Policy Document

Communications and Operation Management Policy

[23/08/2011]

Document Control

Organisation	Redditch Borough Council
Title	Communications and Operation Management Policy
Author	Mark Hanwell
Filename	Communications and Operation Management Policy.doc
Owner	Mark Hanwell – ICT Transformation Manager
Subject	Communications and Operation Management Policy
Protective Marking	Unclassified
Review date	23/08/2011

Revision History

Revision Date	Revisor	Previous Version	Description of Revision

Document Approvals

This document requires the following approvals:

Sponsor Approval	Name	Date
Head of Business Transformation	Deborah Poole	23rd August 2011

Document Distribution

This document will be distributed to:

Name	Job Title	Email Address

Contents

1 Policy Statement

Redditch Borough Council will ensure the protection of the Council IT service (including any information systems and information processing equipment used by the Council) against malware and malicious and mobile code.

Only authorised changes will be made to the Council IT service (including any information systems and information processing equipment).

Information leakage will be prevented by secure controls.

2 Purpose

This policy covers the key areas in day to day operations management of the Council's IT services.

This policy exists to protect the information and IT Infrastructure owned by Redditch Borough Council and to ensure people are aware of any restrictions in their use.

3 Scope

This policy applies to all Redditch Borough Council Councillors, Committees, Departments, Partners, Employees of the Council, contractual third parties and agents of the Council with access to Redditch Borough Council's IT facilities and equipment. 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.

4 Definition

This policy should be applied whenever users access Redditch Borough Council's IT facilities and equipment, and especially when managing, developing, configuring or maintaining Redditch Borough Council's IT facilities and equipment.

Local procedures, standards and work instructions may be defined in the appendices to allow flexibility of organisational practices. This policy provides a minimum requirement to be met under nationally recognised standards.

5 Risks

Redditch Borough Council recognises that there are risks associated with users accessing and handling information in order to conduct official Council business.

This policy aims to mitigate the following risks:

- The non-reporting of information security incidents, inadequate destruction of data, the loss of direct control of user access to information systems and facilities etc.].
    - Malware and malicious and mobile code.
    - Information leakage.
    - Un-authorised changes

6 Applying the Policy

6.1 Operational Procedures and Responsibilities

6.1.1 Documented Operating Procedures

Operating procedures are used in all day to day maintenance of Redditch Borough Council IT systems and infrastructure in order to ensure the highest possible service from these assets. These operating procedures must be documented to an appropriate level of detail for the departmental team that will be using them.

6.1.2 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, operations and risk.
- Formal approval process.
- Communication to all relevant people of the changes.
- Procedures for aborting and rolling back if problems occur.
- Process for tracking and audit.

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.

6.1.3 Separation of Development, Test and Operational Facilities[1]

- The development and test environments will be separate from the live operational environment to reduce the risk of accidental changes or unauthorised access.

6.2 System Planning and Acceptance

6.2.1 Capacity Planning

All Redditch Borough Council IT infrastructure components or facilities are covered by capacity planning and replacement strategies to ensure that increased power and data storage requirements can be addressed and fulfilled in a timely manner.

Key IT infrastructure components include, but are not restricted to, the following:

- File servers.
- Domain servers.
- E-mail servers.
- Web servers.
- Printers.
- Networks.
- Environmental controls including air conditioning.

[1] This should include reference to authorisation levels and references to 3rd party capabilities

6.2.2 System Acceptance

All departments must inform ICT via the Helpdesk of any new product requirements or of any upgrades, service packs, patches or fixes required to existing systems. All new products must be purchased through the ICT.

New information systems, product upgrades, patches and fixes must all 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 also be monitored for service packs and patches.

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

6.3 Protection against Malicious and Mobile Code

Appropriate steps are taken to protect all Redditch Borough Council IT systems, infrastructure and information against malicious code. Effective and up-to-date anti-virus software is run on all servers and PCs. Redditch Borough Council staff are responsible for ensuring that they do not introduce malicious code into Redditch Borough Council IT systems – as stated within the Software Policy.

Where a virus is detected on a Redditch Borough Council system, the individual must contact the ICT Helpdesk.

6.3.1 Patching

All servers must have appropriate 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. Patches must be applied to all software on the Council network where appropriate.

Unpatchable software must not be used where there is a GCSx connection provided.

There must be a full record of which patches have been applied and when.

6.3.2 Controls against Malicious and Mobile Code

In order to prevent malicious and mobile code, appropriate access controls (e.g. administration / user rights) shall be put in place to prevent installation of software by all users.

Requests for software installation shall only be accepted where there is a clear technical verification.

Anti-malware software will be installed on appropriate points on the network and on hosts.

6.3.3 Examples of Malicious and Mobile Code

Mobile code represents newer technologies often found in web pages and emails, and includes, but is not limited to:

- ActiveX.
- Java.
- JavaScript.
- VBScript.
- Macros.
- HTTPS.
- HTML.

