Radiant Renewables

IT & Data Security Policies

This policy must be reviewed by the following date:

31/05/2024

Company Name	Signed By	Review Date
Radiant Heating Solutions T/A Radiant Renewables	Martin Badley	31/05/2024

1. Introduction

1.1 Radiant Renewables (hereinafter referred to as "the Company") is dedicated to maintaining the highest standards of information technology (IT) and data security to protect its assets, sensitive information, and ensure the privacy of individuals and organizations we interact with.

1.2 These IT and Data Security Policies outline the expectations, responsibilities, and guidelines for the appropriate use, protection, and management of the Company's IT resources, systems, and data.

2. Acceptable Use of IT Resources

2.1 All employees, contractors, and authorized users are required to use the Company's IT resources responsibly and in compliance with applicable laws, regulations, and contractual obligations.

2.2 Unauthorized use, reproduction, distribution, or storage of copyrighted materials, software, or other intellectual property without appropriate permissions is strictly prohibited.

2.3 Employees must not engage in any activities that could disrupt the availability, integrity, or confidentiality of the Company's IT resources or systems.

3. Information Security

3.1 Employees are responsible for safeguarding the Company's sensitive information and data, including but not limited to customer data, financial data, proprietary information, and personal data.

3.2 Confidential information must be protected against unauthorized access, disclosure, alteration, or destruction. Employees must use encryption, strong passwords, and other security measures as appropriate to protect data integrity and confidentiality.

3.3 The Company utilises firewalls, intrusion detection systems, and other security technologies to protect against unauthorized access and malware. Employees must not attempt to circumvent or disable these security measures.

4. Data Protection and Privacy

4.1 The Company is committed to protecting personal data in accordance with applicable data protection laws, including but not limited to the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

4.2 Employees must adhere to the Company's Data Protection and Privacy Policy, which outlines how personal data is collected, processed, stored, and shared.

4.3 Personal data must only be collected for specified, legitimate purposes, and must not be used for unauthorized or unlawful activities. Employees must not access or disclose personal data unless it is necessary for their job responsibilities.

5. Access Controls and User Accounts

5.1 Employees shall have unique user accounts and must not share their account credentials or grant unauthorized access to any individual.

5.2 Access to sensitive information and systems must be granted based on the principle of least privilege, ensuring that employees have access only to the resources necessary to perform their job responsibilities.

Company Name	Signed By	Review Date
Radiant Heating Solutions T/A Radiant Renewables	Martin Badley	31/05/2024

5.3 User accounts belonging to employees who have left the Company or changed roles must be promptly deactivated or updated to reflect the appropriate access permissions. Any dormant or inactive accounts must be regularly reviewed and disabled.

6. Incident Reporting and Response

6.1 All employees are responsible for promptly reporting any suspected or actual security incidents, data breaches, or other IT-related incidents to the designated IT or security department.

6.2 Employees must cooperate fully in investigations related to IT security incidents and comply with incident response procedures as directed by the IT or security department.

6.3 The Company maintains an incident response plan that outlines the steps to be followed in the event of a security incident, and employees must familiarize themselves with this plan.

7. Training and Awareness

7.1 The Company shall provide regular IT security awareness and training programs to all employees to ensure understanding of security policies, procedures, and best practices.

7.2 Employees are expected to actively participate in these training sessions and apply the knowledge gained to their daily work activities.

7.3 The Company may conduct periodic phishing awareness campaigns and other simulated attacks to enhance employee awareness and response to potential threats.

8. Compliance and Consequences

8.1 Non-compliance with these IT

and Data Security Policies may result in disciplinary action, up to and including termination of employment.

8.2 Employees who violate laws, regulations, or engage in activities that compromise IT and data security may also be subject to legal consequences.

8.3 The Company reserves the right to monitor, access, and review any information or activity on its IT resources or systems to ensure compliance with these policies and applicable laws.

9. Policy Review and Updates

9.1 These IT and Data Security Policies shall be reviewed periodically to ensure their effectiveness and alignment with legal and industry standards.

9.2 Updates to these policies will be communicated to employees, and their continued compliance is expected.

By signing below, I acknowledge that I have read, understood, and agree to abide by the Company's IT and Data Security Policies.

Company Name	Signed By	Review Date
Radiant Heating Solutions T/A Radiant Renewables	Martin Badley	31/05/2024

Employee's Name: _____

Employee's Signature: _____

Date: _____

Company Name	Signed By	Review Date
Radiant Heating Solutions T/A Radiant Renewables	Martin Badley	31/05/2024