Hindustan Oil Exploration Company Limited

POLICY MEMORANDUM NO: HOEC / CSDP / 2023

DATE OF ISSUE:	01 - 01 - 2023
VALID TILL:	30 - 12 - 2025
PROPOSED BY:	IT Manager
APPROVED BY:	Managing Director, HOEC
DISTRIBUTION	**ALL EMPLOYEES**

CYBER SECURITY AND DATA PROTECTION POLICY

Oil and gas companies such as HOEC deals with proprietary data that need to be protected with utmost care. Disclosure and sharing of data need to be a controlled process.

To manage this, company currently has the following procedure:

A. Internal Data Security

- User access to the particular folder is permitted with department head mail permission.
- Only folders with access enabled can be accessed.
- Only authorized IT administrators and security personnel are allowed access to the data center, which is managed and monitored by access control systems.

B. (Internet) Cyber Security

- Internet access with Firewall and Antivirus Security enabled.
- Through firewall security, websites that request access to personal data using insecure scripts are blocked.
- Anti-Spam cloud configured to filter spam emails and restrict spoofing through emails.
- Multi-factor authentication (OTP) allows users to access email apps other than Outlook in the official systems.
- Adult and social media websites were prohibited.
- Installing security updates on a regular basis into the users' operating systems, the firewall, and the anti-virus program.

Our Company Data Protection Policy extends its commitment to treat information of employees, stakeholders and other interested parties with the utmost care and confidentiality. Human errors, hacker attacks and system malfunctions could cause great financial damage and may jeopardize our company's reputation. With this policy, we ensure that we gather, store and handle data fairly, transparently and with respect towards individual rights.

This policy refers to anyone we collaborate with or acts on our behalf and may need occasional access to data and applicable to employees, consultants, Contractors, partners and any other external entity.

To exercise data protection, we will continue to:

- Restrict and monitor access to sensitive data.
- Develop transparent data collection procedures.
- Train employees in online privacy and security measures.
- Build secure networks to protect online data from cyberattacks.
- Establish clear procedures for reporting privacy breaches or data misuse.
- Include contract clauses or communicate statements on how we handle data.
- Establish data protection practices (document shredding, secure locks, data encryption,frequent backups, access authorization etc.)

All employees are responsible for upholding measures relevant to data protection, information security measures, and cyber security according to their fields of activity and all principles described in this policy must be strictly followed. A breach of data protection guidelines will invoke disciplinary and possibly legal action.

Contact:

Please direct all questions regarding this policy to the Manager IT.