South Lakes Housing Cyber Security Policy

Title:	Cyber Security Policy
Person Responsible:	IT Manager
Customer consultation arrangement:	N/A
EIA required?	No
EIA Completed (date):	N/A
Approved by:	Audit and Risk Committee
Business Strategy Objective	4. Improving the running of our business
Approval Date:	January 2019
Links to other Policies	Information Security Policy, Email Policy, Internet Policy, IT Access Policy, Internet Policy
Review Date:	January 2020

Document management		
Version	**Date amended**	**Amendments**
1	**03.01.19**	**Approved by Director of Corporate Services & IT Manager**

1. Purpose

1.1 The purpose of this policy is to provide guidelines and make provision for the security of organisational and personal data and technology infrastructure.

1.2 The policy recognises the increased reliance on technology means an increased vulnerability to severe security breaches. The purpose of this policy is to prevent financial and reputational damage to South Lakes Housing (SLH) by mitigating human error, hacker attack and system malfunctions.

1.3 This policy sets out how we will implement a number of security measure and mitigate security risks.

2. Regulatory and Legislative Requirements

2.1 This policy adheres to the following regulation and legislation:

- Computer Misuse Act 1990

- Official Secrets Act 1989
- Communications Act 2003
- Data Protection Act 1998
- Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426)
- Data Protection Act 2018
- General Data Protection Regulation 2016/679 (GDPR)

3. Scope

3.1 This policy applies to all our Board members, employees, contractors, tenants, volunteers and anyone who has permanent or temporary access to our systems and hardware.

4. Cyber Security – Our Approach

4.1 Effective approach to risk management

Our approach to risk is underpinned by an empowered governance structure, which is actively supported by the Board and senior managers. We clearly communicate our approach to risk management through the development of applicable policies and processes, such as this policy. This policy ensures that all Board members, employees, contractors, tenants, volunteers, etc are aware of the approach, how decisions are made, and any risk boundaries.

This policy conforms with SLH's Risk Management Strategy (May 2018). This outlines how SLH's responsibility to managing risks using a structured and focused approach. This enables the Board to identify partnership, strategic and operational risks, assess the risks for likelihood and impact, identify mitigating controls and allocate responsibility for both risks and controls. Cyber-crime is one of the corporate processes listed in the strategy that is deemed a risk.

4.2 Confidential data

Personal and confidential data is secret and valuable. Common examples are:

- Unpublished financial information
- Commercially sensitive data
- Personal and confidential data relating to housing applicants, residents, contractors and partners
- Personal and confidential data relating to all those employed or in remuneration from SLH

All employees are obliged to protect this data. In this policy, we will give our employees instructions on how to avoid security breaches.

4.3 Security configuration

The IT Manager will restrict the functionality of every device, operating system and application to the minimum needed for business to function. Every process, user and programme will apply the ‘principle of least privilege’, whereby permission is given allowing access to information and resources only where this is necessary for its legitimate purpose.

4.4 Protect personal and company devices

When employees use their digital devices to access company emails or accounts, they introduce security risk to our data. We advise our employees to keep both their personal and company issued computer, tablet and cell phone secure. They can do this if they:

- Keep all devices password protected
- Choose and upgrade a complete antivirus software
- Ensure they do not leave their devices exposed or unattended
- Install security updates of browsers and systems monthly or as soon as updates are available
- Log into company accounts and systems through secure and private networks only

We also advise our employees to avoid accessing internal systems and accounts from other people’s devices or lending their own devices to others.

When new starters receive company-issued equipment they are automatically setup with the following configuration:

- Device Disk encryption
- Installation of mobile device management software
- Web Filtered Browser
- Restriction on apps and settings on the device
- Unable to connect to unsecure WiFi Connections

They should follow instructions to protect their devices and refer to the IT Servicedesk Team if they have any questions.

4.5 Keep emails safe

This section is to be read in conjunction with SLH’s email policy. Emails often host scams and malicious software. To avoid virus infection or data theft, we instruct employees to:

- Avoid opening attachments and clicking on links when the content is not adequately explained (for example, “watch this video, it’s amazing”)
- Be suspicious of clickbait titles (for example, offering prizes, advice)
- Check email and names of people they received a message from to ensure they are legitimate
- Look for inconsistencies or give-aways (for example, grammar mistakes, capital letters, excessive number of exclamation marks.)

If an employee isn’t sure that any email they received is safe, they can refer to our IT Servicedesk.

The IT Manager regularly commissions phishing emails to employee’s to see who is clicking on phishing emails. Every Month, these reports are published to the relevant staff member and line manager of the staff member to inform them of the potential harm to SLH. If employee’s were to click on these links, they are advised to complete online training to protect them from cybercrime.

All employee’s that join SLH are inducted into Data Protection and Cyber Security training within the first 3 months of starting and also yearly conduct e-learning courses where they get assessed.

