INFORMATION SECURITY AND CYBERSECURITY POLICY

1. PURPOSE

SierraCol Energy Limited and its subsidiaries (hereinafter referred to as the “Company” or “SierraCol Energy”) establish their commitment and strategic direction to protect the confidentiality, integrity, and availability of information. Additionally, they foster a cybersecurity culture at all levels of the organization and lay the foundation for regulatory compliance in information security, cybersecurity, and IT risk management.

2. APPLICATION

This policy applies to all employees and contractors, in the development of the Company's activities and operations, working on the Company's premises or third-party locations. It also applies to any third party with an email domain @sierracol.com or @cedco.com, or with access to the Company's systems, information, and digital processes.

3. REQUIREMENTS

a. General

Under the leadership of the IT management, SierraCol Energy will oversee information security and cybersecurity by identifying threats and vulnerabilities that may compromise the Company's assets. The Company will implement appropriate measures to reduce the likelihood or impact of risk events that affect the integrity, confidentiality, and availability of information.

b. Specific

To manage information security and cybersecurity, the IT Manager and the Cybersecurity Leader will apply the following guidelines:

- Establish standards, procedures, and guidelines for information security and cybersecurity.
- Implement practices and awareness’ campaigns to strengthen the culture of information security and cybersecurity among employees, suppliers, and contractors.
- Define, implement, operate, and continuously improve the Information Security Management System (ISMS).
- Ensure business continuity in the face of information security and cybersecurity incidents.
- Maintain cybersecurity maturity levels to minimize risk in the Company's most important functions.
- Support technological innovation.
- Protect technological assets.

4. RESPONSIBILITIES

4.1 Strategic Cybersecurity Committee

The Committee is responsible for providing strategic guidance to maintain alignment between business objectives and appropriate levels of integrity, confidentiality, and availability of technological systems and information. This committee is led by the Company's CEO and includes the participation of selected VPs, as detailed in the cybersecurity committee manual.

4.2 IT Manager, Cybersecurity Leader

They are responsible for the strategic design and establishment of the specific requirements mentioned in section 3.b. above.

Establish an Information Security Management System (ISMS) with the main purpose of fostering a business trust environment with partners, investors, employees, contractors, the state, and any interested party, in line with the Company's mission and vision and regulatory compliance.

4.3 Supervisors

Supervisors are responsible for ensuring that projects developed and approved within their areas or functional disciplines comply with the requirements of this policy and the information security and cybersecurity standard.

4.4 Employees and third parties with access to the Company's systems

Company personnel at all levels are responsible within their areas for taking reasonable measures to prevent, detect, mitigate, and report cybersecurity events and activities that compromise the Company's assets. Each Company employee and contractor employee with access to and/or managing information must:

a. Comply with information security and cybersecurity principles inside and outside the Company's premises.
b. Timely report suspicious activities or cybersecurity incidents; and
c. Cooperate in any cybersecurity investigations conducted by the Company.

5. GOVERNANCE, IMPLEMENTATION, AND COMMUNICATION

The IT Manager is directly responsible for the implementation, communication, and compliance of this policy, as well as the information security and cybersecurity standard. They are also responsible for providing the necessary resources to implement and effectively communicate the policy to all Company employees, as well as any contractor with an email domain @sierracol.com or @cedco.com, and any third party with access to the Company's systems, information, and digital processes.

The Finance Vice Presidency will be responsible for overseeing the implementation of this policy and facilitating its communication and coordination with other areas of the Company.

6. TRAINING

The IT Manager is responsible for developing a training and education program for employees and any third party with an email domain @sierracol.com or @cedco.com, and any third party with access to the Company's systems, information, and digital processes about this Policy and the information security and cybersecurity standard, as well as its updates or changes.

7. REFERENCES

No.	Type	Title
65.050.003	Standard	Information Security and Cybersecurity Standard

8. NON-COMPLIANCE

If the Company determines that a violation of this Policy has occurred, it may impose disciplinary measures as appropriate, which may include training, written or verbal warnings, disciplinary sanctions, suspension, reassignment, or contract termination.