adani

Ports and Logistics

Adani Cyber Security Policy

Statement of Applicability

Objective:

Information systems and data of Adani are fundamentally essential for its business operations and effective customer services. Business units and functions shall implement adequate security policies, processes, and controls to protect confidentiality, maintain integrity, and ensure availability of all information assets.

Adani Group is committed to establishing and improving cyber security posture and minimizing its exposure to risks to safeguard Adani assets that shall:

- Consistently meet and exceed expectations of stakeholders and customers.
- Empower Adani employees through training and development.
- Comply with the applicable international cyber security standards.
- Apply effective risk management to identify and treat current and expected risks attached to Adani business.
- Protect Adani stakeholders, information and assets from threats that could potentially disrupt business and Adani brand and reputation.
- Apply efficient business continuity and disaster recovery management controls.
- Ensure compliance with all applicable regulatory and other legal requirements to protect the Company's financial health and to preserve Adani's brand image and reputation.

adani

Ports and Logistics

Scope:

This policy applies to all stakeholders mentioned below who access Adani Group'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 Adani Group or its service providers and covers manifestations of other Adani Group's information such as voice and data.

Policy:

It is the Policy of the Organization to ensure that:

a) Risks to information and cyber systems are identified & mitigated to the acceptable level through a formal documented procedure.

b) Critical information is protected from unauthorized access, use, disclosure, modification, and disposal, whether intentional or unintentional.

c) The confidentiality, integrity and availability of such information acquired permanently or in transit, provided or created are always ensured.

d) All Business Heads/Department Heads are directly responsible for ensuring compliance with our information security policy in their respective business domains.

e) All breaches of information security, actual or suspected, are reported, investigated by the designated personnel and appropriate corrective and preventive actions initiated.

f) Awareness programs on Information Security are available to all employees and wherever applicable to third parties e.g., Sub-contractors, consultants, vendors etc. and regular training is imparted to them.

g) Business Continuity Plan shall be maintained and tested for business-critical information assets.

h) All audit, legal, statutory, regulatory, and contractual requirements about information security are met wherever applicable.

i) The policy will 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.

It is the responsibility of all employees to understand and adhere to the Information Security Policy. The Management reserves all rights to take disciplinary action in case of its violation.

Changes:

Any changes/modifications in this policy can be done with the approval of business leadership.