work plan that is designed to best meet the organizations objectives. The approach in summary entails the following key phases:

1. Audit Plan Development
2. Research and Programme Development
3. Audit Programme Delivery
4. Reporting and Monitoring
5. Follow-up Review

The audit approach has 5 steps to laying down the strong internal audit foundation. The detail of the above-mentioned graph is as follows:

Audit Plan Development - The audit plan is designed to identify and concentrate on areas of importance, to provide an effective and efficient review and seek to add value to the organization's activities. Detailed plans are prepared and updated annually. In the audit planning it is important to identify the key auditable areas followed by the plan approval and plan review and update.

In performing our Statutory Audit of Financial Statement in accordance with the applicable Standards and laws, we intend to obtain a reasonable assurance on the automated/programmed controls. Our reliance on automated/programmed controls is dependent on effectiveness of IT General Controls. Accordingly, we need to perform a review of IT General Controls.

1. Therefore, in NSIL following areas has been identified and priorities which shall be audited by the third party on a periodic basis.

- Program Development/Change involving - Test
- Version Control

2. Logical Access Controls for the identified applications involving

- Granting
- Modification - Deletion
- Password Controls
- Critical id management
- Remote Access Management
- Access Controls over Version Control software (if Version Control software is used)

3. Security Management Process involving

- Hardening of OS and Database
- Infrastructure Change management

4. Computer Operations

- Backup of data and applications - Job scheduling / monitoring of interfaces - Incident /

problem management

5. Application Controls.

Audit Programme Delivery

Specific audits will be undertaken in accordance with the agreed audit plan. The key steps and audit approach in conducting an audit are highlighted below:

Key Stages	Approach
Research Planning and information gathering	Define the objectives; Review documentation and policies and procedures; Interviews with relevant key stakeholders or undertake file work
Evaluation and Analysis	Evaluation and Analysis based on the collected information
Reporting and Strategy Development	Draft Report Issue Final Audit Report

Audit Reporting and Documentation

The third-party Audit team will report to NSIL management on a periodic basis on:

- Audits completed
- Progress in implementing Internal Audit work plans
- The status of the implementation of agreed audit recommendations.

Once the audit findings are reviewed by the management. The audit findings are further reported to the IT Strategy Committee/Board.

IT Strategy Committee

IT Strategy Committee will be set up to effective implementation of Cyber Security Policy and oversight of IT systems, evaluating adequacy of processes and internal controls, recommend corrective action to address deficiencies and follow-up. IT Strategy Committee Meeting will be scheduled on a quarterly basis.

Following are the Roles and Responsibilities of IT Strategy 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 those 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 NBFC's growth and becoming aware about exposure towards IT risks and controls.
- Ensuring that Committee should meet at an appropriate frequency but not more than six months should elapse between two meetings.

Compliance

NSIL management and IT Department is responsible for deciding the appropriate action to be taken in response to reported observations and recommendations during IS Audit. Also, Internal Audit's performance encompasses the following responsibilities:

- To ensure all work complies with internationally recognized standards
- To maximise use of resources,
- To minimise costs
- To supplement resources where necessary with professional expertise on an as required basis.