6.7 The Care Trust Policy on Cyber-Security

Policy Statement

Cybersecurity is the protection of devices, services and networks—and the information on them—from theft and/or damage *via* electronic means.

This policy outlines the guidelines and provisions for preserving the security of our data, devices, services and technology infrastructure from theft and/or damage *via* electronic means.

It outlines security measures TCT have put in place and includes guidelines and instructions to mitigate security risks.

This policy should be read in conjunction with other relevant documents of The Care Trust:

- Risk Management Policy
- Data Protection Policy
- Code of Conduct
- Staff Handbook

Scope

This policy applies to all TCT directors, employees, contractors, volunteers and anyone who has permanent or temporary access to TCT systems and hardware.

The Care Trust Responsibilities

Cybersecurity is central to the health and resilience of The Care Trust, and this places the policy within the responsibilities of the Board. Cybersecurity is included on the Risk Register for regular review.

The Chief Executive and SMT are responsible for ensuring all directors, staff, contractors and other users of the IT systems or hardware (temporary or permanent) are informed of the cybersecurity policy and are given adequate training and tools to implement it fully.

All directors, staff, contractors and any other users of the IT systems or hardware are responsible for ensuring they understand and implement the security measures at all times.

Confidential data

Confidential data is secret and valuable. Common examples are unpublished financial information and data related to Contributors/Beneficiaries/employees. The Care Trust has a full policy on Data Protection. This policy provides instructions on how to avoid security breaches.

Responsibilities of the SMT

The SMT and Director of IT, in conjunction with our IT support providers, will:

- Ensure data security through the installation of firewalls, anti-malware software and access authentication systems
- Arrange for security training for employees and directors
- Regularly communicate on new scam emails or viruses and ways to combat them
- Investigate security breaches thoroughly
- Follow this policy and data protection guidelines as other employees do.

Data Security

The Care Trust no longer holds any systems data on site in the Blackrock office. Systems data is hosted in two separate locations:

1. CIX Data Centre (Cork):

This data centre holds TCT's servers and logical virtual machines. All back-office data is stored here. This has physical security 24 hours x 7 days x 365 days to protect access to the hardware.

2. Microsoft (Europe):

Microsoft hosts TCT's connected Office 365 data, including Email, SharePoint, Power BI, etc. Microsoft security is included with TCT's professional licenses and protects against cyber-attacks in real time.

Other IT Measures

- **Firewalls:** Firewalls are installed in the Blackrock office to protect network traffic on the local area network - and in the CIX data centre to protect server traffic
- **Anti-virus software**: Sophos anti-virus software is installed to protect all software and operating systems. This software is continuously updated by licence agreements

- **Azure active directory with multi-factor authentication**: Network access to TCT's remote desktop servers is controlled and maintained by Microsoft Azure services. If a login attempt is tried from a new location or on a new device, then user access is prompted for verification on a separate device (*via* text message code or authenticator app). Passwords are forced to expire at time intervals - usually 60 days
- **Data encryption**: Sensitive data is encrypted in the SQ Server using a 256-bit AES algorithm. If the database becomes compromised, sensitive data such as bank account details will not be readable without a separate decryption key. This decryption key is securely held in an encrypted password manager in The Care Trust.
- **Off-site backups**: TCT ensures that all system data is backed up each day. These daily backups are stored on a NAS drive connected to the server. The backups are also shipped off-site to a 3rd party (asigra.com) so that restoration can be enabled independently of the data centre, if necessary
- **Disaster recovery**: TCT commissions a continuous snapshot system synchronised to Microsoft Azure, where all servers are backed up every 15 minutes. This provides a separated extra layer of redundancy if TCT's physical servers, on-site backups and off-site backups are unavailable. TCT can switch over to a complete mirror of the systems within one hour, with a maximum 15-minute data loss
- **Mobile Device Management**. All mobile devices that access TCT resources such as email, SharePoint, RDS are subject to minimum security requirements and are controlled by the Microsoft Portal Application.
- **User training**: Users are trained to recognise phishing messages – which can come via email or text messages. Users are aware not to enter authentication details into any 3rd party website. Policies and procedures are in place to authorise any payments and bank transfers; an email instruction on its own is not sufficient to effect a payment

Responsibilities of directors, staff and contractors

1. Protect personal and company devices

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

- 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 TCT accounts and systems through the secure and private RDS

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

When new staff receive company-issued equipment they will receive instructions for:

- Accessing and using the RDS and Sharepoint
- Generating strong passwords and using KeePass
- Installing antivirus/ anti-malware software

They should follow instructions to protect their devices and refer to our Director of IT if they have any questions.

2. Keep emails safe

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 (e.g. "watch this video, it's amazing.")
- Be suspicious of clickbait titles (e.g. 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 (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)

If a director an employee isn't sure that an email they received is safe, they can refer to the Director of IT.

3. Manage passwords properly

Password leaks can compromise our entire infrastructure. Not only should passwords be secure so they will not be easily hacked, but they should also remain secret. For this reason, we advise:

- 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.)
- If passwords need to be documented, use KeePass. This is a password management tool that is used by TCT as a whole, and individual accounts can also be set up.
- Exchange credentials only when absolutely necessary. When exchanging them in-person is not possible, employees should use Teams, text or the phone.
- Change passwords at least every two months.

4. Transfer data securely

Transferring data introduces security risk. Employees must:

- Avoid transferring sensitive data (e.g. customer information, employee records) to other devices or accounts unless absolutely necessary. When mass transfer of such data is needed, the Director of IT must be contacted.
- Share confidential data over the RDS or Sharepoint and not over public Wi-Fi or private connection.
- Ensure that the recipients of the data are properly authorized people or organizations and have adequate security policies.
- Report scams, privacy breaches and hacking attempts

The SMT is responsible for advising employees on how to detect scam emails. We encourage you to reach out to them with any questions or concerns.

The SMT needs 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. The SMT will investigate promptly, resolve the issue and send a companywide alert when necessary.

The Care Trust has a Data Breach Plan to advise on how to proceed in the event of a serious data breach. This can be found in the Appendix of the Data Protection Policy.

Additional measures

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

- Turn off screens and lock devices when leaving the desks
- Report stolen or damaged equipment as soon as possible to the SMT
- Change all account passwords at once when a device is stolen
- Report a perceived threat or possible security weakness in systems
- Refrain from downloading suspicious, unauthorized or illegal software on company equipment
- Avoid accessing suspicious websites

We expect employees to comply with TCT's policy on using email, social media and internet. This can be accessed in the Staff Handbook.

Remote Working

This policy's instructions also apply in full to people working remotely. Since they will be accessing TCT's systems and accounts from a distance, they are obliged to follow all data encryption, protection standards and settings, and ensure the private network is secure.
Disciplinary Action

We expect all our employees and contractors to follow this policy. We will examine each incident on a case-by-case basis but those who cause security breaches may face serious disciplinary action up to and including dismissal, as outlined in the Staff Handbook.