T: 0333 733 1111
E: support@hsqe.co.uk
W: HSQE.co.uk & VitalSkills.co.uk

Cyber Security Policy Statement

"Protecting your digital world"

Safeguarding the integrity, confidentiality, and availability of our information assets and systems is a cornerstone of our operations. We recognise the critical importance of cyber security in protecting our clients, employees, and business partners against digital threats. This policy outlines our comprehensive approach to cyber security, encompassing risk management, data protection, and incident response.

1. Risk Management

- **Continuous Risk Assessment:** We commit to regularly assessing cyber security risks associated with our operations, technologies, and third-party services.
- **Preventive Measures:** We will implement preventive measures, including access controls, firewalls, anti-malware solutions, and encryption, to protect against unauthorised access and data breaches.
- **Employee Training:** All employees will receive ongoing training on cyber security best practices and emerging threats to ensure they are equipped to recognise and prevent cyber attacks.
- **Cyber Essentials:** Our cyber security controls are aligned with, and certified against, the UK Government's Cyber Essentials scheme, providing independent assurance of baseline cyber security controls.
- **Third-Party Risk Management:** We assess the cyber security posture of key suppliers and service providers where they process, store, or access our data. Appropriate contractual, technical, and organisational safeguards are applied to manage third-party cyber risks.

2. Data Protection

- **Data Privacy:** We are committed to upholding the privacy of our clients and employees by adhering to data protection laws and best practices in data handling and storage.
- **Access Control:** Data will be accessed only when necessary. Access to sensitive information will be restricted to authorised personnel only, based on the principle of least privilege.
- **Strong Authentication:** Where available, multi-factor Authentication (MFA) is implemented for privileged accounts and key systems to reduce the risk of unauthorised access.
- **Secure Use of Systems:** Company systems and devices must be used in accordance with defined acceptable use requirements, including secure configuration, timely updates, and protection against unauthorised software or activities.
- **Data Backup and Recovery:** We will maintain robust data backup and recovery procedures to ensure the resilience of our operations in the event of data loss or system failures.

3. Incident Response

- **Incident Detection and Reporting:** We employ appropriate monitoring and logging controls to support the timely detection of cyber security incidents.
- **Response and Recovery:** In the event of a cyber security incident, we have a response plan in place to contain, eradicate, and recover from the incident, minimising its impact on our operations and stakeholders.
- **Regulatory and Client Notification:** Where required, relevant stakeholders and regulatory bodies will be notified of cyber security incidents in a timely and proportionate manner.
- **Post-Incident Analysis:** After an incident, we will conduct a thorough analysis to identify lessons learned and improve our cyber security posture.

Implementation and Monitoring

- **Accountability**: The Chief Information Security Officer (CISO) role is performed by our Continuous Improvement Director. They oversee the implementation, monitoring, and ongoing refinement of this policy.
- **Employee Engagement:** Cyber security is a shared responsibility. All employees are expected to adhere to this policy and contribute to a secure digital environment.
- **Review and Adaptation:** This policy will be reviewed annually and updated as necessary to adapt to new cyber security challenges and regulatory requirements.

We understand that robust cyber security is not just about technology but also about people and processes. By adopting a holistic approach to cyber security, we aim to protect our assets, build trust with our clients, and maintain our reputation as a secure and reliable provider of consultancy and online training solutions.

Original Signed Date: 22 February 2026

John Constable
Chairman & Professional Head
MIoD CMIOSH MCQI CQP MIEMA CEnv FCMI MIIRSM