LIQUEFIED NATURAL GAS LIMITED

Information Management and Security Policy

27 March 2015

Liquefied Natural Gas Limited

Information Management and Security Policy

This policy is a key part of Liquefied Natural Gas Limited's ("LNGL" or the "Company") strategy and reflects the Company's values and expected behaviors contained in our Business Principles.

Everyone who works for and with LNGL - employee, contractor, partner or supplier ("Workforce") - has responsibility for adhering to our Business Principles and, thus, this Policy. Read this Policy in conjunction with LNGL's Business Principles, other policies and related guidance, which establish governance of the Company.

1. Information Management and Security Policy

Information (both physical and computer-based) represents a key asset supporting sustainable business delivery. We manage LNGL's records and information within a secure environment designed to safeguard the confidentiality and integrity of proprietary, personal, and commercially sensitive information, and to protect it against loss or misuse. We maintain all forms of information, records, and other data in accordance with applicable legal, tax, regulatory, and auditing requirements.

Company information, data and files are LNGL's property and the Workforce or other individuals shall not misuse it for personal purpose or gain.

Misuse or unauthorized disclosure of proprietary, personal and commercially sensitive information can have severe consequences for LNGL. All personnel have a duty to prevent the loss, misuse or unauthorized disclosure of LNGL's records and information.

2. Policy implementation -

In order to protect and manage information LNGL:

- Operates a security classification system defining required security levels for key information and documents;
- Retains, stores, preserves and manages information for appropriate periods based on business need and applicable legal, tax, regulatory and auditing requirements;
- Maintains a secure IT environment designed to safeguard the confidentiality and integrity of proprietary and commercially sensitive information supporting business continuity;
- Protects and maintains personal information in accordance with applicable data privacy laws and regulations;
- Protects third party confidential information in conducting ordinary course business;
- Provides adequate direction, training, and supervision so that personnel understand their obligations relating to the security of information and the proper use of IT systems;
- Permits limited personal use of IT systems, provided that such use does not interfere with individual's work related duties or LNGL activities or operations; and
- Reserves the right to monitor the usage of information and IT systems and equipment.

When working for LNGL companies, the Workforce must:

- Use information obtained from LNGL solely for legitimate business purposes;
- Create, use, store and retain LNGL records, information and other data in ways that do not threaten unauthorized disclosure or misuse of such data;
- Take appropriate steps in line with the relevant security classification system to protect LNGL and confidential third-party information in their possession against misuse or unauthorized disclosure;
- Observe security protocols relating to the use of IT systems and equipment, not share passwords, nor allow unauthorized access to IT systems;
- Respect personal information by taking appropriate care to protect the privacy of personal information relating to individuals;
- Respect third-party copyrights and therefore not copy, download, store, install or transmit copyrighted materials unlicensed to LNGL;
- Not create, copy, download, distribute or endorse any statements, images, information or sounds on LNGL systems or equipment that are, or could be deemed to be, abusive, obscene, defamatory or discriminatory, could cause offense or might otherwise bring LNGL into legal proceedings or disrepute;
- Promptly report to their line manager any:
    - Loss or suspected loss of any proprietary, personal or commercially sensitive information and/or equipment containing such information; or
    - Damage, disruption or attempted unauthorized access to any LNGL IT systems, information, document stores or libraries;
- Not connect equipment or load software onto LNGL IT systems, networks or equipment without prior Level 1 written approval (Level 1 employees per the Approving Authorities Manual); and
- Not destroy, remove, conceal, tamper with or otherwise alter any LNGL information, records or other data whenever they are aware, or have reason to suspect, that litigation or a criminal or regulatory investigation is, or may be, underway, threatened or pending.

3. Management Responsibility

The Chief Financial Officer is responsible for the implementation and maintenance of this Policy.

4. Applicability

Every employee, director or officer of every wholly owned LNGL company and in every joint venture company under LNGL control must follow this Policy. We apply this Policy in all joint operations where LNGL is the operator. When participating in joint venture companies not under LNGL control we encourage the adoption of a similar policy.

Contractors and consultants are required to act consistent with this Policy when working for LNGL companies as our agent, on our behalf or in our name on any business activity including when delivering outsourced services.

Breach of a LNGL Policy may result in disciplinary action, up to and including dismissal. LNGL reserves the right to amend or update this Policy as required from time-to-time.