6.4 Backups

6.4.1 Information Backup

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.
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 and be readily accessible. 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.

6.4.2 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 and this should comply with the agreed change management process.

6.5 Storage Media Handling

Storage media includes, but is not restricted, to the following:

- Computer Hard Drives (both internal and external).
- CDs.
- DVDs.
- Optical Disks
- USB Memory Sticks
- Media Card Readers.
- MP3 Players.
- Digital Cameras.
- Backup Cassettes.
- Audio Tapes (including Dictaphones and Answering Machines).

6.5.1 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. Appropriate arrangements

must be put in place to ensure future availability of data that is required beyond the lifetime of the backup media.

For further information, please refer to Removable Media Policy.

6.5.2 Physical Storage Media in Transit

Storage 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 such as encryption or special locked containers should also be used.

For further information, please refer to Removable Media Policy.

6.5.3 Disposal of Storage Media

Storage media that is no longer required must be disposed of safely and securely to avoid data leakage.

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

For further information, please refer to Removable Media Policy.

6.5.4 Security of System Documentation

System documentation must be protected from unauthorised access. This includes bespoke documentation that has been created by ICT staff. This does not include generic manuals that have been supplied with software. Examples of the documentation to be protected include, but are not restricted to, descriptions of:

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

Effective version control should be applied to all documentation and documentation storage.

6.6 Monitoring

6.6.1 Audit Logging for Restricted Data and GCSx Services

Audit logs must be kept for a minimum of six months which record exceptions and other security related events[2]. As a minimum audit logs must contain the following information:

- System identity.
- User ID.
- Successful/Unsuccessful login.
- Successful/Unsuccessful logoff.

[2] It is good practice to keep all audit logs for 6 months

- 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.
Where appropriate, classified data should be stored separately from non-classified data. Data sent or received via GCSx must be stored separately from non-classified data.

6.6.2 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.

6.6.3 Clock Synchronisation

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

6.7 Network Management

6.7.1 Network Controls

Connections to the Redditch Borough Council network infrastructure are made in a controlled manner. 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 (please refer to the Remote Working Policy and Removable Media Policy).
- 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. All components of the network should be recorded in an asset register.

All hosts must be security hardened to an appropriate level. Operating systems will have their network services reviewed, and those services that are not required will be disabled.

6.7.2 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. WPA2 should be applied as a minimum.

6.8 Systems Development and Maintenance

6.8.1 Protection of System Test Data

If personal information is used during the development and test phase of preparing application software it must be protected and controlled in line with the Data Protection Act (please refer to the Legal Responsibilities Policy) and where possible depersonalised. If operational data is used controls must be used including, but not limited to, the following:

- An authorisation process.
- Removal of all operational data from the test system after use.
- Full audit trail of related activities.
- Any personal or confidential information must be protected as if it were live data.

6.9 Annual Health Check

An annual health check of all Council IT infrastructure systems and facilities must be undertaken by ICT every 12 months. This health check must include, but is not restricted to, the following:

- A full penetration test.
- A network summary that will identify all IP addressable devices.
- Network analysis, including exploitable switches and gateways.
- Vulnerability analysis, including patch levels, poor passwords and services used.
- Exploitation analysis.
- A summary report with recommendations for improvement.

7 Policy Compliance

If any user is found to have breached this policy, they may be subject to Redditch Borough Council's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from ICT via the Helpdesk.

8 Policy Governance

The following table identifies who within Redditch Borough Council is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	ICT Transformation Manager
Accountable	Head of Business Transformation

Consulted	Corporate Management Team
Informed	All Council employees, councillors, all temporary staff, all contractors etc

9 Review and Revision

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

Policy review will be undertaken by ICT Transformation Manager.

10 References

The following Redditch Borough Council policy documents are directly relevant to this policy, and are referenced within this document:

- Software Policy.
- Remote Working Policy.
- Removable Media Policy.
- Legal Responsibilities Policy.
- IT Infrastructure Policy.

The following Redditch Borough Council policy documents are indirectly relevant to this policy:

- Email Policy.
- Internet Acceptable Usage Policy.
- GCSx Acceptable Usage Policy and Personal Commitment Statement.
- IT Access Policy.
- Computer, Telephone and Desk Use Policy.
- Information Protection Policy.
- Human Resources Information Security Standards.
- Information Security Incident Management Policy.

11 Key Messages

- Changes to the Council's operating systems must be follow the Council's formal change control procedure.
- Unpatchable software must not be used where there is GCSx connection provided.
- Appropriate access controls shall be put in place to prevent user installation of software and to protect against malicious and mobile code.
- Regular backups of essential business information will be taken to ensure that the Council can recover from a disaster, media failure or error.
- Storage media must be handled, protected and disposed of with care.
- Audit logs for RESTRICTED data and GCSx services must be kept for a minimum of six months.
- Connections to the Council network are made in a controlled manner.
- An annual health check must be made of all Council IT infrastructure systems.