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 POLICY

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

Table of Contents

1. Background

The Information Technology Policy (IT Policy) provides an integrated set of protection measures that must be applied across Nalwa Sons Investments Limited ("Company") to ensure a secured operating environment for its business operations.

2. Scope

2.1. Scope of this IT Policy is the Information stored, communicated and processed within Company and data across outsourced service provider's locations.

2.2. This policy applies to all staffs, contractors, service providers, Interns/Trainees working in Company. Third party service providers providing hosting services or wherein data is held outside Company premises, shall also comply with this policy.

3. Objectives

The objective of the IT Policy is to provide Company, an approach to managing information risks and directives for the protection of information assets to all units, and those contracted to provide services.

4. Responsibility

4.1. The Board of Directors shall delegate the powers, responsibilities and action plans as outlined in this policy as and when required based on the business requirements and the need to manage the IT and Cyber assets in an effective manner.

4.2. The overall power to review the compliance with this policy lies with the Information Strategy Committee (ISC) which may comprise of

a. Chairperson (Independent Director)
b. Member-Executive Director/Whole Time Director
c. Member-Non Executive Director

4.3. To avoid conflict of interest, CIO shall not be a member of IT department.

4.4. All the staffs and external parties as defined in policy are responsible to ensure the confidentiality, integrity and availability of Company's information assets.

4.5. The Executive Director/Chief Executive Officer/Whole Time Director, if any, would be designated as the Chief Information Officer (CIO) and is responsible for articulating the IT Policy that Company uses to protect the information assets apart from coordinating the information security related issues within the organisation as well as relevant external agencies.

4.6. ISC shall give recommendations regarding the Information Security risk and responsible for maintenance / review of the IS Policy and also for formulating/review of all sub policies derived from IS Policy.

4.7. To avoid conflict of interest in formulation of policy and implementation / compliance the policy has to remain segregated. Therefore, the Information Strategy Committee (ISC) will be the owner of the IT Policy and Implementation responsibility shall rest with Admin/IT department of Company.

5. Periodic Policy Review

5.1. The policy shall be reviewed every two years or at the time of any major change in existing IT environment affecting policy and procedures, by ISC and placed to Board for approval.
5.2. This policy will remain in force until next review / revision.

6. Policy Approval

This policy should be reviewed and approved by Board of Director. Any exception to the policy is to be approved by CIO.

7. IT Governance

IT governance is an integral part of corporate governance of Company, and effective IT governance is the responsibility of the board of directors of Company ("Board") and its executive management.

8. IT Policy

8.1. Acceptable IT Usage

It is imperative to ensure that all the users and staff at Company are aware of their responsibilities towards the IT Resources of Company. The following guidelines shall be adhered to:

8.1.1. Company staffs have been provided with a company desktop / laptop or portable electronic device. It is the staffs' responsibility for the proper care and use of their desktop / laptop / Portable Electronic Device, data and accompanying software while using the same
8.1.2. All electronic communication should be courteous, professional and business like as they may be subject to discovery in both criminal and civil proceedings.
8.1.3. Forwarding of incorrect information or inadvertent distribution can occur more easily than with other means of communication so care needs to be taken to ensure that particularly sensitive, controversial or confidential information is not sent via the internet.
8.1.4. Intellectual property guidelines are to be observed
8.1.5. Employees must not copy, modify or transmit documents, software, information or other materials protected by copyright, trademark, patent or trade secrecy laws without authorization of the owner of such rights in such materials
8.1.6. Do not use another individual's e-mail account or login - logins and passwords should not be divulged to anyone.
8.1.7. Accessing another individual's electronic mail and other electronic media should only be done where Employees have a legitimate business need and with the knowledge and approval of that individual or the responsible partner.

8.2. Acceptable use

The following are considered as acceptable use:

8.2.1. Company's IT and electronic communication tools may be used to communicate internally with other internal people or externally with customers, suppliers and other business contacts which enhance productivity.
8.2.2. Incidental and limited personal use is permitted as long as it does not breach this policy, unreasonably interfere with the performance of the employee's job, consume significant resources, give rise to more than nominal additional costs or interfere with the activities of other Company's people.

