Cyber Security Policy

Adani Green Energy Limited

(Document Classification: Public)

1. Introduction

Adani Green Energy Limited (AGEL) recognizes that it's Information and cyber assets are fundamentally essential for its business operations and effective customer service.

The realization of AGEL business goals depends on the ability to safeguard its' information and Cyber assets by ensuring their confidentiality, integrity, and availability at all times.

Accordingly, AGEL is committed to establishing and improving its' cyber security posture and minimizing its exposure to cyber risk. AGEL business units and functions shall implement adequate security policies, processes, and controls to protect confidentiality, maintain integrity, and ensure availability of all information and cyber assets.

2. Objectives

The objectives of this policy are to:

- Ensure information and cyber systems are available to authorized users as per business needs and are used effectively to promote AGEL's mission.
- Protect stakeholders, information, and cyber assets from cyber risks that could potentially disrupt business operations, brand value, and reputation.
- Apply effective risk management to identify and treat current and expected cyber risks attached to its business.
- Apply efficient business continuity and disaster recovery management controls.
- Ensure compliance with all applicable regulatory and other legal requirements.
- Empower employees through ongoing training and development programs.
- Comply with applicable cyber security standards.
- To achieve these objectives, AGEL shall establish a management framework that initiates, implements, and controls cyber security operations.

3. Scope & applicability

The policy is applicable to all AGEL employees, vendors, service providers, third party consultants, associates, and business partners. This policy covers all information, computer, communication systems, and cyber systems owned/ licensed by AGEL or its service providers.

4. Policy Statement:

It is the policy of AGEL that:

- Risks to information and cyber systems shall be identified and mitigated to an acceptable level through a formal, documented procedure.
- Critical information shall be protected from unauthorized access, use, disclosure, modification, or disposal, whether intentional or unintentional.
- Confidentiality, integrity, and availability of critical information shall be ensured during processing, transmission, and at rest.
- All breaches of cyber security, actual or suspected, shall be reported and investigated by designated personnel, and appropriate corrective and preventive actions initiated.
- Awareness programs on cyber security shall be made available to all employees and, wherever applicable, to third parties such as subcontractors, consultants, and vendors.
- Business Continuity Plans shall be maintained and tested for business-critical information and cyber assets.
- All applicable audits, legal, statutory, regulatory, and contractual cyber security requirements shall be complied.
- Information security requirements shall be established and enforced for third parties, including suppliers, to safeguard data and systems.
- Robust systems shall be established and maintained for monitoring, detecting, and responding to information security threats in alignment with risk management frameworks and critical infrastructure needs.
- Information security systems shall go through continual improvement to ensure the integrity and protection of data across all operations.

5. Policy Compliance

- All employees are responsible for understanding and complying with this Cyber Security Policy.
- Business Heads and Department Heads are accountable for ensuring compliance within their respective areas of responsibility.
- AGEL Management reserves the right to take disciplinary action in the event of any policy violation.

6. Review

This policy has been approved by the Board of Directors and shall be reviewed periodically to check for its effectiveness, changes in technology, and changes in Risk Levels that may have impact on Confidentiality, Integrity and Availability, legal and contractual requirements, and business efficiency.

---------- END OF DOCUMENT----------