Cyber Security Policy

Adani Total Gas Limited

(Document Classification: Public)

1 Introduction

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

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

Accordingly, ATGL is committed to establishing and improving its' cyber security posture and minimizing its exposure to cyber risk. ATGL 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 the business needs and used in an effective manner to promote ATGL's mission.
- Protect stakeholders, information and cyber assets from cyber risks that could potentially disrupt business, brand, 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 training and development
- Comply with the applicable cyber security standards

To achieve the above objectives ATGL shall establish a management framework that initiates and controls the implementation and operation of cyber security.

3 Scope & applicability

The policy is applicable to all ATGL 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 ATGL or its service providers.

4 Policy Statement:

It is the policy of ATGL that:

- Risks to information and cyber systems shall be identified & mitigated to the acceptable level through a formal documented procedure.
- Critical information shall be protected from unauthorized access, use, disclosure, modification, and disposal, whether intentional or unintentional.
- Confidentiality, integrity, and availability of critical information shall be ensured during processing, transit and at rest.
- All breaches of cyber security, actual or suspected, shall be reported, investigated by the 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 e.g., Sub-contractors, consultants, vendors etc.
- Business Continuity Plan shall be maintained and tested for business-critical information and Cyber assets.
- All applicable audit, legal, statutory, regulatory, and contractual requirements about Cyber security shall be complied.

5 Policy Compliance

- It is the responsibility of all employees to understand and adhere to the Cyber Security Policy of the organization.
- All Business Heads/Department Heads shall be directly responsible for ensuring compliance with cyber security policy in their respective business domains
- ATGL Management reserves all rights to take disciplinary action in case of its violation.

6 Review

This 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.

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