Information Security Document

Operational Management Policy

Version 10.0

Version	Date	Detail	Author
1.0	27/07/2011	Completed for distribution	Jo White
1.0	24/08/2011	Approved by Information Governance Group	Jo White
2.0	31/10/2012	Reviewed by Information Governance Group	Jo White
3.0	29/11/2013	Reviewed by Information Governance Group. No changes.	Jo White
4.0	16/12/2014	Reviewed by Information Governance Group. Updated with ISO27001:2013 controls.	Jo White
5.0	08/02/2016	Reviewed by Information Governance Group. Date and time added to audit logging, also secure disposal of test data.	Jo White
6.0	06/03/2017	Reviewed by Information Governance Group.	Jo White
7.0	08/05/2018	Reviewed by Information Governance Group.	Jo White
8.0	10/06/2019	Reviewed by Information Governance Group. All links reviewed and updated.	Jo White
9.0	14/07/2020	Reviewed by Information Governance Group. Links updated. Addition of risk assessment advice and use of Password Manager.	Jo White
10.0	10/08/2021	Reviewed by Information Governance Group. No changes.	Jo White

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

ISO Control	Description
12.1.1	Documented operating procedures
8.1, A.12.1.2	Responsibility for assets/Change management
6.1.2	Segregation of duties
12.1.4	Separation of development, testing and operational environments
12.1.3	Capacity management
14.2.9	System acceptance testing
12.2.1	Controls against malware
12.3.1	Information back-up
13.1.1	Network controls
8.3.1	Management of removable media
8.3.2	Disposal of media
13.2.1	Information transfer policies and procedures

1 Introduction

Derbyshire County Council's implementation of an Information Security Management System (ISMS) is essential to ensuring the security, confidentiality, integrity and protection of data, information and ICT systems.

2 Purpose

The purpose of this policy is to detail the requirements for the correct and secure use of the Council's information processing facilities with the aim of ensuring the protection of information and data through the implementation of an effective ISMS (Information Systems Management System) in accordance with the ISO 27001 standard and to maintain certification of this standard. The ISO 27001 standard covers all aspects of data and information security.

3 Scope

This scope of this policy extends to all departments, employees, elected members, contractors, vendors and partner agencies who utilise or who are responsible for the development, management/maintenance of information within the Council's ICT processing facilities.

4 Policy Statement

Maintaining and managing the Council's ICT data and information processing facilities requires a comprehensive and robust policy. The ISO 27001 Information Security Management System (ISMS) standard process provides the Council with a framework and methodology which enables a focused and structured approach to achieving this.

All policies and procedures outlined in the Council's Information Security policy and ratified by the Council's Information Governance Group must be referred to and adopted by all departments to establish and maintain professional good working practices and procedures for the management of an effective ISMS - vital to counter threats to the availability, integrity and confidentiality of the Council's data and information.

There are a number of controls which must be in place if the Council is to achieve this:

4.1 Documentation

All Council operating procedures and system processes outlined in the Council's IT Security Policy must be documented:

Operating procedures must be documented to an appropriate level of detail for individuals/departments using them and should include the following areas:

- Processing and handling of information (information classification, confidentiality requirements): https://staff.derbyshire.gov.uk/document-classification
- Backup procedures - Information Backup and Restore Policy: https://staff.derbyshire.gov.uk/hardware
- Work scheduling requirements (considering interdependencies, completion times etc)
- Instructions and guidance for handling errors

- Contact and reporting details in the event of unexpected operational issues
- Procedures for handling special outputs (e.g. special stationery like cheques, payslips)
- System restart and recovery procedures in the event of system failure
- Procedures for all 'housekeeping' functions
- Procedures for audit and assurance reviews

4.2 Change Control (Management)

Changes to the ICT infrastructure must only be undertaken by authorised personnel working in an IT function/capacity (or contractors, vendors etc., authorised by the Council) and are subject to auditable change management procedures in accordance with the Council's Information Systems Development and Maintenance Procedures: https://staff.derbyshire.gov.uk/software and Financial Regulations:

Changes to the Council's ICT infrastructure and operational systems must be controlled with a formal, documented change control procedure. The change control procedure should include references to:

- A description and reason for the change
- Information about any testing phase(s)
- Impact assessment including security, operational etc…
- Formal approval process – managerial approval and authorisation prior to proceeding with changes which may have a significant impact
- Communication to all relevant people of the changes which includes:
    - Advance communication/warning of changes
    - Proposed schedules
    - Description of reasonably anticipated outcomes provided to all relevant personnel
- Procedures for aborting and rolling back if problems occur
- Processes for planning and testing of changes, including fall-back (abort/recovery) measures
- Documentation of changes made and all the steps taken in the change management process
- Identification of significant changes and relevant risk assessments - including analysis of any potential impact and necessary countermeasures or mitigation controls

All changes to the ICT infrastructure need to be assessed for impact on the security of data and information as part of standard risk assessments

4.3 Separation of Development, Test and Operational Facilities

Development and test environments must be separated from live operational environments in order to reduce the risk of accidental changes, configuration/data incompatibilities and unauthorised access. Development and live environments must be segregated by the most appropriate controls including:

- Running on separate computer/systems
- Running on different domains
- Secure disposal of data/information used in the test environments
- Use of test/temporary usernames and passwords
- Access control procedures which apply to operational systems should also apply to test applications

In addition, a risk assessment should be undertaken in instances where 'real' personal, sensitive and special category data is used in a test environment. Such development facilities may not be subject to the full security features inherent in the live/production system and thus put such test data at an increased risk of unauthorised access.