8.3. Prohibited use

Using Company's IT and communication systems for the following is not acceptable and may invite disciplinary/legal proceedings ("Prohibited use"):

8.3.1. Creating or forwarding hoax messages or chain mail messages.
8.3.2. For Personal financial gain or profit or Gambling.
8.3.3. Soliciting others for non-business activities or in connection with political campaigns or lobbying.
8.3.4. Accessing or downloading pornographic or other offensive/repulsive material.
8.3.5. Representing an employee's personal opinion as that of the firm.
8.3.6. Transmitting material which violates any law or is damaging to the reputation of any person or legal entity.
8.3.7. The infringement of the intellectual property rights of another person or legal entity, such as copyright.
8.3.8. To reveal or publish any proprietary, classified or confidential information of Company and its associates/partners.
8.3.9. Attempting to penetrate computer network security of any legal entity or other system or unauthorized access or attempted access to another individual's computer, e-mail or voicemail accounts or equipment.
8.3.10. To carry messages or material which are defamatory, obscene, harassing, embarrassing, offensive, sexually explicit, intimidating or which seek to discriminate against or vilify any person or group such as offensive, repulsive and explicit messages, images, cartoons, jokes or innuendos.

8.4. Access Control

Data must have sufficient granularity to allow the appropriate authorised access. There is a delicate balance between protecting the data and permitting access to those who need to use the data for authorised purposes. This balance should be recognised. Key aspects in this regard to be considered are:

8.4.1. Access rights and privileges to Company's information systems and network must be allocated based on the specific requirement of a user's role / function rather than on their status.
8.4.2. The criteria used for granting access privileges must be based on the principle of "least privilege" whereby authorized users will only be granted access to

information system and network domains which are necessary for them to carry out the responsibilities of their role or function.

8.4.3. Care must be taken to ensure that access privileges granted to users do not unknowingly or unnecessarily undermine essential segregation of duties.

8.4.4. The creation of user access accounts with special privileges such as administrators must be rigorously controlled and restricted to only those users who are responsible for the management or maintenance of the information system or network.

8.4.5. When available audit logging and reporting must be enabled on all information systems and networks.

8.5. Backup & Recovery

In order to safeguard information and computing resources from various business and environmental threats, all business data and related applications shall be backed up on a scheduled basis and in a standardised manner.

The backup and recovery procedures must be automated wherever possible using the system features and be monitored regularly.

8.6. Hardware Acquisition & Maintenance

During hardware acquisition, it shall be ensured that hardware is of the required quality and helps in meeting the desired business objectives. Hardware thus procured shall be maintained and supported systematically during its lifetime to the extent possible

8.7. Social Media Usage

8.8.1. Usage of Social Media within Company's network is restricted, unless approved specifically.

8.8.2. Staffs are personally responsible for the content they publish on-line, whether in a blog, social computing site or any other form of user- generated media.

8.8.3. Staffs are not authorised to publish or discuss on Social Media Company's confidential or other proprietary information

8.8. Data Classification

8.9.1. To ensure that Confidentiality, integrity and availability of information is maintained, a data classification scheme has been designed.

8.9.2. The level of security to be provided to the information will depend directly on the classification of the data.

8.9.3. The classification of the data shall be done by Heads of Departments / General Managers for their respective departments / business functions.

9. Information and Cyber Security

9.1. Website & Application Security

It may be required to develop and maintain software, applications and add- on modules from time to time. Proper procedures, access controls and security requirements in line with the standard industry practices shall be adhered to during the entire process. Key guidelines pertaining to website and application security include:

9.1.1. It is recommended that the website is security audited and an audit clearance certificate is issued by a CERT-IN empanelled vendor before hosting in production environment. The Security Audit should be done every six months or as and when any changes are done.

9.1.2. Use site-wide SSL certificate which uses at least 2048-bit SHA 256 encryption or higher.

9.1.3. Ensure that the SSL Certificate is valid and keep track of the certificate expiry date and take necessary action to renew/replace the certificate before expiry.

9.1.4. Disable weak ciphers like DES, 3DES, RC4. Use Strong Ciphers like AES, GCM.

9.1.5. Any "non-https" requests received on the website/applications, should be forcefully redirected to "https".

9.1.6. Ensure that all Websites and Applications and their respective CMS (Content Management System), 3rd party plugins, codes, etc., are updated to the latest versions.

