Data Encryption Policy

1 What is encryption?

Encryption is the process of converting information using an algorithm to make the information unreadable to anyone except those possessing the decryption key required.

TCHC GROUP wishes to ensure that its electronically held data is adequately protected from loss and inappropriate access, whether by theft or accident. In addition, the Data Protection Act requires TCHC GROUP to have in place appropriate policies and procedures which provide for the efficient and safe storage of data covered by the Act at all times.

To reduce the risk of unauthorised access, TCHC GROUP has established a comprehensive policy of encrypting data which covers data which is stored on:

- Laptops
- Handheld devices such as Smart Phones and Tablets
- Portable storage devices e.g. memory sticks, external drives
- Removable media e.g. CDs or DVDs, backup tapes

2 Encryption standards

TCHC GROUP has determined that all data stored on portable equipment should be encrypted using a minimum of AES 256-bit encryption. Software and systems to support this have been and continue to be implemented comprehensively.

- The security of TCHC GROUP data is the responsibility of every individual working for TCHC GROUP
- It is incumbent upon the individuals to understand their responsibilities to protect data at all times and to use encryption tools and services to achieve this
- The use of personal equipment to store TCHC GROUP data is strictly prohibited as it is unlikely that the necessary safeguards are in place to protect TCHC GROUP data in line with national guidance

3 Implementation

By default, encryption will be applied to all laptops, so that any data saved will automatically be encrypted. Users will not be asked for specific passwords for individual documents or groups of documents unless they form part of specific departmental work areas.

For portable storage devices, such as memory sticks, encrypted devices will be supplied. These will be encrypted using individual passwords so that their portability is maintained. The use of non-encrypted storage devices is prohibited for all types of data storage.

For removable media such as writeable and readable CDs and DVDs encryption will be applied by prompting the user for a password. Magnetic tapes used for backup can also have their contents encrypted automatically and those provided by TCHC GROUP already do.

Handheld devices including Smart Phones and Tablets will be encrypted using the built in Content Protection facility.

If a handheld device cannot be encrypted:

- It must not be used to store customer/person identifiable data
- It must not be connected to any other TCHC GROUP system, whether by a physical (for example, Ethernet, USB or Firewire cable) or wireless connection (for example infra-red, Bluetooth or 'WiFi')
- Devices which cannot be encrypted should not be used. If possible and cost-effective, any such devices should be replaced.

4 Password management

In general, the password for a device or storage medium allows data to be decrypted. Passwords must be kept confidential and follow the guidelines defined in the Password Policy.

In addition, if the device is used to transfer information, the password must be sent separately so that only the intended recipient has the ability to decrypt the data.

5 Responsibilities

Staff and Contractors who are permitted to use removable devices in the performance of their duties must ensure the data is encrypted in accordance with TCHC GROUP guidance.

The IT Manager is responsible for ensuring that TCHC GROUP has appropriate data encryption capabilities in order to protect data that is processed.

The IT Officers are responsible for assuring that the data encryption functionality and procedures used by TCHC GROUP have been implemented correctly and are of appropriate strength and fit for purpose.

Line Managers are responsible for the day to day management of their staff to ensure policies and procedures are being implemented appropriately.

6 Monitoring Compliance

- Distribution and maintenance of encryption software will be managed by the IT Support Department
- Non- compliant devices may be detected and disabled using management systems installed for this purpose without notice
- Regular monitoring checks will be undertaken to ensure compliance with the criteria set out above
- All incidents or problems must be reported to IT Support.
- Loss of Customer/Personal Identifiable Data is deemed a serious incident and must be reported by the Board of Directors to the Information Commissioner's Office

7 Failure to Comply

Failure to comply with the criteria set out above will be subject to TCHC GROUP's disciplinary policy.

____

Dale Morgan, Chief Executive Officer – TCHC GROUP