Where practical, separation of duties should be maintained to ensure no one individual can gain unacceptably high levels of access to the Council's ICT systems and information processing facilities.

4.4 Capacity Management

ICT Services must monitor the capacity demands of the Council's systems and make projections of future capacity requirements so that adequate power and data storage requirements can be fulfilled.

Utilisation of key system resources must be monitored so that additional capacity can be brought on line when required.
These include:

- File/storage servers
- Domain/Network infrastructure devices and equipment
- E-mail/web servers
- Printers – managed by the Business Centre

Increases in Council business activities and staffing levels must be monitored by departments to inform ICT Services of any extra facilities which may be required e.g. number of available workstations etc.

4.5 System Acceptance

All departments must inform ICT Services, via the Service Desk, of any new software requirements or of any upgrades, service packs, patches or fixes required. Appropriate levels of testing must be undertaken for new ICT systems, product upgrades, patches and fixes prior to acceptance and release into a live environment. The acceptance criteria must be clearly identified, agreed and documented and should involve appropriate levels of authorisation.

Software must be monitored for service packs, updates and patches which should be tested and applied as soon as possible when released and once it has been approved by the Change Advisory Board (CAB). Major system upgrades must be thoroughly tested in parallel with the existing system in a safe test environment which duplicates the 'live' operational system.

4.6 Patching

All security based service packs, patches and fixes supplied by 3rd party software vendors should be applied as soon as they become available. In the event that this is not possible these systems will be placed on the respective risk register.

All Council ICT system servers must have critical security patches applied as soon as they become available. All other patches and updates must be applied as appropriate. There must be a full record of which patches have been applied and when. More information is available in the Council's Server Security Policy https://staff.derbyshire.gov.uk/hardware

4.7 Protection against Malicious and Mobile Code

The security and integrity of the Council's information and data, including all software applications, must be protected from malicious software (malware). Appropriate controls and user awareness procedures must be put in place to ensure the Council is protected.

4.8 Controls against Malicious Code

Antimalware/Antivirus software must be installed and maintained on all workstations and servers and any other computing device which uses software to function and is capable of being scanned by Antimalware/Antivirus software. The software must be from an established vendor with consistent results in recognising and removing all types of malware. All updates must be installed as soon as they are available. Any unauthorised files or software must be formally investigated and deleted as appropriate.
To protect systems from malware, users must not:

- Install software from any external source including the internet, CD / DVD-ROMs, USB memory sticks, etc on their workstation.
- Add their own screensavers, desktop images, photos or utilities to the workstation.

All software must be approved and installed by ICT Services. Software must also be controlled to ensure compliance with licensing and other legal requirements.

Malware and viruses can be introduced through emails and users must be vigilant and follow the Council's guidelines on dealing with suspicious emails and attachments. If there is uncertainty with the safety of particular emails or attachments, the ICT Service Desk should be contacted on extension 37777.

The Council must ensure that all email and attachments are checked for malware and viruses at the point of entry into the network.

More information is available in:

- the Council's Malicious Software and Antivirus Procedures: https://staff.derbyshire.gov.uk/hardware

- Internet, Email and Social Media Acceptable Use Policy: https://staff.derbyshire.gov.uk/internet-email

4.9 Controls against Mobile Code

Mobile code is often found in web pages including:

- ActiveX
- Java
- JavaScript
- VBScript
- MSWord Macros

Certain websites rely on the use of these scripts which either run automatically or via user interaction with the site. The Council must protect its users and computers as much as reasonably possible by ensuring that, wherever possible, users are warned of the script to be run and by blocking connections and/or scripts to known 'bad' or harmful websites.

Mobile code must be prevented from entering the network, with the exception of web sites that have been approved for use after the risk of the site has been assessed. Controls must be in place for the protection of all Council computers from harmful and unwanted running of mobile code.

4.10 Back-ups

The Council must ensure that regular backups of information, data and ICT systems configuration are routinely carried out to ensure the Council can recover from unforeseen events, system failure, accidental or deliberate loss of information or facilities - in line with Disaster Recovery Procedures.

All backup routines must be fully documented as described in the Council's Information Backup and Restore Policy:
https://staff.derbyshire.gov.uk/hardware

To ensure all information and data is backed up, all employees must store their work on the network drive areas provided by ICT Services and not stored 'locally' on computer drives e.g. C: drive. The exception to this is during a loss of network connectivity when data must be temporarily stored locally until the network becomes available again. All users of portable devices e.g. laptops, PDA's, smart phones and USB memory sticks must ensure that data is not permanently stored on these devices and must transfer the data to the Council network – more information on this is available in the Council's Desktop and Mobile Device Procedures:
https://staff.derbyshire.gov.uk/mobile-working

All 3rd party/software vendors hosting or supplying services/facilities containing or handling Council information and data must ensure appropriate, secure backup routines and facilitate access for the Council's internal audit requirements when necessary - confirmation of this should be provided during the tender process.

