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-110015
Branch Office: O.P. Jindal Marg, Hisar-125005, Haryana
T: +91 11 45021854, 45021812 E: investorcare@nalwasons.com
Website: www.nalwasons.com

CYBER SECURITY POLICY

(Approved by the Board of Directors on May 30, 2023)

At Nalwa Sons Investments Limited(hereinafter referred to as "NSIL" or the "Company") Information is our most valuable asset and protecting this is mission-critical for our business operations.

Management at NSIL demonstrates strong commitment towards cybersecurity. It strives to continuously review and provide the necessary means to strengthen the cyber security posture and safeguard Company assets.

Cyber Security Scope:

The policy applies to all businesses operations at NSIL including information and business assets hosted across all geographies. This is applicable to employees, consultants, contractors, associates, suppliers / third-party personnel having access to Company's information assets.

Cyber Security Policy Statement:

NSIL will

- Consistently thrive to upgrade technology, systems and processes to be ahead of the curve from cyber security perspective.
- Continuously protect internal information and information related to suppliers, customers, business partners and other stakeholders from unauthorized access, disclosure and/or modification.
- Ensure that all Business Heads / Department Heads are directly responsible for ensuring compliance with Company's Information security policy in their respective business domains.
- Ensure compliance with applicable regulatory, and legal requirements and information security management system.
- Apply effective risk management framework to identify and treat current and emerging risks to Company's business with potential to disrupt operations and/or brand reputation.
- Ensure that information is protected against known and future cyber security threats by designing, implementing, and continually improving security controls.
- Shall periodically review the effectiveness of the cyber security controls deployed and take corrective and preventative actions to improve the posture.