9.1.7. All passwords, connection strings, tokens, keys, etc., should be encrypted with salted hash.

9.1.8. There should not be any plain passwords stored in config files or source code or in database.

9.1.9. All exceptions should be handled appropriately. Custom error pages should be displayed for any errors/exceptions. At no point of time, a portion of source code should be displayed on the page in case of an error or exception.

9.1.10. Ensure that the Computer/system, from where CMS/site updates are being done is installed with the latest OS + Antivirus Updates and Patches. No unauthorized software/cracks, should be installed on the machine.

9.1.11. In case of the website/application is integrated with any 3rd party Applications or using any APIs for external communication, then ensure that all such communications are done through encrypted channel.

9.2. Password Security

The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords and the frequency of change. The following are the minimum guidelines to be adhered to with respect to password security:

9.2.1. All passwords should be reasonably complex and difficult for unauthorized people to guess, but easy to remember for user.

9.2.2. Employees are advised to choose passwords that are, preferably, at least eight

characters long and contain a combination of upper- and lower-case letters, numbers, and punctuation marks and other special characters. These requirements will be enforced with software wherever possible.

9.2.3. In addition to meeting those requirements, employees should also use common sense when choosing passwords. They must avoid basic combinations that are easy to crack. For instance, choices like "password," "password1" and "P@$$w0rd" are bad from a security perspective.

9.2.4. It is recommended that the passwords be changed regularly, preferably once in **90 days**.

9.2.5. If the security of a password is in doubt– for example, if it appears that an unauthorized person has logged in to the account — the password must be changed immediately.

9.2.6. Default passwords — such as those created for new employees when they start or those that protect new systems when they're initially set up must be changed as quickly as possible.

9.2.7. Passwords may never be shared or revealed to anyone other than the authorized user.

9.3. Network Security

9.3.1. Appropriate controls should be established to ensure security of data in private and public networks, and the protection of connected services from unauthorised access.

9.3.2. Company's Network infrastructure shall be protected from unauthorised access by deploying required firewalls and other security measures.

9.4. E-mail Security

Company shall implement effective systems and procedures to ensure that e- mails are used as an efficient mode of business communication and implement control procedures so that the e-mail facility is not misused by the users. It also needs to be ensured that e-mail service and operations remain secure, efficient while communicating within intranet as well as through the internet. Key guidelines to be adhered to include:

9.4.1. All access to electronic messages must be limited to properly authorized personnel.

9.4.2. Usage of E-mail system is limited to business needs or any helpful messages.

9.4.3. All E-Mails must be in compliance with Company's standards regarding decency and appropriate content and as laid out in para 8.1: Acceptable IT Usage.

9.5. Security Awareness

All staffs of Company and, where relevant, contractors and third-party users shall receive appropriate awareness training and regular updates in organisational policies and procedures, as relevant for their job function

9.6. Data Security Measures

9.6.1. Appropriate physical, technical and organisational security procedures that restrict access to and disclosure of personal data within Company shall be implemented.

9.6.2. Wherever possible, to prevent unauthorised physical access, damage and interference to the organization's premises and information, critical or sensitive information processing facilities shall be housed in secure area, protected by secure parameters, with appropriate entry controls.

9.6.3. Company shall deploy firewalls and other security procedures to help protect the accuracy and security of sensitive information and prevent unauthorised access or improper use.

9.7. Information Security Incident Management

Incident management is required and needs to be established to ensure a quick, effective, and orderly response to security incidents. Such a policy would vary in scope depending on the sensitivity and size of the information systems being managed. Key guidelines for incident management include:

9.7.1. Incidents are detected as soon as possible and properly reported.
9.7.2. Incidents are handled by appropriate authorized personnel with 'skilled' backup as required.
9.7.3. Incidents are properly recorded and documented.
9.7.4. All evidence is gathered, recorded, documented and maintained properly with proper backup.
9.7.5. The full extent and implications relating to an incident are understood.
9.7.6. Incidents are dealt with in a timely manner and services restored as soon as possible.
9.7.7. Analyze the incidents to learn from them to ensure similar incidents do not recur.
9.7.8. Learning from the incidents are recorded.

