NAVA LIMITED
(Formerly Nava Bharat Ventures Ltd.)

Cyber Security and Data Privacy Policy

We, at Nava Limited **("Nava")** recognizes the importance of cyber security and data privacy in ensuring sustainable growth and business continuity across the organization. Information systems and data resources of Nava are critically important assets for its business operations and effective customer services.

Nava is committed in establishing and improving cyber security preparedness and minimizing its exposure to associated risks to safeguard Nava assets. All Nava businesses and functions implement adequate security policies, processes, and controls to protect confidentiality, maintain integrity, and ensure availability of all information assets.

This policy requires all Businesses under Nava:

- to comply with the applicable national and international cyber security standards.
- for implementation of control and monitoring measures for all hardware and software assets in use throughout the organization
- for implementation of management protocols for protection and security of stakeholders' assets
- in identifying the risks to information and cyber systems and also in mitigating the same to an acceptable level through a formal documented process
- to ensure that the critical information is protected from unauthorized access, use, disclosure, modification, and disposal, whether intentional or unintentional
- to ensure the confidentiality, integrity and availability of such information acquired permanently or in transit, provided or created
- to conduct regular cyber-security audits following appropriate national and international standards to maintain compliance
- to establish clear-cut reporting channels for any form of violation of the Cyber Security and Data Privacy policies and any other specific information security and management policy as the case may be.
- to protect Nava stakeholders, information and assets from threats that could potentially disrupt business and Nava's brand and reputation
- to communicate the importance of cyber security and to continually enhance information security capabilities to all the concerned
- to collaborate with cyber security and data privacy experts to continually upgrade the information management infrastructure
- To ensure compliance with this policy by all the Business Heads/Department Heads in their respective business domains
- To report periodically all breaches of information security, actual or suspected, and thereafter the same be investigated by the designated personnel and to take appropriate corrective and preventive actions

This policy applies to all stakeholders who access Nava's information or networks: Full Time Employees (FTE), Off-roll employees, including but not limited to subsidiary staff, contractors, consultants, temporary staff affiliated with third parties, including system vendors and staff from outsourcing companies.

This policy also applies to all information, computer, and data communication systems owned, licensed, and administered by Nava or its service providers and covers manifestations of other Nava information such as voice and data.

The content and robustness of implementation of this policy will be reviewed periodically and revised accordingly, as needed.