Information Security Document

Encryption & Cryptographic Controls Policy

Version 10.0
## Version History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Detail</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>22/10/2010</td>
<td>Completed for distribution</td>
<td>Jo White</td>
</tr>
<tr>
<td>1.0</td>
<td>24/11/2010</td>
<td>Approved by Information Governance Group</td>
<td>Jo White</td>
</tr>
<tr>
<td>2.0</td>
<td>26/05/2011</td>
<td>Reviewed by Information Governance Group</td>
<td>Jo White</td>
</tr>
<tr>
<td>3.0</td>
<td>25/10/2011</td>
<td>Reviewed by Information Governance Group</td>
<td>Jo White</td>
</tr>
<tr>
<td>4.0</td>
<td>28/11/2012</td>
<td>Reviewed by Information Governance Group</td>
<td>Jo White</td>
</tr>
<tr>
<td>5.0</td>
<td>13/01/2014</td>
<td>Reviewed by Information Governance Group</td>
<td>Jo White</td>
</tr>
<tr>
<td>6.0</td>
<td>09/02/2015</td>
<td>Reviewed by Information Governance Group</td>
<td>Jo White</td>
</tr>
<tr>
<td>7.0</td>
<td>11/05/2015</td>
<td>Reviewed by Information Governance Group. Renamed from Encryption Policy.</td>
<td>Jo White</td>
</tr>
<tr>
<td>8.0</td>
<td>13/06/2016</td>
<td>Reviewed by Information Governance Group</td>
<td>Jo White</td>
</tr>
<tr>
<td>9.0</td>
<td>10/07/2017</td>
<td>Reviewed by Information Governance Group. Transformation changed to ICT. Moving of documents from removable storage to network added.</td>
<td>Jo White</td>
</tr>
<tr>
<td>10.0</td>
<td>06/08/2018</td>
<td>Reviewed by Information Governance Group. Clarification of TPM chip added.</td>
<td>Jo White</td>
</tr>
</tbody>
</table>

This document has been prepared using the following ISO27001:2013 standard controls as reference:

<table>
<thead>
<tr>
<th>ISO Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.15.1.2</td>
<td>Addressing security within supplier agreements</td>
</tr>
<tr>
<td>A.8.2.1</td>
<td>Classification of information</td>
</tr>
<tr>
<td>A.8.2.2</td>
<td>Labelling of information</td>
</tr>
<tr>
<td>A.13.1.1</td>
<td>Network controls</td>
</tr>
<tr>
<td>A.8.3.1</td>
<td>Management of removable media</td>
</tr>
<tr>
<td>A.8.3.2</td>
<td>Disposal of media</td>
</tr>
<tr>
<td>A.8.2.3</td>
<td>Handling of assets</td>
</tr>
<tr>
<td>A.13.2.1</td>
<td>Information transfer policies and procedures</td>
</tr>
<tr>
<td>A.13.2.2</td>
<td>Agreements on information transfer</td>
</tr>
<tr>
<td>A.8.3.3</td>
<td>Physical media transfer</td>
</tr>
<tr>
<td>A.13.2.3</td>
<td>Electronic messaging</td>
</tr>
<tr>
<td>A.6.2.1</td>
<td>Mobile device policy</td>
</tr>
<tr>
<td>A.10.1.1</td>
<td>Policy on the use of cryptographic controls</td>
</tr>
<tr>
<td>A.10.1.2</td>
<td>Key management</td>
</tr>
<tr>
<td>A.18.1.5</td>
<td>Regulation of cryptographic controls</td>
</tr>
</tbody>
</table>
1 Introduction
The protection of electronic information and access to storage systems is vitally important - especially with the ever increasing, greater demand on the use of ICT systems across the Council. Protecting person identifiable and business critical information from unauthorised access, disclosure or loss whether by theft or accident is of paramount importance.
A secure, robust ICT infrastructure along with appropriate policies and procedures will help to ensure that wherever possible, all steps have been taken to protect this information.