Full back-up documentation including a complete record of what has been backed up along with the recovery procedure must be stored at an off-site location in addition to the copy at the main site. This must also be accompanied by an appropriate set of media tapes and stored in a secure area. The off-site location must be sufficiently remote to avoid being affected by any disaster which may take place at the main site.

Critical paper files must be identified and backed up with either a scanned digital copy or complete photocopies stored at a remote location.

4.11 Restores

Full documentation of the recovery procedure must be created and stored. Regular restores of information from backup media must be carried out and tested to ensure the reliability of the backup media and restore process.

Retention periods for information and data must be defined in accordance with agreed Council retention schedules and applied to the backup schedule planning. Long term backup and restore solutions need to be identified and applied wherever necessary.

More Information is available in the Council's Back-up and Restore procedures.

4.12 Media Handling

Removable media such as USB data sticks, CD/DVDs, magnetic tapes, external hard drives etc., must be protected to prevent damage, theft or unauthorised access. Documented procedures must be in place for backup tapes that are removed on a regular rotation from Council buildings. Backup media must be kept in a secure environment e.g. a fireproof safe in a lockable room/area. Appropriate arrangements must be put in place to ensure future availability of data that is required beyond the lifetime of the backup media.
The Council's Corporate Digital Preservation Policy provides more information: https://staff.derbyshire.gov.uk/at-work

Media being transported must be protected from unauthorised access, misuse or corruption. Where couriers are required a list of reliable and trusted couriers should be established. If appropriate, physical controls should also be used e.g. encryption or special locked containers for the secure transfer of Information.

4.13 Disposal of Media

Media which is no longer required must be disposed of safely and securely. Media containing sensitive or person identifiable information must be disposed of appropriately in accordance with all existing Council disposal procedures: https://staff.derbyshire.gov.uk/at-work

Items that should be considered for secure disposal include:

- Paper documents
- Voice or other recordings
- Magnetic tapes
- Removable disks
- USB Memory sticks
- CD/DVD ROMs

All media for disposal must be completely erased using methods which eliminates the possibility of data recovery and reconstruction from devices or media.

ICT Services must be contacted for the secure disposal of ICT media and devices.

4.14 Security of System Documentation

All ICT system documentation must be protected from unauthorised access. This includes documentation that has been created by ICT Services or any other departmental IT employees (this does not include manuals that have been supplied with software). Examples of the documentation to be protected include descriptions of:

- Applications
- Processes
- Procedures
- Data structures
- Authorisation details

4.15 Information Exchange Policies and Procedures

Procedures and processes must be in place to protect the exchange of information using all methods and formats e.g. email, letter and fax etc.

Procedures must be designed to protect exchanged information against:

- Interception
- Copying
- Modification
- Mis-routing
- Destruction

Information and data must be protected with appropriate controls based on the information's classification e.g. Confidential.

Formal agreements for the exchange of information between the Council and external organisations must be made and reviewed on a regular basis.

4.16 Audit Logging

ICT system audit logs must be kept for a minimum of six months which record exceptions and other security related events. As a minimum, audit logs must contain the following information:

- Date and time of activity
- Details of data before and after an update
- System identity or IP address (*Workstation name*)
- User ID (*employee number*) and user name
- Successful/Unsuccessful login
- Successful/Unsuccessful logoff
- Unauthorised application access
- Changes to system configurations
- Use of privileged accounts (e.g. account management, policy changes, device configuration). In addition, access to the privileged accounts should always be controlled via Password Manager Pro (PMP).

Access to the logs must be protected from unauthorised access that could result in recorded information being altered or deleted. System administrators must be prevented from erasing or deactivating logs of their own activity. Access to logs should be provided for the Council's internal audit requirements upon request.

Operational staff and system administrators must maintain a log of their activities. The logs should include:

- Back-up timings and details of exchange of backup tapes
- System event start and finish times and who was involved
- System errors (what, date, time) and corrective action taken

The logs should be checked regularly to ensure that the correct procedures are being followed.

4.17 Network Security Management

The management and security of the data and communications network is critical to ensuring the integrity and security of the Council's systems and data. The following controls must be applied:

- Operational responsibility for networks should, wherever possible, be separated from computer operations activities

- There must be clear responsibilities and procedures for the management of remote equipment and users
- Where appropriate, controls must be put in place to protect data passing over the network e.g. encryption

The network architecture must be documented and stored with configuration settings of all the hardware and software components that make up the network.

Wireless networks must apply controls to protect data passing over the network and prevent unauthorised access. Encryption must be used on the network to protect information and data and to prevent information being intercepted.

5 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, 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.

The Council will take appropriate measures to remedy any breach of the policy and its associated procedures and guidelines through the relevant frameworks in place. Where it becomes apparent that there may have been a breach of this policy by an employee then the matter may be dealt with under the 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.