Policy on Information Security

Table of Contents

1 Policy Statement

GGL recognizes the need for its investors, employees, and visitors to have access to the information they require in order to carry out their work and recognizes the role of information security in enabling this.

We manage GGL records and information that are in electronic form within a secure environment, which is designed to safeguard the confidentiality, integrity and availability of proprietary, personal and commercially sensitive information and protect it against loss or misuse. We will maintain information, records and other data that lies in electronic form in accordance with applicable legal, statuary, regulatory and auditing requirements.

2 Policy Rationale

The purpose of this policy is to ensure management commitment towards information security and the ISMS. The top management is responsible for ensuring periodic reviews of ISMS and improvements based on the results of the reviews. Information is a key asset which supports delivery of our business goals and helps maintain our competitive advantage. Its efficient management, use and retention within a securely designed environment enables us to comply with applicable legal, tax, regulatory and auditing requirements, assures the information's integrity, and protects it against loss or misuse.

Misuse or unauthorized disclosure of proprietary, personal and commercially sensitive information can have severe consequences for GGL and its employees. All personnel have a duty to prevent the loss, misuse or unauthorized disclosure of the GGL's records and information. This Policy specifically supports the business principles (Refer GGL Policies – Business Principles).

3 Applicability

This policy is directed towards the management of Gujarat Gas Ltd and covers only electronic information that is created, processed, stored and transmitted across GGL IT Systems.

Top management of GGL is responsible for supporting Information security initiatives by ensuring adequate resources and periodically reviewing the effectiveness of the security measures. Every stakeholder i.e. employees at all levels & onsite contract employees must follow this Policy. Contractors and consultants are required to act consistently with this policy when working for GGL as our agent, on our behalf or in our name on any business activity including when delivering outsourced services. Breach of this Policy may result in disciplinary action up to and including dismissal. Contracted personnel who fail to comply with this Policy may have their contract terminated, not renewed, or be subjected to other

appropriate action. GGL reserves the right to amend or update this Policy as required from time to time.

4 ISO 27001 Clauses Addressed

- A.5.1.1 – Information Security Policy Document
- A.5.1.2 – Review of the Information Security Policy

5 Policy Implementation

5.1 GGL Information Security Vision

Create a committed culture towards information protection and align Information Technology and Security activities with Gujarat Gas business processes in order to achieve the organizational vision.

Information Security Policy

"The GGL's Information Security policy is an explicit commitment to delivering high standards in information security management and it is integral to our approach for delivering superior business performance in all the ways we do. This policy supports our commitment to the safety and well-being of our personnel and the security of our operations and assets. Information Security is the responsibility of each one of us, and we must all actively share in making this policy work."

In implementing this Information Security Policy, management of GGL will:

- Identify and periodically assess the Information security threats arising from its business operations.
- Develop and maintain an effective Information Security Management system.
- Safeguard the accuracy and completeness of information assets and processing methods including all company's physical assets, personnel, corporate image, proprietary information, and key business processes, from all forms of harm.
- Consider information security at all stages of planning.
- Mitigate or minimize identified risks by the use of proactive and cost-effective measures and procedure, provide data protection and ensure that all third parties collecting, storing, and processing personal information on behalf of the Company provide adequate data protection.
- Encourage a positive commitment to information security by all levels of management by providing sufficient resources commensurate with the assessed risks.
- Conduct information security operations in full compliance with the statement of business principles, IT acts / regulations, contractual obligations and

international standards and where practical improve on the performance standards they may specify.

- Produce response, contingency and business plans to cover all foreseeable events to minimize the impact of any incident or emergency, and test and train personnel in their effective and efficient implementation.
- Record, analyze and investigate all reported Information & Cyber security incidents and irregularities and develop improvements to prevent their re-occurrence.
- Introduce and maintain active programs to develop information security awareness and responsibility among all employees and contract onsite employees.
- Ensure compliance with the information security policy through a process of education, review and audit.
- Develop policies, procedures, guidelines and provide awareness to users for implementation of this Information Security Policy.

6. Policy Review

In case the Policy is required to be amended due to any change in the regulatory requirement or due to any other reasons, the Policy shall be appropriately modified with the approval of the Managing Director of the Company.

7. Dissemination of Policy

This policy will be uploaded on the website of the company and internally shared with all the relevant stakeholders.