Cryptographic keys are used in the practise of providing secure keys to enable secure communication in the presence of third parties. They form part of the protocols that block adversaries to ensure confidentiality, integrity and authentication during secure communication.
Cryptographic keys work by converting (encrypting) data to make it inaccessible and unreadable to unauthorised individuals. The only way to read the encrypted data is by using a decryption key.

The Data Protection Act requires the Council to have appropriate policies and procedures in place to ensure the safe keeping, use, retrieval and access to data covered by the Act. The Council has a responsibility to ensure the integrity, security and protection of all data which it holds.

2 Purpose
The purpose of this policy is to:
- Determine the requirements for managing cryptographic keys though their whole lifecycle including generating, storing, archiving, retrieving, distributing, retiring and destroying keys.
- Select cryptographic algorithms, key lengths and usage according to best practice.
- Protect cryptographic keys against modification and loss, unauthorised use or disclosure,
- Ensure equipment used to generate, store and archive keys is physically protected.
- Detail the specification and deployment of data encryption software for the protection of electronic information held by the Council
- Provide guidance on the responsibilities of the use and handling of portable media
- Provide clarity on the types of portable storage and mobile devices which are allowed for use
- Describe how encryption will be used and applied to devices
- Provide guidance on the responsibilities of the use of encrypted devices
- Detail the method of reporting breaches of this policy whether intentional or accidental

3 Scope
This policy covers encryption for the following devices and applications:
- Desktop, laptop, tablet computers
- Handheld devices such as mobile phones and PDAs
- Portable storage devices e.g. USB memory sticks, external drives
- Removable media e.g. floppy disks, DVDs/CDs.
- Email
The Council’s “Internet and E-mail Acceptable Use Policy” provides more general information on the e-mail service and use and is available from the Council’s intranet (Dnet) or by request to the ICT Service Desk.

4 Policy Statement

Full disk encryption will be rolled out gradually to all computers across the Council. The encryption software employed for use at the Council uses the AES 128 bit (Advanced Encryption Standard) which is a symmetric-key encryption with a 128 bit key.

4.1 Application

Full disk encryption will be rolled out to all computers by the ICT Service as part of desktop upgrades via the build process.

- The build process checks the make and model against a list of machines.
- If the device has a Trusted Platform Module (TPM) chip on board, it checks to see if they are available
  - If a TPM chip is not on-board the build continues with encryption being implemented and USB key containing the encryption Key is created.
- If the TPM chip is available the build process will enable the TPM and start the encryption process.
  - A random key is generated by the TPM chip
- As part of the process the relevant cryptographic key will be written back to the Active Directory.
  - If for some reason the network is unavailable, this will not write back to the Active Directory
  - Remediation techniques will be run on machines that have not written their keys back to Active Directory to force them to do this.
- Access to the list of the keys in the Active Directory is restricted to senior level team members within the Server Management Team and Desktop Management Team.
- Relevant keys for a machine can be obtained from the Active Directory through formal application to the Server Team where a senior level member of the team will review the request.

Council data should not be stored on computers or portable media devices unless access is required when network connectivity is not available. When it is necessary restricted and controlled data should only be stored on encrypted devices.

Where exceptions have been identified for not encrypting specific devices, computer policy settings (enforced at domain level) which enable/disable encryption can be applied individually to a specified computer and/or groups of computers.

When a portable, Council recommended, data storage device is used, the instructions for the correct use must be followed to ensure the data is encrypted.

Personal storage media and equipment must not be connected to the Council’s network and must not be used to store Council data.

Other portable USB devices include mobile phones, cameras, PDAs etc. These other devices should not be used to store Council data. Data collected as part of their use should be transferred to the appropriate system at the earliest opportunity.
If clarification is needed as to the recommended USB data storage devices allowed for use, the ICT Service Desk should be contacted.

The ICT Service Desk will advise on the best method to encrypt individual files.

