CYBER SECURITY POLICY

QUBIT INTERIOR SOLUTIONS LIMITED
PIER HOUSE, THAMES ROAD, DARTFORD, DA1 4SL

CYBER SECURITY POLICY

Company: Qubit Solutions Limited
Location: Pier House, Thames Road, Dartford, DA1 4SL
Prepared By: Kyle McGimpsey
Position: Managing Director
Date Issued: 18/05/2026
Document Number: QUBI0020
Revision: 1

1. Purpose

This policy establishes the cyber security principles, responsibilities, and controls implemented by Qubit Interior Solutions to reduce cyber risks, protect information assets, and support secure business operations.

2. Scope

This policy applies to all employees, directors, contractors, consultants, temporary workers, suppliers, and third parties who access company systems, devices, networks, or information.

3. Cyber Essentials Commitment

Qubit Interior Solutions maintains Cyber Essentials accreditation and is committed to implementing and maintaining the core technical controls required under the scheme, including:

- Secure configuration
- Access control
- Malware protection
- Security update management
- Firewall and internet gateway protection

4. Cyber Security Objectives

The company aims to:

- Protect confidential and sensitive information.
- Prevent unauthorised access to systems and data.
- Reduce cyber security vulnerabilities.

- Maintain operational resilience.
- Support compliance with legal and contractual obligations.
- Promote cyber security awareness across the organisation.

5. Roles & Responsibilities

Management is responsible for ensuring appropriate cyber security controls are implemented and maintained.

All personnel are responsible for:
- Following cyber security procedures.
- Protecting passwords and credentials.
- Reporting suspicious activity immediately.
- Using company systems responsibly.
- Completing cyber awareness training where required.

6. Access Control

Access to company systems and data shall be restricted to authorised users only.

Controls include:
- Unique user accounts
- Strong password requirements
- Multi-factor authentication (MFA)
- Restricted administrator access
- Prompt removal of leaver accounts

7. Device & Endpoint Security

Company devices must:
- Use approved anti-virus and anti-malware protection
- Be regularly updated and patched
- Use password-protected screen locking
- Be encrypted where appropriate
- Be used only for authorised purposes

8. Security Updates & Patch Management

Critical security updates and software patches shall be applied promptly to reduce exposure to known vulnerabilities.

Unsupported or obsolete software should not be used on company systems.

9. Email & Phishing Protection

Personnel must remain vigilant against phishing attacks, social engineering, and suspicious communications.

Employees must:
- Avoid opening suspicious attachments or links
- Verify unusual requests
- Report phishing attempts immediately
- Use approved company email systems only

10. Data Protection & Confidentiality

Sensitive and confidential information shall be protected against unauthorised access, disclosure, alteration, or loss.

The company supports compliance with UK GDPR and Data Protection legislation.

11. Remote Working & Mobile Security

Remote workers must:
- Use secure internet connections
- Protect company devices from unauthorised access
- Avoid unsecured public Wi-Fi where possible
- Report lost or stolen devices immediately

12. Backup & Disaster Recovery

Critical business systems and data shall be securely backed up to support business continuity and disaster recovery arrangements.

Recovery procedures are supported by the company Business Continuity Plan and Disaster Recovery Plan.

13. Incident Reporting

Any cyber incident, suspected breach, malware infection, phishing email, or unauthorised access attempt must be reported immediately to management or the designated IT support provider.

---

14. Third-Party Security

Qubit Interior Solutions aims to work with suppliers and service providers who maintain appropriate cyber security standards and controls.

---

15. Monitoring & Compliance

The company reserves the right to monitor systems, devices, and network usage to protect company operations and ensure compliance with company policies.

---

16. Breach of Policy

Failure to comply with this policy may result in disciplinary action, removal of access privileges, termination of employment or contract, and/or legal action where appropriate.

---

17. Policy Review

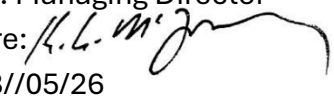
This policy shall be reviewed annually or following:

- Significant cyber incidents
- Cyber Essentials reassessment
- Regulatory changes
- Technology or operational changes
- Emerging cyber threats

---

11. Declaration

Reviewed / Approved By:

Name: Kyle McGimpsey
Position: Managing Director
Signature: 
Date: 18//05/26