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

Third-party Vendor Security Policy Statement

“Unified security, shared success”

All third-party vendors engaged by HSQE Ltd are required to uphold stringent security measures to safeguard sensitive and confidential information. This entails the development and maintenance of a robust information security program. Such a program must encompass detailed policies, procedures, and standards specifically crafted to protect the integrity and privacy of data.

The security controls implemented by these vendors must mirror, if not exceed, the rigor of HSQE Ltd's internal security protocols, adhering closely to the prevailing laws, regulations, and industry best practices.

Third-Party Vendor Security Requirements

- **Robust Data Protection Measures:** Vendors are required to implement robust data protection measures, including but not limited to encryption, access control, and data anonymisation, to prevent unauthorised access, disclosure, alteration, or destruction of HSQE Ltd's data.
- **Compliance with Privacy Policies and Regulations:** Additionally, vendors must adhere to HSQE Ltd's privacy policies and comply with all relevant data protection regulations, such as GDPR, in the handling and processing of personal data, as defined by HSQE Ltd and applicable laws.
- **Immediate Breach Notification and Cooperation:** In the event of a data breach or any incident potentially impacting HSQE Ltd's data privacy, vendors must notify HSQE Ltd within 72 hours of discovering the breach. Vendors are also required to fully cooperate with HSQE Ltd in the investigation and resolution of the incident, which includes providing necessary documentation, access to affected systems, and facilitating interviews with relevant personnel.
- **Robust Authentication and Authorisation:** Implement multi-factor authentication and ensure users are granted access based on their specific roles, strictly adhering to the need-to-know and least privilege principles.
- **Principle of Least Privilege:** Limit access strictly to personnel who need it to fulfil their job responsibilities. This approach minimises the risk of unauthorised access and data breaches.
- **Regular Access Reviews**: Conduct frequent audits of access rights to ensure they align with current job functions. Adjust or revoke access immediately if job roles change or employment ends.
- **Efficient Record Keeping:** Maintain up-to-date records of access controls and user activities for review during audits.

Implementation and Monitoring

- **Vendor Governance and Accountability:** Third-party vendors must ensure that their operations are in alignment with our company's standards for security.
- **Compliance and Ethical Conduct:** Vendors are required to ensure that their teams are well-informed about our compliance requirements, including data protection, privacy policies, and any industry-specific regulations. Vendors must integrate these practices into their daily operations and decision-making processes to maintain a consistent standard of conduct.
- **Ongoing Review and Compliance Adaptation:** Vendors must engage in continuous review and updating of their compliance policies to reflect new legal and regulatory developments, feedback from both internal and external stakeholders, and best practices in operational and ethical governance.

We expect a strong partnership with our third-party vendors, built on mutual responsibility, ethical behaviour, and ongoing progress. We need our vendors to meet our standards for compliance and operations and to aim for high quality and continuous improvement in everything they do.

Original Signed   Date: 22 February 2024

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