# CORPORATE INFORMATION SECURITY POLICY

*Published date: January 2024*
*ID Number: IPC-IT-POL-0001 / 012024*
*Document Owner: Chief Operating Officer*

**We are all responsible for keeping data and assets secure to protect the Company's information systems from unnecessary risk or exposure.**

## 1. Purpose

The purpose of this policy is to establish the overall framework for the information system and IT security while maintaining an appropriate balance between people, process, and technology. This Policy applies to the Company's information systems or data involved in business processes, administration, and operations, both existing and planned.

## 2. Scope

The Company expects all authorized users to use Company data, information, IT services, cloud services and assets (together referred to as Information Systems) in a responsible and professional manner to safeguard against loss, theft, damage, corruption, unauthorized access or unavailability. Attention shall be taken by all employees to safeguard systems and data when using Company information systems so as to not adversely affect others and to avoid fraudulent use.

## 3. Requirements

3.1 The Company shall put relevant measures in place at all levels by management, to protect confidentiality, integrity and availability. The level and impact of the measures for the users will depend on the risk evaluated and the criticality of the systems to be maintained.

3.2 Only the IT provider shall approve storage spaces that will be set up and used, to ensure that regular backups can be done to safeguard loss and confidentiality maintained. Devices such as mobile phones and computers shall be kept up to date with the manufacturer, supplier or network-provided patches.

3.3 A detailed information systems security inventory including the named System owners shall be maintained.

3.4 The Company will make available cyber security and data protection awareness training for all users of the Information Systems. All users are expected to complete such training, and to comply with the secure work habits

3.5 Individuals and departments dealing with personal data must comply with the applicable data protection legislation on country or regional level.

3.6 All employees are responsible for notifying the IT provider if a device was lost or stolen or if there are suspicious emails or unusual activity in terms of data content, system messages, requests for access to systems or computers or similar. The IT provider follows an established process, as per the IPC Information System Manual, to investigate and address the matter.

3.7 The IT provider of the Company shall be responsible for maintaining the stability and availability of Company systems.

3.8 Only the company appointed individual who is responsible for IT shall make decisions on whether to adopt and use cloud-based information systems or network services. This shall be done by evaluating the risks posed by these systems and services and balancing those risks with the business needs of the organization. The COO has the overall responsibility for information security and technology.

**William Lundin**
*CEO*
*International Petroleum Corporation*