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.

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.
- **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 will employ advanced monitoring tools to detect cyber security incidents promptly and establish clear procedures for reporting these 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.
- **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 2024

John Constable
Managing Director & Professional Head
CMIOSH MCQI CQP MIEMA CEnv FCMI MIIRSM MSc

VitalSkills®.co.uk