10. IT Operations

10.1. Physical Security

10.1.1. Company's primary data center entrance is equipped with a biometric finger print reader with a keypad and isolated key. Access to the computer room area is restricted to the technical services personnel who are responsible for operations of the equipment.
10.1.2. All access to the IT data center and other computer rooms must be authorized by IT Leadership.
10.1.3. Additional computer rooms are protected via traditional lock & key. Access is limited to facilities leadership and personnel within the Office of Information Technology.
10.1.4. The computer room access reviewed and signed by IT Leadership on an annual basis.

10.2. Environmental Security

10.2.1. Company's data center is equipped with separate air conditioning units, temperature sensors, water based fire suppression system, appropriate UPS systems and a generator.
10.2.2. Periodic maintenance and tests are performed and recorded to ensure these units are functioning normally.

10.3. Media Protection

10.3.1. Backup tapes should be securely stored in a separate building which are backed up.
10.3.2. Backup tapes are rotated and stored off-site in a secure safety deposit box. User access is initiated by the Office of Information Technology in conjunction with designated safety deposit box authorized officials.
10.3.3. Access to tape backups should be restricted to personnel within the Office of Information Technology.

11. Information Systems Audit

11.1. Information Systems Audit is a managerial, technical and organisational process to ensure proper utilization of Information Technology and systems to strategically align with the overall mission and goal of organisation.
11.2. Audits shall be conducted to ensure compliance with the information security policies, procedures and guidelines
11.3. The use of information systems audit tools shall be controlled and authorised to prevent any possible misuse of tools.

12. Business Continuity Planning

12.1.1. BCP forms a significant part of any organisation's overall Business Continuity Management plan, which includes policies, standards and procedures to ensure continuity, resumption and recovery of critical business processes.
12.1.2. BCP at Company is also designed to minimise the operational, financial, legal, reputational and other material consequences arising from a disaster.
12.1.3. Company requires its service providers to develop and establish a robust framework for documenting, maintaining and testing business continuity and recovery procedures. Company ensures that the service provider periodically tests the Business Continuity and Recovery Plan and occasionally conducts joint testing and recovery exercises with its service provider
12.1.4. In order to mitigate the risk of unexpected termination of the outsourcing agreement or liquidation of the service provider, Company retains an appropriate level of control over their outsourcing and the right to intervene with appropriate measures to continue its business operations in such cases without incurring prohibitive expenses and without any break in the operations of Company and its services to the customers.
12.1.5. Company ensures that service providers are able to isolate Company's information, documents and records and other assets. In appropriate situations, Company can remove, all its assets, documents, records of transactions and information given to the service provider, from the possession of the service provider in order to continue its business operations, or delete, destroy or render the same unusable.
12.1.6. Company also has in place necessary backup arrangement.
12.1.7. These shall be tested on a regular basis.

13. IT Services Outsourcing

13.1. Outsourced Infrastructure services shall be provided by strategic outsourced partners with Service Level agreements.
13.2. The service providers are custodians of IT assets on behalf of Company and are responsible for the implementation and operation of the infrastructure as appropriate to meet the Confidentiality, Integrity and Availability ratings specified by Company.
13.3. Develop Standard Operating Procedures (SOP's), Security Guidelines for the assets managed.
13.4. Manage IT assets as per Company approved policies and procedures.

14. Compliance

14.1. Compliance with Regulatory requirements

14.1.1. Compliance to statutory, regulatory and contractual requirements such as Information Technology Framework for the NBFC Sector, 2017, directives and recommendations given by Reserve bank of India shall be ensured
14.1.2. Compliance with terms/conditions and license requirements for the usage of copyrighted software or any other proprietary information/material shall be maintained
14.1.3. Cross border movement of data shall be in accordance with legal and regulatory requirements
14.1.4. Records shall be retained and managed based on legal and regulatory requirements

14.2. Compliance with Information Security policy & procedures

14.2.1. Information processing facilities shall be used as per information security policy and acceptable usage policy
14.2.2. While Company respects the privacy of its staffs it reserves the right to audit and/or monitor the activities of its staffs and information stored, processed, transmitted or handled on any assets/devices/services used by staff
14.2.3. Exception to security policy and procedure shall be approved through the exception management process
14.2.4. Policy exceptions shall be reviewed at least annually and as deemed necessary based on security risks envisaged, emerging threats etc.
14.2.5. Violations or any attempted violations of security policies and procedures shall result in disciplinary/legal actions