08035449254, 07011279339
info@geraldsenergy.com
support@geraldsenergy.com
www.geraldsenergy.com

INFORMATION & CYBERSECURITY POLICY STATEMENT

1. Policy Statement

The Management of Geralds Energy Resources Nigeria Limited, operating across fleet management, executive mobility, logistics, marine and business support services, is committed to protecting the confidentiality, integrity, and availability of the Company's physical and electronic information assets.

The Company recognizes that effective information security is essential to protecting its business operations, employees, clients, commercial interests, contractual obligations, and reputation.

2. Information Security Objectives

Geralds Energy's information security approach is designed to:

- Protect confidential business and client information.
- Prevent unauthorized access, disclosure, alteration, or loss of information.
- Maintain the availability and integrity of critical business information.
- Minimize information and cybersecurity risks.
- Support business continuity and operational resilience.
- Comply with applicable legal, regulatory, contractual, and data protection requirements.

3. Information & Cybersecurity Controls

Geralds Energy maintains appropriate controls relating to:

- Access control and user authorization.
- Password and account security.
- Confidentiality and information handling.
- Data backup and recovery.
- Protection against malware, viruses, and unauthorized access.
- Secure use of company devices and systems.
- Incident identification and reporting.
- Business continuity and contingency planning
  .

Employees and relevant third parties are expected to promptly report suspected information security incidents or breaches to Management.

4. Employee and Third-Party Responsibilities

All employees, contractors, consultants, and relevant third parties are required to comply with applicable Geralds Energy information security and confidentiality requirements.

Relevant personnel shall receive appropriate information security, cybersecurity, confidentiality, and security awareness training based on their roles and responsibilities.

5. Risk Management

Geralds Energy adopts a risk-based approach to identifying, assessing, and mitigating information and cybersecurity risks.

Management periodically reviews relevant risks and implements reasonable controls proportionate to the Company's operations, systems, information assets, and contractual obligations.

6. Business Continuity and Disaster Recovery

Information security is integrated into the Company's **Continuity of Business (COB) Plan**.

The Company maintains appropriate arrangements for:

- Backup of critical business information.
- Recovery of essential records.
- Continuity of critical operations.
- Incident response.
- System and information recovery following disruption.

7. Data Protection and Privacy

Geralds Energy is committed to complying with applicable Nigerian data protection requirements, including the **Nigeria Data Protection Act (NDPA) 2023** and relevant regulatory guidance.

The Company seeks to minimize the collection and processing of personal information and does not ordinarily require clients to provide sensitive personal data for its fleet management and logistics services.

8. Incident Management

Information and cybersecurity incidents shall be promptly reported, assessed, contained, and managed.

Depending on the nature and severity of an incident, Management may:

1. Identify and assess the incident.
2. Restrict affected access or systems.
3. Protect critical information and assets.
4. Restore affected operations.
5. Notify relevant stakeholders where required.
6. Document and review the incident.
7. Implement corrective and preventive measures.

9. Training and Awareness

Geralds Energy is committed to maintaining security awareness among employees and relevant service providers.

Training and awareness activities may cover:

- Cybersecurity awareness.
- Password and access security.
- Confidentiality.
- Phishing and malware awareness.
- Incident reporting.
- Safe use of company systems.
- Data protection.
- Physical and operational security.

10. Policy Review and Continuous Improvement

This Policy shall be reviewed periodically and updated where necessary to reflect changes in the Company's operations, technology, regulatory requirements, contractual obligations, or emerging cybersecurity threats.

Geralds Energy is committed to continually strengthening its information security practices and developing its cybersecurity framework in line with recognized industry standards and best practices.

11. Management Responsibility

The Managing Director has overall responsibility for the implementation and oversight of this Policy, supported by relevant operational and administrative personnel.

Management shall ensure that appropriate resources, controls, awareness, and monitoring mechanisms are maintained to support the Company's information and cybersecurity objectives.

APPROVAL

For: Geralds Energy Resources Nigeria Limited

Name: Obinna Ogbudike

Designation: Managing Director

Signature: 

Date: May 7th 2025