INFORMATION SECURITY POLICY

1. PURPOSE

This policy establishes Climax Energy Pvt Ltd's commitment to safeguarding information assets against unauthorized access, disclosure, modification, loss, or destruction. It is designed in line with internationally recognized best practices (including ISO/IEC 27001 principles), Sri Lankan laws, and client confidentiality requirements

2. SCOPE

Applies to:

- All employees, contractors, and third-party service providers.
- All forms of information (electronic, paper, verbal) and IT systems owned or operated by Climax Energy Pvt Ltd.

3. PRINCIPLES OF INFORMATION SECURITY

1. ***Confidentiality*** – Protect information from unauthorized disclosure.
2. ***Integrity*** – Ensure information is accurate, complete, and reliable.
3. ***Availability*** – Ensure information and systems are accessible when required for business.

4. POLICY COMMITMENTS

4.1 Access Control

- Information and systems access is restricted to authorized personnel only.
- Strong passwords, multi-factor authentication, and user account management are mandatory.

4.2 Data Classification & Handling

- Information is classified (e.g., Confidential, Internal, Public).
- Sensitive information must be encrypted during storage and transmission.

4.3 IT and Cybersecurity Measures

- Firewalls, antivirus, and intrusion detection systems must be maintained.
- Regular system updates and patches are applied.
- Remote access is controlled and monitored.

4.4 Physical Security

- Offices and server rooms must be secured against unauthorized entry.
- Paper records must be stored in locked cabinets and disposed of securely (e.g., shredding).

4.5 Third-Party Security

- Vendors and partners must comply with equivalent information security standards.
- Confidentiality agreements are required when sharing sensitive information.

4.6 Incident Reporting & Response

- All employees must report suspected security incidents immediately.
- A defined response plan ensures timely containment, investigation, and resolution.

4.7 Training & Awareness

- All staff receive training on data security, phishing, and safe handling of information.

4.8 Compliance & Monitoring

- Regular audits and risk assessments will be conducted.
- Non-compliance may result in disciplinary action or termination of contracts.

5. RESPONSIBILITIES

- ***Management***: Provide resources and enforce compliance.
- ***Employees****:* Follow this policy and report security risks.
- ***IT Department****:* Implement and monitor technical controls.

6. REVIEW

This policy will be reviewed annually or when significant changes occur in operations, laws, or technology.

Climax Energy Pvt Ltd

Uthum Perera
Director – Project and Engineering
Date: 01/9/2025

Chamal Indrajith
Director – QHSE and Sustainability
Date:01/9/2025