4.6 Manage passwords properly

Password leaks are dangerous as they can compromise our entire infrastructure. Not only should passwords be secure, so they won’t be easily hacked, but they should also remain secret. For this reason, we advise our employees to:

- Choose passwords with at least eight characters (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed (e.g. birthdays.)
- Remember passwords instead of writing them down. If employees need to write their passwords, they are obliged to keep the paper or digital document confidential and destroy it when their work is done
- Exchange credentials only when absolutely necessary. When exchanging them in-person isn’t possible, employees should prefer the phone instead of email, and only if they personally recognise the person they are talking to.
- Change their passwords every two months

Remembering a large number of passwords can be daunting. Employee’s can store passwords using the inbuilt password management tools within Google Chrome, Firefox or Internet Explorer. Employees are obliged to create a secure password.

4.7 Transfer data securely

Transferring data introduces security risk. Employees must:

- Avoid transferring sensitive data (for example, customer information, employee records) to other devices or accounts unless absolutely necessary
- When mass transfer of such data is needed, we request employees to ask our the IT Servicedesk Team for help
- Share confidential data over the company network/ system and not over public Wi-Fi or private connection
- Ensure that the recipients of the data are properly authorised people or organizations and have adequate security policies
- Report scams, privacy breaches and hacking attempts

- Encrypt sensitive data files using tools such as 7zip

Our IT team need to know about scams, breaches and malware so they can better protect our infrastructure. For this reason, we advise our employees to report perceived attacks, suspicious emails or phishing attempts as soon as possible to our specialists. Our IT Servicedesk must investigate promptly, resolve the issue and send a companywide alert when necessary.

4.8 Removable Media Controls

Removable media, such as discs or memory sticks provide a common route for the introduction of malware and the accidental or deliberate export of sensitive data.

As set out in your email policy discs or memory sticks are restricted from being used with SLH equipment unless approved by the IT Team who can unblock such devices.

4.9 Additional measures

To reduce the likelihood of security breaches, we also instruct our employees to:

- Turn off their screens and lock their devices when leaving their desks
- Report stolen or damaged equipment as soon as possible to the IT Servicedesk
- Change all account passwords immediately when a device is stolen
- Report a perceived threat or possible security weakness in company systems
- Refrain from downloading suspicious, unauthorised or illegal software on their company equipment
- Avoid accessing suspicious websites
- Wipe any such device if possible from mobile device management system or email exchange

We also expect our employees to comply with our social media and our internet policy and procedure.

Our IT Team should:

- Install firewalls, anti-malware software and access authentication systems
- Arrange for security training to all employees
- Inform employees regularly about new scam emails or viruses and ways to combat them. Investigate security breaches thoroughly
- Follow this policies provisions as other employees do

Our company will have all physical and digital shields to protect information.

4.10 Remote employees

Remote employees, including home workers and mobile working must also comply with this policy. These employees will be accessing SLH’s accounts and systems from a distance, they are obliged to follow all data encryption, protection standards and settings, and ensure their private network is secure.

We encourage them to seek advice from our IT Team where necessary.

4.11 Disciplinary action

We expect all our employees to always follow this policy. Those who cause security breaches may face disciplinary action in accordance with the terms and condition of their employment:

- First-time, unintentional, small-scale security breach: We may issue a written warning and train the employee on security.
- Intentional, repeated or large scale breaches (which cause severe financial or other damage): We will invoke more severe disciplinary action up to and including termination. We will examine each incident on a case-by-case basis.

Additionally, employees who are observed to disregard our security instructions will face progressive discipline, even if their behaviour hasn't resulted in a security breach.

4.12 Take security seriously

Everyone, from our customers and partners to our employees and contractors, should feel that their data is safe. The only way to gain their trust is to proactively protect our systems and databases. We can all contribute to this by being vigilant and keeping cyber security top of mind.

4.13 Incident management processes

This is as set out in your Information Security Incident Management Procedure (ICT012). Specifically addressing, responsibilities, reporting, evidence gathering, investigating and learning from incidents so systems and processes are changed to reflect this learning.

5. Monitoring and Review

The Audit and Risk Committee are regularly updated on the cyber security risk impacts on SLH's reputation and financial risk and are given assurances that data and information have been thoroughly assessed and mitigations put in place for their vulnerability to attack.

Cyber Security breaches are reported to the Audit and Risk Committee via the Compliance Report setting out the nature of the breach, the actions taken to prevent it or minimise its impact and the consequence of such a breach. Where necessary, reporting this to the Information Commissioners Office (ICO) and Regulator of Social Housing (RSH) and data subject.

Annual security penetration testing is completed against all internal and external systems to mitigate further risk to the organisation with remedial actions taken from the report.

This policy will be reviewed by the Audit & Risk Committee annually given that cyber security is a fast paced and changing environment, or where there has been significant changes to regulation or legislation to warrant a further policy review. The policy may also be reviewed sooner where there is a need to address operational issues or where best practice has evolved and there is a need to incorporate this.