PETROFAC LIMITED GROUP INFORMATION SECURITY POLICY

Vision

Deploy a contemporary, integrated and multi-faceted Information security framework to ensure Petrofac's ability to prevent, detect, respond, and recover from Information and cyber security events.

Commitment

The Petrofac Board of Directors has ultimate responsibility for Information Security. Petrofac and its business units are committed to protecting information, meeting the requirements of the policy, ensuring availability of resources, checking and acting to ensure the Information Security Management System (ISMS) is effective for the purpose

Objectives

- Establish a risk-based ISMS as the foundation to manage information and cyber security risks.
- Preserve confidentiality, integrity, and availability of Petrofac's information (digital, physical and/or other forms) and safety of assets.
- Take all necessary precautionary measures to safeguard our information in accordance with Petrofac's information classification and the information security risk to which the business is exposed.
- Take all necessary precautionary measures to safeguard our operational systems to mitigate cyber risk to which the business is exposed.
- Create an assurance framework for enabling actions for compliance to global information security and cyber security standards by way of conforming assessment of people, process, and technology.
- Continually improve our information and cyber security performance using a risk-based approach, including setting and review of realistic and achievable objectives.

To meet this commitment at a Group level, Petrofac will apply the following key guiding principles:

Principle 1: The organisation shall define a set of standards and procedures for information and cyber security, approved by management, published and communicated to staff and relevant external parties. The suitability and effectiveness of this policy and its associated standard shall be reviewed annually or as and when there is a significant change to Petrofac's security risk exposure. Any significant deviation from this policy must be formally approved by the executive management and by the Board.

The ISMS shall be founded on a risk-based process to provide direction in managing information, cyber security and safety in accordance with the organisation's desired outcome and relevant laws or regulations.

The organisation shall promote the adoption of prudent management of information and cyber security risk with due care to ensure confidentiality, integrity and availability of information and safety of assets.

Principle 2: The organisation shall establish a program based ISMS, provide sufficient resources and investments and core capabilities to control its implementation and operation.

The organisation shall clearly define the roles and responsibilities of the department and committee responsible for managing information and cyber security risk. Users are responsible for safeguarding information, complying with the information security policy and reporting information security incidents to ensure appropriate actions are taken.

Principle 3: The organisation shall implement enterprise security tools and associated capabilities, and a platform to manage information and cyber security proportionate to the risks. The tools shall have the capabilities to prevent, detect, respond and recover from information and cyber security threats.

Principle 4: The organisation shall create a culture for information and cyber security and privacy enabling user responsibility and action through an effective communication strategy.

Principle 5: The organisation shall observe and monitor compliance with legal, regulatory and contractual obligations related to information and cyber security.

Principle 6: The organization shall have well-defined procedures and a robust business continuity arrangement.

Each Petrofac business unit will:

- develop and maintain business unit and functional level relevant procedures to support effective implementation of this policy and the associated standard(s);

- promptly report all information security incidents to ensure appropriate action is taken; and
- implement this policy through their documented business management system and conduct periodic reviews to verify compliance and promote continual improvement.

Responsibility and implementation

Responsibility for compliance with this policy lies with the Group Chief Executive, the Chief Financial Officer and the business units' Chief Operating Officers and Group Managing Directors.

This policy applies to all operating companies and service lines within Petrofac Limited and all partnerships or Joint Ventures over which we have management control.

The Group Chief Information Officer will be responsible for developing, maintaining, disseminating, and measuring compliance with this policy through the group information and cyber security standards. Governance of the information security management system is achieved through a cross-functional, coordinated management structure that includes Business Units, IT, Legal, Internal Audit, Enterprise Risk, HR, Facilities, HSSEIA, Corporate Communications, Compliance, Procurement and other departments where relevant.

Tareq Kawash

Group Chief Executive