Information Security Statement

Information Security Statement

Somerford Associates are dedicated to protecting data and utilising security best practices. We utilise some of the most advanced technology for Internet security available today. We understand the importance of data security and make every effort to ensure that any data held on our systems is fully protected.

We recognise that the confidentiality, integrity and availability of information and data created, maintained and hosted by our suppliers are vital to the success of our business and privacy of our customers. We view these primary responsibilities as fundamental to best business practice to ensure compliance with all applicable laws, regulations and obligations.

Security and Compliance

All our information systems are protected in accordance with their associated risk. We follow the UK Government's Cyber Essentials Plus Scheme and certify our compliance on an annual basis. We have adopted a set of security controls and countermeasures based upon ISO 27001 and we are certified to IASME Cyber Assurance Standards. We fully comply with prevailing data protection law, including the UK Data Protection Act and the EU General Data Protection Regulation (GDPR).

Network & Device Security

We deploy endpoint protection across our estate including servers, laptops and mobile devices. Our networks, data and critical assets are protected by firewalls and advanced threat protection technologies.

Access Control & Two Factor Authentication

Employees are granted only the access needed for their job role. Employees are required to review and accept our Information Security, Acceptable Use and Data Protection policies before being granted access.

All access is revoked immediately on employee termination. Our core business applications can only be accessed using two factor authentication.

Security Policies

We review and update our information security policies regularly, including a formal review at least annually. Employees must review and acknowledge these every year.

Staff Screening

We conduct background screening when hiring a new employee. In addition, we communicate our information security policies to all personnel, require employees to sign non-disclosure agreements, and provide ongoing data privacy and security training.

Dedicated Security Personnel

We have a dedicated Head of Information Security, who focuses on application, network, and system security and is also responsible for security compliance and education.

Security Awareness Training

Security awareness training is mandatory for all employees. It aims to raise awareness of the risks and threats to our systems and information, and reminds employees of their roles and responsibilities in preventing security issues. Regular Phishing Simulation exercises are conducted and additional training allocated automatically as required.

Patching & Vulnerability Management

We update and maintain all our critical software, firmware, systems, applications and devices. This includes promptly applying relevant security patches and updates. Our vulnerability management program includes frequent scans using technologies from market leading vendors, identification and remediation of security vulnerabilities on servers, laptops, network equipment, and applications.

Encryption

We use cryptographic controls to protect the confidentiality, authenticity and integrity of information based upon the sensitivity of the data. In practice this means that all data stored on our servers, laptops and mobile devices is encrypted and data in transit uses secure cryptographic protocols.

Logging and Auditing

Application and infrastructure systems logs are stored for troubleshooting, security reviews, and analysis by authorised personnel using an industry leading Log and Audit management tool.

Change Control

We manage changes that occur to information technology in a way that minimises risk and impact. Change Management ensures that proposed changes that impact production environments are reviewed, tested, authorised, implemented, communicated and released in a controlled manner; and that the status of each proposed change is monitored to completion or retraction.

Data Disposal

Data requiring deletion is securely erased on all storage media in accordance with current industry best practices.

Asset Management

We maintain an asset register which includes all company assets including laptops and other mobile devices. Company issued laptops are equipped with firewalls, hard disk encryption and up-to-date antivirus software and compliance is monitored on a real-time basis.

Third Party Risk Monitoring

We have implemented leading cybersecurity products that continuously monitor the cyber security health of organisations within our supply chain. The same technology is used to monitor the cybersecurity posture of our partners.

Information Security Incident Management

Our Information Security Incident Management policy includes processes covering identification, initial response, investigation, customer notification, public communication, and remediation.

When criminal activity affecting information security is identified, we will liaise with the Information Commissioner's office and local Police as necessary.

Breach Response & Notification

We are committed to keeping customers fully informed of any matters relevant to the security of their data.

Although we take all necessary actions to protect data, no method of transmission over the Internet and or electronic storage is perfectly secure. Should we learn of a security breach affecting an individual's personal data, we will notify those affected so that they can take appropriate protective steps.

Our breach notification procedures comply with all relevant data protection laws and regulations.

Business Continuity & Disaster Recovery

We have business continuity plans in place to counteract interruptions to information systems and business activities from the effects of major failures or disasters. This includes a data backup regime which adopts a rotating schedule of full and incremental backups which are encrypted and stored securely offsite.

Signed by:

RUSSELL TOMPKINS

Head of Information Security
April 2024