INFORMATION SECURITY POLICY

DOCUMENT TITLE: Information Security Policy

REVISION: 1.01

DOCUMENT CONTROL LOG:

	Name	Role	Signature	Date	Rev
Prepared By	Luke Deasy	Managing Director		10/02/2023	1.01
Reviewed By	Luke Deasy	Managing Director		12/06/2023	1.01
Reviewed By	Luke Deasy	Managing Director		12/06/2024	1.01
Reviewed By	Peter Lane	EHS Officer		12/06/2025	1.01

INFORMATION SECURITY POLICY:

At Copper Coast Renewables, we recognize the importance of safeguarding sensitive information and maintaining the confidentiality, integrity, and availability of our data assets. Our Information Security Policy outlines the principles and practices that guide our efforts to protect information from unauthorized access, disclosure, alteration, or destruction.

POLICY STATEMENT:

1. Confidentiality: We ensure that sensitive information, including customer data, proprietary information, and personal identifiable information (PII), is accessed, and disclosed only to authorized individuals for legitimate business purposes. We implement access controls, encryption, and other security measures to prevent unauthorized disclosure of confidential information.
2. Integrity: We maintain the accuracy, completeness, and reliability of our data assets by implementing controls to prevent unauthorized modification, deletion, or corruption. We employ data validation, version control, and backup procedures to ensure the integrity of our information throughout its lifecycle.
3. Availability: We strive to ensure the availability and accessibility of our information resources to support business operations and continuity. We implement measures such as redundancy, disaster recovery planning, and incident response procedures to minimize downtime and disruptions to our services.
4. Access Control: We grant access to information resources based on the principle of least privilege, ensuring that individuals have access only to the information necessary to perform their job duties. We enforce strong authentication mechanisms, password

policies, and user access controls to prevent unauthorized access to our systems and data.

5. Data Protection: We implement measures to protect data from unauthorized access, theft, loss, or corruption. This includes encryption, data masking, and secure transmission protocols to safeguard information both in transit and at rest. We also educate employees on data handling best practices and provide training on security awareness to mitigate the risk of data breaches.
6. Compliance: We comply with all applicable laws, regulations, and industry standards related to information security and data protection. We regularly assess our security controls, conduct risk assessments, and undergo audits to ensure ongoing compliance with legal and regulatory requirements.
7. Incident Response: We maintain an incident response plan to promptly detect, respond to, and recover from security incidents or breaches. We designate incident response teams, establish communication protocols, and document procedures for reporting and investigating security incidents.

- All employees are responsible for adhering to this Information Security Policy and following established security procedures and guidelines.
- Managers and supervisors are responsible for enforcing compliance with security policies and providing support and resources to employees to fulfill their security responsibilities.
- The Information Security Officer (ISO) is responsible for overseeing the implementation of this policy, monitoring compliance, and coordinating security initiatives and training programs.

POLICY REVIEW:

This Information Security Policy will be reviewed and updated periodically to reflect changes in technology, business practices, and regulatory requirements. Employees will be notified of any revisions to the policy, and training will be provided as necessary to ensure understanding and compliance.

CONCLUSION:

By adhering to the principles outlined in this Information Security Policy, Copper Coast Renewables is committed to protecting the confidentiality, integrity, and availability of our information assets and maintaining the trust and confidence of our customers, partners, and stakeholders.

_____

Luke Deasy
Managing Director