****

**Cyber Security Policy**

**TEC Installations LTD**

**Effective Date:** 01/06/2025
**Review Date:** Annually

* **1. Introduction**

TEC Installations LTD is committed to safeguarding its digital assets, information systems, and data integrity against cyber threats. This policy sets out our approach to managing cyber security risks to protect our business operations, employees, clients, and stakeholders.

* **2. Purpose**

The purpose of this policy is to establish a framework for identifying, preventing, detecting, and responding to cyber security threats while ensuring compliance with relevant UK legislation, standards, and best practices.

* **3. Scope**

This policy applies to all employees, contractors, third-party vendors, and any authorized users who access TEC Installations LTD’s information systems, networks, and data.

* **4. Policy Principles**
* **4.1 Asset Management**
* All information assets and systems are to be identified, classified, and protected in accordance with their importance to business operations.
* **4.2 Access Control**
* Access to information systems is granted on a need-to-know basis, with strong authentication mechanisms (e.g., passwords, two-factor authentication).
* User access rights are reviewed regularly and revoked when no longer necessary.
* **4.3 System Security**
* All systems and software shall be kept up-to-date with the latest security patches and updates.
* Anti-malware, firewalls, and intrusion detection/prevention systems are deployed to monitor and mitigate threats.
* **4.4 Data Protection**
* Sensitive and personal data are protected in compliance with UK data protection laws, including GDPR.
* Data is encrypted during transmission and storage where appropriate.
* Backup procedures are in place, tested regularly, and stored securely off-site.
* **4.5 Incident Response**
* All cyber security incidents must be reported immediately to the designated incident response team.
* An incident management procedure ensures prompt containment, investigation, and recovery.
* **4.6 User Responsibilities**
* Employees are responsible for maintaining the security of their login credentials, avoiding suspicious links or attachments, and adhering to security best practices.
* Employees are trained regularly on cyber security awareness.
* **4.7 Supplier and Third-party Security**
* Third-party vendors and suppliers with access to TEC Installations LTD’s systems must comply with our security standards through contractual obligations and assessments.
* **5. Monitoring and Compliance**
* Regular audits and vulnerability assessments will be conducted to evaluate our cyber security posture.
* Non-compliance or breaches will be addressed through disciplinary measures and corrective actions.
* **6. Training and Awareness**
* All employees undergo mandatory cyber security training.
* We promote ongoing awareness campaigns to reinforce best practices and emerging threats.
* **7. Continuous Improvement**
* TEC Installations LTD commits to regularly reviewing and enhancing our cyber security measures in line with technological advances, industry standards, and regulatory requirements.
* **8. Legal and Regulatory Compliance**

This policy complies with UK legislation, including the Data Protection Act 2018, UK GDPR, and relevant standards such as ISO/IEC 27001.

**Approval and Review**
This policy has been approved by senior management and will be reviewed annually or following any significant security incident or legislative change.

**Dale Carroll**

**Managing Director**

**01/06/2025**