Cyber Security Policy

Updated October 2024

At Sewell Wallis, we're committed to protecting our digital assets and ensuring the security and privacy of information. Our Cyber Security policy sets out our guidelines and processes to safeguard our IT systems, data and service users from cyber threats. All employees, contractors and third parties with access to Sewell Wallis IT systems are required to follow this policy.

Purpose of this policy

The purpose of this policy is to protect Sewell Wallis's information and IT assets from cyber threats, and ensure compliance with relevant laws, regulations and best practices. It also serves to maintain the integrity, confidentiality and availability of data, and establish clear responsibilities and procedures for the management of our cyber security.

Scope

This policy applies to all employees and any other individuals with access to Sewell Wallis's IT systems and data. It covers all organisational systems, including but not limited to, computers, mobile devices, networks, and cloud services.

Roles and Responsibilities within our Organisation

Keeping on top of our cyber security is the responsibility of everyone within our business. Specific roles and their responsibilities include:

- **Our IT service providers:** the team we use take responsibility for the implementation, monitoring and management of our cyber security measures, including providing any training our staff may need on cyber security best practices
- **Employees:** Follow the guidelines and procedures outlined in this policy. Report any suspicious activity or security incidents to the IT department immediately.
- **Management:** Ensure compliance with the cyber security policy and support enforcement measures.

Cyber Security Measures

To ensure the safeguarding of our IT systems and data, the following security measures will be enforced:

- **Access Control:** Access to IT systems and data will be controlled based on the principle of least privilege. Multi-factor authentication (MFA) will be used where possible.
- **Data Encryption:** Sensitive data must be encrypted both in transit and at rest. Data encryption standards will be enforced for all storage and transmission of sensitive information.
- **Software Updates:** All software, including operating systems and applications, must be regularly updated to patch known vulnerabilities.
- **Incident Response:** A clear procedure must be in place for responding to security incidents, including identification, documentation, and reporting.
- **Training and Awareness:** We will ensure all staff are given training during their induction period, and when updates are necessary to ensure they are all aware of cyber security threats and best practice.
- **Device Management:** All company-owned devices are managed and monitored by our Administration Manager, and we advise staff to use the given equipment for work purposes, not their personal devices.

We advise all of our employees to ensure they keep their laptops and mobile phones secure by:

- Keeping all devices password protected
- Having the latest anti-virus software
- Ensuring they do not leave their devices exposed or unattended
- Only log into company accounts and systems through secure and private networks only.

Keeping emails safe

Emails can often play host to scams and malicious software that cyber criminals can use to acquire data. To avoid this, we instruct out employees to:

- Avoid opening attachments and clicking on links when the content is not explained adequately (E.G. an email titled ‘ watch this video it’s amazing!”)
- Be suspicious of clickbait titles (E.G. offering prizes or advice)
- Check the email and names of people they have received emails from to ensure they are legitimate
- Look for inconsistencies or obvious give-aways, such as poor grammar and spelling, random capital letters, excessive use of exclamation marks etc.)
- If an employee isn’t sure an email is safe, they can refer it to our IT department who will make the call

Additional measures

To reduce the likelihood of security breaches, we make sure our employees:

- Lock devices and screens when leaving their desk, even for short periods
- Report stolen or damaged equipment to their line manager as soon as possible
- Change all passwords immediately if a device is lost or stolen
- Report perceived threats or security weaknesses in company systems
- Refrain from downloading suspicious, unauthorised or illegal software on company equipment - if they have legitimate need for a program, our IT provider will be able to help with this
- Avoid using suspicious websites

Additional measures

Employees must report any suspicious activity or security breaches immediately to the IT department. Early detection and response are critical in minimizing potential damage.

Due Diligence

Non-compliance with this Cyber Security policy may result in issues being raised to management and in disciplinary action. Please take care when using company equipment.

Monitoring and Review

This policy will be reviewed annually by the management team to ensure it is still relevant and is effective in line with any changes in legislation.

18/10/2024, H. Blakey