Vectis Housing	Board Date:	16/5/24
	Author:	Martyn Pearl
	Title:	IT Security Policy

Summary and recommendation:
Members are asked to review and approve the update policy
Financial Implications:
None
Risk Implications:
Failure to effectively manage the use of technology and result in the loss of confidential data, vulnerability to external hacking into systems, financial and reputational loss.

Summary

The use and management of information is a key component of VHAs daily activities. The nature of that use has changes in recent years, particularly since the pandemic, with a significant emphasis on remote and electronic working. As a result, virtually all of our data is `virtual' and thus more vulnerable to inappropriate access, either due to accidental misuse or criminal intent.

This has become even more important following the introduction of the GDPR regulations, there are requirements on organisations to properly and effectively manage any sensitive and personal data. Failure to achieve this, can result in punitive action being taken by the Information Commissioner (ICO) in the form of actions or financial penalties.

The attached policy sets out VHAs approach to IT security and places an obligation on all staff/users for standards of usage and vigilance.

The policy was initially adopted in 2021 and is due for review. Altthough we have reviewed and upgraded our practical tools for security i.e anti-virus, etc in that time, there are no suggestions for change in this policy.

Members are asked to review and approve the updated policy.

VHA Policy Document

IT Security Policy

Reviewed: May 2024

Next Review Due: May 2027

VHA IT Security Policy

1. Introduction

The Board of Management and staff have legal responsibilities to preserve the integrity of information and to comply with the Data Protection Act at all times. In some circumstances the programmes or other material in use may have copyright protection and it is therefore a further responsibility for the Association not to breach this protection.

The hardware, software and data utilised by the Association in its business represent considerable investments in terms of both cash and staff time, and therefore it is vital that measures be taken to preserve their integrity and confidentiality.

The Board of Management and staff must at all times follow the Security Policy **whether working in the office or remotely**.

2. Definition of IT Security

Security in the context of this Policy relates to data, control of digital processes and equipment.

T he key areas of risk are:

- Confidentiality of Information
- Integrity of data
- Stewardship of physical assets
- Efficient and appropriate use of information and equipment
- System availability

3. Policy Aims

The aims of this policy are to:

- Provide staff with suitable IT for their working needs, including access to the programmes and data they require
- Prevent unauthorised access to confidential data and vulnerable programmes
- Deny access to all programmes, data and hardware to unauthorised users
- Comply with all legal requirements for data protection
- Preserve data for subsequent use
- Protect hardware from theft, fire and other risks
- Minimise the risk of introduction of unauthorised programmes, data, viruses or other risks

4. Procedure

To achieve these aims the following procedures are required and will be enforced:

4.1 Staff will be given unique user identities which allow access to the system, and are further protected by passwords, which must not be shared or written down.

4.2 All users must lock their PCs by pressing ctrl+alt+del if they leave their desks for any period of time which could allow another user or visitor to be left alone with access to their systems.

4.3 All users must log out of the system if they:

o Leave the building

o Leave their desks for more than one hour

o Log into another machine

4.4 Any floppy disks, CD's etc. from any source must be virus checked before being loaded onto one of the Association's machines**.**

5. Document Security

5.1 All staff are expected to protect our electronic communications systems and equipment from unauthorised access and harm at all times. Failure to do so may be dealt with under our Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

5.2 All users have access to the directories within the VHA Shared Drive on the file server (F:) dependent on their operational requirements. Files which are deemed to be confidential, or those which are final and/or approved documents should located in locations with restricted access to those authorised members of staff.

5.3 All documents pertinent to the business of the Association should be saved to the Company Drive (F:) on the file server so that the system can back up every evening.

5.4 All users have access to their own folder within the Shared Drive which is exclusive to them but held on the file server and backed up nightly with all other files.

6. **Equipment security and passwords**

6.1 Staff are responsible for the security of the equipment allocated to or used by them, and must not allow it to be used by anyone other than as permitted by this policy.

6.2 If given access to the e-mail system or to the internet, staff are responsible for the security of their terminals. If leaving a terminal unattended or on leaving the office they should ensure that they lock their terminal or log off to prevent unauthorised users accessing the system in their absence. Staff without authorisation should only be allowed to use terminals under supervision.

6.3 Desktop PCs and cabling for telephones or computer equipment should not be moved or tampered with without first consulting the Association's IT consultants or the CE.

6.4 Passwords are unique to each user. Passwords must be kept confidential and must not be made available to anyone else unless authorised by the CE. For the avoidance of doubt, on the termination of employment (for any reason) staff must provide details of their passwords to the CE and return any equipment, key fobs or cards.

6.5 Staff who have been issued with a laptop, PDA or smartphone must ensure that it is kept secure at all times, especially when travelling. Passwords must be used to secure access to data kept on such equipment to ensure that confidential data is protected in the event of loss or theft. Staff should also be aware that when using equipment away from the workplace, documents may be read by third parties, for example, passengers on public transport.

7. **Systems and data security**

7.1 Staff should not delete, destroy or modify existing systems, programs, information or data which could have the effect of harming our business or exposing it to risk.

7.2 Staff should not download or install software from external sources without authorisation from the CE. This includes software programs, instant messaging programs, screensavers, photos, video clips and music files. Incoming files and data should always be virus-checked by the Association's IT consultants, or those within the organisation suitably qualified/experienced to do so, before being downloaded. If in doubt, staff should seek advice from the aforementioned persons. The following should not be accessed from the network: online video streaming, instant messaging and webmail (such as Hotmail or Yahoo) and social networking sites (such as Facebook, YouTube, Twitter). This list may be modified from time to time.

7.3 No device or equipment should be attached to our systems without the prior approval of the IT department. This includes any USB flash drive, MP3 or similar device, PDA or telephone. It also includes use of the USB port, infra-red connection port or any other port.

7.4 We monitor all e-mails passing through our system for viruses. Workers should exercise caution when opening e-mails from unknown external sources or where, for any reason, an e-mail appears suspicious (for example, if its name ends in .ex). The IT consultants and CE should be informed immediately if a suspected virus is received. We reserve the right to block access to attachments to e-mails for the purpose of effective use of the system and for compliance with this part of our handbook. We also reserve the right not to transmit any e-mail message.

7.5 Staff should not attempt to gain access to restricted areas of the network, or to any password-protected information, unless specifically authorised.

7.6 Staff using laptops or wi-fi enabled equipment must be particularly vigilant about its use outside the office and take any precautions required by the IT consultants or the CE from time to time against importing viruses or compromising the security of the system. The system contains information which is confidential to our business and/or which is subject to data protection legislation. Such information must be treated with extreme care and in accordance with our Data Protection Policy.