4.2 Method

On encryption of portable storage device (e.g. USB data stick) the user will need to set a password for accessing the device. The password for encrypted portable devices must be in line with the Council’s password policy and be enforced at the domain level. Using the portable device on any other computer after being encrypted will require a password in order to access it. It is important that local procedures are put in place to ensure that passwords used to encrypt devices are approved by line managers, so that in the event an individual leaves the Council access can be gained to the Council’s data. In the event that local procedures for the creation of encryption passwords have not been followed, employees may be asked to provide details of encryption passwords used on all such portable devices. Under no circumstances should network or other IT system passwords be disclosed to anyone including the ICT Service.

The use of DVD/CD devices and floppy drives will be restricted to read-only access – this will be enforced at the domain level by Group Policy. Where there is a need for a particular job function requiring write access to CD/DVD or floppy drives, this can be enabled as an exception and recorded formally with agreement from the ICT Service. Any agreement to allow write access of CD/DVD or floppy devices will include the conditional use of appropriate 3rd party archiving (zip) compression/encryption software to be used to encrypt any data stored or written to these devices. This conditional encryption/compression software will be made available as recommended by the ICT Service.

Any other requirement for portable storage device such as portable hard drives, magnetic/DAT tapes and devices must be discussed with the ICT Service and only hardware and software on the Council’s approved software and hardware list is to be used.

Computers requiring encryption for the protection of vulnerable and sensitive data will use Windows Bitlocker encryption.

5 Responsibilities

The Council has a responsibility to provide its employees with the appropriate secure storage mechanisms, procedures devices and software for the secure handling, storage and retrieval of all electronic data held by the Council. The use of portable devices may be subject to random periodic review by the Council to ensure compliance with the encryption policy.

All Council employees, elected members, volunteers, partner agencies, contractors and vendors have a duty to abide by all Council policies and procedures to ensure the safe, secure handling of all electronic data.

5.1 Use of portable storage media and devices

Council employees, elected members, volunteers, partner agencies, contractors and vendors undertaking work for the Council who are issued with portable storage
devices, writing to portable storage media, viewing / transmitting encrypted data or accessing have a responsibility to ensure:

- No one other than authorised person/s are aware of the encryption/decryption password for the device, media or system.
- Any portable device or media is not given to any unauthorised persons for safe keeping
- Any portable device or media is not left discarded or unattended in a public place
- All reasonable steps are taken to ensure that during transit, any portable device/media is locked via a key or combination lock and securely located. Portable devices/media must not be left unattended in any vehicle at any time due to insurance requirements
- Any portable device or media is adequately protected from physical damage
- Any portable device or media is not hired, lent out or given without authorisation from line managers who are required to ensure that procedures are in place to retrieve the device and sharing agreements are in place for the data held on such devices.
- Any portable device or media which is no longer required or has reached its lifespan must be handed over to the ICT Service. All data on the device / media must be wiped, destroyed and disposed of through the Council’s ICT disposal procedure
- The device / media is handed back to your line manager or the ICT Service on cessation of employment with the Council
- The device / media is handed back to your line manager or the ICT Service when no longer authorised to use the device / media
- The loss of any portable device is notified immediately via the Council’s Security Incident Management procedure.

6 Breaches of Policy

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to Council assets, or an event which is in breach of the Council’s security procedures and policies. All Council employees, elected members, volunteers, partner agencies, contractors and vendors have a responsibility to report security incidents and breaches of this policy as quickly as possible through the Council’s Incident Reporting Procedure. This obligation also extends to any external organisation contracted to support or access the Information Systems of the Council.

In the case of third party vendors, consultants or contractors non-compliance could result in the immediate removal of access to the system. If damage or compromise of the Council’s ICT systems or network results from the non-compliance, the Council will consider legal action against the third party. The Council will take appropriate measures to remedy any breach of the policy through the relevant frameworks in place. In the case of an employee then the matter may be dealt with under the Council’s disciplinary process.

This document is owned by the Information Governance Group and forms part of the Council’s ISMS Policy and as such, must be fully complied with.