Sefton Council

Information Security Policy

Chapter 9

Communications and Operations Management Policy

Author:	Policy & Strategy Team
Version:	0.2
Date:	February 2008

Document Control Information	
Document ID	
Document title	Communications and Operations Management Policy
Version	0.2
Status	Draft
Author	D. Windel
Job title	Policy & Strategy Manager
Department	Information Services
Publication date	
Approved by	
Next review date	
Distribution	

Contents

1. Communications and Operations Management Policy

1.1. Overview

This policy covers the key areas in day to day operations management of the Council's IT services. The policy covers topics that include: protection of the service against malware e.g. viruses and Trojans, unauthorised changes and information leakage.

This policy applies in the majority to IT Support staff with the exception of sections 1.6.2. and 1.8. that have elements that apply to all employees across the Council.

1.2. Policy Statement

All Sefton Council employees, contractors and users with access to Sefton Council's equipment and information (in any format including electronic and paper records) are responsible for ensuring the safety and security of the Council's systems and the information that they use or manipulate.

1.3. Scope of this Policy

This policy applies to all users of the Council's facilities and equipment including staff and any third party suppliers and contractors. All users have a role to play and a contribution to make to the safe and secure use of technology and the information that it holds.

1.4. Operational Procedures and Responsibilities

1.4.1. Documented Operating Procedures

Operating procedures must be documented to an appropriate level of details for the departmental team that will be using them. The procedures must include procedures and work instructions for the following areas:

- Processing and handling of information (information classification, confidentiality requirements)
- Backup procedures (see Section 1.8)
- 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

1.4.2. Change Management

Changes to the Council's operational systems must be controlled with a formally documented change control procedure. The change control procedure should include references to:

- A description of the change and business reasons
- Information concerning the testing phase
- Impact assessment including security, operational etc
- Formal approval process
- Communication to all relevant people of the changes
- Procedures for aborting and rolling back if problems occur

All significant changes to the main infrastructure (e.g. Network, Directories) need to be assessed for their impact on information security as part of the standard risk assessment.

1.4.3. Separation of Development, Test and Operational Facilities

The development and test environments must be separate from the live operational environment to reduce the risk of accidental changes or unauthorised access. The environments must be segregated by the most appropriate controls including:

- Running on separate computers
- Running on different domains
- Different usernames and passwords

1.5. System Planning and Acceptance

1.5.1. Capacity Management

Information 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 servers
- Domain servers
- E-mail servers
- Web servers
- Printers

Increases in business activities and staffing levels must also be monitored to allow for the extra facilities that will be required for example numbers of workstations.

1.5.2. System Acceptance

All departments must inform Information Services via the Helpdesk of any new product requirements or of any upgrades, service packs, patches or fixes required to existing systems (Information Services will also monitor these areas).

New information systems, product upgrades, patches and fixes all must undergo an appropriate level of testing prior to acceptance and release into the live environment. The acceptance criteria must be clearly identified, agreed and documented and should involve management authorisation.

3rd party applications must be monitored for service packs and patches. These should be tested and applied as soon as possible after release once confirmed to not negatively impact the application.

Major system upgrades must be thoroughly tested in parallel with the existing system in a safe test environment that duplicates the operational system.

1.6. Protection against Malicious and Mobile Code

The Council's information and the integrity of its software applications must be protected from malicious software (malware). Appropriate controls and user awareness procedures must be put in place to ensure this protection.

1.6.1. Patching

All vendor supplied service packs, patches and fixes must be applied as soon as they become available and have passed the system acceptance testing on web servers in the DMZ environment.

All other servers must have critical security patches applied as soon as they become available and have passed the system acceptance testing. All other patches must be applied as appropriate. There must be a full record of which patches have been applied and when.

1.6.2. Controls against Malicious Code

Anti malware software must be installed and maintained on all workstations and servers and provided on appropriate points on the network. The software must be from an established vendor with consistent results in recognising and removing malware. All updates must be installed as soon as they are available.

A regular review of all business critical systems must be conducted to identify all software running on the systems. Any unauthorised files or software must be formally investigated and if appropriate deleted.

To protect systems from malware users must not:

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

All workstation software must be approved and installed by Information Services. Software must also be controlled to ensure compliance with licensing requirements (see Chapter 2 - Compliance).

