SECURITY POLICY

Published date: December 2025
ID Number: IPC-HSE-POL-0008 / 122025
Document Owner: Chief Operating Officer

Security of people, assets and data is a prerequisite for our operations and offices worldwide. It is everyone's responsibility.

1. Introduction

International Petroleum Corporation (IPC) recognises its ability to keep people, operations and information secure from malicious threats as a key factor in maintaining licences to operate and being a successful business. Understanding actual and potential security threats and evaluating the risk on a continuous basis are critical to implementing measures reflecting the relevant risk picture, and maintaining people, assets and information secure at all times.

IPC is committed to the ongoing improvement of its information security management systems and controls, ensuring they evolve to address emerging threats and business needs. This commitment is integrated into IPC's strategic and operational objectives.

2. Security Definition and Scope

Security is the protection against a malicious intent, distinguished from safety, which is the protection against accidents. A security risk is the conjunction of a threat (someone intending to harm employees or the company), a vulnerability (a weakness or gap in protective measures) and a potential consequence (causing damage or disruption).

Security comprises three areas:

- **Personnel security** – the protection against those who seek to access the company or exploit employees for unauthorised or criminal purposes. Policies and procedures are in place to reduce the risk of unauthorised access and use of Company assets.
- **Physical Security** – the protection of people and assets. Physical Security measures are designed to safeguard personnel, prevent unauthorised access to facilities, equipment and documents, and safeguard against, sabotage, damage and theft.
- **Information Security** – the protection of confidentiality, integrity and availability of data. Information security ensures that only authorised users can access the Company's network. Data protection ensure personal data is processed in accordance with applicable laws, such as the EU General Data Protection Regulation (GDPR).

3. Requirements

3.1. Implement security preparedness plans, such as for cyber security, business continuity, evacuation of premises, and traveler security.

3.2. Awareness on various security aspects is raised at all levels to build and maintain a strong security culture.

3.3. Security incidents are investigated and barriers evaluated to prevent future occurrences.

3.4. Focus on continual improvement across all security domains and conduct security analysis for new and changing activities.

3.5. Continuously strengthen information security by conducting regular internal assessments, independent third-party audits, and periodic vulnerability analyses to verify control robustness and drive ongoing improvement.

4. Responsibilities

4.1. The country General Manager is responsible for the implementation of adequate security measures, preparedness and investigations after incidents.

4.3. Line managers are responsible for reporting security vulnerabilities and ensuring mitigation measures are implemented.

4.2. Everyone should identify and understand security risks they faces, and act to reduce such risks. Be vigilant and never complacent, comply with security requirements at all times, and report incidents and concerns.

William Lundin
President and Chief Executive Officer
International Petroleum Corporation