Information and Cyber Security Policy

1. Introduction

Adani technology landscape is ever-growing owing to our increasing footprint across multiple industries. Information and technology assets are one of the most valuable assets for any modern organization to run its business operations, enable innovation and maintain competitive advantage in the market. These assets gain further importance in the critical business sector of the economy for Adani Power.

As we move towards the digitization of our businesses and operations, it is essential to protect our ecosystem to minimize intrusions and cyber-attacks.

This document sets out the management policy and guidance for information and cyber security of Adani Power's information and technology assets.

2. Scope and Applicability

This policy applies to all stakeholders mentioned below who access the Adani Power's information or networks:

- Full time employees.
- Off-roll employees and interns.
- Subsidiary staff, contractors, consultants, temporary staff affiliated with third parties, including system vendors and staff from outsourcing companies.

3. Objectives

The objective of this policy is to define the baseline requirements to establish and maintain a healthy cyber security posture, by minimizing the exposure of Adani Power's assets, protecting Adani Power's information from unauthorized access, loss, and leakage, and promoting cyber safe practices among employees.

4. Policy

Adani Power is committed to providing a secure, reliable, and resilient environment to safeguard critical infrastructure, & information of employees, businesses, partners, and customers through a well-defined Cyber security framework aligning to international standards.

Adani Power resolves to implement and maintain Cyber Security best practices and controls to protect critical infrastructure and information assets by ensuring confidentiality, integrity, and availability (CIA) as per international standards like ISO-27001:2022.

All the Adani Power's Information and Technology assets must conform cyber security policies, and procedures as broadly outlined below:

a) Policy Framework

The cyber security team shall formulate policies for the information and cyber security of the organization. Roles and responsibilities of all the stakeholders shall be defined and allocated according to the organization needs. Segregation of duties shall be implemented in the conflicting areas of responsibility. Additionally, Standard Operating Procedures (SOPs) shall be formulated for cyber security operations and communicated to the respective stakeholders.

b) Protection of Information Assets

All information assets of Adani Power (including but not limited to hardware, software, and information in electronic and other forms) shall be protected to ensure confidentiality, integrity, and availability (CIA). Inventory of all information assets shall be maintained and updated in case of changes. All Intellectual Property assets of the Adani Power shall also be protected using IP Protection mechanisms like Copyright and Patents.

c) Protection of Critical Infrastructure Assets

All technology assets (including the operations technology assets being used across various business units) shall be protected to ensure control, availability, integrity, and confidentiality (CAIC). Inventory of all technology assets shall be maintained and updated in case of changes.

d) Protection of Customer Data

Unless any specific requirements have been documented and/ or contracted by a customer, all customer information assets shall be handled following the applicable Adani Power cyber security policies and processes. Any Personally Identifiable Information (PII) shall be collected and processed in accordance with the applicable laws and regulations and privacy shall be managed throughout the entire PII lifecycle.

e) Regulatory Compliance

All information and technology assets shall be used for business operations in compliance with the prevalent laws of the land and the guidelines issues by various regulatory agencies. The cyber security team shall maintain contact with relevant authorities and special interest groups/forums to remain apprised of the changes in the external cyber security landscape. While using third-party/supplier products and services, protection of Third-party Intellectual Property Rights shall be ensured in accordance with the prevalent laws and the supplier agreements.

f) External Engagements and Threat Intelligence

The cyber security team shall maintain contact with relevant authorities and special interest groups/forums to collect threat intelligence and get information regarding the changes in the external cyber security landscape.

g) Acceptable Usage Policy

All information and technology assets shall be used in accordance with the acceptable usage policy defined by the organization. Users of Adani Power information systems shall respect the rights of other users, protect the confidentiality and integrity of the systems and associate physical resources, and adhere to prevalent laws and regulations.

h) Cyber Security in Project Management

Cyber security requirements shall be incorporated in all new Information Technology (IT) and Technology projects. All such project plans shall be reviewed to ensure the incorporation of appropriate cyber security controls in the design stage.

i) Business Continuity and Information Backup

Business continuity planning shall be done for all critical information and technology assets and the plan implemented to ensure continuity of operations in case of any adverse event. Provisions of information security shall be built into the business continuity plans.

j) Ownership of Information

All information residing on the Information and Technology assets of Adani Power, which has not been identified as the property of other parties, shall be considered as the property of Adani Power.

