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

Network Security Policy Statement

“Networks built to defend”

In today's digital age, safeguarding our network infrastructure is paramount to maintaining the integrity, confidentiality, and availability of our data and services. Our Network Security Policy is designed to establish a robust framework that protects our organisation's digital assets against evolving cyber threats, ensuring the safety of our information and the trust of our stakeholders.

Our commitments

- **Secure Online Transactions:** HSQE Ltd ensures the security of purchaser details during website transactions.
- **Data Processing and Transfer:** We ensure all payment-related data is transmitted over secure, encrypted connections (HTTPS/TLS). Payment card information is submitted directly to Stripe for processing via secure integration with WooCommerce and is not processed or stored on HSQE Ltd systems.
- **Credit and Debit Card Security:** All credit and debit card details are processed exclusively by Stripe, which maintains Level 1 PCI DSS (Payment Card Industry Data Security Standard) compliance. HSQE Ltd does not store or process cardholder data entered via this method, significantly reducing risk to customers’ financial information.
- **Online Training Data Security:** HSQE Ltd is responsible for the security and integrity of user data related to online training courses. This data is stored on our Learning Management System (LMS), which is hosted by a hosting subcontractor and is protected by access controls and security monitoring appropriate to its sensitivity.
- **Subcontractor and Data Centre Certifications**: We use Google Cloud infrastructure. Google data centres are certified against recognised international standards, including ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, and SOC 2, alongside additional security frameworks such as PCI DSS, HIPAA, and FedRAMP.
- **Regular Updates and Maintenance:** We ensure that our software and hardware are up-to-date with the latest security patches and updates.
- **Rule Review and Optimisation:** We continuously review and optimise firewall rules to ensure they effectively block unauthorised access while permitting legitimate traffic.
- **Monitoring and Alerting:** We implement and monitor systems to alert our security team of unusual traffic patterns or potential breaches, enabling rapid response to threats.

Implementation and Monitoring

- **Accountability**: The Chief Information Security Officer (CISO) role is performed by our Continuous Improvement Director. They oversee the policy's implementation. This ensures that network security measures are applied rigorously, maintaining the integrity, confidentiality, and availability of our digital assets.
- **Employee Engagement**: All employees are encouraged to increase their knowledge of network security best practices and to incorporate these practices into their daily activities and decision-making processes.
- **Review and Improvement:** This policy will be reviewed at least annually to reflect new insights, feedback from stakeholders, and evolving security standards.

We commit to upholding the digital safety and integrity of our stakeholders' information. This commitment not only protects our operations but also reinforces our reputation as a reliable and secure partner in the digital landscape.

Original Signed Date: 24 February 2026

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