ADANI TRANSMISSION LIMITED

INFORMATION SECURITY POLICY

TABLE OF CONTENTS

1. Introduction

The dominance of Information Technology (IT) in the day to day functioning of the Adani Transmission Limited (ATL) 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 ATL objectives. It is therefore essential for the continued successful operation of the ATL 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 ATL 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 ATL as per the business needs and used in an effective manner to promote ATL'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 ATL 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 ATL.

- To create a level of awareness on information security as part of the day to day operations of the ATL 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.

1.1 Policy Scope

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

1.2 Policy Statement

A security policy statement is an overall declaration of the security objectives and expectations, which will allow effective utilization of information systems for effective and efficient achievement of business goals.

3. 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 ATL. 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.

4. 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.

5. Compliance

Failure to comply with the requirements of the information security policy may result in disciplinary action.