k) Information Classification, Labelling and Secure Transfer

All information residing on the Information and Technology assets of Adani Power shall be classified and labelled by the respective data owners. All information that is not classified (regardless of ownership) shall be considered Internal unless Adani Power has released it as public information. Information transfer with other parties shall be done in a secure manner.

l) Identity and Access Management (IDAM)

The complete lifecycle of the identities created in the information systems shall be managed to ensure cyber security of these identities. Access to information and technology assets shall be controlled based on the business and cyber security requirements. The access rights provisioned for the identities shall be managed during the entire identity lifecycle.

m) Authentication, Authorization and Accounting (AAA)

Only authorized personnel shall be allowed to access the organization's information and technology assets. Authentication shall be implemented for all kinds of access to these assets. All access actions performed on critical information and technology assets shall be monitored and reviewed periodically.

n) Use of Personally Owned Information Assets

In cases where an employee or partner uses a personally owned device to generate, transmit, receive, store, process or otherwise interface with the Adani Power's information and technology assets, the personal computing device profile and the information contained therein must conform to all applicable Adani cyber security policies and processes.

o) Cyber Risk Management and Governance

Cyber risk management shall be performed for all projects and regular operations. The identified risks shall be mitigated by applying appropriate controls.

p) Information Security in Supply Chain and Supplier Relationships

Cyber security requirements shall be incorporated into the supplier agreements based on the type of supplier relationship. Cyber security risks associated with the supply chain shall also be addressed in the technical requirements and supplier agreements. The supplier services shall be monitored and reviewed to manage the cyber security practices and service delivery of the supplier.

q) Cloud Services Security

Cyber security requirements shall be incorporated and managed during the acquisition, use, management and exit from cloud services.

r) Cyber Security Incident Management

Cyber security incidents shall be managed according to a formalized process to minimize risk to the organizations' assets, processes, and reputation. The evidence related to incidents shall be collected and preserved as per the prevalent laws and regulations. Knowledge gained from cyber security incidents shall be used to strengthen and improve the cyber security controls.

s) Cyber Security Audit

An independent review of the cyber security implementation in the critical IT and OT systems in the organization shall be conducted on an annual basis.

t) Physical Security of Information and Technology Assets

All the information and technology assets of the organization shall be protected from physical and environmental threats. Critical information and technology assets shall be installed in secure areas and access control shall be implemented to restrict physical access to these assets. Secure areas shall be monitored for unauthorized physical access.
Employees and partners shall return the organization's assets in their possession upon change or completion of their employment or service agreement. The disposal of information and technology assets shall be done in a secure manner at the end of their life cycle.

u) Cyber Security in HR Hiring Process

All new hires shall be subject to background screening. Requirement of non-disclosure of organization's information shall be incorporated in employment agreements. These requirements shall include the responsibilities which shall continue to remain valid after termination or change of employment.

v) Cyber Security Training and Awareness

Adani Power is committed to continually improve its cyber security management system and shall communicate this policy to all employees and ensure that they are given appropriate training to raise awareness on cyber security.

w) User Monitoring and Privacy

All actions occurring on or over Adani Power's information assets may be monitored without notice for their security and other business requirements.

x) Incident Reporting

It shall be the responsibility of all employees and partners to report any incident or event that has the potential to negatively impact the cybersecurity posture of Adani Power, as per the reporting process defined by the organization.

y) Disciplinary Process

Violation of the cyber security policies or procedures may lead to disciplinary action as per the HR policies of the Adani group up to and including, but not limited, termination of employment.

z) Technical Controls

The cyber security team and other stakeholder teams shall design, implement, and operate the relevant technical controls to secure the information and technology assets of the organization.

5. Exceptions and Limitations

Exceptions may be granted in cases where security risks are mitigated by compensating controls, and in cases where security risks are at a low, acceptable level and in compliance with minimum security requirements, not interfering with legitimate business needs.

6. Policy Non-Compliance

Non-compliance to the minimum requirements or violation shall result in the invocation of the Adani IT Consequence Management Policy governed by the HR Team. Policy non-compliances by off-roll employees shall be referred to the relevant functional/ BU head for appropriate actions as per procurement/ legal norms and rules to be taken up with the concerned Vendor/partner. (Refer to the Adani IT Consequence Management Policy).

7. Review

This document shall be reviewed annually to check for its effectiveness, changes in technology, organization structure, legal & regulatory requirements and changes in risk levels that may impact Adani business environment. Document version control will only be followed in case of change/updating in its content during annual or ad-hoc review and subsequent approval will be taken accordingly. Document effective date shall be as per the document approval date.

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