VitalSkills™ by HSQE.co.uk

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 data entered is processed on a secure page operated by Woo Commerce, utilising SSL (Secure Socket Layer) technology to encrypt data during transmission. Following this, the data is transferred securely to SagePay for processing.
- **Credit and Debit Card Security:** We ensure all credit and debit card details are processed exclusively by SagePay, which maintains security measures in compliance with Level 1 PCI DSS (Payment Card Industry Data Security Standard) certification. It is our policy that HSQE Ltd does not store credit/debit card information entered through this method, minimising the risk to our customers' financial data.
- **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.
- **Subcontractor and Data Centre Certifications**: We use a hosting subcontractor that operates within a UK data centre that is certified to ISO 27001 (Information Security Management), ISO 9001 (Quality Management), TIA-942 Tier 3 (Telecommunications Infrastructure Standard for Data Centres), and is approved to hold data up to HMG InfoSec IL5 (UK Government's Security Classifications).
- **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: 22 February 2024

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

VitalSkills® .co.uk