Malware can be introduced through hoax emails and users must be vigilant to guard against this. Users must not forward emails that claim to be warnings these are often chain emails (see Chapter 5 - Email Policy). Users must report the email to the Information Services Helpdesk on ext. 4999.

All email attachments should be checked for malware at the point of entry onto the network.

1.6.3. Controls against Mobile Code

Mobile code represents newer technologies often found in web pages including:

- ActiveX
- Java
- JavaScript
- VBScript
- MSWord Macros

Mobile code must be prevented from entering the network with the exception of for web sites that have been approved for use after a risk assessment. Controls must also be put in place on the workstation to prevent this code from running by default.

1.7. Back Up

1.7.1. Information Back Up

Regular backups of essential business information must be taken to ensure that the Council can recover from a disaster, media failure or error. An appropriate backup cycle must be used and fully documented.

To ensure all essential business information is backed up all employees must store their information on the network drives and not on local drives e.g. C: drive. All users of portable devices for example laptops, PDA's, smart phones and USB memory sticks must ensure the information is also stored on the network drives. For details of network drives see http://intranet.sefton.gov.uk/docs/Brief%20description%20of%20drive%20letters%20V0.5.doc.

Any 3rd parties that store Council information must also be required to ensure that the information is backed up.

Full backup 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 remote location must be sufficiently remote to avoid being affected by any disaster that takes 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.

1.7.2. Information Restore

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

The retention period for business information (in particular legal requirements) must be defined and applied to the backup data. Long term backup and restore solutions may need to be identified for certain business information.

1.8. Media Handling

1.8.1. Management of Removable Media

Removable computer media e.g. tapes, disks, cassettes and printed reports must be protected to prevent damage, theft or unauthorised access.

Documented procedures must be kept for backup tapes that are removed on a regular rotation from Council buildings. Media stores must be kept in a secure environment e.g. a fireproof safe. Appropriate arrangements must be put in place to ensure future availability of data that is required beyond the lifetime of the backup media.

1.8.2. Physical Media in Transit

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. (see Appendix B – Secure Transfer of Information).

1.8.3. Disposal of Media

Media that is no longer required must be disposed of safely and securely to avoid data leakage. Media containing personal or sensitive information must be disposed of through the confidential waste bins provided. 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

Any previous contents of any reusable media that are to be removed from the Council must be erased. This must be a thorough removal of all data from the media to avoid the potential of data leakage.

Please contact the Data Protection Officer on ext 4416 for any further advice on disposal of these type of items.

1.8.4. Security of System Documentation

System documentation must be protected from unauthorised access. This includes bespoke documentation that has been created by Information Services or any other departmental IT staff (not general manuals that have been supplied with software). Examples of the documentation to be protected include descriptions of:

- Applications
- Processes

- Procedures
- Data structures
- Authorisation details

1.9. Exchange of Information

1.9.1. Information Exchange Policies and Procedures

Procedures and protocols must be in place that protects the exchange of information through any format e.g. email, letter and fax (Also see Appendix A - Mobile Devices Acceptable Use Policy and Appendix B - Secure Transfer of Information Policy).

The procedures must be designed to protect exchanged information from:

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

Information must be protected with appropriate controls based on the information's classification e.g. Confidential. (see Asset Management Policy – Chapter 12).

1.9.2. Exchange Agreements

Formal agreements for the exchange of information between the Council and external organisations must be in place. The agreement must detail the classification of the information being exchanged and the controls to be applied to protect it.

1.10. Monitoring

1.10.1. Audit Logging

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:

- System identity
- User ID
- 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)

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.

1.10.2. Administrator and Operator Logs

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.

1.10.3. Clock Synchronisation

All computer clocks must be synchronised to ensure the accuracy of all the systems audit logs as they may be needed for incident investigation.

1.11. Network Security Management

1.11.1. Network Controls

Network management is critical to the provision of Council services and must apply the following controls:

- Operational responsibility for networks should, where possible be separate 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.

1.11.2. Wireless Networks

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

1.12. Policy Compliance

If you are found to have breached this policy, you may be subject to the Council’s disciplinary procedure.
If you have broken the law, you may be subject to prosecution.
If you do not understand the implications of this policy or how it may apply to you, seek advice from Information Services via the Helpdesk.