ADANI ENERGY SOLUTIONS LIMITED

(formerly known as Adani Transmission Limited)

INFORMATION SECURITY POLICY

Document Title	INFORMATION SECURITY POLICY
Document Type	Policy, ~~Manual, Report~~
URL/Location	https://www.adanienergysolutions.com/-/media/Project/Transmission/Investor/documents/Policies/Information-and-Security-Policy.pdf
Language in which the document is written	English
Relevant keywords to facilitate search and classification	• Information Security • IT assets • Information systems • Business processes • Confidentiality • Integrity • Availability • Threats • Accidental threats • Deliberate threats • Regulatory compliance • Risk management • Security controls • Cybersecurity • Data protection • Third-party security • Acceptable usage • Policy implementation • Compliance

1. Introduction

The dominance of Information Technology (IT) in the day to day functioning of Adani Energy Solutions Limited (AESL) has brought to the fore the growing importance of IT in its Corporate Governance. Access to, confidence in, and reliability of information is integral to business processes and critical to the success of the AESL objectives. It is therefore essential for the continued successful operation of AESL that the availability, integrity and confidentiality of its information systems and associated data are maintained, in a cost effective manner and at a level that is appropriate to its business. The need for such protection arises because information systems are potentially vulnerable to two main categories of unwanted events, or threats. These are accidental threats (human error/equipment failure/ natural hazards) and deliberate or malicious threats (fraud/sabotage/vandalism/theft). There is also the threat of legal action if information systems are misused, which AESL and its employees must be aware of.

Documented policies and procedures help in defining the processes, roles and structure and the path for attaining industry standard maturity levels in the use of IT. Implementation of policies will result in a strong and effective management of Information Security processes and controls over time. The Security Policy is aimed at enhancement of its ability to transmit, collect, store and process information electronically and to assure the confidentiality, integrity and availability of the information systems at all times.

2. Policy Objectives

There are five main policy objectives:

- To ensure information and information systems are available to authorized users within and outside AESL as per the business needs and used in an effective manner to promote AESL's mission.
- To ensure that all the information assets including data, intellectual property, computer systems, and IT equipment are adequately and consistently protected from damage, inappropriate alteration, loss, and unauthorized use or access. The level of protection must be commensurate to the level of information services required by the AESL to conduct its business.
- To meet all regulatory and statutory requirements pertaining to information collection, storage, processing, transmittal and disclosure that are applicable to the AESL.
- To create a level of awareness on information security as part of the day to day operations of the AESL group and to ensure that all employees understand their responsibilities for maintaining information security.
- To establish detailed information security standards and procedures based on this policy and ensure compliance against such standards and procedures.

3. Policy Scope

This security policy applies to all IT assets, information systems, business processes supported by IT and personnel across AESL. Personnel constitute AESL's employees, trainees, contractors, consultants, auditors and third parties who access information using information systems deployed by AESL. The policies are applicable for all offices and locations of AESL, and any new entities that may be added to the AESL from time to time.

4. Policy Statement

The company shall:

- → Safeguard internal and external information from unauthorised access, disclosure, modification, or destruction, ensuring confidentiality, integrity, and availability throughout its lifecycle.
- → Adhere to applicable laws, regulations, and standards including the Information Technology Act and other statutory requirements relevant to cybersecurity and data protection.
- → Identify, assess, and mitigate current and emerging information security risks that may impact operations, reputation, or stakeholder trust.
- → Design, implement, and periodically review security controls to address evolving threats and vulnerabilities. Adani Energy Solutions shall strive to remain ahead of the curve in technology, systems and processes ensuring confidentiality, integrity and protection of the data.
- → Maintain active surveillance of cybersecurity risks and respond promptly to incidents. The company shall ensure transparency with affected stakeholders and document mitigation actions.
- → Require suppliers, contractors, and other third parties to comply with the company's information security standards. Contracts and engagements shall include clauses to protect shared infrastructure and data.
- → Align its IT strategy with business goals, ensuring high availability, cost efficiency, and seamless service delivery. Invest in structured systems design and continuous training of the concerned IT professionals.

5. Acceptable Usage

IT assets are provided for business purposes and authorized users shall adhere to safe usage practices that do not disrupt business or bring disrepute to the AESL. Acceptable usage standards shall be defined and communicated to all users and should contain detailed guidelines for the protection information and IT assets. Acceptable Usage standard shall cover requirements for users and security best practices on safe usage of desktops, computer accounts, business applications, computer networks and for protection of information in physical or logical form and maintenance of Intellectual Property Rights by the users of information systems.

6. Policy implementation

The Heads of departments are responsible for implementing and enforcing the policies within their departments. All employees have the responsibility to understand and adhere to the policies.

All employees are responsible for upholding information security standards. Specific roles and responsibilities shall be defined across departments, with Business and Functional Heads accountable for compliance within their domains, as per the internal RACI matrix.

Data Steering Committee serves as the apex body guiding the strategic direction of information technology and data privacy at the company, while the Chief Information Security Officer (CISO) is responsible for managing the day-to-day operations of the company's information security and IT systems.

This policy shall be reviewed periodically to reflect changes in the threat landscape, business operations, and regulatory environment. Updates shall be approved by the Information Technology & Data Security Committee of the board of directors and communicated to all relevant stakeholders.

7. Compliance

Failure to comply with the requirements of the information security policy may result in disciplinary and or Legal actions.

The Company will only do business with organizations who fully comply with this policy, or those who are taking verifiable steps towards compliance.